

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES



**DESARROLLO DE ESTRATEGIAS DE IDENTIFICACIÓN BIOMÉTRICA,
UTILIZANDO DATOS DE IDENTIFICACIÓN PERSONAL PARA AGILIZAR
DETECCIÓN DE ACTIVIDADES ILÍCITAS.**

CALEB SAMUEL DE LEÓN LÓPEZ

GUATEMALA, MARZO 2020

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES

**DESARROLLO DE ESTRATEGIAS DE IDENTIFICACIÓN BIOMÉTRICA,
UTILIZANDO DATOS DE IDENTIFICACIÓN PERSONAL PARA AGILIZAR
DETECCIÓN DE ACTIVIDADES ILÍCITAS.**

TESIS

Presentada a la Honorable Junta Directiva

de la

Facultad de Ciencias Jurídicas y Sociales

de la

Universidad de San Carlos de Guatemala

Por

CALEB SAMUEL DE LEÓN LÓPEZ

Previo a conferírsele el grado académico de

LICENCIADO EN CIENCIAS JURÍDICAS Y SOCIALES

y los títulos profesionales de

ABOGADO Y NOTARIO

Guatemala, MARZO de 2020.

**HONORABLE JUNTA DIRECTIVA
DE LA
FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES
DE LA
UNIVERSIDAD DE SAN CARLOS DE GUATEMALA**

DECANO: Lic. Gustavo Bonilla
VOCAL I: Licda. Astrid Jeannette Lemus Rodríguez
VOCAL II: Lic. Henry Manuel Arriaga Contreras
VOCAL III: Lic. Juan José Bolaños Mejía
VOCAL IV: Br. Denis Ernesto Velásquez González
VOCAL V: Br. Abidán Carías Palencia
SECRETARIO: Lic. Fernando Antonio Chacón Urizar

**TRIBUNAL QUE PRACTICÓ
EL EXÁMEN TÉCNICO PROFESIONAL**

Primera Fase:

Presidente: Lic. William Armando Vanega Urbina
Vocal: Licda. Raquel Eleonora García Recinos
Secretario: Lic. Héctor Rolando Guevara González

Segunda Fase:

Presidente: Lic. José Luis Portillo Recinos
Vocal: Lic. Jaime Rolando Montealegre
Secretario: Lic. Ignacio Blanco Ardón

RAZON: “Únicamente el autor es responsable de las doctrinas sustentadas y contenido de la tesis”. (Artículo 43 del Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Exámen General Público)

DEDICATORIA

- A DIOS: Por ser el ser supremo en mi vida y en todo el universo, Adonai, Melej Tzadik, Yahushua Ha Mashia; Fons omnia bonitatis, sapientiam et misericordiam; Qui erat, qui est, et qui venturus est. Aquel por Quien todas las cosas son posibles.
- A MIS PADRES: Carlos De León, por todo el apoyo en mi vida académica, por su amor, ejemplo, consejos, paciencia y dedicación. Adelia López (Q.E.P.D.) quien fue motivo de inspiración, quien enseñó a nunca rendirme y siempre luchar en la vida, hasta alcanzar la meta de vivir para siempre con Cristo Jesús.
- A MIS HERMANOS: Carlos Josué, Lesly Adelia, Soliel Saraì y también a mi cuñada Claudia Natalia Villatoro, por todo su apoyo en cada acontecimiento de la vida. Asimismo a mis hermanos en Cristo quienes a través de sus oraciones me ayudaron a permanecer firme en cada situación en la vida.
- A MIS AMIGOS: Carlos Suy, Rosa Morales, Natalie Tecum, Nohemí Citalan, Cristian Casia, Daniel Chávez, Víctor Juárez, Edgar Díaz (Q.E.P.D.) por su amistad y apoyo cada momento del transcurso de toda la carrera; asimismo

todas las amistades que me apoyaron durante cada etapa.

A MI ASESOR DE TESIS

Lic. Franklin Azurdia por su amistad, por todo el conocimiento que me ha compartido en todo el proceso de preparación profesional, y la elaboración de la presente investigación y sus apreciados consejos; que Dios le bendiga grandemente.

AL

Licenciado Sergio García, por todo su apoyo a mi persona durante toda la carrera, por sus recomendaciones y su amistad tan sincera.

A:

Mi alma mater, Universidad de San Carlos de Guatemala, en especial a la Facultad de Ciencias Jurídicas y Sociales, por todo el conocimiento sustentado, misma que me honra con una meta más en mi vida profesional.

PRESENTACIÓN

La presente investigación es de tipo cualitativa, desarrolla el análisis sobre las estrategias de identificación biométrica como un avance en la ciencia para la investigación criminal, poniendo especial atención en la implementación de tecnologías de identificación facial, su desarrollo y funcionamiento como apoyo en el proceso penal guatemalteco. Debido al progresivo incremento de la actividad criminal especialmente en el Departamento de Guatemala y en el Municipio de Guatemala.

El presente estudio pertenece a la rama del derecho procesal penal, toda vez que se aborda la investigación criminal como parte del proceso penal, la identificación biométrica como parte de la evidencia que es parte esencial para iniciar este proceso, pues su objetivo es vincular al individuo de la manera más exacta posible, por el hecho mismo de ser la prueba un acto que vincula numerosas disciplinas que sirven como auxiliares en la investigación, de manera que existe una relación entre los Artículos números: 246, 248, 315, 317, 318, 348, del Código Procesal Penal y el Artículo número 9 del Reglamento del Instituto Nacional de Ciencias Forenses de Guatemala.

El presente tema se delimita espacial y geográficamente en el Municipio de Guatemala del Departamento de Guatemala, la delimitación temporal a partir del año 2003 hasta el año 2018. En tal virtud, se plantea esta investigación la contribución científico y el aporte legal de la tecnología de identificación facial efectiva y considerablemente puede optimizar la parte investigativa en el derecho procesal penal guatemalteco.

HIPÓTESIS

Debido al progresivo aumento de actividad delincencial en el Departamento de Guatemala, es necesario desarrollar estrategias de identificación biométrica basados en tecnología de identificación facial, reforzando el Departamento Técnico Científico que se describe en el Artículo 9 del Reglamento General del Instituto Nacional de Ciencias Forenses de Guatemala, Acuerdo número 001-2007 del Congreso de la República de Guatemala.

De manera que se pueda crear una Unidad que tenga los medios tecnológicos para obtener la información digital de las cámaras de vigilancia, necesitando técnicos calificados para esta tarea; de esta manera el Ministerio Público obtendrá los medios de investigación que constituyan la prueba pertinente, misma que puede plantearse en el proceso preparatorio.

COMPROBACIÓN DE LA HIPÓTESIS

El desarrollo de tecnologías de identificación biométrica presentes en todo el mundo ha sido un proceso que ha favorecido la identificación del individuo en el campo del derecho procesal penal, debiendo desarrollarse también en el sistema legal guatemalteco para implementarse como estrategia en detección de actividades criminales.

Desarrollándose en la investigación, la comprobación de la hipótesis sobre el desarrollo de la tecnología biométrica en identificación facial, sobre la implementación y legislación de esta estrategia de manera que se desarrolle un equipo técnico en el Instituto Nacional de Ciencias Forenses de Guatemala, el cual es el encargado de obtener los datos necesarios a petición del Ministerio Público el cual se encarga de realizar la investigación, para vincular con la mayor exactitud posible a los individuos que cometan actos ilícitos en el municipio de Guatemala del departamento de Guatemala.

ÍNDICE

Pág.

Introducción.....	i
-------------------	---

CAPÍTULO I

1. Tecnología biométrica.....	1
1.1 Antecedentes.....	1
1.1.1 Mediciones manuales por Bledsoe (1960).....	3
1.1.2 Mayor precisión con 21 marcadores faciales (1970).....	4
1.1.3 Eigenfaces (finales de 1980 – principios de 1990).....	5
1.1.4 Programa feret (1993-2000).....	5
1.1.5 Superbowl xxxv (2002).....	6
1.1.6 Pruebas de proveedores de reconocimiento facial (2000).....	7
1.1.7 Base de datos forenses de aplicación de la ley (2009).....	8
1.1.8 Medios sociales (2010-presente).....	9
1.1.9 Primera instalación principal del reconocimiento facial en un aeropuerto (2011).....	10
1.1.10 Osama Bin Laden identificado (2011).....	11
1.1.11 Reconocimiento facial en la ciencia forense.....	12
1.2 Definición	15
1.3 Finalidades	15
1.4 Importancia	16

CAPÍTULO II

2. Consideraciones generales sobre la prueba en el derecho procesal penal.....	19
2.1 Concepto de prueba:	20
2.2 La incorporación de la prueba al proceso:	21
2.3 Medios probatorios que requieren de autorización judicial:	22
2.4 La prueba incorporada irregularmente al proceso:	23
2.5 Antecedentes	26
2.6 Objeto.....	29
2.7 Ámbito de aplicación.....	31
2.8 Agilización en la investigación penal por la Identificación biométrica como prueba.....	32

CAPÍTULO III

3. Situación actual de la vigilancia a distancia en el territorio nacional.....	35
3.1 Cámaras de vigilancia instaladas en el departamento de Guatemala	38
3.2 Sistema biométrico utilizado en Registro Nacional de las Personas de Guatemala.....	40
3.2.1 Face Recognition System –FRS-.....	42
3.2.2 Identificación de puntos característicos de rostro.....	43
3.2.3 Análisis de Confiabilidad de los Sistemas AFIS y FRS.....	44
3.2.4 Sistemas para el reconocimiento facial más populares en el mundo.....	45
3.2.4.1 Algoritmos para la detección facial.....	46
3.2.4.2 Redes neuronales.....	47

3.2.4.3 Algoritmo para reconocimiento facial “Análisis de Componentes Principales (PCA)”.....	49
3.2.4.4 Algoritmo Análisis de Discriminación Lineal (LDA).....	50
3.2.4.5 Aprendizaje automático, Máquinas de vectores de soporte SVM.....	51
3.2.4.6 Microsoft Face API.....	52
3.2.4.7 Luxand, Inc.....	53
3.2.4.8 LuxandFaceSDK.....	54
3.3 Programas que se utilizan actualmente para la vigilancia en las cámaras de seguridad.....	55

CAPÍTULO IV

4. Países que sobresalen en tecnología de identificación biométrica y beneficios obtenidos.....	57
4.1 Estados Unidos y su política contra el terrorismo	57
4.2 España y su legislación de cesión de datos personales para la investigación penal.....	59
4.3 China y su sistema de control de ciudadanos.....	65

CAPÍTULO V

5. Implementación de tecnología avanzada de detección biométrica en el departamento de Guatemala.....	69
5.1 Requerimientos para su implementación.....	69
5.1.1 Tipo de hardware necesario.....	70
5.1.2 Software que se deberá utilizar para su eficacia.....	71

5.2 Cobertura.....	72
5.3 Costos.....	74
5.4 Viabilidad.....	74
CONCLUSIÓN DISCURSIVA.....	77
6. Anexos.....	79
6.1 Beneficios de la tecnología biométrica.....	79
6.2 Ventajas del reconocimiento de rostros en la biometría en contraste con otros sistemas de identificación biométrica.	80
6.3 Aspectos desventajosos de la implementación de tecnología biométrica.....	84
6.3.1 Dada una imagen bidimensional.....	86
6.3.2 Funcionamiento de la tecnología biométrica en reconocimiento facial.....	88
6.3.3 Reconocimiento facial, proceso para la autenticación.....	91
6.3.4 Arquitectura de los sistemas biométricos.....	92
6.3.5 Funcionamiento de la inteligencia artificial en reconocimiento de rostros.....	94
6.3.5.1 Entrenamiento.....	95
6.3.5.2 Reconocimiento.....	96
6.3.6 Reconocimiento facial en sistemas de seguridad.....	97
6.3.7 Diseño de la tecnología en reconocimiento facial aplicado al campo de la criminalística, en la etapa de investigación.....	98
6.3.8 Modelo conceptual del sistema biométrico en reconocimiento facial.....	100
6.3.9 Adquisición y preprocesamiento.....	101

BIBLIOGRAFÍA.....	106
-------------------	-----

INTRODUCCIÓN

Con el avanzar de la ciencia, no es extraño sorprenderse por los hallazgos y logros que se han dado en el presente siglo, somos testigos de una nueva era donde casi cualquier información está al alcance de todos, cada día surgen nuevas herramientas que apoyan numerosos campos de estudio, el cual no excluye el campo de la investigación penal, la cual en su etapa preparatoria tiene como objetivo determinar la responsabilidad penal del individuo en la comisión de un hecho delictivo.

A medida que el tiempo transcurre es evidente que debido a la creciente población y el aumento del número de actividades delictivas, que cada vez es más difícil obtener la información necesaria para identificar a los presuntos delincuentes y vincularlos a un proceso penal, la cual se detiene al no tener la evidencia suficiente que determine la participación del sujeto, sin necesidad de que se tenga que tomar declaraciones testimoniales u otro medio para vincular a un sindicado, y solicitar peritajes, o en los casos en que las víctimas de un delito, están en determinada situación física que no se pueda identificar por otros medios.

En la presente investigación se logró fundamentar en el presente trabajo, la hipótesis planteada, la cual afirma que es posible desarrollar estrategias de identificación biométrica utilizando datos de identificación personal para agilizar la detección de actividades ilícitas, implementando en el Instituto Nacional de Ciencias Forenses de Guatemala una Unidad que tenga los medios tecnológicos para adquirir información digital de las cámaras de vigilancia y cotejarlas con una base de datos.

Las causas por las que no se han implementado de una manera avanzada las técnicas biométricas en Guatemala para la individualización del sujeto infractor de la ley penal son: el desconocimiento de las técnicas biométricas en reconocimiento facial y de sus beneficios; la falta de estrategias y recursos financiero-económicos para implementar una base de datos a las que se pueda realizar los cotejos con la evidencia de un hecho ilícito y los constantes enfrentamientos con los defensores por los principios de privacidad y de integridad de las personas que indican que el uso de datos personales para tales fines sería atentar contra su privacidad.

En el primer capítulo de la presente investigación se desarrolla una breve reseña del desarrollo histórico de la tecnología biométrica en reconocimiento facial y de cómo a través del tiempo se ha logrado implementar en muchos lugares del mundo en la lucha contra la delincuencia y los logros más relevantes en su desarrollo.

En el segundo capítulo se desarrolla el análisis de la prueba anticipada en el proceso penal, dando inicio en los antecedentes de la misma, su ámbito de aplicación y como la tecnología de reconocimiento biométrico puede agilizar la detección efectiva de actividades ilícitas favoreciendo así la justicia guatemalteca.

EL tercer capítulo analiza la situación actual de la seguridad guatemalteca en los lugares a investigar, poniendo especial atención en las cámaras de vigilancia, su efectividad y la actual estrategia para el funcionamiento del sistema, así mismo se le otorga un lugar no menos importante al Registro Nacional de las Personas de Guatemala, el cual ya utiliza un sistema de reconocimiento biométrico muy efectivo que ha revolucionado el tema de

identificación facial, también se analiza brevemente el software utilizado, para valorar si es un sistema eficiente el que se utiliza actualmente.

El cuarto capítulo perpetra un conciso análisis enfocado en la legislación internacional relacionado al tema de identificación biométrica, pues en algunos ha sido motivo de debate entre los defensores del derecho a la privacidad y los que apoyan la seguridad civil antes que la privacidad, un número considerable de países en el mundo han aplicado este sistema y logrado superar las barreras ideológicas; de esta manera se analizaran las naciones que han sobresalido en su evolución de la tecnología de reconocimiento biométrico y como la voluntad política es el motor principal en la lucha contra la delincuencia.

El quinto capítulo analiza y evalúa el actual sistema de seguridad por cámaras de vigilancia en el lugar de estudio sobre el funcionamiento de las estrategias utilizadas en la actualidad, así mismo se realiza un estudio sobre la posibilidad de implementar esta tecnología, específicamente el equipo mínimo que se necesita para que puede tener éxito, también el software imprescindible que este método utilizaría, sus costos y su viabilidad.

CAPÍTULO I

1. Tecnología biométrica

Conjunto de conocimientos propios de los procedimientos basados en el reconocimiento de un rasgo único e intransferible entre los individuos; en el campo del derecho existen muchas características que la ciencia criminalística utiliza para identificar a una persona; con el desarrollo de la tecnología se han podido detectar rasgos como la huella dactilar, la voz, retina, medidas antropométricas entre otros. El presente trabajo sitúa especial atención en una tecnología que se ha desarrollado recientemente, la cual ha resultado muy efectiva en muchos lugares en el mundo, en la lucha contra el crimen, se trata del reconocimiento facial.

1.1 Antecedentes

El sistema de reconocimiento facial tiene sus orígenes en la propia naturaleza, el cerebro humano encuentra similitudes suficientes entre alguno de sus recuerdos y la imagen que se ve en ese momento, entonces se reconoce a la persona que se ve, de lo contrario, asume que esta ante alguien a quien no se conoce, aunque se podría pensar en la biometría como una ciencia-ficción futurista, los principios básicos de la biometría eran comprendidos y utilizados miles de años antes.

“Muchas son las referencias de personas, que en la antigüedad, han sido identificados por diversas características físicas y morfológicas como cicatrices, medidas, color de los ojos, tamaño de la dentadura entre otras características”¹. Antes del descubrimiento del Ácido Desoxirribonucleico, unas de la maneras más efectivas de identificar un cadáver era por el registro dental. “En el siglo XX hubo un pico de interés por parte de investigadores en criminología, cuando intentaron relacionar características físicas con tendencias criminales. Esto resulto en una variedad de equipos de medición y gran cantidad de datos recogidos, sin embargo los resultados no eran concluyentes, pero la idea de medir las características físicas de un individuo parecía efectiva”.²

El estudio de muchas disciplinas como la psicología y la biometría entre otros métodos colaboraron a la creencia de la existencia de delincuentes natos porque estos compartían ciertos rasgos en común, aunque hay aún profesionales que creen que estas investigaciones han aportado mucho al campo de la criminalística, no hay resultados conclusivos, pues los rasgos no determinan el comportamiento de un sujeto, hay muchos factores como la sociedad, economía, violencia intrafamiliar entre muchos otros que pueden alterar el comportamiento humano.

¹Cesare Lombroso, famoso Criminólogo, identificó ciertas características en lo que el describía como criminal nato, este se caracterizaría, desde el punto de vista físico, por los siguientes rasgos: cráneo pequeño, gran órbita ocular, frente hundida. Velásquez G. **Tras las huellas de la peligrosidad: la teoría criminológica de Cesare Lombroso en el siglo XIX**.2015, págs. 266-246.

² Tolosa C. & Álvaro Giz **Sistemas Biométricos** 2000, recuperado de https://www.dsi.uclm.es/personal/MiguelFGraciani/mikicurri/Docencia/Bioinformatica/web_BIO/Documentacion/Trabajos/Biometria/Trabajo%20Biometria.pdf, pág. 1.

1.1.1 Mediciones manuales por Bledsoe (1960)

En el campo de la biometría, se considera que el padre del reconocimiento facial fue el reconocido matemático Woodrow Wilson Bledsoe en los Estados Unidos de América. Fue en la década de 1960 cuando Bledsoe desarrolló un sistema que podía clasificar fotos de rostros a mano utilizando lo que se conoce como una tableta RAND, un dispositivo que las personas podían usar para ingresar coordenadas horizontales y verticales en una cuadrícula utilizando un lápiz óptico que emitía pulsos electromagnéticos.

“El sistema podría usarse para registrar manualmente las ubicaciones de coordenadas de varias características faciales, incluidas los ojos, la nariz, la línea del cabello y la boca, estas métricas podrían insertarse en una base de datos; luego, cuando el sistema recibió una nueva fotografía de un individuo, fue capaz de recuperar la imagen de la base de datos que más se parecía a esa persona”.³

Este sistema marcó el inicio de la tecnología en identificación facial, aunque las imágenes no eran de la calidad como las que se pueden apreciar en los dispositivos actuales; en ese momento, el reconocimiento facial por desgracia estaba limitado

³ Antes de la creación del Documento Personal de Identificación (DPI) emitido por el Registro Nacional de las Personas de Guatemala (RENAP) el Registro Civil extendía Cédulas de Vecindad en las cuales se incorporaban datos físicos como el color del cabello, color de la tez, estatura, color de los ojos, raza, altura, cicatrices visibles, con el objetivo de evitar que de alguna manera se alterara el documento. Pacheco, E. (2005). **El documento de identificación denominado cédula de vecindad**. Tesis de grado. Universidad de San Carlos de Guatemala.

grandemente por la tecnología de la época y el poder de procesamiento de la computadora, el cual era bastante lento comparado con los dispositivos actuales. Sin embargo, fue un primer paso importante para probar que el reconocimiento facial era una biometría viable.

1.1.2 Mayor precisión con 21 marcadores faciales (1970)

En la década de 1970, en los Estados Unidos, “Goldstein, Harmon y Lesk fueron capaces de agregar una mayor precisión a un sistema de reconocimiento facial manual. Utilizaron 21 marcadores subjetivos específicos, incluidos el grosor del labio y el color del cabello, para identificar caras automáticamente. Al igual que con el sistema de Bledsoe, la biometría real tuvo que ser aún computada manualmente”.⁴

Estos marcadores son los campos que aún son utilizados en muchos de los sistemas de identificación facial, ya que el rostro humano tiene ciertas características que resultan únicas para cada individuo, al momento de combinar todos estos marcadores eficientemente el margen de error es mínimo, dichos campos son registrados en los sistemas implementados por el Registro Nacional de las Personas de la República de Guatemala, como se presentará más adelante.

⁴Tolosa C. **Ob. Cit.** pág. 2

1.1.3 Eigenfaces (finales de 1980 – principios de 1990)

En 1988, Sirovich y Kirby de la Universidad de Brown, Rhode Island, Estados Unidos, comenzaron a aplicar el álgebra lineal al problema del reconocimiento facial. “Lo que se conoció como el enfoque Eigenface comenzó como una búsqueda de una representación de baja dimensión de las imágenes faciales. Sirovich y Kirby pudieron demostrar que el análisis de las características de una colección de imágenes faciales podría formar un conjunto de características básicas. También pudieron demostrar que se necesitaban menos de cien valores para codificar con precisión una imagen de cara normalizada”.⁵

En 1991, Turk y Pentland de Massachusetts Estados Unidos, ampliaron el enfoque Eigenface descubriendo cómo detectar rostros dentro de las imágenes, esto condujo a las primeras instancias de reconocimiento facial automático; su enfoque se vio limitado por factores tecnológicos y ambientales, pero fue un gran avance en la demostración de la viabilidad del reconocimiento facial automático.

1.1.4 Programa Feret (1993-2000)

La Agencia de Proyectos de Investigación Avanzada de Defensa (DARPA) agencia del Departamento de Defensa de Estados Unidos responsable del desarrollo de nuevas

⁵Ibid pág. 2.

tecnologías para uso militar y el Instituto Nacional de Estándares y Tecnología lanzaron el programa de Tecnología de Reconocimiento Facial (FERET) a partir de la década de 1990 con el fin de fomentar el mercado de reconocimiento facial comercial, involucró la creación de una base de datos de imágenes faciales.

“La base de datos se actualizó en 2003 para incluir versiones en color de alta resolución de 24 bits. Incluido en el conjunto de prueba fueron 2.413 imágenes faciales todavía que representan 856 personas. La esperanza era que una gran base de datos de imágenes de prueba para el reconocimiento facial podría inspirar la innovación, que podría dar como resultado una tecnología de reconocimiento facial más poderosa”.⁶

Lo que en un principio se desarrolló como una estrategia para la seguridad por parte del departamento de defensa de los Estados Unidos de Norte América, evolucionó a una tecnología que actualmente es utilizada en muchas áreas, como sistemas bancarios, entretenimiento, seguridad entre muchos otros.

1.1.5 Superbowl xxxv (2002)

En el Super Bowl (nombre que se le da al partido final del campeonato de la National Football League, principal campeonato profesional de fútbol americano en los Estados

⁶Ibid pág. 2.

Unidos de Norte América) de 2002, los funcionarios encargados de hacer cumplir la ley utilizaron el reconocimiento facial en una prueba importante de la tecnología. “Si bien los funcionarios informaron que se detectaron varios “delincuentes menores”, en general, la prueba fue vista como un fracaso.

Los falsos positivos y la reacción de los críticos demostraron que el reconocimiento facial no estaba del todo preparado para el horario de máxima audiencia. Una de las grandes limitaciones tecnológicas de la época era que el reconocimiento facial aún no funcionaba bien en grandes multitudes, una funcionalidad que es esencial para usar el reconocimiento facial para la seguridad de eventos”.⁷ En esta prueba se dio a conocer una de las debilidades del reconocimiento facial, el cual consiste en la dificultad para localizar imágenes en multitudes, sin embargo aun así se demostró su efectividad pues lo que el ojo humano no podía percibir, era posible por la tecnología de reconocimiento facial.

1.1.6 Pruebas de proveedores de reconocimiento facial (2000)

El Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés) es una agencia de la Administración de Tecnología del Departamento de Comercio de los Estados Unidos de Norte América. “Comenzó las pruebas de reconocimiento facial

⁷ Durante la SuperBowl de la NFL, se tomaron infinidad de imágenes de vigilancia, siendo comparadas con los archivos disponibles y obteniendo al menos 19 coincidencias válidas de personas con antecedentes; esto supuso un gran avance de la tecnología de reconocimiento facial a pesar de las deficiencias que se presentaron en aquel momento. Di Tulio Brian, **SuperBowlFacts**, consultado en septiembre de 2019.

(FRVT) a principios de la década de 2000. Partiendo de FERET, los FRVT se diseñaron para proporcionar evaluaciones gubernamentales independientes de los sistemas de reconocimiento facial que estaban disponibles comercialmente, así como también tecnologías de prototipo. Estas evaluaciones se diseñaron para proporcionar a las agencias encargadas de hacer cumplir la ley y al gobierno de EE. UU. La información necesaria para determinar las mejores formas de implementar la tecnología de reconocimiento facial”.⁸

El gobierno de los Estados Unidos de Norte América a través de sus departamentos de seguridad Nacional, son los pioneros en implementar la tecnología de reconocimiento facial para temas de seguridad nacional, ellos iniciaron pruebas y prototipos para determinar la viabilidad de esta tecnología que aparentaba ser de ciencia ficción, sorprendentemente en años recientes esta tecnología ha avanzado de tal manera que se vuelve algo bastante común en muchos dispositivos digitales.

1.1.7 Base de datos forenses de aplicación de la ley (2009)

En 2009, la Oficina del Alguacil del Condado de Pinellas creó una base de datos forense que permitía a los oficiales acceder a los archivos de fotos del Departamento de Seguridad Vial y Vehículos Motorizados (DHSMV) del estado. “Para 2011, unos 170 diputados habían sido equipados con cámaras que les permitían tomar fotografías de

⁸ Williams G. **Breve Historia Del Reconocimiento Facial**. California, Estados Unidos, Agosto 2018, extraído de: <https://www.facefirst.com/blog/breve-historia-del-reconocimiento-facial/>

sospechosos que podrían cotejarse con la base de datos. Esto resultó en más arrestos e investigaciones criminales de lo que hubiera sido posible de otro modo”.⁹ Esto marcó un momento muy importante en los avances en identificación facial, pues resulta necesario tener un registro de manera digital en donde se puedan cotejar las imágenes capturadas por las cámaras de seguridad, de esta manera esta tecnología alcanzó un éxito muy grande en la investigación policial para la detección de criminales en los Estados Unidos.

1.1.8 Medios sociales (2010-presente)

A partir de 2010, Facebook comenzó a implementar la funcionalidad de reconocimiento facial que ayudó a identificar a las personas cuyas caras pueden aparecer en las fotos que los usuarios de Facebook actualizan a diario. Si bien la función fue instantáneamente controvertida con los medios de comunicación, lo que generó una gran cantidad de Artículos relacionados con la privacidad, a los usuarios de Facebook en general no pareció importarles. Al no tener un impacto negativo aparente en el uso o la popularidad del sitio web, más de 350 millones de fotos se cargan y etiquetan mediante el reconocimiento facial cada día.¹⁰

⁹Ibid pág. 2.

¹⁰La mundialmente famosa red social Facebook cuenta con tecnología de reconocimiento facial con el objetivo de acelerar el proceso de etiquetar a los amigos y conocidos de las fotos que son publicadas, esta tecnología identifica automáticamente las caras en las fotos recién cargadas al compararlas con anteriores imágenes que los usuarios han etiquetado. Maria Rubal Thomsen, **El reconocimiento facial de Facebook te busca en fotos sin etiquetar**, consultado el 20 de diciembre de 2018. <https://www.lavanguardia.com/tecnologia/20171220/433775705940/reconocimiento-facial-facebook-fotos-etiquetas.html>

Actualmente numerosas aplicaciones utilizan la tecnología de reconocimiento facial, las más conocidas son: Instagram, Snapchat, con finalidades de entretenimiento y otras como FACEFIRST y FACE2GENE entre muchas otras, que son utilizadas para empresas en concepto de seguridad, asimismo teléfonos inteligentes utilizan el escáner de rostro para desbloquear el aparato, aumentando la seguridad de manera que solamente el usuario podía desbloquearlo (en un principio no funcionaba eficientemente pues con una fotografía podía ser desbloqueado) posteriormente los escáner fueron mejorados necesitando que la persona rote la cabeza para obtener una imagen tridimensional.

1.1.9 Primera instalación principal del reconocimiento facial en un aeropuerto (2011)

En 2011, el gobierno de Panamá se asoció con el entonces gobierno de los Estados Unidos de Norte América. “La secretaria de Seguridad Nacional Janet Napolitano, autorizó un programa piloto de la plataforma de reconocimiento facial de Face First para reducir la actividad ilícita en el aeropuerto Tocumen de Panamá (conocido como un centro para el contrabando de drogas y el crimen organizado)”.¹¹ Sin embargo los resultados fueron extraordinarios pues “Poco después de la implementación, el sistema resultó en la aprehensión de múltiples sospechosos de Interpol. Satisfecho con el éxito del despliegue inicial, Face First se expandió a la terminal norte de la instalación. La

¹¹Ibid pág. 2.

implementación de Face First en Tocumen sigue siendo la instalación biométrica más grande en un aeropuerto hasta la fecha”.¹²

En Guatemala existe el Instituto Nacional de Estudio Estratégicos de Seguridad, El Consejo de Seguridad Nacional y La Secretaria de Seguridad Nacional en Guatemala, los cuales son encargados de proporcionar estrategias de seguridad, estas entidades deben considerar implementar la misma iniciativa en el aeropuerto internacional la Aurora, el cual frecuentemente también es objetivo del contrabando

1.1.10 Osama Bin Laden identificado (2011)

El reconocimiento facial se ha utilizado cada vez más para la medicina forense por parte de profesionales de la ley y militares. A menudo es la forma más efectiva de identificar positivamente cadáveres. “De hecho, el reconocimiento facial se usó para ayudar a confirmar la identidad de Osama Bin Laden después de que fuera asesinado en una redada en los Estados Unidos de Norte América”.¹³

El reconocimiento facial es actualmente una herramienta que muchos países utilizan para combatir el terrorismo, haciendo la comparación que en Guatemala han existido

¹² **Ibid** pág. 3.

¹³ Williams G, **Breve Historia del Reconocimiento Facial, FACEFIRST**, Agosto 29, 2018, extraído de: <https://www.facefirst.com/blog/breve-historia-del-reconocimiento-facial/>

propuestas para declarar a las pandillas como grupos terroristas, de esta manera se podría implementar el reconocimiento facial para la detección de criminales menores hasta grupos terroristas, lo cual utilizado correctamente tendría los mismos resultados positivos que han tenido otros países.

1.1.11 Reconocimiento facial en la ciencia forense

Cuando no existe ninguna foto del sospechoso, los retratos hechos a mano son necesarios; el retrato forense es la interpretación de la descripción verbal creada por un artista. Dichos retratos pueden ser engañosos debido a una mala descripción o la subjetividad del mismo artista, por lo que el problema principal es la incapacidad de la víctima o testigo de acordarse de la apariencia del sospechoso. Además, se necesita mucho tiempo para dibujar un retrato por lo que sólo se utilizan en los crímenes más atroces.

El reconocimiento facial forma una parte importante de la investigación forense. “El primer intento de identificar a un sujeto comparando su rostro con un pequeño conjunto de imágenes data del año 1871 usado en el tribunal británico. Y el primer método sistemático de reconocimiento fue desarrollado por el criminólogo francés Alphonse Bertillon en el año 1882, cuando él empezó a tomar medidas y crear una base de datos de los rasgos faciales. El método que usaba Bertillon consistía en identificación, toma

de medidas y clasificación de todos los rasgos posibles. El primer Artículo científico sobre el reconocimiento facial automático apareció en 1966 publicado por Bledsoe”.¹⁴

En Guatemala en el Instituto Nacional de Ciencias Forenses, los técnicos encargados de reconocimiento de cadáveres tienen un protocolo cuando se obtiene el cadáver de una persona a la cual no se tiene identificación, en los casos de que el cuerpo este demasiado deteriorado para ser reconocido, se realizan necropsias médico-legales para establecer la causa de la muerte y recolectar indicios que orienten al investigador, así como individualizar a la persona efectúan necropsias médico-legales a cadáveres exhumados por orden de autoridad competente.

“En el proyecto desarrollado se trabajaba con unas imágenes de la cara en las cuales, se calculaba una lista de veinte distancias entre los puntos característicos del rostro. Entre los puntos característicos se pueden mencionar las pupilas, las esquinas de la boca, ojos, cejas, etc. Basándose en las diferencias y similitudes entre estas 20 distancias se conseguía identificar dos caras iguales. Poco a poco la lista de los puntos característicos fue aumentando para mejorar el resultado de la identificación forense y se calculó que era necesario obtener 6 características diferentes para una base de datos de 255 imágenes y 14 características para una base de datos de 4.000.000 imágenes”.¹⁵

¹⁴Bledsoe et al. 1966.

¹⁵Ibid pág. 3

Estos sistemas han ido avanzando de manera que ahora son capaces de identificar singularidades casi imperceptibles, como lunares, cicatrices, pero son detalles que también hacen a una persona única, incluso pueden ser clave para poder identificar a alguien.

“El primer sistema completamente automático fue desarrollado por Kanade usando una lista de las características faciales sacadas de las imágenes en escala de grises. Para dichas fotos se calculaban los histogramas locales para conseguir la identificación de la persona. El sistema de Kanade utilizando 20 imágenes daba una precisión de 75% por lo que se necesitaba un sistema más preciso”.¹⁶

En el título mencionado anteriormente se realizaron grandes avances en la técnica de tanatología forense, debido a la dificultad de precisar al actor de algún crimen en aquella época, dichas técnicas ayudaron a que hoy en día se tengan grandes mejoras como lo es en Guatemala el Instituto Nacional de Ciencias Forenses el cual realiza análisis e interpretación de restos óseos con fines de identificación, restauración y reconstrucción craneo facial. Realiza análisis arqueológicos de restos para determinar características del cadáver, cuenta con laboratorios de Serología y Genética Forense que son de altísimo impacto en la investigación.

¹⁶Blnetskaya M. **Reconocimiento Facial En El Ámbito Forense**, Universidad Autónoma De Madrid, Proyecto Fin De Carrera, Ingeniería De Telecomunicación, Septiembre 2013, pág.7

1.2 Definición

Según el diccionario de la real Academia Española Biometría significa “Estudio mensurativo o estadístico de los fenómenos o procesos biológicos”¹⁷ El concepto biometría proviene de las palabras bio (vida) y metría (medida), por lo tanto con ello se infiere que todo equipo biométrico mide e identifica alguna característica propia de la persona. Biometría es el conjunto de características fisiológicas y de comportamiento que pueden ser utilizadas para verificar la identidad del individuo, lo cual incluye huellas digitales, reconocimiento del iris, geometría de la mano, reconocimiento facial y otras técnicas. Actualmente es considerada como el método ideal de identificación humana.

1.3 Finalidades

La biometría busca encontrar sistemas de seguridad que sean infalibles, seguros y rápidos, mediante la identificación de rasgos únicos de cada persona, impidiendo la posibilidad de compartir claves, códigos de ingreso entre otros, logrando que la suplantación de identidad de una persona sea prácticamente imposible.

“A nivel justicia, la biometría permite identificar delincuentes, evitar la suplantación de identidad, la evasión de la justicia, individualización más asertiva de los implicados, agilización en la investigación además que es un buen medio para no exponer al

¹⁷Significado de Biometría, recuperado de: <https://dle.rae.es/biometr%C3%ADa?m=form>

recurso humano, el cual tiene la ventaja de poder identificar a distancia y ser mucho más efectivo que el ojo humano”.¹⁸

A nivel empresarial la utilización de tecnología biométrica ofrece múltiples ventajas de seguridad especialmente para Sistemas de Control de Acceso, Control de Asistencia y Tiempo Laborado, protección de bienes, protección de información y de equipos. Cada vez más se desarrollan dispositivos biométricos que combinan las diferentes formas de identificación, administrados y gestionados por software amigable que entrega datos y reportes de todos los movimientos del personal.

1.4 Importancia

Un equipo biométrico es aquel que tiene capacidades para medir, codificar, comparar, almacenar, transmitir y/o reconocer alguna característica propia de una persona, con un determinado grado de precisión y confiabilidad. “La tecnología biométrica se basa en la comprobación científica de que existen elementos en las estructuras vivientes que son únicos e irrepetibles para cada individuo, de tal forma que, dichos elementos se constituyen en la única alternativa, técnicamente viable, para identificar positivamente a una persona sin necesidad de recurrir a firmas, passwords, pin, códigos u otros que

¹⁸SEAT. **Equipos de seguridad y alta tecnología**, Cali, Colombia, consultado en septiembre de 2019, extraído de: <https://seguridadseat.com/articulos-seguridad/objetivos-seguridad-biometrica.html>

sean susceptibles de ser transferidos, sustraídos, descifrados o falsificados con fines fraudulentos”.¹⁹

Con el gran avance de la ciencia, la aplicación de técnicas de identificación biométrica es necesaria, con la finalidad de prevenir delitos como la suplantación de identidad, robo de tarjetas de crédito, falsificación, entre muchos otros delitos debido a que se llevan a cabo por la facilidad de engañar a otros atribuyéndose calidades y/o cualidades de otra persona para beneficio del infractor, aplicando las tecnologías de identificación biométrica se podrán evitar una gran cantidad de delitos que en parte son efecto de una tecnología aún muy débil y desactualizada en Guatemala.

¹⁹**Ibid** pág. 13.

CAPÍTULO II

2. Consideraciones generales sobre la prueba en el derecho procesal penal:

Se considera indicio todo aquel elemento inteligible, material o no, que resulta o se ve implicado de la escena de un crimen y que permite imaginar la existencia de una circunstancia determinada vinculada al suceso o crimen investigado. La evidencia se entiende como todo aquel elemento que permite establecer, de manera clara, la relación entre dos elementos encontrados en la escena del crimen. Se considera Prueba a todo aquel elemento o argumento que se emplea con el fin de demostrar la veracidad o falsedad de un hecho, es aquel instrumento empleado para demostrar judicialmente un hecho y que permiten alcanzar el nivel de convicción.

“El derecho probatorio es el conjunto de normas que regulan la prueba en general; al hablar de prueba en general, se hace referencia a un concepto amplio, que comprende no sólo la actividad desplegada en el proceso para establecer los hechos materia del mismo, que se califica como prueba judicial, sino las formalidades consagradas por las normas sustanciales tendentes a dejar constancia de ciertos actos, a los cuales, por su trascendencia, los condiciona a determinadas formalidades o solemnidades”.²⁰

²⁰ Camacho, Azula, **Manual de derecho probatorio**, pág. 3.

El derecho probatorio comprende un aspecto sustancial y otro procesal; para que exista una prueba primero se debe tener un indicio, este indicio puede ser el registro de las cámaras de seguridad que es objeto de la presente investigación; el cual será valorado por el juez competente, el valor de este medio de prueba está directamente relacionado si este verdaderamente aporta evidencias al proceso, si las imágenes obtenidas de las cámaras de seguridad no tienen la calidad suficiente, pueden existir dificultades para determinar quién es la persona de las imágenes obtenidas, podría incluso tener consecuencias al vincular a un sujeto que no sea el actor de algún hecho delictivo.

2.1 Concepto de prueba:

Como fuente legítima de conocimiento de la verdad real o histórica que el proceso penal aspira a descubrir (finalidad inmediata) para dar base a la actuación justa de la ley sustantiva (finalidad mediata); como principio en donde se debe basar, necesariamente, la discusión del Ministerio Público y las partes y el pronunciamiento (provisional o definitivo) del órgano jurisdiccional, la prueba es “Todo elemento (o dato) objetivo que se introduzca legalmente en el proceso y sea susceptible de producir en el ánimo de los sujetos procesales un conocimiento cierto o probable acerca de los extremos fácticos de la imputación delictiva”.²¹

²¹Vélez Mariconde A. **Derecho procesal penal**, pág. 341.

Con base en estas dos definiciones, es evidente que el órgano jurisdiccional, no puede basarse legítimamente en prueba que no se ha incorporado al proceso en forma legal, ni en meras conjeturas o impresiones (elementos subjetivos o internos) que surjan de su imaginación, o en opiniones carentes de base externa, porque si lo hiciese, el vicio de la resolución afectaría, al mismo tiempo, los principios fundamentales sobre la verdad real y la inviolabilidad de la defensa (el contradictorio).

2.2 La incorporación de la prueba al proceso

Durante el procedimiento preparatorio surge el indicio y una vez establecidos los elementos que se consideren importantes como elementos del delito surge la evidencia, la prueba (elementos de convicción), reintroducen al proceso a través de la investigación del Ministerio Público. Cuando el defensor o el querellante desean introducir elementos de convicción, deben de solicitar al Ministerio Público que los incorpore. Tan sólo en el caso de que éste se oponga, recurrirán al juez (Art. 116 y 315 del Código Procesal Penal) para que ordene la práctica de diligencia.

“En el juicio oral, la prueba se introduce a través del escrito del Artículo 347 y excepcionalmente en el mismo debate, cuando surgieren nuevas pruebas sobre nuevos hechos que se relacionen con el sometido a juicio (Art. 381 Código Procesal Penal).

Tan solo la prueba válidamente introducida al juicio oral, podrá ser valorada para fundamentar la sentencia.”²²

Es necesario comprender que existen riesgos al momento de utilizar videos e imágenes proporcionadas por un equipo de vigilancia de pobre calidad, pues existen casos donde se han confundido a las personas o en otros casos donde ni siquiera es posible establecer al sujeto que está vinculado a un hecho delictivo, si los indicios no son concluyentes no servirán como medio de prueba en un juicio.

2.3 Medios probatorios que requieren de autorización judicial:

En la legislación Guatemalteca no se permite al Ministerio Publico realizar de manera ilimitada realizar todas las pruebas que sean posibles, con la finalidad de proteger las garantías constitucionales. “Existen algunos medios de prueba que por afectar derechos fundamentales de las personas, sólo serán admisibles con orden de juez competente” por ejemplo: Los Artículos 23 y 24 de la Constitución la Constitución Política de la República de Guatemala, establecen la inviolabilidad de la vivienda, correspondencia, comunicaciones y libros, pero autoriza como excepción la afectación de este derecho con autorización judicial debidamente razonada.²³

²³ La vivienda, no el domicilio, la garantía de inviolabilidad se aplica a la vivienda de la persona, es inviolable en el sentido que nadie puede ingresar a la misma sin permiso o autorización. El permiso debe ser voluntario, expreso. Debe existir una orden de allanamiento de un juez Penal. Castillo Gonzales Jorge Mario. **CONSTITUCION POLITICA DE LA REPUBLICA DE GUATEMALA**, Pág. 88

En la presente investigación se hace énfasis en la precisa autorización de las autoridades correspondientes como Gobernación a través de la Municipalidad para poder utilizar las bases de datos de instituciones como el Registro Nacional de las Personas de la República de Guatemala para poder vincular el registro obtenido por las cámaras de seguridad en un hecho delictivo, con la finalidad que no se viole el derecho a la privacidad, estos acuerdos de directorio se han llevado a cabo con lo cual se han podido identificar delincuentes de alto impacto.

2.4 La prueba incorporada irregularmente al proceso:

El ingreso del dato probatorio en el proceso deberá ser realizado respetando el modo para hacer lo previsto en la ley (o el analógicamente más aplicable en caso de que el medio de prueba utilizado no estuviera expresamente regulado). Por ejemplo, si se tratara de la declaración de un testigo, éste deberá ser protestado. Además, cuando la ley impusiera alguna formalidad especial para su producción, relacionada con el derecho de defensa de las partes, la observancia de ella será también condición “sine qua non” para que la prueba que se obtenga pueda ser regularmente incorporada.

Por ejemplo, si se tratara de un acto definitivo e irreproducible, se deberá notificar previamente a los defensores. Otras veces, en virtud de los caracteres propios de la etapa del proceso que se transita, se impone una forma de recepción determinada (durante el juicio, los testimonios serán recibidos en forma oral); o se la condiciona a la

observancia de ciertos requisitos (a las actas judiciales sólo se las podrá incorporar al debate si fueron labradas conforme a las normas de la instrucción).

“La inobservancia de cualquiera de estas disposiciones impedirá utilizar el dato conviccional, recibido sin resguardarlas, en la fundamentación de toda resolución (si el desarreglo determinó la nulidad del acto de recepción de la prueba), o sólo en la sentencia definitiva (un reconocimiento practicado en la instrucción, sin observar formas no impuestas bajo pena de nulidad.”²⁴

El Código Procesal Penal detalla en su Articulado una serie de requisitos formales necesarios para incorporar la prueba al proceso. Estas formalidades son indispensables para asegurar la veracidad de la prueba obtenida y el derecho de defensa. Por ejemplo, el Artículo 246 establece un procedimiento en el reconocimiento de personas que deberá respetarse para que la prueba sea legal o los Artículos 317 y 318 que exigen la presencia de la defensa en las pruebas anticipadas.

“La inobservancia de las formalidades exigidas por la ley impedirá la valoración de las pruebas obtenidas (Art. 281). Por ello, el Ministerio Público tendrá que ser muy cuidadoso durante la etapa de la investigación en realizar las diligencias probatorias respetando las exigencias legales. De lo contrario, se podrán perder medios probatorios de suma importancia, sin perjuicio de las responsabilidades en las que pueda incurrir el funcionario por su actuar doloso negligente.”²⁵

²⁴CafferataNores, **Ob. Cit**; págs. 24 y 25

²⁵Ministerio Público, **Ob. Cit**; pág. 125

Regula el Artículo 17 de la Constitución Política de la República de Guatemala que “no son punibles las acciones u omisiones que no estén calificadas como delito o falta y penadas por la ley anterior a su perpetración”, asimismo en el Artículo 1 del Código Penal, Decreto 17-73 del Congreso de la República de Guatemala, establece: “Nadie podrá ser penado por hechos que no estén expresamente calificados como delitos o faltas, por ley anterior a su perpetración; ni se impondrán otras penas que no sean las previamente establecidas por la ley “, lo cual se integra a lo regulado por nuestra Constitución y a lo establecido en el Artículo 1 del Código Procesal Penal, Decreto 51-92 del Congreso de la República “No hay pena sin ley”. (Nullum poena sine lege).

No se impondrá pena alguna si la ley no lo hubiere fijado con anterioridad, así el Artículo 2 del citado Código regula “No hay proceso sin ley. (Nullum proceso sine lege)”. No podrá iniciarse proceso ni tramitarse denuncia o querella, sino por actos u omisiones calificados como delitos o faltas por una ley anterior. Sin ese presupuesto, es nulo lo actuado e induce responsabilidad del tribunal.

“Con el límite al poder coercitivo, las personas pueden tener la seguridad que el Estado únicamente podrá intervenir por la vía penal, cuando se le impute como autor de la comisión de un hecho señalado como delito o falta por una ley previamente promulgada; de igual forma, sólo podrán imponerse medidas coercitivas, que restrinjan sus derechos, que se encuentren establecidas previa y expresamente en la ley penal nacional, a su vez estas serán impuestas por una autoridad judicial utilizando como

medio una sentencia dictada en un proceso llevado con todas las garantías establecidas”.²⁶

El principio de legalidad es un principio constitucional a través del cual se establece un límite al ius puniendi del Estado. Sin este principio se pueden vulnerar muchos derechos de las personas, haciendo una relación en la presente investigación al derecho a la privacidad, pues muchos defensores argumentan que la extrema vigilancia es un medio de control social, en el cual se restringe la garantía de la libertad. En la Universidad de San Carlos de Guatemala en el año 2019, un grupo de jóvenes hizo manifestación en contra de la administración de ese momento por la instalación de varias cámaras de vigilancia las cuales tenían la finalidad de evitar que se perpetraran hechos ilícitos sin embargo no fue bien visto por ese grupo de estudiantes que calificaron dicha medida como un medio de control y coerción al estudiante.

2.5 Antecedentes

Garantías procesales: Regulada en los Artículos 8, 12, 14, 17 de la Constitución Política de la República de Guatemala, 1 del Código Penal; 1, 2, 3, 4, 6, 14, 20, 71, del Código Procesal Penal, consiste en la protección a la seguridad que tiene cualquier persona a la que se sindicue que la comisión de un hecho delictivo que únicamente podrá ser juzgada de acuerdo a un procedimiento previamente establecido ya que ni los tribunales, ni sujetos procesales podrán variar la forma del proceso; en los citados

²⁶ **Ibid.** pág. 13

Artículos se indican las garantías mínimas que un proceso penal debe respetar durante cualquier etapa del mismo.

Garantías jurisdiccionales: Protección regulada en los Artículos 2, 4 y 7 del mencionado Código en la cual se establece el juzgamiento y decisión de las causas penales a jueces preestablecidos previamente a la comisión del delito o falta; esta garantía se encuentra relacionada con el inicio del proceso por actos u omisiones calificados como delitos o faltas, de lo contrario es nulo lo actuado; con el juicio previo, el cual indica que nadie puede ser condenado o sometido a medidas de seguridad o corrección sin una sentencia firme obtenida con el procedimiento que se estipula en el Código Procesal Penal; asimismo se relaciona con la garantía de juez natural ya que no se podrá juzgar a nadie ante un juez o tribunal que no sea por los designados para el efecto por la ley penal.

Garantías de ejecución: Garantía que protege a las personas, indicando que una vez resuelta su situación jurídica y establecida su responsabilidad en la participación en la comisión de un hecho delictivo con el pronunciamiento de una sentencia por un tribunal competente, para ello le corresponderá en única instancia a los jueces de ejecución la ejecución de la misma en los lugares destinados para el efecto.

El derecho procesal es el conjunto de normas que regulan la aplicación de las leyes de fondo o derecho sustancial; por lo que, en el derecho procesal penal también existe un conjunto de normas que regulan el proceso desde el inicio hasta el fin. Tiene la función de investigar, identificar, y sancionar (si fuese necesario) las conductas que constituyen delitos, evaluando las circunstancias particulares de cada caso concreto.

El derecho procesal penal es pues aquella disciplina jurídica encargada de proveer de conocimientos teóricos, prácticos y técnicos necesarios para comprender y aplicar las normas jurídicas–procesal–penales, destinadas a regular el inicio, desarrollo y culminación de un proceso penal. La prueba se produce entonces en el propio mecanismo de defensa y acusación derivado de la relación jurídica que existe entre el Estado como acusador privilegiado y el ciudadano común, cuando está siendo sujeto a una investigación y un proceso penal.

El Artículo 315 del Código Procesal Penal admite la proposición de medios de investigación en cualquier momento del proceso preparatorio, tanto al imputado como a las personas a quienes se les haya dado intervención en el procedimiento, sus defensores y los mandatarios, los cuales se llevarán a cabo si son considerados pertinentes y útiles. El principio de libertad de la prueba principio es uno de los fundamentales del derecho probatorio nos indica que: La averiguación de la verdad debe desarrollarse sin obstáculos preestablecidos y artificiales, puede usarse en cualquier medio que lo exprese la ley o que resulte impertinente. La libertad probatoria tiene cuatro principios:

- 1) Que los hechos que se presenten pueden justificarse directa o indirectamente.
- 2) Al juzgador permite ver si es suficiente o no las pruebas.
- 3) Da la posibilidad de probar hechos por cualquiera que sea su medio ilícito.
- 4) Hace imposible que el juzgador obtenga pruebas por medios de violaciones o derechos fundamentales de la persona involucrada.
- 5) Otorga una amplia valoración de los elementos que se incorporen con las pruebas.

Esto abre las puertas a la admisión de técnicas que pueden ser útiles para poder esclarecer un delito; actualmente existe vigilancia por cámaras de video pero muchas veces es difícil que esta tenga relevancia en una investigación penal pues no se puede identificar con claridad suficiente para vincular a un proceso a un individuo; la tecnología de reconocimiento facial produciría de ser incorporada un medio seguro, rápido y económico para aportar pruebas contundentes en un proceso penal.

2.6 Objeto

La prueba anticipada en el derecho procesal penal

La prueba anticipada se define como: Aquel medio de prueba pertinente que por motivos fundados y de extrema necesidad debe ser desahogado (es decir, llevado a cabo) a petición de las partes y ante el Juez de Control, de forma previa a la audiencia de Juicio Oral. La prueba anticipada es un proceso especial de cognición, afín al de las diligencias preliminares, que tiene por objeto facilitar el desarrollo de un proceso

principal ulterior mediante la realización de una prueba que, por determinadas circunstancias, sea previsible que no podría efectuarse dentro del proceso principal.

“Es deber del Ministerio Público reunir las pruebas útiles para dar base a la acusación o determinar el sobreseimiento. También el Ministerio Público, teniendo en cuenta su actuación imparcial puede proponer pruebas favorables al imputado”.²⁷

El Ministerio Público es un ente de justicia y no de condena de manera que no debería únicamente acusar a quien le fuere posible, cabe afirmar que en el Proceso Penal guatemalteco no existe distribución alguna de la carga de la prueba. De este punto podemos entender que la identificación facial ayudará a esclarecer la verdad absoluta porque es un medio de convicción el cual difícilmente puede ser alterado o utilizado maliciosamente para favorecer a conveniencia a alguna de las partes en un proceso.

“El objeto de la prueba anticipada en el derecho penal es aquello que puede ser probado, aquello sobre lo cual debe o puede recaer la prueba. Aquello que se investiga y sobre lo cual se interroga al testigo para que diga lo que sepa al respecto.”²⁸

²⁸Álvarez M. **Al Juzgado de Instrucción 28 de Madrid para Diligencias Previas**, Madrid, 2018, recuperado de: www.cita.es/recurso28 y www.miguelgallardo.es/recurso28.pdf, pág. 1

La finalidad de la prueba es esclarecer cuestiones que resultan controvertidas y que requieran conocimientos especiales en alguna ciencia, arte o industria, quedando excluidas las cuestiones de derecho, de manera que cuando es admitida dentro del proceso el juez podrá valorarla para posteriormente dictar la sentencia que conforme a derecho corresponda.

2.7 Ámbito de aplicación

En el capítulo anterior fueron expuestas algunas de las aplicaciones comunes de la tecnología de reconocimiento facial, dentro de las cuales sobresalen la seguridad, el entretenimiento y el registro de personas en varios sectores como la industria, empresarial y justicia, siendo el tema que resalta en esta investigación el de la seguridad como garantía constitucional y la agilización de la justicia:

“La aplicación de reconocimiento facial en personas investigadas por la justicia puede aplicarse en muchos campos de la averiguación penal propiamente, específicamente los delitos que ocurren en lugares transitados donde las cámaras de seguridad están instaladas, siendo los más comunes, los delitos de hurto, robo, abuso sexual, delitos contra la vida e integridad de la persona, entre muchos otros que son susceptibles a ser detectados por cámaras inteligentes, esto con el objetivo principal de incrementar los índices de seguridad colectiva brindando un sistema sólido que pueda ser utilizado en

diversos lugares concurridos como: terminales, carreteras transoceánicas, avenidas concurridas, etc.”²⁹

Atendiendo a la importancia de la seguridad en la sociedad como parte fundamental para lograr el bien común, ya que una sociedad donde hay seguridad es una sociedad que vive sin temor a realizar sus actividades diarias sin que se vulneren sus derechos humanos; se enfatiza que la vigilancia por cámaras de seguridad es actualmente uno de los medios indispensables para disminuir los delitos mencionados en el párrafo anterior que son actualmente un martirio para los guatemaltecos.

2.8 Agilización en la investigación penal por la Identificación biométrica como prueba

Según el diccionario de la Real Academia Española, se entiende por agilización como la acción de dar rapidez y facilidad al desarrollo de un proceso o la realización de algo (<https://dle.rae.es/>); de esta manera el reconocimiento facial es uno de los métodos más eficaces “toda vez se tenga una imagen del sospechoso, al cual se obtiene en cuestión de minutos, el sistema de reconocimiento en poco tiempo realiza un cotejo de

²⁹Ibid pág. 13.

imágenes para identificar a una persona de manera efectiva; agilizando de manera exponencial una investigación y aportando así datos significativos”.³⁰

Debido a la gran cantidad de denuncias que se plantean diariamente, el proceso penal puede tomar más tiempo de lo esperado, uno de los factores principales que retardan dicho proceso, es como lo estipula el Artículo 108 del Código Procesal Penal, que el Ministerio Público deberá formular requerimientos y solicitudes, conforme al plazo no mayor de quince días de recibida la denuncia, el problema surge cuando dentro de este plazo no existe suficiente información que pueda aportar al proceso, el juez puede ordenar un plazo de no más de treinta días para que se informen de nuevos avances; en este orden de ideas se comprende que debido a la falta de información un proceso penal puede tomar inclusive años en resolverse.

³⁰ Blnetskaya M. **Reconocimiento Facial En El Ámbito Forense**, Universidad Autónoma De Madrid, Proyecto Fin De Carrera, Ingeniería de Telecomunicación, Septiembre 2013, pág.7

CAPÍTULO III

3. Situación actual de la vigilancia a distancia en el territorio nacional

Según el diccionario de la Real Academia Española Vigilancia proviene del latín *vigilantía*, que significa: “Cuidado y atención exacta en las cosas que están a cargo de cada uno”. Este vocablo se define a la atención, celo, atención, custodia, diligencia, esmero y asistencia exacta de las cosas o elementos que están a cargo de cada uno. Servicio dispuesto, habilitado, presto, listo, ordenado, cuidadoso o metódico para vigilar. Actividad destinada para brindar seguridad en algunos sitios aplicada en esta finalidad.

El propósito de la vigilancia es proveer de seguridad al ciudadano. Desde el enfoque de los derechos humanos, la seguridad no se puede ni se debe circunscribir a la lucha contra la criminalidad, la delincuencia o el crimen organizado sino que implica y se considera indispensable la creación de un ambiente, un clima, un entorno, un contexto, la existencia de condiciones propicias y adecuadas para la convivencia pacífica y armónica de las personas.

Según el portal de Guatecompras, las cámaras adquiridas por el Ministerio de Gobernación para el control Migratorio, en concurso NOG número: 10835687, se adquirieron 300 cámaras del tipo LED, el 30 de septiembre de 2019, con las siguiente descripción:

ESPECIFICACIONES TÉCNICAS

Cámara de transmisión de escritorio con luz de anillo de varios pasos

Vídeo HD de alta definición (720p 60 fps / 1080p 30 fps)

Compatible con Open Broadcaster Software y Xsplit

Cámara

Tipo de conexión: USB2.0

Resolución de la imagen: 4 megapíxeles

Resolución de video: 1080p @ 30FPS / 720p @ 60FPS / 480p @ 30FPS / 360p @ 30FPS

Codificación de video: YUY2 / MJPEG o H.264

Resolución de imagen fija: 2688x1520

Configuración de calidad de imagen Personalización: Sí

Campo de visión diagonal (FOV): 81.6 °

Tipo de enfoque: Automático

Longitud del cable: 1,5 metros de cable trenzado

Luz del anillo

Iluminación: 12 LED blancos

Temperatura de color: 5600K "luz del día"

LED difusor: blanco lechoso

Botones: esfera de 12 pasos

Brillo: 10 Lux a 1m

Con las anteriores especificaciones podemos comprender que son cámaras de alta definición con las cuales el software de identificación facial que se expondrá más adelante puede funcionar, pero antes se hará un contraste con las cámaras de la municipalidad de Guatemala para monitorear los espacios públicos; la siguiente es el concurso NOG número: 9324925, realizado en el mes de noviembre de 2018, se adquirieron 400 cámaras de vigilancia para espacios públicos, las especificaciones son las siguientes:

Sensibilidad: 0.01 LUX

Resolución: 308 líneas de resolución

Sensor de 2.1 megapíxeles

Memoria de 1Gb de RAM y 512 MB Flash

Lente: SR varifocal 9-22 mm F1.6 con corrección de infrarrojos

El portal posee numerosas especificaciones pero por no ser parte del estudio jurídico, se limitaron las demás características pero el lector puede revisar el proyecto completo si así lo desea. Solamente se hará el comentario que el tipo de cámaras es de muy buena capacidad, sin embargo la cantidad no es lo suficiente para vigilar la ciudad, comparando con las 300 cámaras adquiridas por el Ministerio de gobernación para el Departamento de Migración y las 400 cámaras con opción a compra de la Municipalidad de Guatemala adquiridas con la finalidad de monitorear espacios públicos.

El marco legal que debe definir la política en materia de seguridad de cualquier gobierno en Guatemala, independientemente de su pertenencia partidaria política e ideológica, está regido en primera instancia por el Decreto 18-2008 del Congreso de la República “Ley Marco del Sistema Nacional de Seguridad” (LMSNS), normativa que a su vez se basa en lo que establece la Constitución Política de la República de Guatemala en sus Artículos 1, 2, 3, 4, y que también a su vez está bajo el manto del Tratado Marco de Seguridad Democrática en Centroamérica, el cual fue suscrito por los Presidentes de Centroamérica el 15 de diciembre de 1995.

3.1 Cámaras de vigilancia instaladas en el departamento de Guatemala

Han existido numerosas compras por parte de la Municipalidad de Guatemala con el tema de vigilancia y seguridad el cual pueden ser observados a través del portal Guatecompras, sin embargo, pocos han sido los planes que se tienen respecto a un régimen revolucionario para establecer estrategias en el tema estudiado, uno de los más recientes es el siguiente:

“En junio de 2014, el Ministro de Gobernación, Mauricio López Bonilla, anunciaba la instalación de 1,018 cámaras de seguridad en distintas zonas de la ciudad de Guatemala, como parte del PNSJP, y que como parte de ello ya se había iniciadora instalación de 300 en la zona 18 así como los postes respectivos. El proyecto de instalación, según medios locales, fue amparado bajo un contrato por excepción adjudicado a la empresa Construcción y Telecomunicaciones, S.A. (CTCI), a cargo del

proyecto, y el cual fue adjudicado por la PNC (Policía Nacional Civil) en mayo de 2013”.³¹

En tal proyecto se adjudicaron 300 cámaras de vigilancia para la zona 18 del Municipio Guatemala, siendo esta zona una como las declaradas “zonas rojas” a pesar de eso la vigilancia proporcionada, el índice de criminalidad no se ha logrado disminuir.

“El 10 de abril de 2014, dos días después de que en tiempo record -dos horas- fuera aprobada de urgencia nacional la Ley de las Telecomunicaciones Móviles en Centros de Privación de Libertad y Fortalecimiento de la Transmisión de Datos, Decreto 12-2014, fue firmado el contrato de arrendamiento entre el Director de la PNC (Policía Nacional Civil), Telémaco Pérez, y el Gerente General y Representante Legal de Comunicaciones Celulares Sociedad Anónima (COMCEL), José Valladares Guillén, para la instalación de cinco mil cámaras en varios municipios de Guatemala y en el municipio de Escuintla, departamento del mismo nombre.”³²

Con este último avance se logra vigilar muchos municipios de Guatemala y de Escuintla, se hace énfasis que aunque se aumenta el número de cámaras no se

³¹El observador, **Violencia y seguridad en Guatemala Un informe de derechos humanos**, Centro de Investigaciones Internacionales en Derechos Humanos (CIIDH) El Observador. Análisis Alternativo sobre Política y Economía, Noviembre de 2014, P. 235,236.

³²**Ibid** pág. 236.

aumenta la cantidad de agentes de seguridad de la Policía Nacional Civil que patrullan las calles, con lo cual se hace difícil mantener la seguridad esperada.

“El contrato de arrendamiento fue realizado mediante el mecanismo de compra directa y por excepción, y aparece en el portal de Guatecompras según ONG de Publicación sin Concurso E11739754, E11739053, E11739355. Tiene una vigencia de cinco años y un costo de Q. 1,232 millones. En éste orden de ideas COMCEL (Comunicaciones Celulares Sociedad Anónima) se compromete a instalar las cinco mil cámaras en los municipios del departamento de Guatemala”³³. Sin embargo a pesar del proyecto de instalación de cámaras, aún no se cuenta con la cobertura esperada, pues existen muchas calles y avenidas que no tienen vigilancia por cámaras de seguridad, esto siempre debido al rápido crecimiento de la Ciudad.

3.2 Sistema biométrico utilizado en Registro Nacional de las Personas de Guatemala

A través del Decreto 90-2005 del Congreso de la República, fue creado el Registro Nacional de las Personas (RENAP) con la finalidad de organizar y mejorar el control del registro de los actos de la vida civil de los ciudadanos; dentro de sus objetivos están los siguientes:

³³ El observador, **Violencia y seguridad en Guatemala Un informe de derechos humanos**, Centro de Investigaciones Internacionales en Derechos Humanos (CIIDH) El Observador. Análisis Alternativo sobre Política y Economía, Noviembre de 2014, P. 235,236.

- Implementar una norma jurídica que regule lo relativo a la documentación personal, para adaptarla a los avances tecnológicos y dar cumplimiento a la modernización electoral. Este compromiso fue adoptado en los Acuerdos de Paz sobre Reformas Constitucionales y Régimen Electoral.
- Mejorar las características de seguridad y calidad del documento de identificación, que hasta entonces era la cédula de vecindad, que era una cartilla que se deterioraba con facilidad y era altamente falsificable.
- Crear una entidad autónoma, con personalidad jurídica, técnica e independiente que se encargue de emitir y administrar el Documento Personal de Identificación.

“Guatemala es uno de los pioneros en implementar dos biometrías como parte de su proceso de verificación para la emisión de un documento de identificación. Para ello la verificación se realiza a través del sistema SIBIO (Sistema de Identificación Biométrica), en el cual se tienen los sistemas AFIS (Automated Finger print Identification System) y FRS (Face Recognition System), funcionando en serie, garantizando que cada DPI (Documento Personal de Identificación) emitido por el Registro Nacional de las Personas –RENAP- tiene una verificación biométrica al 100% por los dos sistemas”.³⁴

³⁴A través del Decreto 90-2005 del Congreso de la República, fue creado el Registro Nacional de las Personas – RENAP, la cual tiene como función, ser la entidad encargada de organizar y mantener el registro único de identificación de las personas naturales, inscribir los hechos y actos relativos a su estado civil, capacidad civil y demás datos de identificación desde su nacimiento hasta su muerte. Extraído de: <https://www.renap.gob.gt/noticias/historia-del-registro-nacional-de-las-personas-renap>

EL Registro Nacional de las Personas la República de Guatemala posee dos de los requisitos indispensables para la aplicación de los sistemas en reconocimiento facial en el territorio Nacional, los cuales son: Una base de datos bastante completa y el sistema FRS (Sistema de Reconocimiento de Rostros), el cual en algunos casos importantes ha sido utilizado mediante acuerdos con el Ministerio de Gobernación para identificar criminales altamente peligrosos, con lo cual han obtenido resultados importantes.

3.2.1 Sistema de Reconocimiento de Rostros (Face Recognition System) –FRS-

Son programas que analizan los campos biométricos que diferencian a los rostros humanos y que son detectables, más adelante se detallara brevemente cómo funcionan estos sistemas y su impacto en la sociedad. “El análisis del rostro se basa en los patrones que no pueden ser modificados por medio de cirugía estética, actualmente por medio de cirugía estética se puede modificar el tamaño del mentón, la forma y tamaño de la nariz, así como de los pómulos, sin embargo es imposible modificar el ancho de los ojos, la separación entre ojos, así como la distancia que existe entre los ojos y la boca, tamaño de la boca, etc.”³⁵

³⁵ El DPI emitido por el Registro Nacional de las Personas de Guatemala, posee mucha información dentro del chip que este documento posee, la cual por cuestiones de seguridad no se dan a conocer al público, existen al menos 31 datos como profesión, o si ha prestado servicio militar, que solo pueden ser leídos por un aparato especial que solo el RENAP posee, haciendo muy difícil la extracción de los datos, de manera que falsificar un DPI es prácticamente imposible; se desconoce con certeza todos los datos que este documento posee respecto a la identidad de una persona. Julio Chinchilla, **Primeros datos extraídos DPI V2 2014.**

Existen rasgos faciales los cuales son difícilmente disimulables, que desde tiempos antiguos han sido objeto de estudio para los criminalistas, estas características biométricas ayudan a diferenciar un sujeto de otro, que por más que se parezcan incluyendo a los gemelos no existen dos rostros completamente iguales en el mundo.

3.2.2 Identificación de puntos característicos de rostro.

Existen campos geométricos que los programas de identificación de rostros analizan, estos son puntos que permiten comprobar la identidad de un individuo pues resultan ser características difícilmente alterables. “Los sistemas FRS (Face Recognition System) al igual que los sistemas AFIS (Automated Finger print Identification System) no analizan las fotografías, analizan la similitud estadística entre los modelos generados a partir de una fotografía. Los sistemas FRS (Face Recognition System) necesitan que las fotografías analizadas cumplan con ciertas características para aumentar su nivel de exactitud”.³⁶

Entre estas características se pueden mencionar las siguientes:

- “El rostro debe de ocupar el 50% de la fotografía
- Las fotografías deben de ser tomadas de frente, con el rostro descubierto
- El ciudadano no deberá portar ningún tipo de accesorio sobre la cabeza.

³⁶Informe De Funcionamiento Del Sistema De Identificación Biométrica -Sibio-(Afis Y Frs) Dirección De Procesos 24-10-2013, renap.gob

– Si la persona posee lentes los mismos no deben de reflejar el flash de la fotografía.

En síntesis se debe cumplir con las normas ICAO/OACI (Organización de Aviación Civil Internacional) para la captura de fotografía”.³⁷

En Guatemala, el Registro Nacional de las Personas (RENAP) tiene ciertas medidas al momento de tomar una fotografía con la finalidad de crear un nuevo Documento Personal de Identificación (DPI), esto con el propósito de evitar que algún individuo pueda alterar sus características biométricas y obtener un perfil no exacto; con las medidas adoptadas por dicho Registro resulta muy difícil ocultar la identidad.

3.2.3 Análisis de Confiabilidad de los Sistemas AFIS y FRS

Existen varias técnicas para la identificación biométrica, las más popular a nivel mundial es el sistema AFIS (Sistema de Identificación de Huellas Digitales) “Se ha demostrado que la probabilidad que dos personas tengan huellas digitales idénticas es de 1 en 64 billones, y la probabilidad de que un par de huellas digitales generen modelos idénticos es menor al 0.01%.

Por el contrario existe una más alta probabilidad de que dos personas sean muy parecidas físicamente, y en los casos de gemelos idénticos los sistemas FRS (Face Recognition System) pueden generar falsos positivos. Derivado de esto se ha calculado

³⁷ Ibid pág. 236.

que la confiabilidad de los sistemas AFIS (Automated Fingerprint Identification System) es mayor al 99.99% mientras que la de los sistemas FRS es de cerca del 89%”.³⁸

Es posible observar que el sistema de Identificación de Huellas tiene menor margen de error, pues es casi cien por ciento efectivo, comparado con el sistema de Identificación facial, el cual tiene una efectividad del 89 por ciento, la verdadera ventaja del sistema de identificación facial es la rapidez para detectar un rostro, considerando que no en todas las escenas de un crimen se encuentran huellas digitales, es más sencillo obtener una imagen que se obtiene en segundos por un medio digital.

3.2.4 Sistemas para el reconocimiento facial más populares en el mundo.

Existe una gran variedad de programas en reconocimiento facial, que no solo detectan el rostro sino que también tienen funciones que verdaderamente agilizan el proceso de vinculación del rostro en una base de datos, incluyendo funciones como mejora de la imagen, eliminación de factores que opaquen el cuadro, detección de patrones de conducta, análisis y comparación de características biométricas; brevemente se darán a conocer a continuación.

³⁸Informe De Funcionamiento Del Sistema De Identificación Biométrica -Sibio-(Afis Y Frs) Dirección De Procesos 24-10-2013, renap.gob

Algunos de los sistemas que hasta finales del año 2018 han sido considerados en muchos lugares como los mejores, sin embargo debido a la gran cantidad de programas solo serán mencionados aquellos que podrían ser aplicados en el orden de ideas del presente trabajo, pues con el rápido avance tecnológico es seguro que en el futuro existirán mejores programas que los que existen en el año 2018.

3.2.4.1 Algoritmos para la detección facial

En el campo de la informática un algoritmo se puede definir como una secuencia de instrucciones que representan un modelo de solución para determinado tipo de problemas. Existen diferentes algoritmos de detección facial, estos tienen el objetivo de reconocer rostros en una imagen o video y si es encontrado este devuelve la posición y dimensión para cada rostro encontrado.

Entre los más citados y comprobados por los científicos y desarrolladores tenemos a los algoritmos de Viola Jones y redes neuronales. El algoritmo de Viola Jones fue creado en el año 2001 por los ingenieros Paul Viola y Michael Jones (Viola & Jones, 2001), muchos desarrolladores y científicos realizaron pruebas con este algoritmo y con otros, como resultado dedujeron que este es el más eficiente y tiene bajo costo computacional, este algoritmo que usa para la detección de objetos que utiliza la clasificación en cascada (HAAR) y un entrenador de clasificador basado en el algoritmo de aprendizaje AdaBoosto “Boosting”, que divide todas las imágenes procesadas en dos tipos de imagen, clase 1 “Cara” y clase2 “No cara”. (González, 2017).

El algoritmo de Viola Jones supone un gran avance dentro de los algoritmos de detección por su gran rapidez, y porque la clasificación se realiza mediante características en vez de píxel a píxel, lo que permite una cierta abstracción del algoritmo respecto al resultado (Wang, 2014). En definitiva, se puede concluir que Viola Jones no es solo una técnica de detección de caras o no caras, sino que es un algoritmo el cual goza de dos procesos bien diferenciados: la detección y la clasificación, en la que es posible ajustar su umbral de decisión para que cometa una menor tasa de error.

3.2.4.2 Redes neuronales

El avance de la ciencia ha dado herramientas a los programadores como son las redes neuronales, la red neuronal artificial es un grupo interconectado de nodos similar a la vasta red de neuronas en un cerebro biológico, se les llama así por la similitud que tienen con las neuronas humanas en su forma de interactuar “Las redes neuronales artificiales son un paradigma de aprendizaje ampliamente tratado en la literatura de la inteligencia. Las redes neuronales artificiales intentan imitar la naturaleza de las neuronas del cerebro humano” (P. P. G. García, 2013).

Algunos investigadores lo mencionan como un método importante para el reconocimiento de rostros, “tienen casi los mismos objetivos que PCA (Principal Component Analysis) para detectar rostros tales como la posición de los ojos u otras

simetrías de rasgos faciales de las personas” (Moreano et al., 2017) pero por su difícil implementación no es muy utilizado para dicho fin ya que se encontró poco material sobre la implementación del uso de este método.

Según (Sánchez & Elizabeth, 2014) “las redes neuronales se han convertido en una técnica popular para el reconocimiento de patrones. Se usan generalmente para la clasificación de imágenes según patrones establecidos”. “La red se entrena usando un conjunto de imágenes que representan rostros de todo tipo y otro conjunto de imágenes que no representan rostros, de forma que la red neuronal pueda establecer el criterio adecuada acerca de lo que es y no es un rostro. Además las redes neuronales tiene un acierto igual mayor a 95% de encontrar un rostro habitualmente se usa en la categorización de imágenes según reglas establecidas, por ejemplo, saber si una imagen está borrosa o no” (Gallardo Calvopiña& Sánchez Quevedo, 2016).

Se mencionan las redes neuronales en el presente trabajo por su importancia en la tecnología, aunque parezca algo muy futurista, como de ciencia ficción, pensar en un sistema que no solo identifique sino que además tenga la capacidad de pensar, de analizar patrones de conducta, detectar inclusive los delitos mismos, e informar inmediatamente a las autoridades, es algo difícil de creer, pero esta tecnología ya se está desarrollando, hay países que han avanzado en esta tecnología los cuales serán mencionados en un próximo capítulo; indudablemente se aproxima una nueva era en el combate contra la delincuencia.

3.2.4.3 Algoritmo para reconocimiento facial “Análisis de Componentes Principales (PCA)”

El análisis de componentes principales (PCA) es una técnica utilizada para describir un conjunto de datos en términos de nuevas variables, es decir analiza un conjunto de datos que son parte de una cosa. El análisis de componentes principales o Eigenface es un método propuesto por (Turk & Pentland, 1991),”este método fue comprobado que es robusto, rápido y eficiente para llevar a cabo el reconocimiento facial” (Eugenio, Manuel, Edgar, Alejandro, & Martin, 2015).

Mediante PCA (Principal Component Analysis) uno puede transformar cada imagen original de la formación que figura en una Eigenface correspondiente. Una característica importante de la PCA (Principal Component Analysis) es que uno puede reconstruir cualquier imagen original desde el conjunto de entrenamiento mediante la combinación de los Eigenface. Recuerde que Eigenface son nada menos que rasgos característicos de las caras.

“Por lo tanto, se podría decir que la imagen de la cara original puede ser reconstruida a partir Eigenface si uno suma todos los Eigenface (características) en la proporción adecuada. Cada Eigenface representa solo ciertas características de la cara, que puede o no puede estar presente en la imagen original. Si la característica está presente en la imagen original a un grado más alto”. (Calli Olvea, 2015).

Muchas imágenes que son captadas por cámaras de vigilancia las cuales no tienen suficiente resolución en la cámara o que están en condiciones donde no hay claridad en las fotos, hacen difícil determinar un rostro en una imagen de manera efectiva.

“Una ventaja del algoritmo PCA (Principal Component Analysis) es la reducción de los datos necesarios en la identificación para una relación 1 a 1000, este algoritmo utiliza Eigenface, las imágenes deben estar normalizadas y del mismo tamaño, así permiten el lineamiento de la boca y los ojos, el PCA (Principal Component Analysis) resulta ser una poderosa herramienta para el análisis de los datos teniendo como objetivo general lo antes mencionado” (Collantes Arana et al., 2013; González, 2017). “Este método es un algoritmo de reducción dimensional, extrae las características principales de la imagen que mejor la define y las agrupa en diferentes vectores, cada uno de los cuales pertenece a una elipse” (González, 2017).

El Análisis de Componentes principales (PCA) es una herramienta que ayudará a mejorar las imágenes obtenidas de cámaras de vigilancia, utilizando un algoritmo que puede darnos un dato estadístico de la compatibilidad de una imagen obtenida con una base de datos a manera de restringir la información y proporcionar datos más exactos.

3.2.4.4 Algoritmo Análisis de Discriminación Lineal (LDA)

Este es un método de análisis de patrones y aprendizaje que puede dimensionar un evento y determinar la probabilidad que algo suceda. “LDA (Análisis de Discriminación

Lineal) se desempeña cuando las mediciones realizadas en variables independientes para cada observación son cantidades continuas. El objetivo es proyectar un conjunto de datos en un espacio de menor dimensión con una separabilidad de clases para evitar la sobre-equitación y también reducir los costos computacionales. Cuando se trata de variables categóricas independientes, la técnica equivalente es el análisis de correspondencia discriminante” (Moreano et al., 2017).

La importancia en este algoritmo es la capacidad de aprender patrones de conducta utilizando secuencias lineales, en el campo de la criminalística, existen programas que de esta manera pueden determinar si el sujeto porta algún tipo de arma o conductas inusuales, e informar a las autoridades de manera casi inmediata.

3.2.4.5 Aprendizaje automático, Máquinas de vectores de soporte SVM

Estas son máquinas que poseen algoritmos de aprendizaje supervisado, tienen la ventaja de que pueden analizar imágenes en dos dimensiones. “SVM (Máquinas de Vectores de Soporte) es un método genérico para resolver problemas de reconocimiento de patrones, dado un conjunto de puntos en un determinado espacio que pertenecen a dos clases distintas, SVM (Máquinas de Vectores de Soporte) encuentra el hiper plano que separa la mayor cantidad de puntos de la misma clase del mismo lado; esto se realiza maximizando la distancia de cada clase al hiper plano de decisión, denominado OSH (Optimun Separating Hyperplane). Los puntos más

cercanos al hiperplano, son los llamados vectores soporte (SupportVectors)". (Sánchez & Elizabeth, 2014)

Este algoritmo es mencionado por la ventaja que tiene para analizar y aprender, además que puede resolver problemas al momento de obtener las imágenes por un conjunto de puntos; este pertenece a la familia de clasificadores lineales.

3.2.4.6 Microsoft Face API

Face API (Application Program Interface) tiene dos funciones principales: detección de rostros con atributos y reconocimiento facial. Detecta hasta 64 rostros humanos con una ubicación de la cara de alta precisión en una imagen. Que indica la ubicación de la cara en la imagen que se devuelve junto con cada cara detectada. Opcionalmente, la detección de rostros extrae una serie de atributos relacionados con la cara, como pose, sexo, edad, pose de cabeza, vello facial y anteojos.

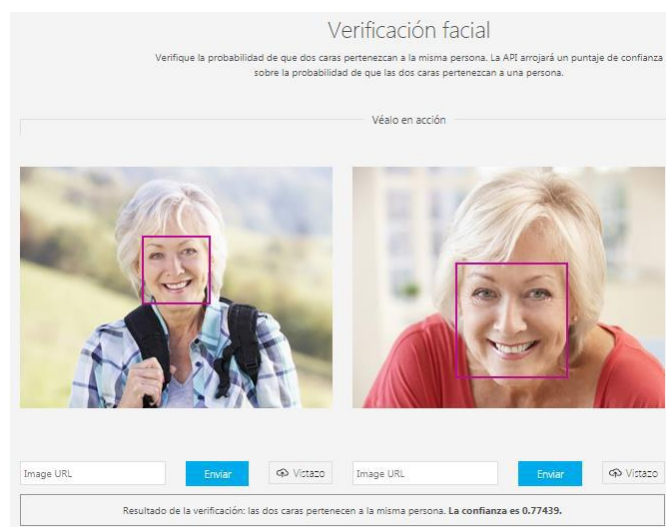


Figura 1: Verificación facial en Face Api

Fuente: <https://azure.microsoft.com/en-us/services/cognitiveservices/face/?v=18.05>

3.2.4.7 Luxand, Inc.

Luxand, Inc. es una empresa privada de alta tecnología formada en 2005. Las actividades de investigación Luxand comenzaron con la inteligencia artificial y las tecnologías de identificación biométrica, permitiendo a la compañía desarrollar un conjunto completo de herramientas y bibliotecas para realizar reconocimiento totalmente automático de rostros humanos y rasgos faciales. Hoy, la compañía ofrece una amplia gama de soluciones de reconocimiento facial. Los productos y las tecnologías de la compañía son utilizados por empresas de seguridad e identificación biométrica, bancos, industria del entretenimiento, industria médica y cosmética, en portales de entretenimiento en línea, salas de chat y sitios web de películas en todo el mundo.

“Las organizaciones policiales y militares están utilizando las tecnologías Luxand para identificar a las personas y localizar registros personales mediante fotografías faciales. Los Gobiernos, Las entidades Municipales y comerciales están utilizando estos productos en su flujo de trabajo de documentos para automatizar el proceso de ingreso de imágenes faciales en una base de datos. Las universidades y las instalaciones de investigación están utilizando herramientas y tecnologías para realizar investigaciones científicas”. (Luxland 2010).

Esta empresa es una de las muchas que ofrecen programas en concepto de seguridad, lo cual también es una opción viable en la implementación de estas técnicas de identificación facial.

3.2.4.8 Luxand Face SDK

Es una aplicación web que tiene el objetivo de verificar e identificar individuos, ofrece una gran cantidad de servicios. “Face SDK permite a los desarrolladores de Microsoft Visual C ++, C#, Objective C, VB, Java y Delphi crear aplicaciones de 32 y 64 bits para Web, Windows, Linux, MacOS, iOS y Android con funciones de reconocimiento facial e identificación biométrica basada en la cara” (Luxand, 2010).

La ventaja de este servicio es que puede ser utilizado en teléfonos inteligentes, tablets, computadoras y aparatos similares que pueden ser transportados. “FaceSDK se utiliza en cientos de aplicaciones para identificar y autenticar usuarios con cámaras web, buscar caras coincidentes en bases de datos de fotos, detectar automáticamente las características faciales en editores gráficos y detectar caras en imágenes fijas y secuencias de video en tiempo real. FaceSDK se ha utilizado para crear sistemas seguros de control de identificación, vigilancia y asistencia” (Luxand, 2010). “Es una excelente herramienta pero tiene un costo para su implementación” (Luxand, 2010).

En Guatemala la mayor parte de personas tienen acceso a los teléfonos inteligentes, esta es una era donde incluso los niños saben utilizar aparatos de alta tecnología; aunque la mayoría de veces no se les da a estos aparatos una finalidad que ayude a la sociedad. Con este servicio web, las autoridades podrán utilizar teléfonos inteligentes para detectar si algún individuo posee antecedentes criminales o inclusive orden de captura, de una manera inmediata y eficaz.

3.3 Programas de Reconocimiento Facial que se utilizan actualmente para la vigilancia en las cámaras de seguridad.

Actualmente las cámaras de vigilancia en Guatemala cuentan con los programas predeterminados que se incluyen con la compra del aparato, dichos sistemas son básicos, cuentan con un sistema elemental de grabación de imagen y algunas cuentan con audio, ampliación de imagen, y algunas con mejoramiento de imagen, según sea la versión de cámaras que se adquieren por la municipalidad por el proceso de Guatecompras.

Aún no se ha implementado la tecnología de reconocimiento biométrico en el país, principalmente porque aunque el Registro Nacional de las Personas de Guatemala (RENAP) posee una base de datos de imágenes con las cuales hacer un cotejo para identificar los rostros y poder identificar algún individuo, se necesita una autorización de Gobernación Departamental para realizar este proceso; actualmente la vigilancia se hace de forma muy manual, siendo necesario el constante monitoreo de las imágenes proyectadas en las pantallas para detectar actos ilícitos.

Existen varios modelos de cámaras instalados siendo los más comunes las tipo Bala: Estas cámaras se caracterizan por contar una mayor capacidad de visión nocturna, y resultan ser más resistentes en exteriores por que cuentan con una carcasa metálica que las protege; dichas cámaras cuentan con los estándares mínimos para poder

monitorear de manera efectiva pero no para reconocimiento facial, si el sospechoso está lejos o fuera del ángulo de visibilidad de la cámara es muy difícil localizar al delincuente. Actualmente existen cámaras en las cuales se puede implementar la tecnología de reconocimiento facial, pero no son utilizadas para el monitoreo en las vías públicas, debido a su alto costo y el temor que pueden ser objeto de hurto.

CAPÍTULO IV

4. Países que sobresalen en tecnología de identificación biométrica y beneficios obtenidos

Cabe mencionar en la presente investigación a los países que han logrado sobresalir en el uso de la tecnología biométrica en reconocimiento facial, de esta manera estudiar las estrategias utilizadas por estas potencias, las cuales han destacado en la historia por los logros obtenidos, los cuales serán estudiados a continuación.

4.1 Estados Unidos y su política contra el terrorismo

Estados Unidos posee una política bastante fuerte en el concepto de seguridad, existen protocolos que se utilizan en los aeropuertos en la lucha contra el Terrorismo, Narcotráfico, Contrabando entre otros delitos. "El atentado del 11S marcó un hito en la historia de la biometría, pues tras ese ataque terrorista, "Estados Unidos empezó a recoger las huellas de todo el que entrara; esos datos se pueden contrastar con la lista de los presuntos terroristas", La reciente tecnología para el reconocimiento facial les permite a los agentes de seguridad del aeropuerto de Washington atrapar a un pasajero que trata de escabullirse en Estados Unidos utilizando el pasaporte de otra persona. La tecnología, que utiliza un nuevo sistema biométrico que compara el rostro

del viajero con la foto que muestra su pasaporte había sido instalada en el aeropuerto apenas tres días antes de que atrapara a un impostor”.³⁹

Lo anterior indica la efectividad del sistema de identificación facial, si en los Estados Unidos que es un país con leyes bastante fuertes, las personas intentar retar al sistema, cuanto más no se cometerán estos delitos en Guatemala.

“El sistema para la comparación facial es importante porque el emparejar el rostro de una persona con la fotografía de identificación puede ser más complicado de lo que parece. Cuando una persona pierde peso, se corta el cabello o comienza a usar anteojos, puede hacer más difícil para los agentes estar seguros de que esa persona sea la que esté presentando su propia identificación”.⁴⁰ Esta es una de las debilidades del sistema de identificación facial, sin embargo hay programas como los explicados en el capítulo anterior que ayudan a mejorar esta situación.

“Ahora, usando la nueva tecnología para el reconocimiento facial biométrico los agentes fronterizos pueden dejar de adivinar cuándo deben dejar pasar a la persona

³⁹Anil J. “**Solo los Gobiernos pueden evitar el abuso del reconocimiento facial o de las huellas digitales**”, EL PAIS, Estados Unidos, 2 de octubre de 2018, p. 1

⁴⁰Una de las debilidades de la tecnología en reconocimiento facial es que el ser humano puede cambiar su apariencia física, la vejez es una de los factores naturales o también por medio de métodos artificiales como las cirugías, de esta manera puede ser difícil su detección, aunque ya existe un software especializado que es capaz de comparar las fotografías en una base de datos e identificar a un individuo por las características que son muy difíciles de alterar, como los ojos, distancia entre los pómulos ente otras. Blnetskaya M. **Reconocimiento Facial En El Ámbito Forense**

que presenta su propia identificación y cuándo frenar los fraudes de identidad e impostores. La nueva tecnología para el reconocimiento facial es parte de un programa puesto en marcha en 14 aeropuertos de Estados Unidos”.⁴¹

Guatemala es también víctima de muchos delitos en los aeropuertos, donde frecuentemente se observan infracciones relacionadas con el narcotráfico, contrabando, suplantación de identidad, entre otros, por lo cual la tecnología de reconocimiento facial será muy favorable para combatir a los delincuentes que tratan de burlar la seguridad en el aeropuerto internacional La Aurora.

4.2 España y su legislación de cesión de datos personales para la investigación penal

Una de las principales barreras en la aplicación de tecnología de reconocimiento facial es que no está legislado, se puede observar que España ha logrado superar estos obstáculos de una manera muy efectiva. “El Reglamento General de Protección de Datos (RGPD) es el Reglamento Europeo relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos. Entró en vigor el 25 de mayo de 2016 y fue de aplicación el 25 de mayo de 2018, dos años durante los cuales las empresas, las organizaciones, los organismos y las instituciones se fueron adaptando para su cumplimiento. Es una normativa a nivel de la Unión Europea, por lo que cualquier empresa de la unión, o aquellas empresas

⁴¹ Anil J. **Ob Cit.** Pág. 2

que tengan negocios en la Unión Europea, que manejen información personal de cualquier tipo, deberán acogerse a la misma”.⁴²

La regulación se aplica si el controlador de datos (una organización que recolecta datos de residentes de la Unión Europea) o el procesador (una organización que trata datos en nombre del controlador de datos, por ejemplo, proveedores de servicios en la nube) o el interesado (persona) tiene su sede en la Unión Europea. Además, la regulación también se aplica a las organizaciones con sede fuera de la Unión Europea si recopilan o tratan datos personales de los residentes de la Unión Europea. Según la Comisión Europea, "los datos personales son cualquier información relacionada con un individuo, ya sea que se refiera a su vida privada, profesional o pública. Puede ser cualquier cosa desde un nombre, domicilio, foto, dirección de correo electrónico, detalles bancarios, publicaciones en sitios web de redes sociales, información médica o la dirección IP de una computadora”.⁴³

El reglamento no pretende aplicarse al tratamiento de datos personales para actividades de seguridad nacional o aplicación de la ley en la Unión Europea; sin embargo, “grupos industriales preocupados por enfrentar un posible conflicto de leyes han cuestionado si el Artículo 48 de la RGPD (Reglamento General de Protección de Datos) podría invocarse para evitar que un controlador de datos sujeto a las leyes de

⁴²**Lawpatentgroup**, visitado el 5 de septiembre de 2019, recuperado de: «<https://via.hypothes.is/http://mlawgroup.de/news/publications/detail.php#annotations:oExZ4PVtEeefHEPs4cEz6w>»

⁴³**Ibid** pág. 2

un tercer país cumpla con un orden legal de la aplicación de la ley de ese país, judicial, o las autoridades de seguridad nacional divulguen a dichas autoridades los datos personales de una persona de la UE, independientemente de si los datos residen dentro o fuera de la Unión Europea”.⁴⁴

El Artículo 48 del Reglamento General de Protección de Datos, establece que “cualquier juicio de un tribunal o tribunal y cualquier decisión de una autoridad administrativa de un tercer país que requiera que un controlador o procesador transfiera o divulgue datos personales solo podrá ser reconocido o exigible de cualquier manera si se basa en un acuerdo internacional, tal como un tratado de asistencia jurídica mutua vigente entre el tercer país (no de la Unión Europea) solicitante y la Unión o un Estado miembro, el paquete de reforma de protección de datos también incluye una Directiva de protección de datos separada para el sector policial y de justicia penal que proporciona normas sobre personal intercambios de datos a nivel nacional, europeo e internacional”.⁴⁵

El Artículo 11 de la Ley Española de cesión de datos personales, en su inciso primero indica “Los datos de carácter personal objeto del tratamiento solo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del

⁴⁴ **Ibid** pág. 2.

⁴⁵ **European Commission’s press release announcing the proposed comprehensive reform of data protection rules.** España, 25 de enero de 2012.

interesado” sin embargo el inciso segundo del mismo Artículo 11 indica que no es necesario el consentimiento de la persona cuando: “La comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo”.⁴⁶

Uno de los fines primordiales en casi todos los países del mundo es la protección a la vida; siendo el derecho a la privacidad un derecho humano, sin embargo si para proteger la vida es necesario revelar ciertos datos, esto no está contra los principios constitucionales, indicados en los Artículos: 1, 2, 3, 4, 5, y 6 de la Constitución Política de la Republica de Guatemala. Pues como lo indica el Artículo tres de la Constitución en mención, es deber del Estado garantizar y proteger la vida desde su concepción, así como su integridad y la seguridad de la persona.

“El Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas o a las instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas y se realice en el ámbito de las funciones que la ley les atribuya expresamente, asimismo el Artículo 10 del mismo cuerpo legal indica que no es necesario el consentimiento del interesado cuando el responsable deba cumplir un deber que le impongan una de dichas normas; dicho cuerpo legal no solo protege los derechos a la distribución a la información personal sino que también antepone el

⁴⁶**Ibid** pág. 3.

interés público y la seguridad ciudadana al permitir la cesión de datos cuando la ley así lo permita”.⁴⁷

Esta misma iniciativa debe implementarse en Guatemala, permitiendo la cesión de datos privados, toda vez sea solicitado por el Ministerio Público o Jueces competentes, toda vez sea para resolver una situación donde los principios constitucionales se vean vulnerados.

“Las garantías del debido proceso penal se están revelando insuficientes para dar respuesta a una cuestión aparentemente simple. Es decir ¿cómo justificar la posibilidad de imponer a un particular la obligación de ceder para los fines de la investigación penal un conjunto de datos personales que previamente habían sido recopilados y tratados por él con una finalidad absolutamente diversa? y, en principio, desconectada del interés público en la persecución del delito. En la medida en que las autoridades encargadas de la investigación penal requieran esa información se originará una revelación de datos a persona distinta del interesado”.⁴⁸

En la legislación Española hubo dificultades para justificar la solicitud de datos cuando estos son de persona no relacionada a la investigación, esto abre puertas al mal uso

⁴⁷ Centro Europeo de Posgrado, **Cesión De Datos Personales**, España, 2018, recuperado de: <https://www.ceupe.com/blog/cesion-de-datos-personales.html>

⁴⁸(LA LEY 4633/1999)i) LO 15/1999, de 13 de diciembre, **de Protección de Datos de Carácter Personal** (LOPD (LA LEY 4633/1999)CP) integra la «cesión o comunicación de datos».

de esta información que potencialmente sería utilizado para otros fines distintos a los de la seguridad.

“Una sucinta mirada al panorama normativo, necesariamente limitada ante la infinidad de datos que pueden revestir utilidad para la persecución de delitos, la cual da muestra de la dispersión en las previsiones aplicables: datos sanitarios, biológicos, biométricos, bancarios, fiscales, del Registro de la Propiedad, sobre comunicaciones, sobre localización geográfica, etc. El requerimiento de la actuación indicada, a pesar de su manifiesta y generalizada realización en la praxis, carece sin embargo de un verdadero soporte legal en las normas procesales más allá del recurso a habilitaciones genéricas. Ello está originando consecuentemente la ausencia de criterios jurisprudenciales dotados de una visión de conjunto y de homogeneidad en atención a todos los intereses en juego”.⁴⁹

Al hacer análisis de la legislación Europea especialmente la legislación Española, está claro que es más importante la seguridad colectiva, que la privacidad de unas personas, pues estos datos pueden servir incluso para salvar la vida a estos individuos, cada año es observable el gran número de delitos que se perpetran a través de dispositivos móviles y ordenadores a través de redes sociales, España ha llegado a un nivel más alto donde en los delitos de secuestro por ejemplo, pueden inclusive acceder

⁴⁹Cesión de datos personales para la investigación penal **Una propuesta para su inmediata inclusión en la Ley de Enjuiciamiento Criminal** (LA LEY 1/1882) Julio PÉREZ GIL, Universidad de Burgos Diario La Ley, Nº 7401, Sección Doctrina, 13 de Mayo 2010, Año XXXI, Editorial LA LEY págs. 1,2

a los mensajes en las diferentes plataformas a solicitud de la autoridad competente para determinar donde estuvo la última vez o con quien tuvo contacto, esto resolvería muchos delitos en Guatemala si se aplicara tal iniciativa.

4.3 China y su sistema de control de ciudadanos

Debido a la gran densidad poblacional de la República Popular de China, la cual para el año 2018 es el país más habitado del mundo con una cantidad de 1, 380, 996,000 habitantes, haciendo una comparación que China posee más de cien habitantes por cada guatemalteco, lo cual parecería imposible vigilar a tantas personas, si para nuestras autoridades la tarea de proporcionar seguridad es un verdadero reto; sin embargo el gobierno chino ha encontrado soluciones a este problema.

“China sigue avanzando en sus pasos hacia el control de los ciudadanos. Ha sido el país pionero en probar el sistema de rating entre sus habitantes, lo que ellos llaman el Sistema de Crédito Social que, utilizando la Big Data puntuará a los más de 1.300 millones de habitantes del país asiático para juzgar si son o no unos ciudadanos fiables. Actualmente se le considera el país de las videocámaras. Meses después de que esta iniciativa apareciera en todos los medios de comunicación, se conoce el

siguiente paso: China ya puede identificar a sus ciudadanos por su forma de caminar. Un gran avance a la inteligencia artificial que se utiliza para vigilar”.⁵⁰

El gobierno Chino no se limita solo a vigilar por medio de cámaras de alta tecnología, sino a registrar conductas inapropiadas entre los ciudadanos.

“Las autoridades chinas ya han empezado a desarrollar y probar esta nueva herramienta de vigilancia: se trata de un software que utiliza las formas del cuerpo de la gente y su manera de caminar para identificarlos, incluso cuando sus caras no están visibles a las cámaras (China es el hogar de la red de cámaras CCTV (Televisión de Circuito Cerrado) más grande del mundo, cuenta con más de 170 millones). Este sistema ya se utiliza por la policía en las calles de Beijing y Shanghái, junto con el reconocimiento facial, para identificar a las personas en las multitudes y atrapar a delincuentes. Además, está desarrollando un sistema nacional integrado de datos de cámaras de vigilancia, según la agencia de noticias AP”.⁵¹

⁵⁰ En China todos los delincuentes son registrados en una base de datos bastante compleja, de manera que al que cometa un delito se le puede detectar con más facilidad su identidad por las características como: su estatura, alguna cicatriz, su forma de caminar, la cual le permite identificar efectivamente a casi cualquier persona.

⁵¹ Pérez J. **Cesión de datos personales para la investigación penal Una propuesta para su inmediata inclusión en la Ley de Enjuiciamiento Criminal** (LA LEY 1/1882), Universidad de Burgos Diario La Ley, Nº 7401, Sección Doctrina, 13 Mayo. 2010, Año XXXI, Editorial LA LEY p. 1,2

Estas cámaras utilizan algoritmos como los expuestos en el capítulo anterior, que pueden emparejar imágenes con una base de datos y así encontrar en segundos algún delincuente, aunque este tenga partes del rostro cubierto.

“La startup Watrix ha sido la responsable de su desarrollo. Su CEO, Huang Yongzhen, explica que se pueden identificar los andares de personas que se encuentran a una distancia de hasta 50 metros, incluso de espaldas o con la cara cubierta. "Esto puede llenar el vacío del reconocimiento facial, que requiere imágenes de primer plano y alta resolución de la cara de una persona para funcionar".

El reconocimiento facial como toda técnica de identificación biométrica no es infalible, el gobierno Chino usa además inteligencia artificial que puede determinar detalles como la altura, ancho de hombros, estructura física, color de piel, por la forma de caminar determinar si posee algún defecto físico, de esta manera analiza la probabilidad de ser ese sujeto algún delincuente buscado.

“El propio Yongzhen reconoce que "no es necesaria la cooperación de la gente para que puedan reconocer su identidad". Además, el sistema no puede ser engañado, caminando con las piernas extendidas o encorvado, porque analiza todas las características del cuerpo. Ahora es más real que nunca, pero las aplicaciones de esta tecnología no son nuevas. Científicos de Japón, Reino Unido y la Agencia de Sistemas

de Información de Defensa de Estados Unidos han estado investigando el reconocimiento de la marcha durante más de una década, intentando superar el escepticismo de que las personas puedan ser reconocidas por la forma en que caminan”.⁵²

China ha logrado desarrollar sistemas para la seguridad ciudadana, tomando medidas un tanto extremas, debido a la gran cantidad de personas que tiene este país y al alto índice delictivo, han logrado un sistema eficiente de seguridad social, en Guatemala no se posee tal tecnología por el momento pero indudablemente será necesario aplicar en el futuro, debido al alto índice de crecimiento poblacional y el índice delictivo.

⁵²China ya puede identificar a sus ciudadanos solo por su forma de caminar, El País Retina, Madrid 8 de Noviembre de 2018, <https://retina.elpais.com/retina/2018/11/07/innovacion/>

CAPÍTULO V

5. Implementación de tecnología avanzada de detección biométrica en el departamento de Guatemala.

Para la implementación de esta tecnología en Guatemala, se debe comprender que concurren factores imposibles de ser evitados; existen dos obstáculos principales para llevar a cabo tal iniciativa: El primero es la situación económica, la implementación de equipo de alta tecnología, también implica contratar un equipo especializado para su manejo, el cual representa un gasto significativo; El segundo obstáculo es el más difícil que es la voluntad política, proporcionar una herramienta de tal magnitud para combatir el crimen, es algo que lamentablemente no va de conformidad con los intereses de muchos poderes siniestros en nuestro país, pues las bases de esta tecnología ya existen.

5.1 Requerimientos para su implementación

Para la implementación de esta técnica se necesitan tres factores fundamentales, los cuales serán desarrollados a lo largo del presente capítulo; no se trata solamente de adquirir las cámaras de vigilancia que es propiamente el hardware que consiste en el aparato físico; el segundo factor consiste en el software o sistema operativo que es la parte intangible en cualquiera de las muchas modalidades presentadas en el capítulo anterior, los cuales pueden ser con inteligencia artificial, redes neuronales o sistemas

de verificación lineal, esto determinará la rapidez con que puede detectarse un rostro que las cámaras puedan captar, mejorar e incluso determinar conductas criminales en la vía pública lo cual agilizará la detección de este tipo de actividades; el tercer factor es que entidad será la encargada del manejo de tal tecnología, pues aunque existen entidades encargadas de la seguridad ciudadana, esta tecnología no requiere solamente de monitoreo sino de técnicos capaces de manipular el software el cual es más complejo de lo que parece, sin lo cual no se obtendrán los resultados óptimos.

5.1.1 Tipo de hardware necesario

Existe una gran cantidad de cámaras para cada propósito, esto está directamente relacionado al lugar donde serán instaladas; para que el reconocimiento facial sea efectivo se requieren unos requisitos mínimos en el hardware; “la plataforma de hardware: Windows, Mac, Linux, PC, Los componentes Smart Surveillance Engine (SSE), Deep Learning Engine (DLE) y Middleware for Large Scale Surveillance (MILS) deben satisfacer los requisitos de sistema de hardware y software mínimos. Las imágenes de cara que están inscritas en la base de datos de lista de observación deben estar en formato de archivo .jpg, tener un tamaño inferior a 4 MB y tener suficiente calidad. La imagen contiene una vista frontal de la cara, iluminación buena y al menos 80 píxeles entre los ojos”.⁵³

⁵³ IBM knowledge center, **Requisitos mínimos para el Reconocimiento Facial**: EU, 2019, recuperado de: https://www.ibm.com/support/knowledgecenter/es/SS88XH_2.0.0/iva/int_frs_min_req.html

En Guatemala para el año 2018 diferentes entidades como Municipalidades y Ministerios entre otros, han adquirido equipo de vigilancia bastante sofisticado, como se puede verificar en el portal web Guatecompras, los sistemas de vigilancia más recientes son capaces de soportar el software de reconocimiento facial bastante bien, aunque la cantidad de cámaras aun no es el ideal para proporcionar una excelente cobertura, aun así, esto afirma que si hay capacidad para implementar las estrategias que son objeto de estudio en la presente investigación.

5.1.2 Software que se deberá utilizar para su eficacia

Los sistemas de inteligencia artificial para reconocimiento de rostros, que se utilizan en muchos países, aún no están implementados en Guatemala. A continuación serán mencionados solamente algunos de los más utilizados que pueden ser situados: El módulo de búsqueda de rostros accionado por el motor de búsqueda Cognitec o VeriLook: Crea una base de datos de todos los rostros capturados por las videocámaras y permite buscar rostros similares en la base de datos. Para buscar debe indicarse una imagen en el archivo de vídeo que contiene un rostro, indique un enlace (URL) a una imagen o cargue la imagen de un rostro en el sistema.

“Los resultados se muestran en forma de una lista de fotografías ordenadas por el grado de similitud. Este módulo hace mucho más rápida la búsqueda de imágenes de vídeo de las personas de interés, así como la recopilación de estadísticas sobre la

captura realizada por varias cámaras. La corriente de vídeo entrante o el vídeo grabado deben ser de un canal que esté configurado para utilizar los perfiles analíticos de Nearfield People Search o Body Camera Analytics”.⁵⁴

El software ideal no solo permitirá identificar a un sujeto sino que en los casos donde no haya una imagen completa, como es común en muchos delitos, este sistema permitirá buscar en la base de datos similitudes con lo cual se podrá agilizar la investigación y evitar falsos positivos, que solo entorpecen el proceso investigativo.

5.2 Cobertura

Es evidente que no solo es necesario tener un buen aparato sino que también están los factores de cantidad el cual tampoco consiste en saturar la ciudad con cámaras de vigilancia sino también de proponer estrategias en su incorporación, enfatizando en elementos como el posicionamiento, el equipo de soporte material, como postes, semáforos, arboles, camuflaje, protección entre otros.

“En la ciudad de Guatemala existían para abril del 2017,620 cámaras en la ciudad de Guatemala cuya densidad poblacional es de más de un millón de habitantes, es decir

⁵⁴Ibid.

un aproximado de una cámara por cada 1612 habitantes”⁵⁵, sin embargo la cantidad no lo es todo sino la estrategia a utilizar, como la ubicación, distribución de las mismas; si se hiciera una comparación entre los países más avanzados, de los cuales los países que cuentan con mayor número de cámaras de vigilancia son: Inglaterra, el cual posee una cámara por cada doce habitantes y China que posee más mil cuatrocientos millones de habitantes, cuenta con más de doscientos millones de cámaras, aproximadamente una cámara por cada siete personas.

Otros países como los Estados Unidos no tienen tantas cámaras de vigilancia pero las que poseen son de alta calidad, costando cientos de dólares cada aparato, además que ellos poseen una estrategia muy efectiva en la colocación de las mismas. Observando los datos anteriores se puede determinar que se necesita al menos el doble de cantidad de cámaras de las que actualmente están instaladas, y considerar que de las existentes, muchas ya son obsoletas, además es necesario ubicarlas en lugares estratégicos, y también aplicar el software de reconocimiento facial, así mismo es posible proyectar que la cantidad actual no es suficiente debido también a que la población sigue creciendo y la delincuencia consigo, por tanto es necesario aplicar nuevas maniobras en contra de este flagelo.

⁵⁵ **Ibid** pág. 2.

5.3 Costos

Cada unidad de cámaras de vigilancia con los requisitos mínimos para el reconocimiento facial tiene un costo mayor a los seiscientos quetzales, y en promedio entre las más avanzadas tienen costos aproximados de mil dólares cada una, asimismo “es necesario un sistema de programación capaz de brindar el soporte necesario para el reconocimiento facial, siendo necesario contar con la licencia de dichos programas los cuales están desde cuarenta dólares al mes, dependiendo del paquete”⁵⁶ a otros cuyos precios son más elevados dependiendo de la cobertura, sin embargo se hace énfasis que existen una gran cantidad de empresas que ofrecen este servicio el cual es accesible y sería de gran ayuda para combatir el crimen.

5.4 Viabilidad

Actualmente ya existe un sistema de vigilancia por medio de cámaras de video, sin embargo es necesaria la actualización y adaptación de programas de reconocimiento facial, mejorar las cámaras de video a unas que puedan detectar de manera eficiente a las personas, además que también es necesario la instalación de equipo como postes, cableado, redes inalámbricas, el recurso humano no es tan extenso pues los programas cuentan con funciones que ayudan a realizar el trabajo.

⁵⁶Gutiérrez P. **La aplicación permite detectar rostros y devolver resultados sobre franja de edad y sexo de la persona con un 90% de precisión y en forma anónima.** EU, 2019, recuperado de: <https://www.fayerwayer.com/2013/05/un-software-ofrece-reconocimiento-facial-para-comercios-por-us40-al-mes/>

Para su funcionamiento legal es necesaria la creación de una legislación que permita el uso adecuado de esta tecnología, por técnicos competentes o la modificación de la ley del Instituto Nacional de Ciencias Forenses, el cual sería el más adecuado; este proyecto sería posible en un futuro no muy lejano; en muchos países ya es aplicada esta tecnología en concepto de seguridad, en muchos otros se ha empezado a implementar pues sus ventajas son indiscutibles.

CONCLUSIÓN DISCURSIVA

Con el exponencial aumento de la actividad criminal en el territorio nacional, es imprescindible generar nuevas técnicas para incrementar la cobertura de los sistemas de vigilancia en el Municipio de Guatemala del Departamento de Guatemala el cual es uno de varios municipios afectados por el alto índice de criminalidad, por diversos grupos delincuenciales los cuales cada día generan nuevas astucias para consumir el delito, mientras que tristemente es perceptible la impotencia del Estado para poder cumplir con salvaguardar el derecho a la seguridad ciudadana y proteger los derechos inherentes a la persona humana.

La falta de estrategias en concepto de vigilancia, en parte no se debe solamente a la falta de voluntad política, sino a diversos factores entre los cuales sobresalen los aspectos financiero-económicos, y aspectos legales. Está comprobado que la tecnología biométrica en muchas partes del mundo ha contribuido a proteger no solamente los bienes económicos sino también ha dado un gran aporte en el campo de la criminalística en la etapa preparatoria en el derecho procesal penal, por la efectividad de la detección e individualización de los delincuentes lo cual siempre ha sido un obstáculo en la investigación cuando se comete un delito, pues no siempre se halla la suficiente evidencia para poder vincular una persona a un proceso penal.

El reconocimiento facial por cámaras de seguridad con inteligencia artificial es parte de una tecnología que aún no es aplicada en el territorio Nacional, en parte porque hay temor que esta pueda vulnerar ciertos derechos a la privacidad. A través de la

observación y análisis de políticas internacionales se puede concluir que la vigencia de los derechos y libertades que la Constitución Política de la República de Guatemala reconoce no es ilimitada, admitiendo la suspensión en casos expresamente establecidos en ésta, tal es el ejemplo de los estados de excepción, regulados también la Ley del Orden Público y Estados de Excepción. Se debe partir de la base de que la suspensión de los derechos no supone su desaparición aunque es cierto que se somete a un régimen jurídico distinto, con más limitaciones que las ordinarias.

Finalmente se establece que las estrategias de identificación biométrica pueden ser aplicadas dentro del territorio nacional para fortalecer la seguridad ciudadana, es posible legislar sobre el uso de datos privados toda vez su finalidad sea cumplir con las garantías constitucionales, al agilizar considerablemente la detección de actividades ilícitas por medio de un sistema complejo que incluye el uso de aparatos de alta tecnología que puedan dar soporte al software de reconocimiento facial y además optimizar las estrategias en vigilancia ciudadana, también es necesario contar con profesionales capacitados para administrar la parte técnica y poner en las manos indicadas la información necesaria que servirá para agilizar un proceso penal con la finalidad de impartir justicia ágilmente.

6. Anexos

6.1 Beneficios de la tecnología biométrica

Las ventajas en esta tecnología es la selección eficiente de características, invariante a escala y localización, en Guatemala muchos municipios necesitan aumentar la seguridad en sus zonas de influencia pero no cuentan con los medios económicos para contratar más policías, adicionalmente en municipios medianos o grandes el tiempo de respuesta de las autoridades es un problema.

“La solución que se ha encontrado a través de la tecnología biométrica, utilizar cámaras para suplir los ojos de los policías, éstas graban 24 horas al día además de identificar matrículas, individuos y hacer muchas otras funciones al desplegar una red radio a través de las calles de un municipio. Para tener una red profesional de vídeo en un ambiente urbano de exteriores es necesario contar con equipos radio de calidad que utilicen protocolos específicos y probados”.⁵⁷

La creación de leyes contra la delincuencia es solamente una parte de la solución para disminuir el índice delictivo, la parte más importante es cómo aplicarlas, en lo referente a las estrategias y técnicas a utilizar para asegurar su cumplimiento, sin lo cual no pasarán de la parte ideológica tales leyes.

⁵⁷ Ubierna O. **Video vigilancia inalámbrica en Municipalidades**, España, 2018, recuperado de: <https://www.comunicacionesinalambricashoy.com/wireless/video-vigilancia-inalambrica-en-municipalidades/>

6.2 Ventajas del reconocimiento de rostros en la biometría en contraste con otros sistemas de identificación biométrica.

En Guatemala ya se tiene conocimiento de tecnologías de identificación biométrica, las cuales son usados por muchas instituciones tanto del sector público como privado, para diferentes propósitos; sin embargo con el avanzar de la ciencia estas técnicas se van perfeccionando, con lo cual se debe observar la utilidad de estos avances en el concepto de seguridad ciudadana; dentro de estas tecnologías algunas tienen ventajas sobre otras. “Mientras que algunos indicadores requieren alguna acción voluntaria, el reconocimiento de rostros puede ser usado pasivamente. Esto es una ventaja para hacer más fácil su utilización y ser convertido, por ejemplo en un sistema de vigilancia policial”.⁵⁸

A diferencia de los que utilizan la tecnología biométrica en los sectores de empresas e industrias, en el sector seguridad y justicia resulta un problema pues en la mayoría de casos no se tiene el consentimiento del individuo a investigar para obtener la información que servirá para relacionar al sujeto en un proceso penal.

“En lo que concierne a la adquisición de datos, es más fácil obtener buenas imágenes faciales que buenas huellas digitales. Por ejemplo un 5% de personas no pueden proveer una suficientemente buena imagen para un lector que es utilizado para

⁵⁸Valvert G. Jorge **Métodos Y Técnicas De Reconocimiento De Rostros En Imágenes Digitales Bidimensionales**, Guatemala, 2006, Tesis de graduación, facultad de ingeniería. Pág. 18.

autenticación. Las razones incluyen piel cortada, dedos vendados, callosidades, piel seca o húmeda etc. Otra desventaja que se encuentra en la detección de huellas es que los scanner de huella digital o de palma de la mano pueden transmitir gérmenes a la mano”.⁵⁹

Es necesario observar que en muchos casos los delincuentes que tienen mayor experiencia, utilizan accesorios en las manos, como guantes o vendajes, con los cuales pretenden no dejar huellas digitales, al perpetrar el delito.

“En contraste con el sistema de reconocimiento de rostros es totalmente higiénico y no requiere mantenimiento debido a que es utilizado a distancia. El reconocimiento de rostros, es muy fácil de operar en interiores y exteriores detectando rostros en fondos complejos”.⁶⁰

Es clara la ventaja de las cámaras de seguridad, pues en la mayoría de casos, los delincuentes no se dan cuenta que están siendo grabados, ya que dependiendo del modelo de la cámara de seguridad estas son capaces de vigilar desde grandes distancias.

“Los scanner de iris pueden proveer una alta efectividad para la identificación de personas, sin embargo, debido a que el iris es muy pequeño, necesita una cámara especial de alta resolución para que este sea capturado. Además la cámara deberá

⁵⁹Ibid. pág. 18

⁶⁰Ibid. pág. 19

estar cerca para capturar toda la resolución del iris, todo este proceso es altamente sensitivo a los movimientos del cuerpo y trae como consecuencia que cualquier persona debe estar muy quieta para no ser rechazada”.⁶¹

Los escáner de iris son muy utilizados en los bancos, por su celeridad e higiene, ya que frecuentemente los lectores de huellas digitales tienden a ensuciarse debido a la grasa propia de las manos y partículas de suciedad que con el continuado uso puede dar problemas a los lectores de huella digitales, siendo una buena alternativa los lectores de iris, en muchos teléfonos inteligentes se utiliza este método para identificar al portador, el cual no permite su desbloqueo si se trata de una persona diferente a la registrada como su dueño.

“Los lectores de retina se basan en los patrones de las venas en la parte de atrás de un ojo. Estos lectores son muy exactos, pero debido a que su funcionamiento requiere de intrusión en el ojo, la mayoría de las personas se resisten a ello. Además tanto los lectores de iris y de retina fallan cuando se usan lentes de contacto, o cuando se parpadea cuando se toma la imagen. Los lentes normales también son un problema para estos scanner”.⁶²

Los lectores de iris o retina son aparatos muy confiables, lamentablemente son bastante sensibles, además que su precio es bastante alto, para el objetivo de proporcionar seguridad a través de vigilancia en lugares públicos es bastante

⁶¹Ibid. pág. 19

⁶²Ibid. pág. 19

complicado por que sería imperativo tener el ojo cerca del escáner, con lo cual los son más efectivos los identificadores faciales.

“El reconocimiento de voz para propósitos de vigilancia, no es muy confiable en entornos ruidosos como lugares públicos o a través de líneas telefónicas con acústica variable. Los sistemas de reconocimiento de voz también son sensitivos a fallar en condiciones en la que la persona está enferma con gripe. Una cinta grabada con la voz de una persona puede falsear a los sistemas de reconocimiento de voz, que no tienen un método de integridad de la voz”.⁶³

En grandes ciudades como Guatemala, Mixco, Villa Nueva, y muchas otras, es muy difícil aplicar el reconocimiento de voz, debido a la gran cantidad de personas y vehículos que transitan en todo momento, el ruido causado por estos vehículos no permite identificar con exactitud la voz de una persona para poderla individualizarla.

El reconocimiento de firma es una de las modalidades conductuales de la biometría. “La firma es utilizada para legalizar documentos, pero usualmente las personas varían significativamente su firma cada vez, debido a el bolígrafo utilizado o muchas veces por el agotamiento de los músculos de la mano al escribir con mucha frecuencia, entonces cada vez que se lee una firma es difícil saber si la persona que la coloca es la dueña de ella, esto reduce la confiabilidad de los sistemas de identificación de firmas”.⁶⁴

⁶³ **Ibid.** pág. 20

⁶⁴ **Ibid** pág. 20.

Esta modalidad ya se utiliza en Guatemala, principalmente por el sector bancario, para determinar si algún documento de crédito es firmado por el legítimo propietario de tal documento, para evitar el robo y falsificación de firmas, el cual ha dado excelentes resultados.

Al comparar estos sistemas con el sistema de reconocimiento facial es posible determinar que “En contraste, un sistema automatizado de reconocimiento de rostros, solamente requiere de una o dos cámaras comunes, y sin necesidad de algún sistema especial ya que el campo de visión es lo suficientemente grande para cubrir el rango de las diferentes estaturas de las personas, independientemente si están paradas o sentadas”.⁶⁵

Aun sin el software de reconocimiento facial la identificación por imágenes de cámaras de video es uno de los mejores métodos, pues al menos permite obtener un medio de prueba donde otros difícilmente podrían lograrlo; un software que pueda determinar con mayor exactitud la identidad de una persona, llenaría los vacíos que las cámaras comunes no pueden establecer.

6.3 Aspectos desventajosos de la implementación de tecnología biométrica

El aspecto más discordante de esta tecnología es que es necesaria la implementación de políticas que permitan la cesión de datos privados, pues muchos creen que la gran cantidad de cámaras de vigilancia que funcionan todo el día suponen una amenaza

⁶⁵ Ibid. Pág. 18.

contra la privacidad individual, por lo cual en muchos países ha sido necesaria alguna legislación en cesión de datos personales, los cuales cuando son necesarios en alguna investigación penal no hay necesidad de darles mayor trámite, de esta manera pueden agilizar la investigación.

Algunas desventajas propias de la tecnología son que las imágenes necesitan actualizarse constantemente por los efectos de la edad y es sensible de iluminación, existen problemas en registrar cuando el sujeto a ser reconocido usa gafas u otros objetos en el rostro, además la iluminación también influye bastante ya que si hay poca iluminación no realiza la función que se desea.

El problema del reconocimiento de rostros puede ser dividido en dos problemas generales:

- “Detección y localización del o de los rostros en la imagen
- Determinación de la identidad de dichos rostros.

Un sistema completo para la detección, localización y reconocimiento o identificación de rostros debe integrar las anteriores tareas”.⁶⁶

Así como toda tecnología creada por el hombre, el sistema de identificación facial puede fallar, debido a fallas en la programación la cuales son muy raras, así como también los factores ambientales externos más comunes, como la lluvia, incendios, sismos, granizo, el polvo, que directamente afectan el funcionamiento de aparato.

⁶⁶Ibid pág. 18.

6.3.1 Dada una imagen bidimensional:

Las imágenes bidimensionales son aquellas que representan dos dimensiones, como son el alto y ancho, esto quiere decir que son la representación plana del alto y el ancho de un objeto, persona, animal o cualquier elemento que se pueda plasmar por medio de un aparato de captura de imágenes. La función de un sistema de análisis de imágenes es:

- “Determinar si la imagen contiene rostros. Si es así, determinar la posición y el tamaño.
- Determinar la identidad de cada rostro presente en la imagen.
- Proporcionar una descripción acerca del rostro (alegría, enojo, tristeza, entre otros).
- Entregar información extra, por ejemplo, hacia donde está mirando la persona, la probable edad, el sexo, si porta lentes o sombrero”.⁶⁷

Cuando son lugares pocos transitados no hay problemas por la facilidad de individualizar a alguien, el problema surge cuando la persona a identificar está dentro de una multitud. “Obviamente, esta tarea es extremadamente compleja, puesto que en el caso general no se conoce ni el número de rostros, ni sus correspondientes posiciones, tamaños y orientaciones en la imagen. Además, es muy difícil resolver el problema cuando se cuenta con una base de modelos con muchos rostros. Otros

⁶⁷ Ibid pág. 19.

factores que dificultan la solución de este problema son la eventual presencia de adornos, por ejemplo: lentes, sombrero, barba o las normales variantes según el sexo, la edad y la expresión facial”.⁶⁸

Desde sus inicios a la fecha, se han propuesto diversas técnicas para dar solución al problema del reconocimiento de rostros, ya sea en tiempo real o no. Sin embargo, este problema es todavía un reto para investigadores y científicos debido a que aún se desconoce en gran medida cómo el ser humano procesa la información durante el reconocimiento de un objeto, en particular de un rostro.

“Sería ideal que un sistema para el reconocimiento de rostros por computadora pueda también ser auxiliado por otros sistemas, como por ejemplo, alguno para el reconocimiento del habla, o algún otro para el control de un determinado proceso, con el fin de generar eficiencia y rapidez en el reconocimiento”.⁶⁹

Como se estudió en el cuarto capítulo, países como China y Estados Unidos, combinan diferentes técnicas con el propósito de obtener mayor seguridad en los datos obtenidos, esto es con la finalidad de proporcionar una información casi infalible.

⁶⁸Ibid. pág. 22

⁶⁹Ibid. pág. 23

6.3.2 Funcionamiento de la tecnología biométrica en reconocimiento facial

El funcionamiento del software es del estudio del campo de la programación, por tanto será explicada de manera breve el funcionamiento de este algoritmo “El reconocimiento facial, es el sistema de identificación mediante la comparación de rostros, los primeros métodos utilizaban algoritmos basados en modelos geométricos simples. En la actualidad este sistema ha sufrido importantes avances, el creciente avance tecnológico, sistemas informáticos, así como la creación de software especializado, han marcado una nueva era en la identificación mediante métodos de reconocimiento facial. En este tipo de reconocimiento existen dos enfoques lo que deben de tomarse en cuenta al momento de realizar un estudio minucioso de sus características siendo los siguientes”.⁷⁰

Enfoque geométrico (rasgos), el cual consiste en los componentes exactos existentes en el rostro a comparar. Enfoque fotométrico, (visual), el cual consiste en el estudio de lo que puede observarse del rostro a comparar. En la historia y evolución del sistema biométrico de reconocimiento facial fueron creados un sin número de algoritmos, siendo los más utilizados los siguientes:

⁷⁰ Paul B. **Cómo funciona el reconocimiento facial**, EU, 2014, recuperado de: <http://www.biometrra.gov.ar/metodos-biometricos/facial.aspx> (19 de noviembre de 2014)

a) Análisis de componentes principales.

Esta práctica ha sido mencionada en el capítulo tercero, siendo una de las más comunes pero bastante efectivas “Es la técnica impulsada por Kirby & Sirivich; con análisis de componentes principales, el sondeo y la galería de imágenes deben ser del mismo tamaño y deben ser normalizadas previamente para alinear los ojos y bocas de los sujetos en las imágenes. La aproximación de análisis de componentes principales, es utilizada para reducir la dimensión de los datos por medio de fundamentos de compresión de datos y revela la más efectiva estructura de baja dimensión de los patrones faciales. Esta reducción en las dimensiones quita información que no es útil y descompone de manera precisa la estructura facial en componentes ortogonales”.⁷¹

Muchas veces las imágenes contienen lo que conocemos como ruido, estos son los factores como luz, sombra, distorsión entre otras que afectan la obtención de una imagen nítida, esta técnica ayuda a mejorar de manera significativa la claridad de la imagen, al eliminar dichos factores.

“Una imagen de sondeo es comparada con una galería de imágenes midiendo la distancia entre sus respectivos vectores de rasgos. La aproximación de Análisis de Componentes Principales PCA (Principal Component Analysis) por sus siglas en inglés, típicamente requiere la cara completa de frente para ser presentada cada vez; de otra forma la imagen dará un resultado de bajo rendimiento. La ventaja primaria de esta

⁷¹Ibid pág. 23.

técnica es que puede reducir los datos necesarios para identificar al individuo a 1/1000 de los datos presentados”.⁷²

Aunque la imagen no se obtenga de manera completa, esta técnica puede dar un indicio al menos de la identidad de la persona, con lo cual los investigadores no estarán con ninguna información.

b) Análisis lineal discriminante:

Mencionada en el capítulo tres como una técnica muy efectiva en la identificación facial, “Es una aproximación estadística para clasificar muestras de clases desconocidas basadas en ejemplos de entrenamiento con clases conocidas. Esta técnica tiene la intención de maximizar la variable entre clases y minimizar la variable de cada clase”.⁷³ Este análisis estadístico puede determinar de manera efectiva la probabilidad de encontrar a un individuo, utilizando algoritmos matemáticos para determinar la identidad de una persona.

c) Correspondencia entre agrupaciones de grafos elásticos:

Las imágenes faciales reales tienen muchas características no lineales que no son tratadas en los métodos lineales de análisis anteriormente expuestos, tales como

⁷²Ibid pág. 23.

⁷³Ibid pág. 24.

“variaciones en la iluminación, postura y expresión”.⁷⁴“Este sistema introduce filtros lineales con el objetivo de extraer las características elásticas de la imagen”⁷⁵

El rostro tiene muchos componentes que son únicos así como la altura de las cejas suele ser diferente, tic nerviosos, cicatrices, lunares, características que ayudan a diferenciar a una persona de otra los cuales son analizados en esta técnica.

6.3.3 Reconocimiento facial, proceso para la autenticación

Será explicado de manera breve el proceso general de autenticación de reconocimiento facial, es decir, “la comparación de los datos almacenados en el registro con los datos obtenidos por las cámaras de seguridad que se presentan al sistema”.⁷⁶

Aunque cada tipo de tecnología biométrica lleva sus respectivos pasos, se puede definir algunos comunes a todos los modelos de autenticación biométrica:

- 1) Captura. Lectura de los datos que la cámara de seguridad a validar presenta.
- 2) Extracción. Obtención de ciertas características de la muestra.
- 3) Comparación. Se toman los datos almacenados en la base de datos y se comparan con los que la cámara está presentando.
- 4) Decisión. Se analiza si el usuario es válido o no.

⁷⁴Ibid pág. 24.

⁷⁵Yoc J. Wolfredo, **La Identificación Biométrica Y La Importancia De Su Aplicación Al Derecho Registral**, Guatemala, 2015, tesis facultad de ciencias jurídicas y sociales, Universidad de San Carlos de Guatemala, pág. 47.

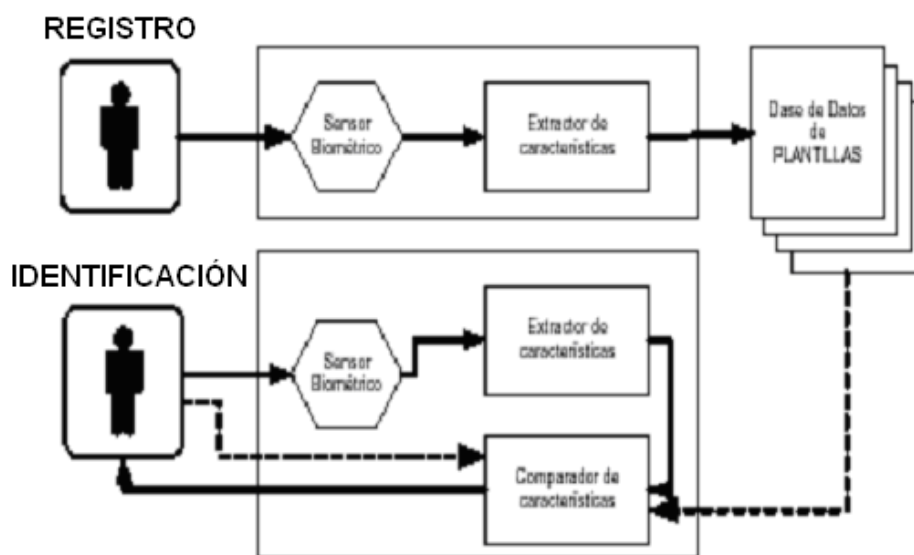
⁷⁶Castillo M. Blanca. **Tecnología Biométrica**, Guatemala, 2005, Tesis de grado, Universidad de San Carlos Facultad De Ingeniería, pág. 30

6.3.4 Arquitectura de los sistemas biométricos

Este conjunto de patrones proporcionan un marco de referencia necesario para guiar la construcción de este sistema “La arquitectura de un sistema biométrico típico refleja esencialmente la arquitectura de un sistema de reconocimiento de patrones:

- 1) Se adquiere un patrón usando sensores.
- 2) Se extrae una representación de la entrada adquirida usando un algoritmo de extracción de características”.⁷⁷

Se toma una decisión basada en la representación de entrada y la representación del patrón previamente almacenado en el sistema. La figura a continuación muestra a grandes rasgos la arquitectura del sistema biométrico.



Fuente: Arquitectura general de un sistema biométrico

Figura 2

⁷⁷Castillo M. Blanca. **Tecnología Biométrica**, Guatemala, 2005, Trabajo De Graduación Presentado A Junta Directiva De La Facultad De Ingeniería, pág. 31

El sistema principalmente consiste de dos módulos:

- 1) “Registro
- 2) Autenticación”⁷⁸

La función del módulo de registro asocia la identidad de las personas registradas con representaciones de su medida biométrica. Cuando la señal biométrica y el nombre de la persona a ser registrada son alimentados al módulo de registro, un algoritmo de extracción de características (por ejemplo, minucias de imagen facial) es aplicado al dato biométrica (por ejemplo, imagen del rostro) y una representación de las características biométricas o patrones son extraídas y almacenadas en la base de datos del sistema.

“El módulo de identificación autentifica la identidad de las personas cuya imagen son extraídas por el sistema. El sensor biométrico captura el dato biométrico de entrada; se extraen las características biométricas capturadas y éstas son comparadas con la representación de la característica biométrica de la persona almacenada en la base de datos del sistema para verificar la identidad dela persona. Un sistema de identificación determina la identidad asociada con la medida biométrica sin que la persona tenga que declarar su identidad”.⁷⁹

⁷⁸Castillo M. Blanca. **Tecnología Biométrica**, Guatemala, 2005, Trabajo De Graduación Presentado A Junta Directiva De La Facultad De Ingeniería, pág. 30.

⁷⁹**Ibid.** pág. 31

Este proceso se realiza en una fracción de segundo, solamente cuando hay problemas en la identificación y es necesaria la aplicación de tecnología de análisis de campos biométricos puede tomar más tiempo dependiendo de la calidad de la imagen obtenida.

6.3.5 Funcionamiento de la inteligencia artificial en reconocimiento de rostros

El reconocimiento de rostros es un área del reconocimiento de patrones que ha sido investigada desde hace varios años. Durante todo este tiempo se han propuesto técnicas diferentes para la resolución de esta tarea, entre las que se pueden mencionar

- “Igualamiento de plantillas
- Cálculo de Eigen caras Características Geométricas
- Métodos que utilizan redes neuronales.”⁸⁰

Independientemente de la técnica que sea implementada, se utilizan siempre dos conjuntos de datos:

- 1) “El primero es utilizado siempre para la etapa de aprendizaje, el cual es llamado conjunto de entrenamiento. Se debe tratar de que los patrones que integran este conjunto sean lo más diferente posible entre sí, y que además, representen al problema, para poder tener un buen porcentaje de generalización”⁸¹.

⁸⁰ Valvert G. Jorge R. **Métodos Y Técnicas De Reconocimiento De Rostros En Imágenes Digitales Bidimensionales**, Guatemala, 2006, Tesis de graduación, facultad de ingeniería. Pág. 3.

⁸¹ **Ibid** pág. 3.

2) El segundo conjunto de patrones, es llamado conjunto de prueba, y es utilizado en la etapa de reconocimiento.

Por último, para reconocer un rostro se deben realizar los siguientes pasos generales:

- “Extracción de componentes básicos del rostro
- Relaciones de distancia entre ojos, nariz, boca y cejas.
- Descriptores Invariantes y vectores de característica”⁸²

Este sistema es capaz de aprender, es decir debido a que su programación cuenta con algoritmos que agilizan la velocidad de respuesta en reconocer rostros, al identificar patrones entre una imagen y otra, además un importante número de delitos es cometido por delincuentes reincidentes, la Policía Nacional Civil cuanta con bases de datos donde se encuentra el perfil de los delincuentes habituales, con el mismo fin de agilizar la identificación de algún infractor de la ley.

6.3.5.1 Entrenamiento

Se le llama entrenamiento, porque en esta etapa se prueba la efectividad del sistema en reconocer los valores a identificar “El entrenamiento básicamente consiste en utilizar alguna forma de aprendizaje que le permita al sistema aprender rostros que formarán el conjunto de entrenamiento. El tipo de entrenamiento a utilizar dependerá de la metodología utilizada para el reconocimiento. Para la metodología de reconocimiento

⁸²Ibid pág. 4.

de redes neuronales, por ejemplo, el entrenamiento consiste en obtener valores correspondientes a cada una de las conexiones (pesos) las cuales forman la red neuronal”.⁸³

Programas mencionados anteriormente funcionan óptimamente con una buena calidad de imágenes, lo cual es lo correcto, pero la imagen puede variar dependiendo de la calidad de la imagen o la capacidad misma de la cámara de vigilancia que puede dificultar otros sistemas cuando no se tiene suficiente calidad; este sistema es capaz de constituir algoritmos que ayudan a obtener información con mayor precisión por la capacidad de analizar los detalles de la imagen.

6.3.5.2 Reconocimiento

La última etapa, en un sistema de reconocimiento de rostros es la etapa de reconocimiento. Consiste en alimentar al sistema con imágenes de rostros diferentes a las utilizadas durante el entrenamiento, esperando obtener como resultado, alguna forma de codificación que permita saber de qué rostro se trata.

“Un buen algoritmo de reconocimiento de rostros trabaja inclusive con reflejos provenientes de lentes o con los ojos cerrados”.⁸⁴

⁸³Valvert J. **Ob. Cit.**; pág. 5.

⁸⁴Valvert J. **Ob. Cit.**; pág. 20.

6.3.6 Reconocimiento facial en sistemas de seguridad

Esta tecnología inicio hace muchos años, aunque al principio no era tan efectiva, con el paso de los años ha ido mejorando, por la mejora de los sistemas de programación, lo cual ha aumentado bastante su popularidad y se ha vuelto muy utilizada en el mundo entero.

“En los últimos años la utilización del reconocimiento facial se ha extendido por todo el mundo y ha sido ampliamente utilizada en numerosas aplicaciones como sistemas de seguridad, sistemas de control de acceso a equipos o ambientes, identificación de conductas, entre otras”. (Barraza, Thuillier, Will & Rodríguez, 2013).”Es en el comienzo de 1970 donde el reconocimiento facial toma validez para los investigadores y desarrolladores” (Parmar & Mehta, 2014) “analizándose para reconocer a una persona mediante una fotografía por la computadora mediante la medición de la distancia entre los ojos u otros puntos importantes o medir diferentes ángulos de componentes faciales”, (Parmar & Mehta, 2014)

(Parmar & Mehta, 2014) Menciona en su trabajo que “el reconocimiento facial es un problema pero a la vez interesante y desafiante que conlleva al analisis de diferentes puntos desde la psicología, reconocimiento de patrones, redes neuronales, visión por ordenador, y gráficos por ordenador tras analizar todos estos puntos llega a la conclusión de que la investigación en el reconocimiento de caras es un área excitante para muchos años y mantendrán muchos científicos e ingenieros ocupados. En el

futuro, 2D y 3D de reconocimiento de caras y aplicaciones a gran escala, tales como el comercio electrónico, identificación de estudiante, licencias de conducir digitales, o incluso de identificación nacional es la difícil tarea de reconocimiento de rostros y el tema está abierto a futuras investigaciones”.⁸⁵

El sistema de reconocimiento facial que es el objeto de investigación del presente trabajo es una tecnología que aún se sigue desarrollando, cada año nuevos programas capaces no solo de identificar, sino de predecir las conductas criminales, obtener la ubicación de delincuentes a través de satélites, pareciera como de películas de ciencia ficción, sin embargo en un futuro no muy distante esta tecnología estará presente en todos los lugares del mundo, por el rápido avance de la ciencia.

6.3.7 Diseño de la tecnología en reconocimiento facial aplicado al campo de la criminalística, en la etapa de investigación

El sistema tiene como propósito realizar el reconocimiento facial de personas buscadas y brindar una alerta en tiempo real, así para luego ser capturado en ese instante. Para lo cual en el desarrollo del sistema se tomó en cuenta algunos requerimientos importantes como lo son: velocidad de procesamiento, eficacia, tamaño, además del costo de elementos empleados en el desarrollo del prototipo de sistema de reconocimiento facial.

⁸⁵ Ibid pág. 4.

En la figura 2 se muestra el modelo conceptual de la identificación facial: Primero el dispositivo tomara una fotografía al individuo sospechoso, para luego realizar la consulta a la base de datos del Instituto Nacional de Ciencias Forenses, si el sujeto presenta antecedentes de por algún delito será inmediatamente registrado y almacenado este dato, posteriormente el Ministerio Público quien es la autoridad delegada para realizar la investigación solicitara estos datos al Instituto Nacional de Ciencias Forenses en un plazo prudencial, estos datos serán cotejados en una base de datos los cuales identificarán según las circunstancias al delincuente, o bien hará una lista de los posibles autores, posteriormente el Ministerio Público se encargara de dar el adecuado seguimiento.

6.3.8 Modelo conceptual del sistema biométrico en reconocimiento facial

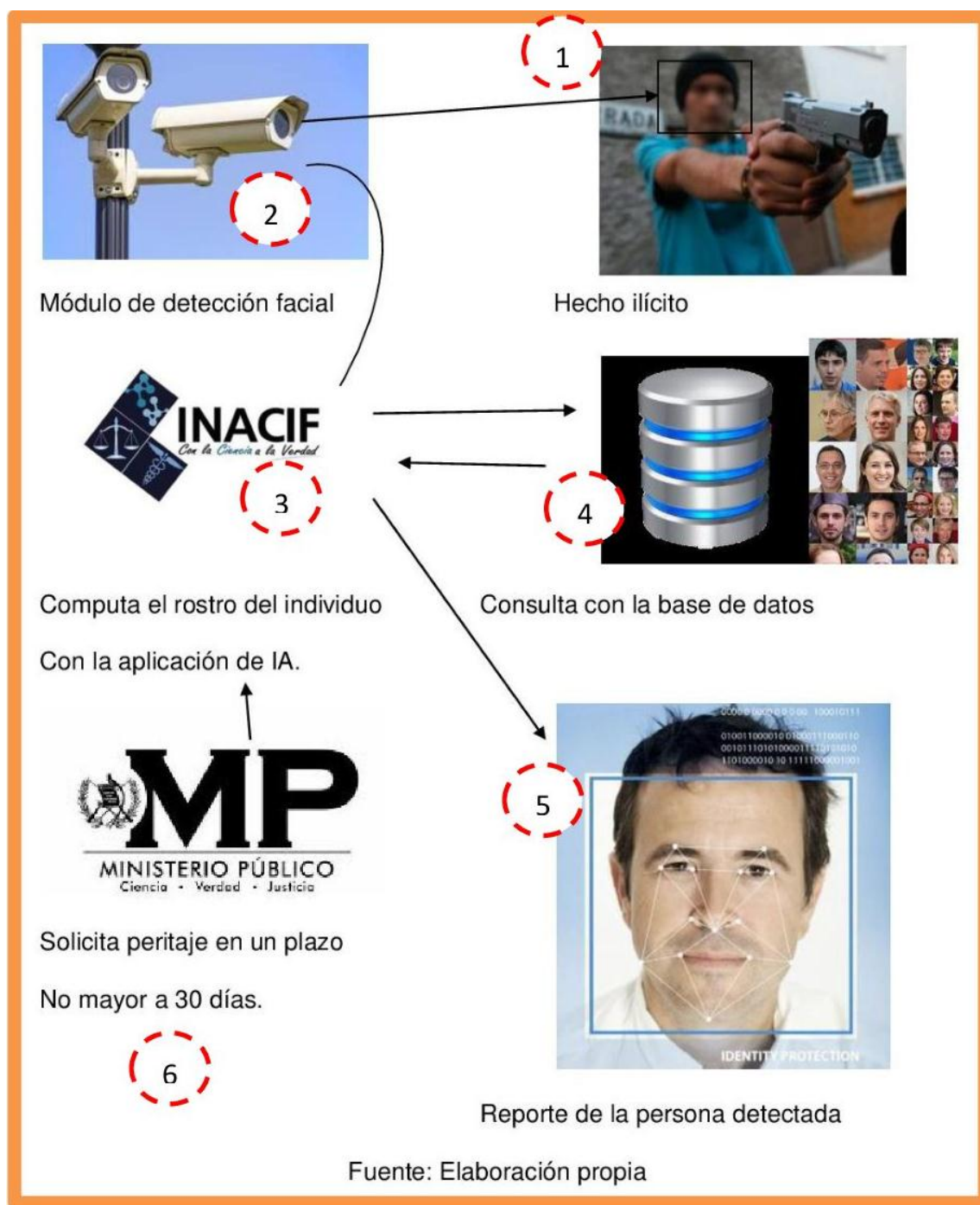


Figura 3

6.3.9 Adquisición y pre procesamiento

La correcta identificación de las personas requiere de un correcto proceso en el cual primeramente se adquiere la imagen mediante la cámara del dispositivo y posteriormente se realiza un pre procesamiento para que la imagen mejore en su resolución, con la finalidad de tener una correcta extracción de características faciales, como se muestra en el diagrama de flujo en la figura, consiste en la captura de la imagen facial de una persona para lo cual el sistema captura una imagen mediante el uso de la cámara para la adquisición de la misma, y es indispensable la utilización de la aplicación adecuada para el uso de la cámara conectada al sistema.

Los pasos a seguir para la detección del rostro son los siguientes:

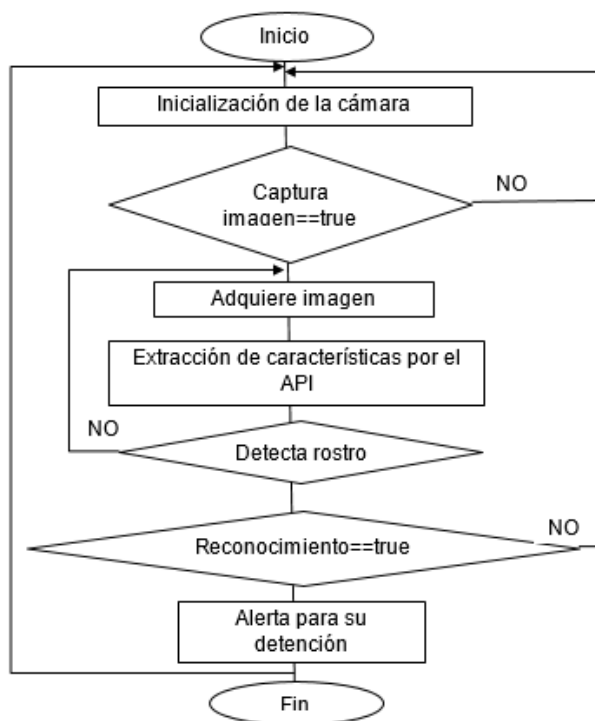


Figura 4. Pasos de detección de rostro
Fuente: Cáceres E.

A. “El primer paso es establecer una conexión entre la cámara de vigilancia y la aplicación de reconocimiento facial, de forma correcta, permitiendo extraer la imagen por medio de un dispositivo no muy sofisticado si no uno promedio que pueda contar exclusivamente con Android 6.0 (Sistema Operativo de teléfonos móviles, por lo general de pantalla táctil) en adelante, mediante este se extraerán las características faciales por medio del uso del Face API (Application Program Interface) de Microsoft para el reconocimiento del rostro de las personas que han pasado por el sistema de reconocimiento”.⁸⁶

B. Envío de la información.

Una vez adquirido la imagen este es enviado por la nube, para lo cual será necesario que el dispositivo móvil esté conectado a internet mediante plan de datos o de preferible un modem LTE (Long Term Evolution (Evolución a Largo Plazo)).

“La información es receptada en la nube por Cloud computing Azure y por la BD (Base de Datos) de la policía. En este caso se utilizará un servidor local con Xampp, que es la encargada de realizar el procesamiento de manera centralizada gracias a que se crea un puente virtual por medio de una dirección IP que es establecida para el ordenador y el celular, haciendo uso del software seleccionado para la extracción de imágenes

⁸⁶ Cáceres M. Erwin, **Aplicación móvil de reconocimiento facial en personas con antecedentes de abuso sexual en la provincia de Andahuaylas**, Aprurimac, Perú - 2018. Tesis para optar el título profesional de ingeniero de sistemas, pág. 70

faciales de las personas que pasen por este sistema de identificación y reconocimiento”.⁸⁷

En este modelo se utiliza la plataforma de servicios web que se desarrolló en el capítulo tres del presente trabajo, el cual es bastante efectivo debido a que las cámaras instaladas en lugares específicos no pueden movilizarse, pero el uso de teléfonos y tabletas ayudaran a los agentes a obtener la información en cuestión de segundos, por la facilidad de su transporte.

C. Extracción de características (Procesamiento principal)

“Con la información disponible en el computador central con relación a los rostros almacenados por carpetas se procede con un análisis de los mismos haciendo uso de las funciones de Face API (Application Program Interface) proporcionadas por Microsoft, para poder extraer las características de la imagen para su reconocimiento, internamente realiza procesos importantes como lo son: Primero utilizar el servicio Face API (Application Program Interface) a través de su biblioteca de clientes .NET (Son nombres de dominio populares y son usados por empresas de todo el mundo para llevar sus compañías a internet) La aplicación detecta caras en una imagen, dibuja un marco alrededor de cada cara y muestra una descripción de la cara en la barra de estado”.⁸⁸

⁸⁷ Ibid pág. 4.

⁸⁸ Ibid pág. 5.

Esta dinámica es muy parecida a la utilizada por la policía municipal de tránsito en el Municipio de Guatemala del Departamento de Guatemala, quienes por medio de una Tablet rastrean los números de placa de los vehículos, para detectar si estos poseen multas sin pagar o si el vehículo ha sido denunciado como robado, con lo cual se han obtenido buenos resultados en poco tiempo.

Uno de los más conocidos es la Plataforma Cognitive Services. “Para lo cual se necesitó una clave de suscripción para ejecutar el algoritmo de inteligencia artificial. Las claves de suscripción de prueba gratuitas se encuentran de Cognitive Services (es un sistema para administrar todo tipo de aplicaciones tecnológicas, para incorporar la capacidad de ver, escuchar, hablar, buscar, comprender y acelerar la toma de decisiones, es proporcionado por Microsoft) .Las características principales son enmarcadas por puntos para hacer referencia de la cara que son una serie de puntos detallados en una cara; Por lo general, los puntos de los componentes faciales como las pupilas, el canto o la nariz”⁸⁹.

Los puntos de referencia de caras son atributos opcionales que pueden analizarse durante la detección de caras. “Puede pasar 'verdadero' como un valor booleano al parámetro de consulta return Face Landmarks (Sistema que detecta rostros dentro de imágenes, detectando el contorno del rostro entre otras características) al llamar a Face-Detect (Detector de Rostros), o usar el parámetro opcional return Face Landmarks para el método Detect Async (es utilizado en el lenguaje de programación C# y Visual Basic para detectar características como rostros en este caso) de la clase

⁸⁹ Ibid pág. 5.

Face Service Client (Es un sistema que sirve para detectar el rostro de una persona específica, comúnmente utilizado en compañías para proveer seguridad en accesos a bancos u oficinas) para incluir los puntos de referencia de la cara en los resultados de la detección⁹⁰.

Por defecto, hay 27 puntos de referencia predefinidos. La siguiente figura muestra cómo se definen los 27 puntos:

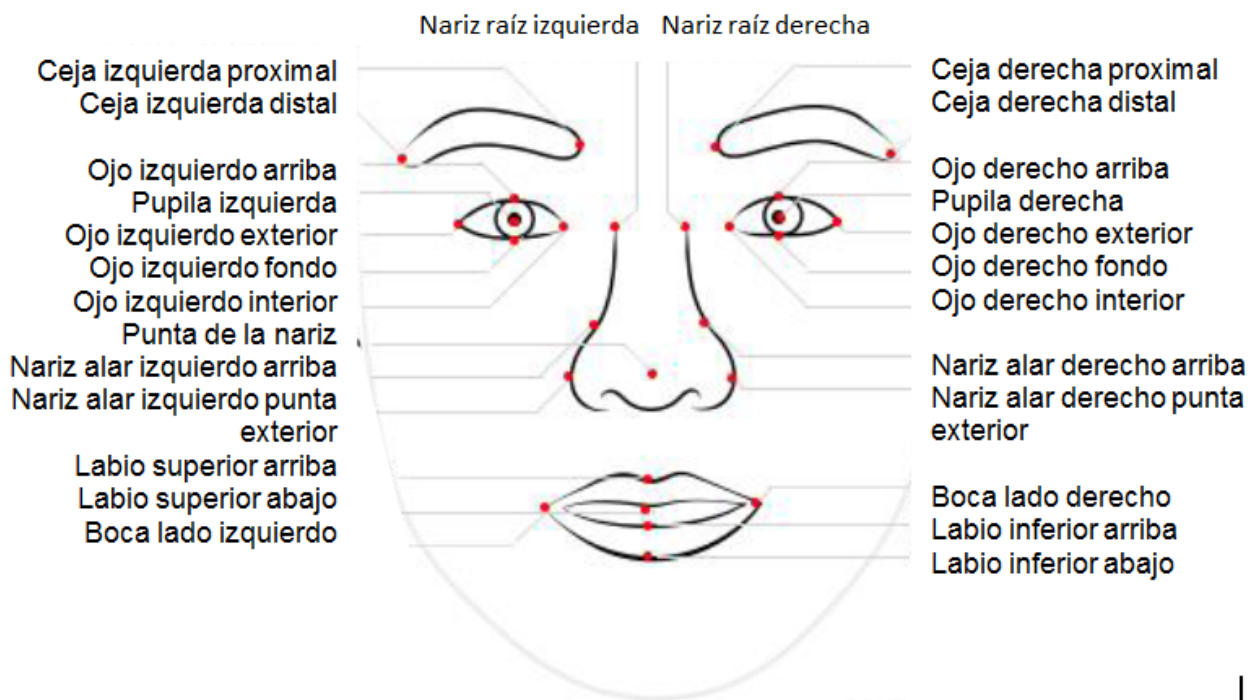


Figura 5. Puntos de referencia

Fuente: (Ggailey, 2017).

⁹⁰Ibid pág. 5.

BIBLIOGRAFÍA

- Álvarez M. **Al Juzgado de Instrucción 28 de Madrid para Diligencias Previas**, Madrid, 2018
- Anil J. **“Solo los Gobiernos pueden evitar el abuso del reconocimiento facial o de las huellas digitales”** EL PAIS, Estados Unidos, 2 de octubre de 2018.
- Blnetskaya M. **Reconocimiento Facial En El Ámbito Forense**, Universidad Autónoma De Madrid, Proyecto Fin De Carrera, Ingeniería De Telecomunicación, Septiembre 2013.
- Cáceres M. Erwin, **Aplicación móvil de reconocimiento facial en personas con antecedentes de abuso sexual en la provincia de Andahuaylas**, Aprurimac, Perú - 2018
- Centro de Investigaciones Internacionales en Derechos Humanos (CIIDH), **Violencia y seguridad en Guatemala, un informe de derechos humanos**, El Observador. Análisis Alternativo sobre Política y Economía, Noviembre de 2014, p. 235, 236.
- Cesión de datos personales para la investigación penal Una propuesta para su inmediata inclusión en la Ley de Enjuiciamiento Criminal (LA LEY 1/1882)** Julio PÉREZ GIL, Universidad de Burgos Diario La Ley, Nº 7401, Sección Doctrina, 13 de Mayo 2010, Año XXXI, Editorial LA LEY.
- Caferata N. José, **La prueba en el proceso penal**, Buenos Aires, Argentina: Ed. Depalma, 1986.
- Castillo M. Blanca. **Tecnología Biométrica**, Guatemala, 2005, Universidad de San Carlos, tesis de grado, Facultad De Ingeniería, Págs. 30,31
- Dirección De Procesos 24-10-2013, **Informe De Funcionamiento Del Sistema De Identificación Biométrica -SIBIO-(AFIS Y FRS)** renap.gob

González-Cuellar Nicolás, **Proporcionalidad y derechos fundamentales en el proceso penal**, España: Ed. Colex, 1990.

Iudiciun et vita, **Publicación de jurisprudencia latinoamericana sobre derechos humanos, del Instituto Interamericano de Derechos Humanos**, (Publicaciones no. 1, 2, 3 y 4)

Julio Pérez Gil, **Cesión de datos personales para la investigación penal Una propuesta para su inmediata inclusión en la Ley de Enjuiciamiento Criminal** (LA LEY 1/1882) Universidad de Burgos Diario La Ley, Nº 7401, Sección Doctrina, 13 Mayo. 2010, Año XXXI, Editorial LA LEY p. 1,2)

Framarino M. **Lógica de las pruebas en materia criminal**, 2 vols. 4ta. Ed.; Colombia: Ed. Temis S.A., 1988.

Moreno C. Víctor, **La defensa en el proceso penal**, España: Ed. Civitas, 1982.

Pacheco Máximo, **Los derechos humanos**, documentos básicos, Santiago, Chile: Ed. Jurídica de Chile, 1987.

Valvert Jorge. **Métodos Y Técnicas De Reconocimiento De Rostros En Imágenes Digitales Bidimensionales**, Guatemala, 2006, Universidad de San Carlos, Tesis de grado, facultad de ingeniería.

Yoc J. Wolfredo, **La Identificación Biométrica Y La Importancia De Su Aplicación Al Derecho Registral, Guatemala**, 2015, tesis facultad de ciencias jurídicas y sociales, Universidad de San Carlos de Guatemala.

Legislación

Constitución Política de la República de Guatemala. Asamblea Nacional Constituyente, 1996.

Código Penal. Congreso de la República de Guatemala, Decreto número 17-73, 1973.

Código Procesal Penal. Congreso de la República de Guatemala, Decreto No. 51-92, 1992.

Ley del Organismo Judicial. Congreso de la República de Guatemala, Decreto Número 2-89, 1989.

Ley del Registro Nacional de las Personas de Guatemala, Congreso de la República de Guatemala, Decreto 90-2005

Reglamento General De La Ley Orgánica Del Instituto Nacional De Ciencias Forenses De Guatemala. Acuerdo número 001-2007

Convención Americana de Derechos Humanos, Pacto de San José Costa Rica. 1978.

Convención Sobre Tortura y Tratos o Penas Cruelles, Inhumanos y Degradantes, Organización de las Naciones Unidas, 1984.