EL RECONOCIMIENTO FACIAL PARA LA PREVENCIÓN DEL DELITO EN AGLOMERACIONES Y SU RELACION CON LOS DDHH

Presentado por:

LAURA JULIETH SILVA MÁRQUEZ

Código: U2601341

Tutor Temático:

JORGE ROMERO CLAVIJO, MSc, CPP

Tutor Metodológico:

JORGE ROMERO CLAVIJO, CPP

FACULTAD DE RELACIONES INTERNACIONALES, ESTRATEGIA Y SEGURIDAD

ESPECIALIZACIÓN EN ADMINISTRACIÓN DE LA SEGURIDAD

BOGOTA D.C.

2020

Resumen

El presente ensayo analiza la confrontación que tiene la implementación de nuevas tecnologías en este caso el sistema de reconocimiento facial versus la posible vulneración de los derechos humanos por la inadecuada manipulación del mismo. En este orden de ideas se mencionan los casos exitosos que ha tenido alrededor del mundo, el apoyo que genera esta herramienta para la prevención del delito en lugares donde se genera alta aglomeración, dando a conocer cada uno de los procesos que conlleva a la detección del individuo con el fin de garantizar la seguridad, el control y la supervisión de la población que se encuentra en estos escenarios. Se define que la evolución de la tecnología es más avanzada que la normatividad, encontrando así una falencia considerable en su implementación, por lo que se identifican los derechos humanos que podrían ser vulnerados de acuerdo a las características del sistema y finalmente se proponen algunos controles que deben implementarse para garantizar su respeto y protección por el uso de estos sistemas en Colombia.

Palabras clave: Reconocimiento, Datos, Aglomeración, Prevención, Delito, Detección, Derechos, Sistema.

Abstract

This essay examines the confrontation of the implementation of new technologies such as the facial recognition system versus the possible violation of human rights by the inadequate manipulation of it. In this order of ideas, it mentions the successful cases that he has had around the world, the support generated by this tool for the prevention of crime in places where high agglomeration is generated, publicizing each of the processes that entails the detection of the individual in order to guarantee the protection, control and supervision of the population in these

scenarios. Seen that the evolution of technology is more advanced than the normativity, thus finding a considerable lack in its implementation, thus identifying human rights that could be violated according to the characteristics of the system and finally proposing some controls that must be implemented to ensure their respect and protection for the use of these systems in Colombia.

Key words: Recognition, Data, Agglomeration, Prevention, Crime, Detection, Rights, System.

Introducción

No hace más de cinco años que la tecnología del reconocimiento facial (RF) se veía solo en películas, pero hoy ya hace parte de nuestra cotidianidad. Es fundamental pensar que esta tecnología fue creada hace muchos años, aproximadamente en la década de 1960 y que, gracias a ella, la elaboración de dispositivos de RF ha traído ventajas importantes en la prevención y control del delito, así mismo ha fortalecido la seguridad en todos sus aspectos. El Sistema de Reconocimiento Facial, de ahora en adelante SRF, para el presente trabajo se define como un conjunto de procesos ordenados que interactúan entre sí con el fin de identificar personas como propósito determinado. Aun así, su implementación no solo trae cosas buenas, por lo que se debe evaluar cada uno de los procesos para evitar vulnerar los derechos humanos (DDHH). Por esta razón el objetivo general de este ensayo es analizar el uso de sistemas de reconocimiento facial para la prevención del delito en espacios de alta aglomeración y su relación con los derechos humanos en Colombia.

La creación de la tableta RAND (tableta digitalizadora) fue uno de los pasos significativos que orientó el desarrollo de estos sistemas en diversos lugares del mundo, los cuales han sido

utilizados para la identificación eficaz de individuos en lugares donde se genera alta aglomeración. Cabe resaltar que el SRF ha mejorado al pasar los años, ya que los procesadores que se utilizan han ido mejorando su capacidad sustancialmente:

> Respecto a la evolución que ha tenido el sistema de reconocimiento facial en diversos países, es importante resaltar uno de los eventos representativos que inició esta gran historia, muchos dirían que el padre del reconocimiento facial fue Woodrow Wilson Bledsoe. en la década de 1960, Bledsoe desarrolló un sistema que podía clasificar fotos de rostros a mano usando lo que se conoce como una tableta RAND, un dispositivo que las personas podían usar para ingresar coordenadas horizontales y verticales en una cuadrícula usando un lápiz que emitía pulsos electromagnéticos. El sistema podría usarse para registrar manualmente las ubicaciones de coordenadas de varias características faciales, incluidos los ojos, la nariz, la línea del cabello y la boca. Estas métricas podrían entonces insertarse en una base de datos. Luego, cuando el sistema recibió una nueva fotografía de un individuo, pudo recuperar la imagen de la base de datos que más se parecía a ese individuo. (SPOT, 2019, p.1)

El reconocimiento facial ha tenido una transformación considerable gracias al desarrollo tecnológico en la última década, pero es necesario tener en cuenta que este mismo grado de evolución no se consideró en el marco normativo, por tal motivo se define como segundo objetivo específico, el analizar la afectación de los derechos humanos por el uso de reconocimiento facial en la prevención del delito con el fin de encontrar falencias en la vulneración de los mismos, teniendo en cuenta la confrontación entre el derecho a la seguridad y el derecho a la privacidad de las personas.

La implementación de estos SRF, es útil en escenarios como centros comerciales, bibliotecas, cines, sistemas de transporte masivo, aeropuertos, escenarios deportivos y de entretenimiento entre otros, donde se requiera el control e identificación de las personas por la aglomeración de las mismas. Una aglomeración consiste en la concentración de gran cantidad de personas en un espacio reducido haciendo más difícil garantizar la seguridad, el control y su supervisión.

Durante el primer semestre de 2019 se registraron 75.483 hurtos en la capital colombiana, lo que representa un incremento del 16,27% (10.564 casos) en comparación con el mismo periodo de tiempo de 2018 (El Espectador, 2019, p.1). Una de las recomendaciones que aparece en el artículo citado anteriormente es evitar estar en zonas donde se genera alta aglomeración, aunque estos delitos se vean disminuidos por el uso de la videovigilancia.

Cabe resaltar que la videovigilancia no consiste solo en la instalación de cámaras, estas también están obligadas a venir acompañadas de manuales de operaciones y protocolos para su correcto funcionamiento; estos deben ser enfocados de acuerdo al lugar donde se desea instalar, la normatividad legal del país y la finalidad del mismo.

Estos SRF no buscan eliminar en su totalidad el delito, su principal objetivo es su prevención por medio del efecto disuasivo que representa, ya que los delincuentes al percatarse que el área cuenta con videovigilancia saben que su identificación es más sencilla sin necesidad de tener la intervención física por parte del personal de seguridad, lo que ayuda sin duda a disminuir las potenciales amenazas. De aquí, el tercer objetivo específico de este ensayo, el cual consiste en caracterizar los sistemas de reconocimiento facial como herramienta para la identificación de personas.

Pese a que la videovigilancia es una herramienta de control de aglomeraciones y contribuye a la disminución de los delitos, puede verse frenada por la coexistencia del derecho a la privacidad y otros derechos relacionados con el manejo de los datos personales, por lo que se debe informar siempre a las personas afectadas por medio de señalizaciones, en especial si se da el caso que las imágenes puedan ser usadas. Por este motivo el último objetivo específico es determinar algunas medidas de control necesarias para la protección de los derechos humanos (DDHH) en el uso de reconocimiento facial en la prevención del delito.

Desarrollo

Casos de éxito del uso de sistemas de reconocimiento facial en el mundo.

Con la implementación de estos SRF se cuenta con numerosas ventajas, los cuales serían esenciales en diferentes escenarios donde se produce alta aglomeración de público, ya que controlando este sistema se podría aprovechar como herramienta para la prevención del delito, de igual manera realizar control y vigilancia a establecimientos públicos y privados para evitar eventos desafortunados o hasta la misma identificación de comportamiento sospechoso del personal que se encuentre en estos lugares. Una de las ventajas más importantes que tiene el SRF es poder detectar sin tener contacto con ninguna persona. El poder detectar al personal desde distancia hace que sea una herramienta estratégica para los procesos de control de acceso en general o en aquellos lugares donde es difícil para la seguridad hacer presencia.

Es importante destacar las experiencias alrededor del mundo con el uso de SRF con el fin de conocer cada uno de los escenarios en el momento de su implementación, pudiendo identificar y analizar tanto los pros como los contras que en su momento generaron.

En Estados Unidos se han implementado sistemas de reconocimiento facial en diversos escenarios como medida de prevención del delito, siendo de gran apoyo para las investigaciones criminales. En el artículo de Miguel Distefano, (2019) publicado por LA NACION indica que “el propio FBI lleva un registro digital de criminales en 16 estados, y las bases de datos tienen el registro facial de la mitad de la población adulta” (p.1). De acuerdo con lo anterior, se deduce que es fundamental contar con una base de datos consolidada de la población, ya que con esta información se genera un margen de error mínimo, siendo así uno de los controles relevantes para el manejo de este sistema.

En Estados Unidos no solo utilizan este SRF para evitar el crimen en espacios públicos y privados, sino que también se están empezando a “incorporar en escuelas, para evitar las masacres tristemente recurrentes en este país” (Miguel Distefano,2019, p.1). La estrategia de implementar SRF en las escuelas tiene como propósito fortalecer los ambientes vulnerables teniendo como fin la identificación eficaz del individuo para evitar o prevenir estos eventos desafortunados.

El artículo citado anteriormente también indica que en Londres se ha elegido el barrio londinense de Romford para una prueba piloto, donde por parte de la policía metropolitana, se produjeron varios arrestos de personas identificadas como autoras de hechos violentos. De manera diferente, en Gales una de las pruebas que se realizaron fue dirigida a escenarios en los cuales se genera alta aglomeración de personas, usando esta tecnología en un partido de fútbol (la final de la Champions League) con un 92% de falsos positivos. Esto pudo suceder porque no se contó con los controles necesarios para la detección e identificación pertinente del individuo, debido a que no se encontraba almacenada correctamente la información en la base de datos. Luego de presentarse la inconformidad del 92% de falsos positivos en el partido de futbol, la policía de Gales

del Sur, quienes cuentan con la misma tecnología de Londres “realizó pruebas más controladas, donde el software pudo identificar a un 81% de las personas” (Miguel Distefano, 2019, p.1).

En China, siendo uno de los países con mayor población pues cuenta con 1.400 millones de habitantes, y por lo tanto uno de los más difíciles de manejar, es una de las naciones más controladas del mundo; la mayoría de sus ciudades cuentan con videovigilancia de manera que se podría decir que se encuentran monitoreados en cada esquina. La innovación en SRF de China va más allá de instalar solo cámaras de videovigilancia en el espacio público: el año pasado la policía de Zhengzhou se había equipado con gafas de sol inteligentes, que utilizan software de reconocimiento facial para poder detectar sospechosos, de manera que en el sur del país se logró detener a un fugitivo de 31 años de edad que pudo ser detectado en un concierto al que asistieron 60 mil personas (Miguel Distefano, 2019, pág. 1).

En Colombia en 2015 empezó la implementación de SRF en diversas ciudades generando así experiencias tecnológicas de innovación. Siendo Medellín una de las primeras ciudades en implementar este sistema en uno de los escenarios donde se genera alta aglomeración de público, como es el estadio Atanasio Girardot de esa ciudad, donde se establecieron cámaras en 36 sitios con el propósito de mantener bajo control los hinchas durante los eventos deportivos. Son 68 cámaras de las cuales 50 son permanentes y 18 para búsqueda forense que detectan incidentes en las graderías. (PORTAFOLIO, 2018 p.1) Es de gran apoyo la implementación de SRF en estos ambientes, ya que su función no solo abarca el proceso de vigilancia, sino que también comprende la detección de individuos para evitar incidentes en las gradas. Cabe destacar la diferencia entre la videovigilancia que solo monitorea la escena, mientras la detección del individuo a su vez realiza un análisis automático haciendo seguimiento e identificando de la persona, entre otras funciones.

No solo se realizó la implementación de estos sistemas en Medellín, también en Bogotá, donde se implementaron las primeras cámaras de reconocimiento facial en las estaciones de Transmilenio, algunas que se encuentran en el centro de Bogotá, una de ellas en la estación de la Jiménez, ubicada en la Av. Caracas entre Calles 11 y 13 en la localidad Santa Fe y Los Mártires. El plan del Distrito (Distrito es utilizado en Colombia para referirse a las entidades territoriales de segundo nivel), es continuar instalando las cámaras en las estaciones más concurridas y también en buses articulados, estaciones y en diferentes zonas de la capital (Canalrcn.com, 2015).

Por otro lado, la policía de la ciudad de Cúcuta, también implementó de forma exitosa sistemas de cámaras de vigilancia en diversos escenarios públicos con el apoyo de la Alcaldía del Municipio, según se pudo establecer esta ciudad contaba en el primer semestre de 2015 con 53 cámaras de videovigilancia instaladas en diferentes lugares públicos, las cuales tienen dentro de sus características técnicas, el poseer un lente con alta definición la cual proyecta los rayos de luz coincidiendo el foco con el sensor de la cámara para tener una imagen nítida con capacidad de giro vertical y horizontal de 360 por 180, con visualización y aproximación de 200 metros, capacidad de grabación y almacenamiento de dos (2) meses, aunque no cuenta con sistema de grabación de audio ni sistema de reconocimiento facial. Estas cámaras de videovigilancia policial fueron instaladas en sitios público con el fin de ser un apoyo para la seguridad de los ciudadanos, quienes fueron críticos al realizar esta implementación realizando un debate referente a la vulneración de los derechos a la privacidad, a la intimidad, a la imagen, manipulación de información, entre otros. (Osorio, 2016, p.73)

Analizando cada uno de los casos exitosos mencionados, es evidente que la instalación de SRF en los escenarios públicos, lo constituyen como una herramienta de respaldo para combatir y enfrentar al delito por medio de la tecnología, de manera eficiente y eficaz dando resultados de

efectividad. De acuerdo con los resultados positivos que genera cada uno de los casos exitosos mencionados, pudiendo ser estos tanto cualitativos como cuantitativos en Colombia, se puede concluir que está tecnología genera un apoyo considerable en la detección e identificación de delincuentes es escenarios de alta aglomeración.

La afectación de los derechos humanos por el uso de reconocimiento facial en la prevención del delito.

Probablemente la implementación de estos SRF trae diversos perjuicios asociados a la vulneración de los DDHH, por lo que a continuación se trata de enumerar cada uno de los que podrían ser afectados por la toma de información por medio de imágenes.

Derecho a la privacidad: Por medio de esta tecnología se presentan diversas vulneraciones al derecho a la privacidad, ya que la información que manejan tanto empresas privadas como públicas la pueden utilizar para su propia conveniencia. El uso de esta tecnología potencia el manejo y el tratamiento de datos personales, lo que conlleva un peligro para la esfera privada de los individuos, y por ello es necesario que los responsables del tratamiento de datos, así como los ciudadanos tenga interés en construir políticas que resguarden la privacidad y los datos personales de los posibles afectados. (Chacón, Ivannia, 2019, p.71) Dentro del derecho a la privacidad también encontramos la inviolabilidad del domicilio, la imagen, el honor, información personal entre otros, todos considerados derechos fundamentales.

Las cámaras de videovigilancia, aunque se encuentren en los espacios públicos pueden vulnerar la privacidad del individuo ya que evidencia las conductas particulares del individuo y éstas pueden ser capturadas, almacenadas y difundidas. Chacón (2019), afirma que “con la videovigilancia masiva e indiscriminada, los ciudadanos que transitan por los espacios vigilados

no tienen la alternativa o determinación de escoger ser o no vigilados, y consecuencialmente decidir el almacenamiento de sus datos personales" (p.76).

Esta información recolectada por este sistema genera una afectación de alto impacto a la privacidad del ser humano, ya que se capturan los comportamientos de cada persona relacionados con su vida íntima como lo es la relaciones entre parejas del mismo sexo, su forma de vestir, los gustos, entre otros; por eso la información almacenada en estos SRF no puede ser de "acceso libre" al público, ya que son datos personales y pueden ser de carácter sensible para cada persona.

> Por tal motivo, la Defensoría del Pueblo en Colombia apoyó una demanda sobre cómo la definición de privacidad incluida en el Código de Policía de Colombia, afecta la intimidad, y dijo: "Ese apartado restringe el derecho a la intimidad al condicionar su ejercicio a los espacios privados, con lo cual desconoce que este derecho comprende una esfera amplia de protección y su ejercicio puede realizarse en distintos ámbitos". Otro concepto es de la organización Privacy International, Organización no gubernamental (ONG) dedicada a la defensa del derecho a la intimidad a nivel internacional, que consideró que: Analizadas desde marcos jurídicos internacionales, las normas demandadas son potencialmente incompatibles con los principios de derechos humanos internacionalmente reconocidos y no ofrecen suficiente salvaguarda de los derechos de los ciudadanos. (Justicia, 2020 p.1) Se concluye que el personal responsable de la manipulación y almacenamiento los datos personales adquiridos mediante el sistema, deben contar con mecanismos seguros para la protección de la información con el fin de que no sean difundidos o publicados.

El derecho a la imagen*:* Este derecho es fundamental, y por consiguiente puede ser vulnerado por medio del proceso de captura de imágenes la cual recolecta el perfil externo más

característico de la persona. Estas imágenes recolectadas se convierten en el dato personal y así es posible hacer la identificación e individualización del sujeto. Por este motivo, se debe contar con el consentimiento de la persona para la captura de imágenes, almacenamiento, reproducción y difusión así está imagen se hubiera capturado en lugares públicos. “El derecho a la propia imagen presenta también una faceta de contenido propiamente económico, derivado de la explotación del nombre, voz o imagen de una persona con fines publicitarios, comerciales o análogos” (Puyol, 2015, p.1).

Derecho a la protección de datos personales: Se puede generar una vulneración en el manejo de los datos personales con el uso de los SRF ya que su manipulación es un proceso complejo, ya que se debe contar con un mecanismo de protección para que la información no salga de contexto y ésta no sea utilizada para fines comerciales fines comerciales, de marketing y publicidad., ya que se pueden identificar comportamientos de las personas, que permitan identificar los gustos que tiene frente a algún tema específico, como por ejemplo, su forma de vestir, los lugares que frecuenta, la comida habitual de cada persona, entre otras. El derecho a la protección de datos establece límites y condiciones para el responsable o encargado de los datos, quien hace uso de los mismos, garantizando que la recolección y el uso sean acordes al fin. Debe entenderse que la protección al tratamiento de los datos personales no solo es frente a los poderes públicos sino también frente a la actuación de los particulares. (Chacón, Ivannia, 2019 p.91)

Caracterización de los SRF como herramienta para la identificación de personas.

Es importante resaltar que los SRF cuentan en su operación con cinco fases: en la primera se captura el rostro de la persona por medio del dispositivo, en una segunda se hace el preproceso de la imagen y se obtiene la información biométrica, la tercera fase es la más importante y consiste

en la extracción de las características faciales, en la cuarta se hace la comprobación de acuerdo a las bases de datos almacenados y finalmente se ejecuta la toma de decisiones de acuerdo al porcentaje de similitud obtenido. Este es el proceso que realiza el sistema de reconocimiento facial al escanear el rostro de un individuo, pero para cumplir con este objetivo se debe contar con un almacenamiento donde se cuente con la información de las personas, definida como una base de datos de las características de cada una. Cabe resaltar que para que el proceso de detección sea eficaz y eficiente, la base de datos de la población definida para identificar debe estar muy bien consolidada y así mismo los lugares donde se generan altas aglomeraciones, entre mejor este consolidada, menor será el porcentaje de error del sistema.

El reconocimiento facial en el trascurso de los años ha evolucionado a pasos gigantescos, se puede decir que estos sistemas ya cuentan con metodologías o técnicas para su manipulación que favorece en la medida de minimizar el margen de error en la lectura del rostro. A continuación, se enumeran de acuerdo con su composición y se definirá los elementos característicos que las componen y su relación con los derechos humanos mencionados en el capítulo anterior.

Una de las metodologías más interesantes son las medidas antropométricas las cuales menciona Briones, (2020) “se encargan de representar las medidas y proporciones del cuerpo humano, en esta ocasión se da importancia al rostro como objetivo principal a medir” (p.9). De acuerdo con lo anterior la antropometría se encarga de definir las líneas mediante la puntualización de las líneas que definen el rostro en dos partes simétrica.

Dentro de este contexto de medidas antropométricas se encuentra también la somatometría que se encarga únicamente de los puntos que están en la cara; la información proporcionada por cada uno de ellos es distancia y ángulos básicos en el posicionamiento representativo en el plano

de la cara desde su vista frontal. Mientras la distancia indica el ancho y el espacio que existen entre los elementos faciales, el ángulo ayuda a realizar correcciones de lectura, en rostros cuya representación frontal no es tan exacta. (Briones, 2020, p.10) Para obtener los resultados de la detección se unen estos puntos convirtiéndose en coordenadas, los cuales se llaman vectores de características y así se establece un valor que es un dato esencial para identificar las distintas personas que se encuentran en el sistema. El proceso inicia con la adquisición de la imagen y continua con la detección de rostros que aparecen en la imagen, siguiendo con posibles extracciones de características faciales y finaliza con el reconocimiento, como ya se ha dicho.

En general, un SRF está "segmentado en tres partes, según se menciona a continuación: Módulo de Almacenamiento, Módulo de Procesamiento, y Módulo de Presentación" (Gárate, 2020, p.18). Se explica cada uno de los módulos, iniciando por el módulo de almacenamiento donde se encuentra la base de datos, el segundo módulo de procesamiento que se conecta con el módulo de almacenamiento, es donde se realiza el reconocimiento facial con el aprendizaje automático, aquí se presenta la verificación en el procesador de imágenes dentro del sistema, y finalmente, el tercer módulo o de presentación, que muestra los resultados anteriormente alcanzados por los anteriores módulos (Briones, 2020).

Dentro del módulo de almacenamiento se encuentra la captación de las imágenes, allí se recolectan los comportamientos de las personas, esto relacionado a el derecho a la privacidad. En le módulo de procesamiento, se enlaza con el derecho a imagen ya que se vincula al proceso anterior pues se genera así la manipulación de la información personal. El módulo de presentación se relaciona con el derecho a la protección de los datos personales, ya que en éste se genera el resultado de la información obtenida y es donde están disponibles los datos de la persona identificada.

Sobre las características de las cámaras en particular para los sitios de alta aglomeración éstas deben contar con detalles técnicos para su óptimo funcionamiento tal como lo afirma Paredes, (2018):

> Las imágenes de los rostros tanto de las fotos como de las capturas de las cámaras deben estar en escala de grises, todas deben ser del mismo tamaño, y tener el mismo alto y ancho (forma cuadrada). El lado de la foto debe tener una longitud potencia. El sistema está construido en el lenguaje de programación Visual, y utiliza una base de datos. Se utiliza el archivo entrenado, para la detección facial. Se utiliza el algoritmo de reconocimiento para el entrenamiento y reconocimiento facial. (p.4)

Estas cámaras de seguridad deben garantizar un procesamiento eficaz de la información capturada, no importando la cantidad de personas que puedan estar pasando por el sistema al mismo tiempo, incluyendo rostros inclinados hacia alguna dirección e incluso aquellos ocultos parcialmente por accesorios como pueden ser gafas, sombreros, bufandas hasta tapabocas. Estos SRF deben estar ubicados estratégicamente con el fin de capturar la mayor cantidad de imágenes posibles, de igual manera tienen que ser manipuladas por personal calificado para la detección temprana de incidentes, búsqueda manual de sospechosos y almacenamiento de videos grabados para futuras detecciones descartando entre más o menos 5 millones de rostros en solo 3 segundos.

Medidas de control para la protección de los DDHH en el uso de reconocimiento facial en la prevención del delito.

En Colombia, Francisco Bernate, abogado experto en temas penales, recalcó que las cámaras de reconocimiento facial no vulneran el derecho a la intimidad, en la medida que sean ubicadas en espacios como en la vía pública, en un centro comercial, en la plaza pública, pero en

los casos en que se ubiquen en espacios como al interior de una vivienda o apuntando a una vivienda o una oficina, si se podría vulnerar la intimidad. (LA FM, 2019, p.1) Teniendo en cuenta lo citado por el abogado, es esencial que las autoridades competentes realicen seguimiento a las empresas o entes responsables de la instalación de estas cámaras de videovigilancia, donde les recomienden puntos específicos para así garantizar que sean ubicadas en lugares estratégicos de la vía pública. De igual manera en los establecimientos públicos donde tengan la necesidad de utilizar esta operación, con el propósito de identificar de una manera eficaz a delincuentes en estos escenarios donde genera una alta aglomeración de personas.

En general, para la implementación de los SRF, las empresas responsables de su implementación deben identificar o definir la finalidad de este sistema en su establecimiento, el cual debe tener como propósito la prevención del delito. Estas empresas responsables de la manipulación de los SRF están obligadas a contar con procedimientos estrictos, medidas técnicas y administrativas entre otras, para garantizar que los datos personales capturados se encuentren seguros y así evitar la pérdida de la información o uso inadecuado de ella, manteniendo la integridad de la información y respetando los derechos del individuo en cada uno de los procesos desde el momento que se realizó la recolección de la información hasta su disposición final.

De acuerdo a lo anterior se propone a partir del derecho que puede ser vulnerado, considerando las características que tiene el sistema de reconocimiento facial, las medidas de control que se deben implementar para evitar vulnerarlo.

Controles para el derecho a la privacidad: El sistema de reconocimiento facial dentro de su funcionamiento puede realizar una captura o grabación constante generando información del personal convertidas en imágenes, esta información almacena aspectos de la personalidad e

identidad de la persona. Si el establecimiento cuenta con la necesidad primordial de ofrecer seguridad a sus visitantes, los encargados o responsables de la manipulación de estos SRF, deben informarle al afectado del tratamiento de sus datos personales, por medio de avisos distintivos, señales y si es necesario anunciarlo por medio de audio, como por ejemplo, que se encuentra en una zona de videovigilancia, con el fin que las personas se encuentren enteradas de las políticas de tratamiento de la información y su finalidad, antes de ingresar a los lugares que pueden ser vigilados y monitoreados. Lo mencionado anteriormente se encuentra explicito decreto 1317 de 2013 “Por el cual se reglamenta parcialmente la Ley 1581 de 2012" por la cual se se expidió el Régimen General de Protección de Datos.

Controles para el derecho a la propia imagen: Una de las posibilidades que tiene el SRF es la captura cualquier tipo de rostros como pueden ser niños (menores de edad), adultos y adultos mayores las cuales se comparan por medio de la extracción de características faciales con la base de datos adquirida.

El responsable o encargado debe contar con procesos estrictos para la captura, manipulación y almacenamiento de las imágenes de terceros la cual se encuentra dentro de la base de datos del sistema. Cabe destacar que las imágenes de menores de edad también son consideradas datos personales por lo tanto el titular responsable del menor debe ser el que autorice el manejo de ellas. De acuerdo a lo establecido en la ley de protección de datos personales mencionado anteriormente, aquellos que están obligados a dar tratamiento a nombre del responsable, deben hacerlo conforme a los principios que los tutelan, deben proteger las bases de datos donde se cuenten con datos personales y por último resguardar la confidencialidad de los mismos.

Controles para el derecho a la protección de datos personales: El proceso más esencial que tiene el sistema de reconocimiento facial es contar con una base de datos consolidada de la población definida dentro del software del sistema, con el fin de ser comparada con las imágenes adquiridas para la detección del individuo. Es importante destacar que la información debe ser conservada bajo los controles de seguridad que sean necesarios para evitar adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento. En segundo lugar, se debe realizar la actualización oportuna de los datos como lo determina la ley mencionada. Adicionalmente, en tercer lugar, mediante un proceso previamente establecido, tramitar las consultas o reclamos que tengan los titulares de estos datos y, por último, establecer un manual interno donde se encuentren las políticas y cada uno de los procedimientos a seguir para la atención de consultas y reclamos por parte de los titulares. Todo lo anterior con el fin de evitar la vulneración de algún derecho relacionado con la debida protección de sus datos personales.

Conclusiones

El sistema de reconocimiento facial (SRF) es una herramienta de gran utilidad para la prevención del delito, ya que por medio de la base de datos consolidada con que debe contar, se puede detectar al individuo de una manera eficaz y sin necesidad de tener contacto físico con él. Por tal motivo, en cumplimiento al objetivo general de este ensayo, se analizó el uso de SRF y su relación con los derechos humanos para la prevención del delito en espacios de alta aglomeración en Colombia. Cabe señalar que estos sistemas son utilizados para tres enfoques esenciales como lo son la seguridad, el control y el orden público, por tal motivo son primordiales en la seguridad ciudadana.

Se ha cumplido con el primer objetivo específico, ya que se enumeraron algunos casos exitosos de utilización de SRF, valorando las experiencias en diferentes escenarios donde se generaba una alta aglomeración de público, pudiendo identificar ventajas en la reducción del crimen y aplicaciones de la ley, según los procesos implementados por esta nueva tecnología.

Al enumerar los derechos humanos afectados por el uso del reconocimiento facial, se determina que aquellos que pueden ser vulnerados por su implementación, se encuentran explícitos en la Ley 1581 de 2012, se mencionan a continuación: el derecho a la privacidad, el derecho a la propia imagen y por último el derecho a la protección de datos personales, por consiguiente es de gran importancia respetarlos y protegerlos por cuanto se circunscriben o corresponden al círculo más personal e íntimo del ser humano.

Al definir las características de los SRF como herramienta para la identificación de personas, en relación con el derecho a la privacidad y el derecho a la seguridad, cómo fundamentales para el ser humano, se concluye que las organizaciones deben contar con controles estrictos en cada uno de los procesos de implementación de SRF, con el fin que sean empleados esencialmente en la prevención del delito, en mayor medida en aquellos lugares donde se genera alta aglomeración como lo son centros comerciales, aeropuertos, escenarios deportivos y de entretenimiento entre otros, con el objetivo de garantizar la seguridad en estos escenarios.

Finalmente, de acuerdo al cuarto objetivo propuesto se puntualiza que establecer los controles necesarios para la protección de las DDHH en el uso del reconocimiento facial con el fin de prevenir el delito, son obligatorios para los responsables o encargados de manejar los datos personales, esto con el fin de prevenir que esta información sea de acceso público o que los mismos sean utilizados para conveniencia o fines de particulares.

Referencia

Ayuda ley protección datos. (22 de 03 de 2019). Obtenido de https://ayudaleyprotecciondatos.es/2019/03/22/reconocimiento-facial/#Ventajas_e_inconvenientes

Briones, E. (2020). *Universidad espiritu santo.* Obtenido de http://201.159.223.2/bitstream/123456789/3194/1/Sistema%20de%20reconocimiento%20de%20personas%20y%20g%c3%a9neros%20aplicando%20t%c3%a9cnicas%20machine%20learning%20en%20establecimientos%20comerciales%20%281%29.pdf

Canalrcn.com. (16 de 03 de 2015). *Noticias.canalrcn*. Obtenido de https://noticias.canalrcn.com/nacional-bogota/asi-funciona-el-sistema-reconocimiento-facial-se-implementa-transmilenio

Chacón, I. M. (2019). El uso de sistemas de videovigilancia como medida de seguridad y su incidencia en los derechos de vida privada, propia imagen y la proteccion de datos personales. *Repositorio.sibdi.ucr.ac.cr*, 70.

Chacón, Ivannia. (29 de 02 de 2019). *Sistema de bibliotecas,documentacion e informacion.* Obtenido de http://repositorio.sibdi.ucr.ac.cr:8080/jspui/bitstream/123456789/9099/1/44119.pdf

El Espectador. (23 de 06 de 2019). *Nacional*. Obtenido de https://www.elespectador.com/noticias/nacional/en-promedio-cerca-de-1136-personas-son-victimas-de-hurto-cada-dia-en-colombia-articulo-872344

Gárate, A. E. (2020). SISTEMA DE RECONOCIMEINTO FACIAL DE GÈNEROS APLICANDO TÈCNICAS MACHINE. *UNIVERSIDAD DE ESPECIALIDADES ESPÍRITU SANTO*, 18.

GAVIRIA, J. J. (2017). VIDEO VIGILANCIA, LIBERTAD PERSONAL Y DERECHO DE HABEAS DATA:. *repository.eafit.edu.co*, 26. Obtenido de https://repository.eafit.edu.co/bitstream/handle/10784/12328/JuanJos%C3%A9_Casta%C3%B1oGaviria_2017.pdf?sequence=2

Justicia. (20 de 01 de 2020). *El Tiempo*. Obtenido de https://www.eltiempo.com/justicia/cortes/camaras-de-seguridad-violan-derecho-a-la-intimidad-en-colombia-453356

LA FM. (23 de 12 de 2019). *https://www.lafm.com.co*. Obtenido de https://www.lafm.com.co/politica/camaras-de-reconocimiento-facial-la-propuesta-de-seguridad-del-gobierno-que-genera

Miguel Distefano. (25 de 04 de 2019). En qué otros países se usan sistemas de reconocimiento facial. *LA NACION*. Obtenido de https://www.lanacion.com.ar/tecnologia/en-que-otros-paises-se-usan-sistemas-nid2241688

Osorio, E. (1 de 6 de 2016). *Dialnet.unirioja.es.* Obtenido de https://dialnet.unirioja.es/descarga/articulo/6713559.pdf.

Paredes, M. (12 de 07 de 2018). *revista.usanpedro.edu.pe.* Obtenido de https://revista.usanpedro.edu.pe/index.php/CPD/article/view/277

PORTAFOLIO. (18 de 09 de 2018). *Portafolio*. Obtenido de https://www.portafolio.co/negocios/reconocimiento-facial-el-futuro-de-los-aeropuertos-521313

Puyol, J. (03 de 05 de 2015). *CONFILEGAL* . Obtenido de https://confilegal.com/20150503-imagen-como-derecho-personal-y-como-dato-de-caracter-personal/

Sistema de vigilancia biométrico facial para el control delincuencial en la división policial. (1 de 10 de 2018). *revista.usanpedro.edu.pe*, pág. https://revistas.unilibre.edu.co/index.php/academia/article/view/283/223. Obtenido de https://revista.usanpedro.edu.pe/index.php/CPD/article/view/277/266.

SPOT. (18 de 03 de 2019). *Una breve historia del reconocimiento facial*. Obtenido de Medium: https://medium.com/@spot_blog/una-breve-historia-del-reconocimiento-facial-vision-blog-5a76fdfe4865