https://repository.uaeh.edu.mx/revistas/index.php/divulgare/issue/archive

DIVULGARE Boletín Científico de la Escuela Superior de Actopan

Publicación semestral, Vol.9, No. 18 (2022) 52-59

DIVULGARE

ISSN: 2395-8596

Identidad facial. Seguridad contra derecho a la privacidad

Face identity. Security versus the right to privacy

Ricardo Castillo Solano [a]

Abstract:

As sensitive personal data, facial identity implies the study of certain fundamental rights like privacy and private life; There are exceptions so that these can be treated differently, such as national security and criminal investigation. If Mexico opts for its use, the fundamental rights provided for in the Constitution and in the International Treaties to which Mexico is party, must always be pondered.

Keywords:

Facial identity, human rights, privacy, security.

Resumen:

La identidad facial como dato personal sensible implica el estudio a ciertos derechos fundamentales como lo es el de Privacidad y el de vida privada; existen excepciones para que estos puedan tratarse de diferente manera como lo es la seguridad nacional y la investigación criminal. Si México opta por su uso deberá ponderar siempre los derechos fundamentales previstos en la Constitución y en los Tratados Internacionales de los que es parte.

Palabras Clave*:*

Identidad facial, derechos humanos, privacidad, seguridad.

Introducción

La implementación de la tecnología facilita las actividades de las personas humanas, es tarea del Estado apoyarse de los avances de la tecnología para facilitar el acceso a la justicia como derecho fundamental y, en materia penal, para cumplir con los principios del proceso penal acusatorio tales como: esclarecer los hechos, proteger al inocente, procurar que el culpable no quede impune y que los daños causados por el delito se reparen.

Día a día la tecnología cambia nuestras vidas y la facilita, por ello, el Derecho se ha apoyado de la misma para implementarla en la procuración e impartición de justicia, como lo es en el uso de la identidad facial.

En este sentido, es importante determinar los alcances en el uso de la tecnología, así como recordar que, los Tratados Internacionales que México ha ratificado, sobre todo aquellos que promueven la protección de datos personales, el derecho a la privacidad, a la intimidad y a la vida privada.

Su regulación es crucial, para determinar la protección de los derechos fundamentales mencionados y también lo es conocer las excepciones que pueden evitar el uso excesivo de facultades por parte del Estado a efecto de afectar la privacidad; ejemplo de ello, podemos encontrar la procuración e impartición de justicia, en especial la investigación de conductas criminales, ya que las tendencias actuales arrojan usar a la identidad facial como medio para obtener una base de datos de la ciudadanía e identificarlos de manera más rápida y así perseguirles.

De lo anterior, destacamos la necesidad de conocer las tecnologías biométricas y su relación con el reconocimiento facial, así como los usos que puede tener, en la identificación de personas.

La potencialización de los derechos fundamentales en México es importante, por lo que todas las medidas que las Autoridades tomen respecto a la implementación de la tecnología, deben encontrarse apegadas a la protección de derechos humanos y se debe realizar un ejercicio de ponderación de los mismos, cuidando que las personas puedan vivir de acuerdo al libre desarrollo de la personalidad, sin sentirse vigiladas o violentadas en su intimidad.

[a] CE&A Litigio y Solución de Conflictos S. C. https://orcid.org/0000-0002-2975-5533, Email: ricvstlo@gmail.com

Fecha de recepción: 21/03/2022, Fecha de aceptación: 29/03/2022, Fecha de publicación: 05/07/2022

Planteamiento del problema

La comisión de delitos es una enfermedad que agrava a la Sociedad, en ocasiones, encontrar a la persona que cometió un delito es muy complicado por la hora en la que se realizó, por la iluminación, por la capacidad para observar de las personas testigos, entre muchos otros factores.

De la misma manera, es muy fácil que las personas cambien sus "rasgos físicos" con la intención de no ser identificadas fácilmente.

Por ello, ¿la identificación por biométricos puede ser la solución? Si otros países la han adoptado ¿Qué necesita estudiar México para poder aplicarla en la investigación criminal?

¿La investigación criminal está encima de los derechos a la Privacidad y vida privada? ¿La seguridad nacional y la seguridad de las personas para evitar conductas delictivas pueden justificar el uso indiscriminado de identificar a todas y cada una de las y los mexicanos?

Fundamentos del Derecho a la privacidad

Además de las garantías de legalidad y seguridad jurídica con las que cuenta la ciudadanía en México y los derechos humanos que se tutelan y protegen, el artículo 16, párrafo segundo de la Constitución, regula el derecho a la privacidad, pues a la letra dicta: "Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley (Congreso de la Unión, 1917, p.17).

Este derecho es trascendental en México, pues debido al uso cotidiano de la tecnología en nuestra vida, hemos aprendido a funcionar como una sociedad conectada al internet, o mejor dicho, nuestras actividades son llevadas a cabo de manera *online*.

De acuerdo con la Asociación de Internet MX en el 2019, las y los mexicanos pasamos alrededor de 8 horas, con veinte minutos conectados a internet de acuerdo con el 15° estudio elaborado por la misma en el 2019 (Asociación de Internet MX, 2019), y al 17° estudio publicado en el 2020 (Asociación de Internet MX, 2020).

Un estudio reciente elaborado por Branch (2021), refleja que actualmente pasamos cerca de nueve horas con un minuto conectados a internet, por lo que toma especial relevancia lo que hacemos dentro de él y nuestra privacidad en línea.

Del artículo 16, párrafo segundo Constitucional, surge el primer punto de debate, ¿Qué es lo que protege? ¿Qué se entiende por privacidad? ¿Cuáles son los datos privados?

Preguntas que conllevan a relacionar el artículo mencionado con el 7 de nuestra Constitución que, en su apartado A, fracción II, indica: "La información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes" (Congreso de la Unión, 1917).

De donde se desprende que la información respecto a la vida privada será protegida, ampliando el ámbito de protección, respecto al derecho fundamental de privacidad.

Diego García Ricci (2013), menciona que el derecho a la privacidad comprende la protección de datos personales y de la vida privada, lo cual consiste en controlar la información de uno mismo (p. 8).

Además, el derecho a la privacidad comprende:

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

Entonces, de acuerdo a la sociedad en la que hoy vivimos, también podemos incluir en el derecho a la privacidad: las páginas web visitadas en los navegadores; las compras utilizando el comercio electrónico; los mensajes enviados y recibidos; las aplicaciones utilizadas; las videoconferencias; los datos y biométricos que las aplicaciones y dispositivos electrónicos guardan de nosotras y nosotros.

Y aunque esto pase desapercibido, a veces, toda esa información puede utilizarse para fines no establecidos o no consentidos, ya que la ciudadanía desconoce para qué se recaban las huellas digitales o nuestro rostro en los sistemas y las nubes de los dispositivos, mucho menos se leen los avisos de privacidad o los términos y condiciones.

Ahora bien, ¿Cuáles son los datos personales que se protegen mediante el derecho a la privacidad?

De acuerdo a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, (Congreso de la Unión, 2017), dispone, en su artículo 3, fracciones IX y XI:

> *"Datos personales: Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es*

identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información; Datos personales sensibles: Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual." (p. 3).

La mencionada Ley, regula el actuar de las Autoridades, Dependencias, Entidades y Organismos Públicos como Sujetos Obligados, y refiere que, en caso de aplicar alguna excepción, debe estar fundamentada.

El derecho a la privacidad, se encuentra protegido en el plano internacional, mediante los siguientes instrumentos: la Convención Americana de Derechos Humanos en su artículo 11 que dicta:

> *1. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad. 2. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación. 3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.* (Organización de los Estados Americanos, 1969, s.p.)

Por el artículo V de la Declaración Americana de los Derechos y Deberes del Hombre, que dicta: "*Toda persona tiene derecho a la protección de la Ley contra los ataques abusivos a su honra, a su reputación y a su vida privada y familiar".* (Organización de los Estados Americanos, 1948, s.p.)

El artículo 12 de la Declaración Universal de Derechos Humanos refiere: "Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques". (Organización de las Naciones Unidas, 1948, s.p.)

Y el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos dicta: "Derecho a la privacidad y su protección por la ley" (Organización de las Naciones Unidas, 1966, s.p.)

De donde desprendemos que el derecho a la Privacidad se reconoce como derecho humano y por lo tanto alcanza su protección en nivel local e internacional.

Por otra parte, el uso de los datos personales y datos personales sensibles por particulares se encuentra regulado en la Ley Federal de Protección de Datos Personales en Posesión de Particulares, pero como nos referiremos a la procuración de justicia como fines de investigación criminal, no será materia de estudio la ley citada.

Excepciones a la protección de datos personales

Ahora bien, el artículo 16, párrafo segundo de nuestra Constitución, refiere que existirá una excepción al derecho de privacidad: "establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros" (Congreso de la Unión, 1917, p.17)

Por otra parte, el artículo 6, segundo párrafo, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (En adelante Ley General) menciona esos casos de excepción: "razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros". (Congreso de la Unión, 2017, p. 6).

Partiendo de la idea que los derechos no son absolutos, es importante considerar el régimen de excepción a la tutela del derecho de privacidad y saber cuándo un dato personal, protegido por una Autoridad, será transmitido a terceros, así como la finalidad y el propósito; esto debe ser informado a la ciudadanía y un medio eficaz para ello es el aviso de privacidad.

El primer supuesto de excepción reglado, se encuentra previsto en el artículo 80 de la Ley General, que establece:

> *"La obtención y tratamiento de datos personales, en términos de lo que dispone esta Ley, por parte de los sujetos obligados competentes en instancias de seguridad, procuración y administración de justicia, está limitada a aquellos supuestos y categorías de datos que resulten necesarios y proporcionales para el ejercicio de las funciones en materia de seguridad nacional, seguridad pública, o para la prevención o persecución de los delitos. Deberán ser almacenados en las bases de datos establecidas para tal efecto".* (Congreso de la Unión, 2017, p. 26

Lo anterior cobra especial relevancia en nuestro Sistema Jurídico Mexicano, porque establece los procedimientos necesarios para que en un Sistema de Coordinación en materia de información y respecto de los datos personales puedan ser solicitados cuando se demuestre fundada y motivadamente una excepción; esto es, dicha solicitud de transferencia de información puede

hacerse por una instancia de Seguridad Nacional, un Agente del Ministerio Público o Fiscal, una o un Juez o Autoridades Administrativas, cuyo ejercicio sea materialmente jurisdiccional.

Y estableciendo el límite (los datos necesarios y proporcionales en materia de seguridad nacional, seguridad pública, o para prevención o persecución de delitos), pues en un Estado de Derecho, ir más allá de una facultad expresa, constituye un abuso de poder y un ejercicio arbitrario del mismo.

La segunda excepción que contiene la Ley General, está prevista en el artículo 138, que establece:

> *Únicamente el Consejero Jurídico del Gobierno podrá interponer recurso de revisión en materia de seguridad nacional ante la Suprema Corte de Justicia de la Nación, en el caso que las resoluciones del Instituto a los recursos descritos en este Título, puedan poner en peligro la seguridad nacional". (Congreso de la Unión*, 1917, p. 44)

Hablar de Seguridad Nacional, implica una actuación del Consejo de Seguridad Nacional conforme a las facultades que se le otorgan en la Ley General del Sistema de Seguridad Pública, y en la Ley de Seguridad Nacional.

La Ley de Seguridad Nacional, define a la Seguridad Nacional como: Las acciones destinadas de manera inmediata y directa a mantener la integridad, estabilidad y permanencia del Estado Mexicano*". (*Congreso de la Unión, 2005, p. 1)

También determina las amenazas a la Seguridad Nacional*:*

> *a) Actos tendentes a consumar espionaje, sabotaje, terrorismo, rebelión, traición a la patria, genocidio, en contra de los Estados Unidos Mexicanos dentro del territorio nacional; b) Actos de interferencia extranjera en los asuntos nacionales que puedan implicar una afectación al Estado Mexicano; c) Actos que impidan a las autoridades actuar contra la delincuencia organizada; d) Actos tendentes a quebrantar la unidad de las partes integrantes de la Federación, señaladas en el artículo 43 de la Constitución Política de los Estados Unidos Mexicanos; e) Actos tendentes a obstaculizar o bloquear operaciones militares o navales contra la delincuencia organizada; f) Actos en contra de la seguridad de la aviación; g) Actos que atenten en contra del personal diplomático; h) Todo acto tendente a consumar el tráfico ilegal de materiales nucleares, de armas químicas, biológicas y convencionales de destrucción masiva; i) Actos ilícitos en contra de la navegación marítima; j) Todo acto de financiamiento de acciones y organizaciones terroristas; k) Actos tendentes a obstaculizar o bloquear actividades de inteligencia o contrainteligencia; l) Actos tendentes a destruir o inhabilitar la infraestructura de carácter estratégico o indispensable para la provisión de bienes o servicios públicos; m) Actos ilícitos en contra del fisco federal a los que hace referencia el artículo 167 del Código Nacional de Procedimientos Penales*. (Congreso de la Unión, 2005, p. 1-3)

De lo anterior se desprende que en temas de seguridad nacional existen hipótesis que el Estado puede usar con el fin de restringir el derecho a la privacidad y este se encuentra legal y fundado para intervenir en el derecho humano de la ciudadanía.

Además que con fines de seguridad nacional y aduciendo fines legítimos, se pueden solicitar los datos personales y datos personales de la ciudadanía para evitar un acto que atente contra el Estado; luego entonces, es importante ponderar esta excepción siempre a la luz del derecho constitucional y de los Tratados Internacionales ya citados para evitar la injerencia del Estado en la vida privada (aún y cuando se justifique la violación al derecho humano de Privacidad por fines de seguridad nacional)

Otro caso de excepción: la salubridad. El artículo 73 fracción XVI de la Constitución, refiere que estará a cargo del Consejo de Salubridad General dictar las medidas en salubridad, esto visible en la Ley General de Salud, en especial en los artículos 181 y 182, las facultades del Consejo para dictar la acción extraordinaria en materia de salubridad general. (Congreso de la Unión, 1984)

Derivado de la pandemia ocasionada por el virus SarS-Cov2 vivimos esta excepción, pero no en materia de violación al derecho a la Privacidad o como fundamento para que el Estado interfiriera en los datos personales o datos personales recabados por los Sujetos Obligados.

Respecto a la excepción del interés público, Carla Huerta Ochoa (s.f.), afirma que: "El interés público es la justificación de habilitaciones constitucionales interventoras expresas, así como límite y garantía de derechos individuales y colectivos". (p. 25).

Si bien, existen diferentes conceptos en la doctrina, la anterior definición establece el límite de las facultades de las Autoridades para evitar el abuso de poder determinando las facultades regladas y, para que en caso de abuso de poder, se reitere que deben subsistir

las garantías a los derechos fundamentales de personas y colectividades, como lo es el derecho a la privacidad sobre cualquier excepción.

La última de las excepciones: el derecho de terceros se verá protegido, mediante la acción que ellos mismos ejerzan, para que los datos personales sean proporcionados por los Sujetos Obligados, en asuntos donde ellos lo soliciten y una Autoridad determine fundada y motivadamente que esta solicitud, es procedente.

De los casos de excepción se concluye: serán las Autoridades encargadas de la Seguridad Nacional, de Salubridad General, Autoridades Administrativas y Judiciales, quienes funden y motiven las resoluciones para restringir el derecho de protección de privacidad, tomando en consideración la naturaleza del dato personal transferido y la proporcionalidad de la acción, así como la razonabilidad en la transmisión de los mismos, la cual, de acuerdo a la Ley General, debe responder a una finalidad específica, para encontrarse en el caso de excepción.

Si una Autoridad transfiere o da a conocer datos personales o datos personales sensibles, sin el consentimiento del titular o un acto de Autoridad que cumpla las formalidades y requisitos de la ley, será ilegal y nulo si es presentado ante cualquier proceso o procedimiento. Además de la Responsabilidad por el manejo indebido de la información que posee.

De todo lo anterior no se desprende que el Estado pueda utilizar los datos personales con fines de persecución penal o, como estrategia para la prevención del delito, por ende, ¿qué pasará con los datos que se recaben utilizando identidad facial? ¿La identidad facial es un dato personal? ¿Nuestro rostro es un dato personal o un dato personal sensible?

Identidad Facial

El Diccionario de la Real Academia Española (s.f.) define la identidad como el "conjunto de rasgos propios de un individuo o de una colectividad que lo caracterizan frente a los demás", y facial como "perteneciente a la cara o rostro" (s.p.)

Entonces, la identidad facial es el conjunto de rasgos propios, pertenecientes a la cara o rostro de un individuo, que lo caracterizan frente a los demás.

El Instituto Nacional de Ciberseguridad de España (en adelante INCIBE), define a la biometría como:

> *Un método de reconocimiento de personas basado en sus características fisiológicas o de comportamiento". Afirmando además que: "la tecnología ha permitido automatizar y perfeccionar estos procesos de reconocimiento biométrico, de forma que tienen multitud de aplicaciones y finalidades.* (Instituto Nacional de Ciberseguridad, 2016, p. 3)

Las leyes mexicanas aún no otorgan una definición sobre identidad facial, ni conciben los datos biométricos como datos personales, pero podemos tomar a la Unión Europea como ejemplo.

El Reglamento General de Protección de Datos, establece qué se entiende por datos biométricos:

> *Datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos*. (Parlamento Europeo y del Consejo, 2016, p. 38)

De acuerdo con esta definición, se cumple el requisito para que los datos biométricos, sean considerados datos personales en México: identifican o hacen identificable a una persona.

No obstante, los datos biométricos son considerados datos personales sensibles por el Reglamento mencionado, pues su utilización podría conllevar discriminación o un riesgo grave cuando su uso no sea debidamente reglado.

El INCIBE, define a las tecnologías biométricas como:

> *Métodos automáticos utilizados para reconocer a personas sobre la base del análisis de sus características físicas o de comportamiento", y refiere que las características biométricas deben cumplir con los siguientes puntos: a) universalidad: todos los individuos las tienen; b) singularidad: distinguen a cada individuo; c) permanencia en el tiempo y en distintas condiciones ambientales; d) medibles cuantitativamente; y las tecnologías, para medir estas características deben tener: a) rendimiento: nivel de exactitud; b) aceptación: por parte del usuario y c) resistencia al fraude y usurpación*. (Instituto Nacional de Ciberseguridad, 2016, p. 5).

Ahora, existen dos tipos de tecnologías para determinar el método utilizado en la biometría, las tecnologías que analizan características fisiológicas de las personas y las que analizan su comportamiento. (Instituto Nacional de Ciberseguridad, 2016, p. 6).

Dentro de las que analizan las características fisiológicas de las personas se encuentran:

> *a) huella dactilar; b) reconocimiento facial; c) reconocimiento de iris; d) reconocimiento de la geometría de la mano; e) reconocimiento de*

> *retina; f) reconocimiento vascular; g) líneas de la palma de la mano; h) forma de las orejas; i) piel, textura de la superficie dérmica; j) ADN, k) composición química del olor corporal. Y las que analizan el comportamiento son: i) reconocimiento de firma; ii) reconocimiento de escritor; iii) reconocimiento de voz; iv) reconocimiento de escritura de teclado; v) reconocimiento de la forma de andar*. (Instituto Nacional de Ciberseguridad, 2016, p. 7-12).

Se determina que se aplica para: "a) control de accesos físicos y lógicos; b) control de presencia; c) lucha contra el fraude; d) *call-centers*; e) medios de pago; f) control de navegación; g) vigilancia" (Instituto Nacional de Ciberseguridad, 2016, p. 13-14).

Es conveniente señalar que la identidad facial se relaciona con el reconocimiento facial, ya que:

> *Es una técnica mediante la cual se reconoce a una persona a partir de una imagen o fotografía. Para ello, se utilizan programas de cálculo que analizan imágenes de rostros humanos. Entre los aspectos clave empleados para la comparación se encuentran mediciones como la distancia entre los ojos, la longitud de la nariz o el ángulo de la mandíbula. A diferencia de otros sistemas biométricos, el reconocimiento facial puede ser utilizado para la vigilancia general, habitualmente mediante cámaras de video. Existen soluciones de software que utilizan esta tecnología para identificación de usuarios en dispositivos móviles y portátiles*. (Instituto Nacional de Ciberseguridad, 2016, p. 8).

De acuerdo con lo anterior, el reconocimiento facial ha sido utilizado para la identificación de personas desde hace tiempo; en el caso de México y la implementación tecnológica, deben observarse los argumentos a favor y en contra para establecer un sistema de reconocimiento facial que respete derechos fundamentales cuando su uso tenga que ver con la investigación criminal.

Propuestas para plantear el uso de la identidad facial en la investigación criminal

Como lo mencionamos anteriormente, una excepción al derecho de Privacidad lo es la seguridad, por lo tanto, esto podría utilizarse éticamente para la investigación criminal o más bien, esto ha sido utilizado en otros países y México debe ponderar su uso y evitar poner encima a la seguridad nacional e interés público sobre la vida privada.

El primer punto a tratar es la forma en la que tendrían que operar: en qué lugares y durante qué horarios se realizará este reconocimiento o si será en todo momento de forma ininterrumpida y en todo lugar, qué empresas llevarán a cabo esta tarea, o en caso de que sean las Autoridades, cómo conservarán toda la información, y si el titular de los datos personales sensibles tendrá que manifestar su aprobación para la creación de sistemas de circuito cerrado que identifiquen a las personas.

Segundo punto importante: crear organismos autónomos que puedan tener el control sobre los datos personales sensibles que se recaben para que su justificación y su uso se encuentre regulado por un Sujeto Obligado distinto a las Procuradurías o Fiscalías y de esa manera utilizar a la identidad facial como último recurso para la persecución final.

Otro punto de conflicto: ¿para qué recabar la identidad facial de las personas? ¿Esto será realizado a través de grabaciones? ¿Por qué medio se harán esas grabaciones? ¿Las grabaciones se harán en lugares públicos? ¿Se harán las 24 horas y 7 días de la semana? Lo anterior ¿cumpliría con los fines del proceso penal? ¿se protegería el derecho a la Privacidad? ¿pesa más el derecho a la seguridad que el derecho a la Privacidad?

En caso de que las Autoridades determinen identificar a la población mediante el reconocimiento facial y el uso de tecnologías para lograr recabar todos sus rasgos físicos, comportamientos y cualidades que los hacen únicos, ¿cuál sería la finalidad? ¿Mejorar los servicios públicos, facilitar el acceso de servicios públicos a las personas, crear una base de datos para así identificarlas y perseguirlas cuando cometan hechos ilícitos?

En la construcción de la política pública para la implementación de la identidad facial, deben tomarse en consideración los Tratados y las Leyes que fundamentan el Estado de Derecho en México; esto es, se debe regular su actuar y las consecuencias de las mismas en el uso de la identidad facial por parte del Estado, para así crear seguridad en la ciudadanía.

Se habla de seguridad cuando la ciudadanía sepa cuál es el fin en tener un Sistema de identidad facial para prevenir e investigar conductas delictivas, pero de la misma manera, informar sobre la existencia del derecho a la Privacidad y la oposición a ser grabada/o.

Por otra parte, si lo que se busca es para fines de seguridad, se debe ponderar entre ella y el derecho de acceso a la justicia para identificar a las personas que probablemente cometen un ilícito.

Y así poder determinar, si los medios de identificación servirán para ofrecerse como pruebas en juicio y, en caso de aplicarse para la prevención e

investigación de los delitos, fundamentar que su uso será para cumplir con las finalidades del proceso penal acusatorio.

La medida que trate de adoptar el Estado debe valorar el derecho a la privacidad (en sentido amplio), ya que este permite que las personas se desarrollen sin sentirse observadas, actuar de tal manera que tengan conocimiento de que su vida cotidiana no tendrán un mal uso (como acusárseles de delitos fabricados) y, que la información recabada mediante sus datos biométricos esté protegida en un máximo nivel.

Además de ello, el pensar en establecer circuitos cerrados de video vigilancia, es pensar en una política ética y de debida diligencia para que quienes observan y "cuidan a la ciudadanía" no sean quienes les dañen o les pongan en peligro.

De lo anterior ¿qué métodos serán utilizados para la contratación de personas que vigilen mediante cámaras de circuito cerrado? El control que se debe tener de las mismas debe ser severo y ético, ya que, estas personas serán quienes puedan transmitir la información a terceros o, en su caso venderla y, con ello, además de violar el derecho a la privacidad, se hará tráfico de información ilícita y por supuesto, violar la protección del dato personal sensible: la identificación facial.

De acuerdo a los modelos que se utilizan en otros países, también debe pensarse en los programadores que desarrollaran esta tecnología, quiénes en caso de utilizarla para fines ilícitos, sean responsables de sus conductas, se les sancionen y no queden impunes las violaciones al uso ilícito de la identidad facial. Por ello, debe tomarse en consideración el uso ético de la tecnología en los sistemas que México desee adoptar.

Lo importante de esta medida será el apoyo multidisciplinario en temas de tecnología y de de derechos fundamentales para evitar lesionar a la ciudadanía y cometer conductas violatorias de estos derechos, sino al contrario, potencializar derechos humanos, y, en caso de usarse para la persecución e investigación del delitos, se cree confianza en las personas y explicarles que se utilizará la identidad facial para evitar la impunidad, identificar al culpable y que se repare el daño cometido por las conductas ilícitas.

Las medidas adoptadas deben ser razonables, poniendo como eje central al interés público, delimitando la actuación del Estado, para que use sus facultades discrecionales y, con ello, violentar derechos humanos. Deben ser proporcionales mencionando las finalidades del uso de esta tecnología y que las personas conozcan los alcances e infracciones por el uso del reconocimiento facial.

Además de ello, es necesario que se identifique a la identidad facial como un dato personal sensible en las leyes de datos personales, para que su protección alcance el nivel alto de seguridad y así regular para evitar transferirse a cualquier persona el conocimiento de los datos biométricos.

Debe educarse a la población para determinar que las tecnologías son neutras: ni buenas ni malas; que las mismas ayudan a facilitar las tareas de las personas y tener un debido control para fortalecer el Estado de Derecho que es reconocido en México. De acuerdo a esto, debe entenderse que el desarrollo de la tecnología, nunca podrá ser usado para identificar a las personas como posibles candidatos a criminales y, evitar la discriminación por ciertos rasgos, educación, etcétera y, con ello concluir que una persona que cuenta con características similares, puede ser candidato a delinquir tal y como lo mencionaba Lambrosso en su teoría.

En la pandemia existieron casos de uso indebido de la información generada a través de la identidad facial como lo fue discriminar a personas contagiadas de COVID-19 a través de datos personales sensibles y a muchas personas trabajadoras de la salud que ofrecían su vida para proteger a las personas enfermas; es por ello que la identidad facial debe planearse y en su caso, ser el último recurso.

En el uso de las tecnologías de identificación, debe planearse el cómo y el para qué, así como delimitar el alcance y aumentar la responsabilidad de las personas que utilicen dicha información.

Los casos de excepción deben estar reglamentados y fundados tomando en consideración doctrina internacional y sus prácticas; para que, en caso de ser necesario, la identidad facial que se recabe sea usada para fines proporcionales, específicos y de investigación criminal fundada, no en un caso de excepción como lo puede ser el Derecho Penal del Enemigo.

Conclusión

En todas las decisiones que México tome se debe de ponderar siempre la protección y garantía de los derechos fundamentales, dejando de lado la persecución e investigación criminal con fines nocivos para una persona. Lo anterior, es importante, ya que, en caso de adoptarse la tecnología de reconocimiento facial, debe pensarse en una política pública ética y, observando las buenas prácticas en materia de uso de tecnología.

A través de la experiencia de otros países que ya han implementado el uso de la tecnología, vemos que

estos procesos han facilitado su vida cotidiana, pero existen problemas con el ejercicio de derechos como en China, que, al manifestarse, son reconocidos mediante sus biométricos y sancionados penalmente.

La implementación debe ser racional y proporcional, tomando en cuenta siempre los derechos de las personas y de los grupos vulnerables.

Debe informarse a las personas cuál será el tratamiento en el uso de sus biométricos y establecer un régimen estricto para proteger esta información; así como un sistema de Responsabilidad para el que cree, para el que comparta y para el que la use.

Debe observarse siempre la neutralidad en el uso de esta tecnología, contar con expertos que ofrezcan soluciones para problemas como vulneración en los sistemas de los Sujetos Obligados; debe potencializarse el derecho a la privacidad, para que las personas realicen sus actividades sin sentirse vigilados y, con la conciencia que sus acciones, si son lícitas, no merecen ser vigiladas.

Además de ello, se debe pensar que la implementación general de esta tecnología en todo tiempo y momento violentaría el interés superior de la niñez.

Para el Sistema de Justicia Penal es útil, en especial a los fines del proceso penal acusatorio; pero esto debe ser valorado y ponderado siempre, por el derecho de Privacidad, ya que no todas las personas delinquen y no siempre se están cometiendo delitos, por ello (hasta el día de hoy) su ineficacia para aplicarla en México.

Referencias

Asociación de Internet MX. (31 de julio de 2019). *Estudio sobre los Hábitos de los Usuarios de Internet en México 2019.* https://irp-cdn.multiscreensite.com/81280eda/files/uploaded/15%2BEstudio%2Bsobre%2Blos%2BHa_bitos%2Bde%2Blos%2BUsuarios%2Bde%2BInternet%2Ben%2BMe_xico%2B2019%2Bversio_n%2Bpu_blica.pdf

Asociación de Internet MX. (Mayo de 2021) *17° Estudio sobre los Hábitos de los Usuarios en Internet en México 2021. https://irp.cdn-website.com/81280eda/files/uploaded/17%C2%B0%20Estudio%20sobre%20los%20Ha%CC%81bitos%20de%20los%20Usuarios%20de%20Internet%20en%20Me%CC%81xico%202021%20v16%20Publica.pdf*

Ayuda Ley. (s.f.). *Datos biométricos – ¿Qué y cuáles son? ¿Cómo cumplir con la Ley?* https://ayudaleyprotecciondatos.es/2019/02/15/datos-biometricos/#Reconocimiento_facial

Branch. (21 de abril de 2021). *Estadísticas de la situación digital en México en el 2020-2021. https://branch.com.co/marketing-digital/estadisticas-de-la-situacion-digital-de-mexico-en-el-2020-2021/*

Congreso de la Unión. (1917). *Constitución Política de los Estados Unidos Mexicanos.* Diario Oficial de la Federación.

Congreso de la Unión. (2005). *Ley de Seguridad Nacional.* Diario Oficial de la Federación

Congreso de la Unión. (2010). *Ley Federal de Protección de Datos Personales en Posesión de Particulares.* Diario Oficial de la Federación.

Congreso de la Unión. (2017). *Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.* Diario Oficial de la Federación.

Congreso de la Unión. (1984). *Ley General de Salud.* Diario Oficial de la Federación

Congreso de la Unión. (2009). *Ley General del Sistema Nacional de Seguridad Pública.* Diario Oficial de la Federación.

Instituto Nacional de Ciberseguridad. (2016). *Tecnologías aplicadas a la ciberseguridad.* https://www.google.com/search?q=gu%C3%ADa+del+incibe+sobre+tecnolog%C3%ADas+biom%C3%A9tricas&rlz=1C1CHBF_esMX813MX814&oq=&aqs=chrome.0.69i59l8.102416j0j7&sourceid=chrome&ie=UTF-8

Ochoa, C.. (s.f.). *EL concepto de interés público y su función en materia de seguridad nacional.* https://archivos.juridicas.unam.mx/www/bjv/libros/5/2375/8.pdf

Organización de las Naciones Unidas. (1948). *Declaración Universal de Derechos Humanos.* https://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/spn.pdf

Organización de las Naciones Unidas. (1966). *Pacto Internacional de Derechos Civiles y Políticos.* https://www.ohchr.org/SP/ProfessionalInterest/Pages/CCPR.aspx

Organización de los Estados Americanos. (1969). *Convención Americana de Derechos Humanos.* https://www.oas.org/dil/esp/tratados_b-32_convencion_americana_sobre_derechos_humanos.html

Organización de los Estados Americanos. (1948). *Declaración Americana de los Derechos y Deberes del Hombre.* http://www.oas.org/es/cidh/mandato/Basicos/declaracion.asp

Parlamento Europeo y del Consejo. (2016). *Reglamento General de Protección de Datos.* https://www.boe.es/doue/2016/119/L00001-00088.pdf

Real Academia Española. (s.f.). *Diccionario de la Lengua Española.* https://www.rae.es/

Ricci, D. (2013). *Artículo 16 Constitucional Derecho a la Privacidad.* https://archivos.juridicas.unam.mx/www/bjv/libros/8/3567/39.pdf

The International Criminal Police Organization. (2020). *Temas de Interés.* https://www.interpol.int/content/download/624/file/GI-01_2020-01_SP_LR.pdf?inLanguage=esl-ES#:~:text=INTERPOL%20facilita%20la%20cooperaci%C3%B3n%20policial,vigentes%20en%20los%20diferentes%20pa%C3%ADses.