



Sistemas de vigilancia y su efecto en el derecho a la intimidad desde el discurso de la seguridad

Surveillance systems and their effect on the right to privacy from the security discourse




Sistemas de vigilância e seus efeitos sobre o direito à privacidade do discurso de segurança

Andres Burbano Ardila ¹
Angela Navia López²
Sthefany Loriet Díaz Losada³

Resumen

En la actualidad, existen sistemas de vigilancia, como las herramientas de reconocimiento facial, que justifican su existencia en la noción de seguridad personal y de los Estados. Sin embargo, este desarrollo tecnológico y el objetivo de brindar esa sensación de seguridad entran en tensión con derechos fundamentales. El presente texto busca analizar cómo los sistemas de reconocimiento facial, enmarcados en la idea de dar seguridad, ponen en riesgo los derechos a la privacidad e intimidad. Para el cumplimiento del objetivo, se acude a un diálogo interdisciplinario entre elementos jurídicos y de la teoría social; lo primero, para comprender el derecho

Recibido: 24-6-2021 - Aceptado: 5-10-2021

- 1 Magíster en Derecho y abogado de la Universidad Mariana. Colombia.  <https://orcid.org/0000-0001-7380-9466>. Correo electrónico: andresardila1989@gmail.com
- 2 Estudiante de doctorado en Sociología de la Universidad Benemérita de Puebla. Magíster en Relaciones Internacionales con mención en seguridad y derechos humanos de la Facultad Latinoamericana de Ciencias Sociales. Abogada de la Universidad de Nariño. Docente universitaria. Colombia.  <https://orcid.org/0000-0002-0640-8037>. Correo electrónico: angela.navia@alumno.buap.mx.
- 3 Magíster en Derecho y abogada de la Universidad Mariana. Colombia. Investigadora voluntaria en el Programa de Investigación de Política Exterior Colombiana (PIPEC).  <https://orcid.org/0000-0002-8278-1220>. Correo electrónico: sthefanydiaz210@gmail.com



a la intimidad y lo segundo, con el fin de examinar los sistemas de seguridad encuadrados en un discurso de poder.

Palabras claves: seguridad, intimidad, sistemas de vigilancia, poder.

Abstract

Currently there are surveillance systems, such as facial recognition tools, that justify their existence in the notion of personal and State security. However, this technological development and the objective of providing a sense of security is in tension with fundamental rights. This text seeks to analyze how facial recognition systems, framed in the idea of providing security, put the rights to privacy and intimacy at risk. For the fulfillment of the objective, an interdisciplinary dialogue between legal elements and social theory is used. First to understand the right to privacy and secondly, to analyze the security systems framed in a discourse of power.

Keywords: security, privacy, surveillance systems, power.

Resumo

Atualmente existem sistemas de vigilância, como as ferramentas de reconhecimento facial, que justificam sua existência na noção de segurança pessoal e do Estado. No entanto, este desenvolvimento tecnológico e o objetivo de proporcionar uma sensação de segurança estão em conflito com os direitos fundamentais. Este texto busca analisar como os sistemas de reconhecimento facial, enquadrados na ideia de oferecer segurança, colocam em risco os direitos à privacidade e à intimidade. Para o cumprimento do objetivo, utiliza-se um diálogo interdisciplinar entre os elementos jurídicos e a teoria social. O primeiro para entender o direito à privacidade e o segundo, para analisar sistemas de segurança enquadrados em um discurso de poder.

Palavras-chave: segurança, privacidade, sistemas de vigilância, poder.

Introducción

En las discusiones alrededor del Estado, se posiciona la categoría de seguridad, entendida como la garantía del orden y la sociedad. Se deriva desde las apreciaciones de Hobbes sobre el Estado, o ese gran Leviatán que permite salir del estado de naturaleza, hasta debates recientes sobre el mantenimiento del Estado ante amenazas globales o locales. En las discusiones sobre la modernidad, emerge la noción de incertidumbre; es decir, el miedo constante en el que viven los seres humanos. Se trata, entonces, esa incertidumbre, entendida como una forma de miedo que, de una u otra forma, maneja la conducta humana.

Bajo ese entendido, cabe preguntarse: ¿por qué la incertidumbre traducida en miedo es uno de los pilares del Estado moderno? Si bien en su momento se asumió la figura de Estado como señal de la convivencia, los cambios históricos en los últimos

decenios posicionan el temor al otro, los otros. En estas modificaciones, se hace necesario dar su lugar a la noción de seguridad en los debates de las ciencias sociales.

En dicho contexto, en las últimas décadas, se han implementado mecanismos para que las sociedades se sientan “seguras”. Entre ellos, se destaca la puesta en práctica de sistemas de vigilancia, desarrollados con la sofisticación tecnológica de los años recientes. Ejemplo de esos sistemas de vigilancia son las herramientas tecnológicas de reconocimiento facial. Sin embargo, si bien ellas se justifican en el requerimiento de seguridad, entran en tensión con derechos como la intimidad y privacidad, reconocidos como fundamentales.

Siguiendo el escenario descrito, el objetivo del presente trabajo es analizar cómo los sistemas de reconocimiento facial, enmarcados en la idea de brindar seguridad, ponen en riesgo los derechos a la privacidad e intimidad. Para el cumplimiento del propósito, se acude a un diálogo interdisciplinario entre elementos jurídicos y de la teoría social.

El texto se compone de cuatro apartados. En el primero, se examina la seguridad como categoría de estudio y como el justificante de los sistemas de vigilancia. En primer lugar, se esboza las principales teorías que se han ocupado de su estudio y, en segunda instancia, se analiza dicha categoría desde las propuestas de vigilancia tratadas por Michel Foucault y Zygmunt Bauman. Establecido este marco analítico, en el siguiente acápite se desarrolla los elementos teóricos y normativos de los derechos a la intimidad y privacidad. En la tercera sección, se describe los sistemas de reconocimiento facial como herramientas biométricas. Este desarrollo permite que, en el cuarto capítulo, se describa esos instrumentos como mecanismos de vigilancia en las sociedades modernas y su impacto en los derechos mencionados. Finalmente, se elevan conclusiones sobre lo disertado.

El discurso de la seguridad

Lineamiento histórico de las teorías de seguridad.

A pesar de que la definición de seguridad podría parecer fácil de conceptualizar, teóricamente puede comprender un gran espectro de significados, según el contexto histórico en el que se desarrolle. Desde la acepción clásica, el término tiene una propiedad objetiva y otra subjetiva. Arnold Wolfers, en su libro *National Security As An Ambiguous Symbol*, citado por Moller (1996), manifestó: “seguridad, en un sentido objetivo mide la ausencia de amenazas a los valores adquiridos, en un sentido subjetivo, la ausencia de temor sobre el ataque a dichos valores” (p. 769).



La definición dada por Wolfers se limita a la amenaza de los valores. Empero, fue un gran avance para su época, ya que, en un primer momento, la seguridad no era vista como un término de interés que valiera la pena conceptualizar a partir de la teoría de las relaciones internacionales y las ciencias políticas, en vista de que se hacía uso de otras categorías como la de poder. A partir de esta noción, la seguridad comienza a jugar un papel importante en la teoría de las relaciones internacionales; sin embargo, fue estudiada por diversos autores como Hobbes, quien estableció que el ser humano, por naturaleza, se encuentra en un estado constante de envidias y odios. Esa condición, lleva a la persona a una permanente lucha que termina convirtiéndose en una anarquía. Y es en este momento cuando surge el Estado como un salvador para abandonar la condición de guerra. Desde tal concepto, se puede establecer la entidad estatal como un todo, un organismo salvador de los más impuros deseos de odio de la humanidad, que la conducen a convertirse en el centro de la seguridad.

A partir de los fundamentos teóricos previos, emanan las primeras corrientes, también teóricas, sobre la seguridad. Entre ellas se posiciona la teoría realista que ubica al Estado como objeto último de la seguridad. Este postulado surgió a finales de la Segunda Guerra Mundial, pero encontró su fortalecimiento con la Guerra Fría. Es posible hablar de él, desde una perspectiva de la primera doctrina común de la seguridad nacional, por llamarla así, la cual tenía como precepto central que mientras el Estado se mantuviera seguro la población se encontraría segura. Bajo este aspecto, se debía hacer uso de todo el poderío militar, a sabiendas de que la mejor manera de salvaguardar la seguridad era mediante el armamento. Es así como surge una competencia acumulativa entre los países por saber quién tenía mejor instrumentaria bélica.

Más adelante, se desprende, entonces, la teoría de la disuasión: uno de los Estados intenta inducir al otro para que realice o se abstenga de ejecutar una acción en su contra. Ese precepto teórico fue usado como uno de los justificantes de la creación y del uso de armas nucleares durante finales de la Segunda Guerra Mundial. No obstante, la praxis de esa idea trajo consigo diversos problemas en el nivel económico, a causa de la excesiva acumulación de armamento, además de ocasionar conflictos sociales que condujeron a buscar una nueva alternativa para salvaguardar la seguridad.

Por otro lado, se encuentra la teoría de la seguridad común, la cual surgió a partir del informe de la Comisión Palme de 1982, titulado *la Seguridad Común un Programa para el Desarme*. Se establece que debe existir una restricción mutua de los Estados, con el fin de establecer relaciones pacíficas; esto supondría un frente al dilema de la seguridad. La teoría está planteada “con el fin de facilitar

y promover la cooperación entre los estados para hacer frente a la situación de anarquía internacional y superar la carencia de una autoridad central supranacional” (Orozco, 2006, p. 172).

También se presenta la teoría del constructivismo, que plantea la existencia de un sistema internacional creado por diversos sujetos como los Estados, las ONG, los grupos étnicos, entre otros, que tienen como propósito ser intermediarios de los conflictos y evitar la germinación de estos. Además, aparece un interés de salvaguardar a cada uno de los sujetos que conforman ese sistema, pero su característica principal es la identidad de la sociedad que conforma el Estado, es así como la seguridad tiene un enfoque colectivo internacional que se genera dada la participación de los diferentes actores, los cuales identifican unos intereses y posiciones comunes.

Estas nuevas dimensiones otorgadas al concepto de seguridad llevaron a que en 1994 el Programa de las Naciones Unidas para el Desarrollo publicara un informe en el que se habla de la seguridad humana:

No será posible que la comunidad de países conquiste ninguna de sus metas principales —ni la paz, ni la protección del medio ambiente, ni la vigencia de los derechos humanos o la democratización, ni la reducción de las tasas de fecundidad, ni la integración social— salvo en un marco de desarrollo sostenible conducente a la seguridad de los seres humanos (Larson et al., 1994, p. 1).

Se formuló, entonces, que la seguridad no solo es un elemento para liberarse de las amenazas, sino que igual debe fungir como mecanismo base del Estado y de su desarrollo; a través de la seguridad es posible alcanzar estos objetivos.

Por otro lado, está la teoría de la integración, que surge de la escuela de Copenhague, la cual intenta reconciliar los diferentes aportes de las otras teorías. Es decir, dicho postulado teórico procura abandonar la idea de seguridad del Estado y ocuparse, a la vez, del bienestar integral de los seres humanos. Por esto, tal escuela contribuye a los estudios sobre seguridad y su posicionamiento en las formas de entender el campo internacional.

La escuela de Copenhague establece la noción de seguridad como una categoría sin significado unívoco. Su definición depende del contexto social, económico y político. Desde esta premisa, esa escuela unifica las otras teorías, determinando que el objeto de la seguridad depende de cada situación y que, en todo caso, es un término multidimensional en la medida de que trabaja desde el individuo y, en otras ocasiones, desde la integridad territorial.



La seguridad desde la perspectiva de Foucault y Bauman

Para analizar la seguridad desde Foucault, es necesario iniciar con la concepción de poder. Una de las formas en las que el filósofo francés Michael Foucault se refiere a este último es como una maquinaria formada por engranajes. En ellos, el componente más violento de todos es el castigo; no se ejerce sin objetivo, recae directamente sobre el cuerpo, el cual no solo sufre por el poder, sino que además es vigilado por este.

El cuerpo humano entra en un mecanismo de poder que lo explora, lo desarticula y lo recompone. Una “anatomía política”, que es igualmente una “mecánica del poder”, está naciendo; define cómo se puede hacer presa en el cuerpo de los demás, no simplemente para que ellos hagan lo que se desea, sino para que operen como se quiere, con las técnicas, según la rapidez y la eficacia que se determina (Foucault, 2002, p. 126).

Es decir, el cuerpo siempre ha sido utilizado como un medio para enviar un aviso a los ciudadanos. En un primer momento, con el fin de castigar, se causaban diferentes laceraciones e incluso la muerte ante un público sediento, destinatario de un mensaje: si tú haces esto, sufrirás esta misma sanción y este escarmiento público. En un segundo momento, el cuerpo se toma como territorio disciplinado según la sociedad lo requiere. Aquí entra la disciplina como un elemento clave para crear cuerpos dóciles, en todos los escenarios, desde los colegios hasta los sitios de trabajo.

Acorde con Foucault (1975), en el proceso de vigilancia están las distribuciones espaciales divididas en cuatro elementos: 1) *la clausura* como algo que se encuentra cerrado sobre sí mismo, por ejemplo, un convento; 2) *zonas o localización elemental* o zona por separado para vigilar; 3) *emplazamientos funcionales*, lugares que responden directamente a la necesidad de un sitio, así que están seccionados por la función que cumplen; 4) *elementos intercambiables*, espacios vinculados a la organización por clasificación o rangos y que, como consecuencia de eso, se distribuyen según su relación.

Seguidamente, se encuentra el control de la actividad, para vigilar a los sujetos de esta forma: primero hace referencia al empleo del tiempo, con el que se deben establecer ritmos y ciclos para esos sujetos, obligándolos a definir ocupaciones determinadas; después, como segunda medida, se elabora el temporal del acto, es decir, se programa su ejecución como su desarrollo, movimiento, cronología y comportamiento (Foucault, 1975). El tercer paso instaura la relación del cuerpo y el gesto, se busca vincular este último a una actitud global, con la cual se pretende

condicionar al cuerpo. En cuarto lugar, se correlaciona el cuerpo con un objeto, lo que significa que aquel reaccione a un objeto. El quinto paso es la utilización exhaustiva, con la que se crea una monotonía temporal: cada instante se fuerza al organismo a ser más mecánico.

Todo lo anterior lleva a comprender que los espacios de disciplina, así como el control de actividades responden a una necesidad del sistema que los crea y del poder que los domina. Por tanto, la disciplina es un proceso lógico que sigue una estructura planteada, pues esta requiere orden y control para implementarse.

En síntesis, como Foucault (1975) lo define, el cuerpo es un instrumento clave: sin este no habría elemento que disciplinar; es un componente primario del sistema de disciplina, vigilancia y poder.

En cuanto a la seguridad entendida desde Zygmunt Bauman, se debe mencionar:

Que la variedad moderna de la inseguridad viene marcada por un miedo que tiene principalmente como objeto a la maleficencia humana y a los malhechores humanos. Este miedo se inocula a través de la sospecha de la existencia de una motivación malévola en ciertos hombres y mujeres concretos, o en ciertos grupos o categorías de hombres y mujeres (Bauman, 2010, p. 170).

Como se observa, el ser humano es un ente inseguro que se ahoga por sus miedos; es así como el hombre, en su objetivo por alcanzar la seguridad, se defiende y permanece en estado de alerta ante el más insignificante elemento de peligro, lo cual lleva a que se genere un sinnúmero de investigaciones, trabajos e inventos que buscan garantizar esa seguridad.

Todas las continuas inseguridades, en la contextualización de la obra *Modernidad líquida* (2012), han llevado a que la seguridad, como una de las bases por las que se sentó el Estado, se haya quebrado. Se viró, así, el interés hacia la seguridad personal. Ella convierte a cada ciudadano en vigilante y vigilado, al mismo tiempo, lo que sentará sus bases en el miedo e incertidumbre que conducen al final del Estado social de derecho (Bauman, 1999).

Al haber convertido, simultáneamente, al hombre en vigilante y vigilado, se desdibujó el valor de algunos derechos como la privacidad, que pasan a perder importancia cuando de seguridad y vigilancia se trata, porque, de un modo u otro, son sacrificados para gozar de esa seguridad que brindan estos tiempos líquidos, tan efímeros y volátiles.

Hoy, las personas ya no tienen miedo a que se conozca hasta el más mínimo de los detalles de su vida, no tienen desconfianza a la vigilancia que en el pasado causaba terror, por la opresión que podía generar. Por el contrario, “ese miedo a ser observados ha sido vencido por la alegría de ser noticia” (Bauman, 2013, p. 25).

Los derechos a la intimidad y privacidad

El derecho a la intimidad y privacidad no es nuevo. Desde hace varios años, se han generado diferentes preocupaciones respecto a cómo salvaguardar la vida privada de una persona y su familia o el *derecho a estar solo*, como se le ha llamado en muchos casos. Es por esto que se han venido desarrollando diferentes teorías en aras de proteger esos derechos que, a la vez, se enfrentan a un reto novedoso ante un mundo cada vez más tecnológico y vigilado.

Conceptualización del derecho a la intimidad y privacidad

Etimológicamente, el concepto de intimidad proviene del latín *intus* que significa dentro. Quiere decir que es algo proveniente del interior o está dentro de la persona, por lo que hace parte de esta.

Lo íntimo no necesariamente es lo que la persona quiera reservar ante la sociedad; por el contrario, es una de las partes sustanciales que componen al ser humano, porque le permite distinguirse de los demás.

En cuanto a la privacidad, es necesario determinar que su uso originalmente se hace en el idioma inglés y no en el castellano. Un ejemplo lo conforma la aplicación creada por Warren y Brandeis para su teoría de Right of Privacy, con la cual exteriorizaron la importancia de un derecho que proteja la vida privada de las personas, la de su familia, así como la necesidad de resguardarse de ataques que se puedan presentar a su reputación y honra (esto respecto a la intromisión por parte de

Ahora bien, se debe tener en cuenta que en la lengua anglosajona no se hace diferencia alguna entre lo que se entiende entre intimidad y privacidad. Desde la concepción de las teorías de Warren y Brandeis, se habla de la privacidad de tal forma que contiene la intimidad, sin explicar o distinguir la una de la otra; incluso, actualmente no existe un término propio que pueda traducir, del castellano al anglosajón, la palabra intimidad, pues, al buscar su equivalente se refiere directamente a la privacidad como su igual.

Pese a lo dicho, otro de los orígenes que se le asigna al término intimidad es aquel fundamentado en la dogmática iusprivatista, con la que los derechos de la

personalidad son entendidos como parte de la propiedad privada, es decir, como un bien más.

Empero, en el idioma castellano el desarrollo de las dos palabras en cuestión es diferente. Es así como el Diccionario Panhispánico del Español Jurídico (2020) define la intimidad como algo del ámbito reservado de una persona o una familia, mientras se refiere a la privacidad como el derecho de una persona a no ser objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra o reputación. No obstante, determinar una definición única entre el derecho a la intimidad y a la privacidad sería, como lo dijo Solove, “un concepto en desorden” (según se citó en [Lucena, 2014, p.22](#)).

A pesar de la difícil conceptualización y diferenciación de la intimidad y la privacidad, en la lengua castellana que nos ocupa, esta se puede definir, con base en las nuevas tecnologías, como aquel derecho que tiene una persona para decidir si da a conocer o no su información a otras personas y en qué medida la comparte.

Teniendo en cuenta lo anterior, es posible concluir que el concepto de intimidad para la lengua castellana contiene el de privacidad y viceversa.

Abordando las teorías de la intimidad y la privacidad, se encuentra la de las esferas o *Spharentheorie*, que proviene del Tribunal Constitucional alemán. Se caracteriza por darle a esos derechos esferas y órbitas para sí mismas, en las cuales están contenidas sus características: habrá una esfera íntima (*Intimsphäre*), que iría referida a lo más secreto del individuo; la esfera privada (*Privatsphäre*), similar a la *privacy* anglosajona y a nuestro derecho a la intimidad, que engloba la vida privada y las relaciones tanto familiares como personales; y, por último, la esfera individual (*Individualsphäre*), que hace alusión a aspectos ligados a la intimidad, pero incluidos en ella, como el honor y la propia imagen. Partiendo de esta teoría, se puede hablar de tres esferas concéntricas: la de lo íntimo, la de lo privado y la de lo público ([Álvarez, 2015](#)).

Por otro lado, se encuentra la teoría del mosaico, postulada por Madrid Conesa (1984), quien expresó que, al contrario de la teoría de las esferas, la intimidad y la privacidad no están formadas por esferas separadas en su propia órbita, sino que la intimidad está constituida por pequeños detalles o datos íntimos que por sí solos no son especiales, pero que en conjunto pueden revelar cuestiones importantes sobre la intimidad de los sujetos.



Con los avances tecnológicos que han ido surgiendo, nace la necesidad de hacer frente a estos, con el fin de proteger el derecho a la privacidad e intimidad. Es por esto que se generó una nueva teoría, planteada por el profesor Daniel J. Solove, conocida como la taxonomía de la privacidad. En ella, existen cuatro categorías relacionadas con la recolección de datos, que se pueden enumerar así: 1) recopilación de datos que a su vez se componen de vigilancia e interrogación; 2) procesamiento de la información constituida por agregación, identificación, inseguridad, uso secundario y exclusión; 3) dimensión de datos conformada por el quebrantamiento de la promesa de confidencialidad, divulgación, exposición, accesibilidad incrementada, chantaje, apropiación, distorsión; 4) invasión formada por la intrusión y la interferencia de decisiones.

Reconocimiento del derecho a la intimidad en el nivel internacional

El derecho a la intimidad no se ha limitado simplemente a un desarrollo lingüístico y doctrinal. Ha tenido un reconocimiento a través de diversos instrumentos internacionales como la Declaración Universal de Derechos Humanos de 1948, que asintió, en su artículo 12, la protección a las injerencias o ataques que se pudieran presentar en la vida privada, honra o domicilio de una persona, así como en su reputación.

Ese mismo derecho a la intimidad fue reconocido en el Pacto Internacional de Derechos Civiles y Políticos de 1976, mediante el artículo 17, en el cual se trata el derecho a la privacidad y su protección por la ley; además, en la Convención Europea para la Protección de los Derechos Humanos y de las Libertades Fundamentales, en su artículo 8, el cual establece que toda persona tiene derecho a su vida privada y no deben darse injerencias en esta por parte de autoridades públicas, salvo cuando la ley lo autorice, ya sea para salvaguardar la seguridad nacional, la seguridad pública, la economía del país o por interés general.

En el 2015, la ONU publicó su resolución denominada *El derecho a la privacidad en la era digital*. Con este instrumento buscó impulsar a los Estados para proteger y respetar el derecho a la privacidad e intimidad, estableciendo, examinando, proporcionando, respetando, elaborando y creando mecanismos que le permitan a las personas salvaguardar tal derecho en una era digital. Si se ha producido ya una vulneración de ese privilegio, los Estados deben brindar herramientas que le permitan a la persona objeto de esa injerencia restablecer su derecho, con el afán no solo de salvaguardar el derecho a la intimidad, sino también el tratamiento de datos personales que se encuentran inmiscuidos en aquel.

La resolución aludida surgió como consecuencia del informe entregado por el “relator especial sobre la promoción y protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo Ben Emmerson” (2015, p. 2), quien hace mención de los sistemas de vigilancia masiva usados en la lucha contra el terrorismo.

Se resalta que, si bien los Estados tienen el deber de proteger a sus ciudadanos, no significa que se deban vulnerar los derechos como libertad, privacidad, entre otros; por el contrario, son ellos los que deben velar siempre por la protección de estos privilegios. Igualmente, las medidas que se tomen para la lucha contra el terrorismo deben ser necesarias, proporcionales y no discriminatorias.

Realizado este análisis teórico de los preceptos de seguridad y los derechos a la intimidad y privacidad, se desarrolla el contexto problematizador del presente estudio: los sistemas de reconocimiento facial como elementos para la seguridad y la tensión con estos derechos fundamentales.

Reconocimiento facial como sistema biométrico: la ficción llevada a casos reales

La búsqueda de la seguridad ha llevado al desarrollo de nuevas tecnologías que, discursivamente, ofrecen una solución a ese constante miedo presente en las sociedades líquidas. Sin embargo, dichas tecnologías, como el reconocimiento facial, manejan un sinnúmero de información, que muchas veces trasgrede derechos como la intimidad.

Bajo ese entendido, es importante conocer cómo funciona la biometría y, en esta, los sistemas de reconocimiento facial, especialmente en el contexto contemporáneo, donde su uso se extiende globalmente y su impacto es mayor de lo que podría imaginarse.

En la era digital se está intensificando, en todo el mundo, un debate social sobre tres realidades que chocan entre sí: la amenaza de una vigilancia electrónica generalizada, técnicamente posible a partir de ahora; la indispensable salvaguardia de la vida privada; y la necesidad de seguridad frente a nuevas formas de criminalidad y terrorismo (Ramonet, 2015, p. 25).

Entre los nuevos aplicativos para el control social y la vigilancia, se destaca la biometría, la cual ha dado lugar a varias formas de vigilancia e individualización de las personas. Por esta razón, ese instrumento es uno de los métodos más utilizados.



El origen de la biometría tiene una relación estrecha con la seguridad. Su génesis se remonta a la antropometría, un complejo sistema planteado por el inspector francés Bertillon, quien, en 1879, propuso un sistema de medidas corporales, con el fin de identificar delincuentes que reincidían en su accionar, tal como lo expresaron Jain y Pankanti (2008).

La biometría se ocupa del estudio, control y análisis de los datos biométricos, características únicas de los seres vivos que pueden ser utilizadas para su identificación. Estos datos podrían ser recolectados a través de diferentes técnicas: la de sistemas de reconocimiento de iris, que compila información desde el ojo del sujeto; el reconocimiento dactilar, que recoge datos de las huellas dactilares de los dedos; el reconocimiento vascular, que extrae el patrón único de las venas de la mano o el dedo, y el reconocimiento facial, que analiza las características únicas faciales de una persona.

De este modo, las peculiaridades que usa la biometría con el propósito de identificar a los sujetos son perfectas y únicas para la individualización y el control de estos. Sin embargo, dependiendo de que método se concentre en una u otra característica, la identificación será efectiva en menor o mayor medida.

En la biometría, se encuentran dos grandes grupos que se encargan del estudio de las características físicas: 1) biometría estática y 2) biometría dinámica (estudio del movimiento y de los gestos de la persona).

Sin importar que tipo de biometría se esté usando, esta debe contar con los siguientes requisitos mínimos para funcionar: 1) una base de datos con la característica biométrica de la persona, 2) un mecanismo para capturar las características biométricas y 3) un procedimiento para comparar dichas características con las almacenadas en la base de datos. Realizados estos pasos, el sistema biométrico permite responder dos preguntas: 1) ¿qué datos biométricos posee X persona? y 2) ¿corresponden los datos biométricos de X persona a los almacenados en la base de datos? Esto es consecuencia de la adiaforización de Bauman (2013), pues, al eliminar la moralidad de los actos y convertirlos en neutro, se obtiene un sistema que puede responder objetivamente sobre la identidad de una persona, sin necesidad de la intervención de esta.

Ahora bien, en los sistemas biométricos, se encuentran los de reconocimiento facial. Su característica radica en que son de los que más ventajas ofrecen para identificar a alguien, puesto que no requieren que el sujeto vigilado interactúe directamente con el dispositivo.

El sistema de reconocimiento facial está conformado por tres partes básicas: 1) sistema de vigilancia, que se refiere a la parte mecánica, ya que está compuesto por las cámaras de vigilancia o de seguridad; 2) *software* de reconocimiento, el cual es el cerebro del mecanismo, porque se encarga de identificar y analizar los datos biométricos recogidos, y 3) bases de datos, formadas con los datos en los cuales se comparará la información biométrica obtenida. Si falta una de estas partes, no es posible realizar el reconocimiento facial.

Adicionalmente, el proceso de reconocimiento facial tiene las siguientes fases específicas de desarrollo: 1) detección: se determina el rostro a través del dispositivo elegido; 2) extracción de características faciales: el *software* de reconocimiento extrae las particularidades del rostro obtenido en una imagen, mediante el dispositivo; 3) comparación: las características faciales sustraídas se comparan con las almacenadas en la base de datos, y 4) reconocimiento o confirmación: el *software*, según un porcentaje determinado, establece, positiva o negativamente, si el rostro detectado es el que se encuentra en la base de datos. Tómese en cuenta que, aunque todos los componentes se encuentren en pleno funcionamiento, no se garantiza el desarrollo completo de las fases. Para que el sistema de reconocimiento facial sea efectivo, se debe tener en cuenta las condiciones ambientales y particulares del sujeto por reconocer, tales como las condiciones de luz, ángulo, lejanía del rostro y etnia racial.

Es importante recordar que cuando se habla de tipos de reconocimiento facial en realidad se está discutiendo sobre técnicas de reconocimiento. Este sistema tiene diferentes formas para distinguir un rostro; se diferencia entre ellas en su efectividad y forma de recolectar los datos faciales.

Las técnicas de reconocimiento se dividen en varios grupos. Primero, la tradicional, se basa en reconocer y extraer datos a través de imágenes fijas; se mapea el rostro humano para clasificar sus características. Tiene una gran desventaja, pues depende mucho de las condiciones de luz, así como del ángulo de visión del rostro. La segunda táctica, el reconocimiento en tres dimensiones, requiere un dispositivo adicional (generalmente, un sensor láser) que captura la forma del rostro en 3D. Su mayor ventaja es que no se ve afectada por las condiciones de luz y, además, una vez que está mapeado el rostro, es más fácil reconocerlo desde diferentes ángulos; pero, igualmente, su desventaja radica en que, para lograr la captura del rostro en 3D, el sujeto debe estar quieto frente al sensor. Por último, se encuentra el método de análisis de textura de la piel, caracterizado por individualizar líneas, formas y tono de la piel de la persona por identificar. Funciona, en gran medida, de igual forma que los métodos tradicionales, por lo que cuenta con sus mismas ventajas y desventajas.



El uso del reconocimiento facial como sistema de seguridad genera diversas controversias. Muestra de estas es lo sucedido con Amazon Rekognition, creado por la compañía que lo denomina. Este tipo de tecnología, en principio, podía ser adquirido por países como Estados Unidos, donde el constante miedo al ataque se vio reforzado por hechos como los del 11 de septiembre del 2001. El obtener estos sistemas permite mantener un control de las personas, sin que, algunas veces, estas se percaten de su existencia.

El 22 de mayo del 2019 se llevó a cabo una reunión, por parte de los accionistas de Amazon, en la cual, si bien se trataron diversos asuntos respecto a la compañía, se abordó, en especial, la venta del sistema de reconocimiento facial Rekognition al ejército de Estados Unidos. Esto como consecuencia de la preocupación de los accionistas ante las posibles amenazas que dicho sistema puede presentar a los derechos civiles y humanos.

Rekognition, como todos los demás sistemas de reconocimiento facial, permite identificar y vigilar a todas aquellas personas que estén a su alcance; sin embargo, preocupa, en especial forma, porque el mayor interesado en su uso es el ejército de Estados Unidos.

Según un reportaje de Leo Kelion de la BBC, en mayo de 2019, un estudio realizado por el

Pero un estudio publicado en enero por investigadores del Instituto de Tecnología de Massachusetts y la Universidad de Toronto sugirió que los algoritmos de Amazon sufrían un mayor prejuicio racial y de género que cuatro productos de la competencia. Dijo que Rekognition tenía una tasa de error del 0% al clasificar a los hombres de piel más clara como tales dentro de una prueba, pero una tasa de error del 31,4% al clasificar a las mujeres de piel más oscura. (Kelion, 2019).

Este sistema no es capaz de garantizar un 100 % de efectividad o, por lo menos, un alto grado de esta, dando lugar a la existencia de falsos positivos, lo que conlleva una vulneración de los derechos de aquellas víctimas de ese fenómeno.

Ahora bien, el caso de Amazon Rekognition es una muestra de los tantos sistemas de reconocimiento facial que pueden ser usados con base en el discurso de seguridad, con el objetivo de garantizar una vigilancia sobre los elementos que representen una amenaza para lo que ella desea proteger.

El reconocimiento facial como sistema de vigilancia ante los derechos a la intimidad y privacidad

Lo anotado en líneas anteriores ratifica que el discurso de seguridad, como fundamento para el uso de un sistema de reconocimiento facial, no es garantía de que los supuestos preceptos de dicha seguridad se cumplan, ni mucho menos de que se cuide el derecho a la intimidad y privacidad.

En palabras de Bauman y Lyon recordemos que

Ésta es la paradoja del mundo saturado de dispositivos de vigilancia, sea cual sea el propósito que persiguen: por un lado, estamos más protegidos que cualquier generación anterior; por otra parte, sin embargo, ninguna generación anterior, o preelectrónica, experimentó como la nuestra esa sensación cotidiana de inseguridad a todas horas (Bauman y Lyon. 2013, p. 25).

La población preelectrónica también sentía un gran temor, solo que los métodos que se utilizaban en ese entonces tenían otro tipo de perspectiva. Si bien la seguridad no se puede separar del discurso del poder, sí se puede hablar acerca de cómo los métodos de persuasión y su fin han ido cambiando.

Primero, se observa un discurso de poder encaminado a la disciplina de los cuerpos, con el fin de no alterar el “orden social” establecido. No obstante, es preciso resaltar que, para dicho objeto, se deseó crear estructuras como el panóptico, donde existía un vigilante y un vigilado. Aquí se encuentran dos perspectivas: una disciplina de bloque, con la que se rompe todo contacto, toda comunicación del detenido con su alrededor, y otra de mecanismo, con la cual se busca mejorar el poder, puesto que este se vuelve mucho más rápido, cuando logra controlar a todos desde una torre con visibilidad a cada una de las celdas. Se llega, así, al fin último de la disciplina, en la que no solo se busca hombres productivos, sino también “normales”.

A pesar de lo anterior, hoy se puede replantear el discurso del poder, ya no desde la palabra, sino a partir de los sistemas binarios, que consisten en una forma de escritura informática mediante la que los números se expresan en dos cifras numéricas, las cuales son uno o cero. Por tanto, el panóptico ya no es el sistema más eficiente para vigilar un objetivo en esta época de sistemas binarios. Como lo dijo el sociólogo Polaco Bauman, el sinóptico, a diferencia del panóptico, ya no se centra en una vigilancia local, por el contrario, se traslada al ciberespacio, convirtiéndose en una herramienta de vigilancia de tipo global, donde las personas se encuentran a su voluntad.



Las nuevas formas de vigilancia encaminadas hacia la “seguridad”, como se dijo, ya no buscan disciplinar el cuerpo y el alma; de modo opuesto, trabajan con el procesamiento de la información, con el fin de observar, evaluar, controlar. Así lo señaló Lyon:

La información, más que en lo que afirmaba Foucault, permite una nueva transparencia en la que no solamente los ciudadanos como tal sino todos nosotros, en cada uno de los roles que asumimos en nuestra vida cotidiana, somos constantemente controlados, observados, examinados, evaluados, valorados y juzgados (Bauman y Lyon, 2013, p. 15).

De esta forma, se puede afirmar que la seguridad no es estática, es maleable, pues los métodos de vigilancia, control y castigo cambian según la época y necesidad de la población, así como los medios que se implantan en ella. Es por esto por lo que surgieron elementos como el sinóptico, que responden a la nueva vida líquida, en la que se encuentra envuelta la humanidad. Con tal mirada sinóptica, se ofrece una aparente seguridad, a partir de la recolección y del procesamiento de los datos compartidos de manera voluntaria por las personas, que ponen en riesgo su derecho a la intimidad.

Conclusión

Es innegable que en el mundo globalizado en el que existe el uso de tecnologías de reconocimiento facial este ha aumentado. En tal contexto, es imperativo entender y tener el conocimiento científico de una ciencia como la biometría; se hace importante comprender su funcionamiento, así como sus alcances, límites y contradicciones.

No obstante, el auge del uso de los sistemas de vigilancia no se ha dado de manera causal. Como se vio reflejado en la presente investigación, dichos sistemas son parte de una maquinaria compleja, en la cual se ha aplicado el discurso de seguridad. Se ha aprovechado el constante miedo que acosa a la sociedad, con el fin de justificar el uso de nuevas herramientas, cada vez más efectivas, para el control y la vigilancia de la población. En este sentido, los estudios de seguridad en el siglo XXI deben ser retroalimentados desde las nuevas dinámicas de la sociedad, con énfasis en cómo se afecta la comunidad del miedo y cómo intervienen las tecnologías novedosas tanto de seguridad como de control en este ecosistema.

Por último, se debe tener en cuenta que el estudio de los sistemas de vigilancia masiva se nutre de aportes teóricos transdisciplinarios, pues el uso de estas herramientas genera una afectación que se puede medir en distintas áreas y ámbitos sociales.

Referencias

- Álvarez, M. (2015). Derecho al olvido en internet: el nuevo paradigma de la privacidad en la era digital. *Derecho al olvido en internet*, 1-144.
- Alto Comisionado de Las Naciones Unidas para los Refugiados. *Promoción y protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo*. <https://www.acnur.org/fileadmin/Documentos/BDL/2016/10390.pdf>
- Bauman, Z. (1999). *La globalización Consecuencias Humanas*. Traducción de Daniel Zadunaisky. Buenos Aires. Fondo de la Cultura y la Economía.
- Bauman, Z. (2007). *Tiempos Líquidos. Vivir en una época de incertidumbre*. Traducción de Carmen Coral. España: Editorial Tusquets Editores, S. A.
- Bauman, Z. (2010). *Miedo Líquido*. Traducido por Albino Santos Mosquera. España: Editorial Ediciones Paidós.
- Bauman, Z. y Lyon, D. (2012). *Vigilancia Líquida*. España: Editorial Ediciones Paidós.
- Bjørn, M. (1996) Conceptos sobre seguridad: nuevos riesgos y desafíos. Reviewed work(s): Source: *Desarrollo Económico*, vol. 36, no. 143, pp. 769-792. Published by: Instituto de Desarrollo Económico y Social Stable. <http://www.jstor.org/stable/34672>
- Childress, S. (2010). *The right to privacy*. New Orleans, Louisiana: Editorial Quis Prod Books.
- Conesa, M. (1984). *Derecho a la intimidad, informática y Estado de Derecho*. Valencia, España: Universidad de Valencia.
- Convención Americana de Derechos Humanos, del 7 al 22 de noviembre, 1969. <http://relap.usta.edu.co/images/1969-Convencion-Americana-sobre-Derechos-Humanos.pdf>
- Convención Europea para la Protección de los Derechos Humanos y de las Libertades Fundamentales, 1 de noviembre, 1998. <https://www.acnur.org/fileadmin/Documentos/BDL/2002/1249.pdf>
- Convención sobre los Derechos del Niño, 20 de noviembre, 1989. <https://www.un.org/es/events/childrenday/pdf/derechos.pdf>
- Convención internacional sobre la protección de los derechos de todos los trabajadores migratorios y de sus familiares. Adoptada por la Asamblea General en su resolución 45/158, del 18 de diciembre, 1990. <https://www.ohchr.org/sp/professionalinterest/pages/cmw.aspx>



- Convenio 108 del Consejo de Europa, del 28 de enero de 1981, para la protección de las personas respecto al tratamiento automatizado de datos de carácter personal. <https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/Convenio108-19811.pdf>
- Declaración Universal de Derechos Humanos, 10 de diciembre, 1948. https://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/spn.pdf
- Diccionario panhispánico del español jurídico (2020). <https://dpej.rae.es/lema/intimidad>
- Directiva 95/46/ del Parlamento Europeo y del Consejo, 1995. <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:es:HTML>
- Directiva 2016/680 del Parlamento Europeo y del Consejo, 2016. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=uriserv:OJ.L_.2016.119.01.0089.01.SPA
- Foucault, M. (1975). *Vigilar y Castigar. Nacimiento de la prisión*. Traducido por Aurelio Garzón del Camino. Siglo XXI Editores, S. A. Buenos Aires, Argentina.
- Foucault, M. (1976). *Defender la Sociedad. Curso en Collage de France*. Fondo de la Cultura y la Economía. Buenos Aires, Argentina.
- Foucault, M. (1977). *Seguridad, Territorio y Población. Curso en Collage de France*. Fondo de la Cultura y la Economía. Buenos Aires, Argentina.
- Herrán, I. (1999). *La violación de la intimidad en la protección de datos personales*. Madrid, España. Editorial Dykinson.
- Jain, A. K. y Pankanti, S. (2008). Beyond fingerprinting. *Scientific American*, 299 (3), 78-81.
- Kelion, L. (2019). Amazon heads off facial recognition rebellion. BBC. <https://www.bbc.com/news/technology-48339142?fbclid=IwAR1YU0eScJofK0DxscAd-Gzk55-n0SzG7417N23Stz84V7fHeJv62qEZEGx4>
- Larson, B. Strong, A. Bieler, K. Imboden H. Hanlon, E. Berndt, J.. (1994). Publicado para el Programa de las Naciones Unidas para el Desarrollo (PNUD). Informe sobre desarrollo humano. http://hdr.undp.org/sites/default/files/hdr_1994_es_completo_nostats.pdf
- Lucena, I. (2014). *El concepto de la intimidad en los nuevos contextos tecnológicos. La protección jurídica de la intimidad y de los datos de carácter personal frente a las nuevas tecnologías de la información y comunicación*. Coords. Alfonso Galán Muñoz y Mónica Arribas.
- Møller, B. (1996). Conceptos sobre seguridad: nuevos riesgos y desafíos. *Desarrollo Económico*, 769-792.

Naciones Unidas. (2011). Anotaciones a la agenda n.º 17, periodo de sesiones del Consejo de Derechos Humanos. https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.1_sp.pdf

Naciones Unidas. Asamblea General. (2016). El derecho a la privacidad en la era digital.

Naciones Unidas. (2016). Promoción y protección de derechos humanos y las libertades fundamentales en la lucha contra el terrorismo. <https://www.acnur.org/fileadmin/Documentos/BDL/2017/10877.pdf>

Orozco, G. (2015). *El concepto de la seguridad en la teoría de las relaciones internacionales*. <http://www.flacsoandes.edu.ec/system/tdf/%25f/agora/files/conceptoseguridadtri.pdf?file=1&type=node&id=62702>

Pacto Internacional de Derechos Civiles y Políticos, 16 de diciembre, 1966. https://www.ohchr.org/documents/professionalinterest/ccpr_sp.pdf

Ramonet, I. (2015). *El Imperio de la Vigilancia*. Traducción de Martín Sacristán. Madrid: Editorial Clave Intelectual.



