GRAN HERMANO 4.0: UNA APROXIMACIÓN A LA UTILIZACIÓN DE SISTEMAS DE RECONOCIMIENTO FACIAL AUTOMATIZADO EN CONSUMIDORES Y USUARIOS[1]

María Celeste Colombo[2]

1. INTRODUCCIÓN

En la era actual, los sistemas de identificación biométrica, y en particular el reconocimiento facial automatizado, han emergido como herramientas cruciales en diversas industrias como apoyo para la gestión de identidades, la seguridad y el marketing personalizado. Estas tecnologías, impulsadas por el desarrollo de la inteligencia artificial[3], han redefinido la manera en que las instituciones y las corporaciones interactúan con los individuos.

Sin embargo, su creciente implementación también ha planteado importantes interrogantes éticos y legales, especialmente en relación con la protección de datos personales y la privacidad.

El reconocimiento facial, como una de las formas más directas y omnipresentes de identificación biométrica, utiliza algoritmos de IA para analizar características faciales únicas en imágenes o videos. Esta tecnología, que puede operar de manera pasiva y sin el consentimiento explícito del individuo, plantea desafíos significativos en términos de consentimiento, protección de datos, sesgos, precisión, discriminación y posibles abusos entorno a su utilización.

[1] Cítese como Colombo, C. 2023. Gran hermano 4.0: una aproximación a la utilización de sistemas de reconocimiento facial automatizado en consumidores y usuarios, Estudios sobre Jurisprudencia, 350-369.

[2] Abogada. Facultad de Derecho y Ciencias Sociales (UNC). Magister en Derecho Civil Patrimonial en la Pontificia Universidad Católica Argentina (UCA). Jefa de Trabajos Prácticos de Obligaciones Civiles y Comerciales - Facultad de Derecho (UBA). Directora del Programa de Inteligencia Artificial y Derecho, Escuela de Negocios, UCES. Especialización en Responsabilidad Civil Contractual y Extracontractual. Facultad de Derecho, Universidad de Castilla - La Mancha (UCLM). Profesora invitada en cursos de posgrado en diversas universidades argentinas. Vicepresidenta del Grupo de Trabajo de Nuevas Tecnologías, Prevención y Seguros- AADS- AIDA Rama Argentina. Secretaria del Instituto de Derecho Civil del CPACF. Directora de la Sección Novedades en el Derecho de Seguros de la Editorial El Derecho. Autora de diversos artículos doctrinarios en su área de su especialización.

[3] En adelante se utilizará el término inteligencia artificial o la abreviatura IA indistintamente.

A medida que el desarrollo de la IA avanza, la precisión y posibilidades de aprovechamiento de estos sistemas mejoran, aumentando su atractivo para aplicaciones tanto gubernamentales como privadas.

Actualmente, al alcance de todos, existen herramientas en línea que utilizan reconocimiento facial para encontrar fotos que coincidan con el mismo rostro que obra en una imagen que hemos subido previamente[4].

Por su parte, en materia de consumo, las empresas proveedoras de bienes y servicios están aprovechando cada vez más de las posibilidades que les ofrece la utilización de sistemas de IA. A través de distintas aplicaciones y dispositivos interconectados se alimentan de nuestros datos con el objeto de perfilarnos y segmentarnos según características demográficas (edad, género, educación, etc.), patrones de comportamiento (frecuencia de conexión, tiempo en línea, polarización ideológica, actividad en redes, etc.), y hábitos de consumo (horario de compras online, visitas a páginas online, búsqueda de productos y servicios, etc.).

Ante este panorama, la regulación de estas tecnologías se ha convertido en un tema de debate intenso a lo largo y ancho del orbe. Por un lado, existe la necesidad de fomentar la innovación y aprovechar los beneficios potenciales de estos sistemas en términos de seguridad y eficiencia. En contrapartida, se torna imperativo proteger los derechos fundamentales de los individuos, en especial el derecho a la privacidad, a la autodeterminación informativa, y a la protección de sus datos personales.

El lado oscuro de este tipo de tecnología es evidente. La naturaleza intrusiva del reconocimiento facial, sumado a su posible uso indebido, puede devenir en un exceso de vigilancia algorítmica en perjuicio de la autonomía personal de los seres humanos, y en particular de los consumidores y usuarios.

Además, la implementación de estas tecnologías puede acentuar discriminaciones en grupos vulnerables ya que los algoritmos de reconocimiento facial, a menudo entrenados con conjuntos de datos sesgados, pueden perpetuar y amplificar las desigualdades ya existentes. Esto plantea interrogantes legales en contextos sensibles como la utilización de este tipo de tecnología en toma de decisiones automatizadas[5] en materia de consumo.

La toma de decisiones automatizadas puede generar situaciones injustas ya que ponen al consumidor en una situación de vulnerabilidad. Más aún cuando los proveedores que

[4] Véase https://www.xataka.com/privacidad/esta-herramienta-reconocimiento-facial-puede-utilizar-asusta-bien-que-funciona [Consultado: 28/11/2023].

[5] En adelante toma de decisiones automatizadas o su abreviatura en inglés ADM (automated decisión making).

utilizan ADM no pueden explicar por qué sus sistemas arribaron a una conclusión en detrimento de otra, lo cual puede vulnerar los derechos de los consumidores y usuarios.

El reconocimiento facial automatizado y los sistemas de identificación biométrica presentan un complejo entramado de beneficios y desafíos. Este trabajo tiene como objetivo profundizar en estas cuestiones, con el objetivo de entender las capacidades y limitaciones de este tipo de tecnología, y establecer una aproximación a las consecuencias legales de su utilización en consumidores y usuarios.

2. ¿QUÉ ES EL RECONOCIMIENTO FACIAL AUTOMATIZADO?

Podríamos empezar por señalar que el reconocimiento facial es una categoría dentro de los que se consideran datos biométricos.

El Reglamento General de Protección de Datos europeo[6] (RGDP) en su artículo 4.14 señala que datos biométricos constituyen 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[7].

Así, pueden obtenerse datos biométricos a través de sistemas de reconocimiento de voz, reconocimiento de huellas dactilares, reconocimiento de la retina o el iris, etc.

La propuesta de Reglamento Europeo sobre IA define a los sistemas de identificación biométrica remota como aquellos sistemas de IA destinado a identificar a distancia a personas físicas comparando sus datos biométricos con los que figuren en una base de datos de referencia, sin saber de antemano si la persona en cuestión se encontrará en dicha base de datos y podrá ser identificada, con independencia de la tecnología, los procesos o los tipos de datos biométricos concretos que se usen.

Como subespecie de los sistemas de identificación biométrica, el reconocimiento facial automatizado puede ser utilizado en tiempo real o diferido.

En el caso de los sistemas en tiempo real, la recogida de los datos biométricos, la comparación y la identificación se producen de manera instantánea o casi instantánea. En este tipo de sistemas el uso de material es en directo, o casi de manera inmediata ya sea a

[6] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE. En adelante RGPD.

[7] Esta definición coincide con la establecida en el art. 3.33 de la Propuesta de Reglamento del Parlamento Europeo y del Consejo en materia de Inteligencia Artificial (Ley de Inteligencia Artificial). Online: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52021PC0206 [consultado el 20/11/2023].

través de grabaciones de vídeo generadas por una cámara u otro dispositivo con funciones similares.

En cambio, en los sistemas en diferido los datos ya se han recabado y la comparación e identificación se producen con una demora significativa, ya sea que utilicen imágenes o grabaciones de vídeo captadas por cámaras de televisión en circuito cerrado o dispositivos privados, que se han generado antes de aplicar el sistema a las personas físicas en cuestión.

En pocas palabras, el reconocimiento facial automatizado es aquel que utiliza sistemas de IA como método para identificar la identidad de una persona utilizando su rostro, ya sea mediante imágenes o filmaciones ya sea en tiempo real o diferido.

Ahora bien, ¿cómo funciona el reconocimiento facial?

Un sistema de reconocimiento facial tiene por objetivo *matchear* rostros de las personas que son obtenidas mediante dispositivos de video, con aquellas imágenes de individuos que se encuentran en una base de datos. Esta base de datos puede corresponderse a listas predeterminadas por organismos públicos o privados que contienen fotografías de cualquier persona (hayan cometido algún delito o no), o bien imágenes provenientes de redes sociales, páginas web, plataformas digitales, etc.

Los sistemas de reconocimiento facial funcionan de la siguiente manera (Cherradi, 2020; Pérez y Madrid, 2021; Mudditt, 2022):

a) *Detección de rostros*: como primer paso la cámara detecta la imagen del rostro de una persona, esta puede ser seleccionada incluso entre una multitud;

b) *Análisis facial*: En esta etapa se analiza la imagen del rostro, el sistema lee la morfología de la cara, ya sea la distancia entre los ojos, la profundidad de las cuencas orbitales, la distancia desde la frente hasta el mentón, la forma de los pómulos y el contorno de los labios, las orejas y el mentón. El objetivo es identificar los puntos de referencia faciales que son claves para distinguir un rostro de otro;

c) *Transformar la imagen en datos*: en este momento el sistema convierte la imagen en un conjunto de información digital, es decir datos que conforman un código denominado *huella facial*. Así, cada rostro tiene su propia huella facial diferente y distinguible de cualquier otro;

d) *Matcheo facial*: el paso siguiente es comparar esa huella facial con una base de datos de otras caras conocidas. Una vez logrado el *matcheo* positivo con una imagen en una base de datos de reconocimiento facial se toma una decisión determinada conforme la finalidad del sistema.

De igual modo, el reconocimiento facial, como método de identificación, puede reconocer dos variantes:

a) *sistema de reconocimiento facial a los fines de la autenticación*, que a su vez reconoce dos procesos según la etapa de recogida del dato biométrico: a1) *como método onboarding*: a través de este procedimiento se identifica el rostro de una persona para registrarlo y asociarlo a una identidad, de tal forma que quede grabado en el sistema; y a2) *como método de verificación*: el sistema autentifica a la persona, luego se cruza la imagen de la persona con las ya existentes en la base de datos. El sistema autoriza el acceso de aquella persona cuyo rostro coincida con una identidad ya registrada.

b) *sistema de reconocimiento facial a los fines de la identificación*, que no es otra cosa que la comparación entre imágenes de una determinada persona con la existente en una base de datos para identificarla e individualizarla (Santisteban Galarza, 2021; Gallego Rodríguez, 2022).

En la actualidad, este tipo de tecnología es de un uso ampliamente difundido.

Aunque parezca extraño, muchas personas en nuestro país utilizan la tecnología de reconocimiento facial con regularidad. Por ejemplo, para desbloquear un teléfono inteligente, para confirmar la identidad en una aplicación bancaria o monedero virtual, para ingresar al trabajo, etc. A nivel gubernamental quizás el caso más paradigmático sea el control que se hace en Migraciones de cada Estado, el sistema de Reconocimiento Facial de Interpol (IFRS) que almacenan las imágenes faciales enviadas por más de 179 países, lo que la convierte en una base de datos policiales de ámbito mundial única[8]. En el ámbito local, el Sistema de Reconocimiento Facial de Prófugos (SRFP) implementado por el gobierno porteño, declarado inconstitucional en primera instancia, pero avalado posteriormente en segunda instancia siempre que se cumpla con los requisitos exigidos por la Justicia[9].

En materia regulatoria, el RGPD europeo, en principio, establece la prohibición del tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual y/o la orientación sexual de una persona física. Salvo, claro está, el consentimiento expreso de la persona, cuando el tratamiento de los datos es necesario para el cumplimiento de obligaciones y el ejercicio de

[8] Véase https://www.interpol.int/es/Como-trabajamos/Policia-cientifica/Reconocimiento-facial [Consultado: 23/11/2023].

[9] Véase https://www.perfil.com/noticias/politica/justicia-prohibio-ciudad-buenos-aires-buscar-profugos-a-traves-camaras-reconocimiento-facial.phtml [Consultado: 23/11/2023].

derechos específicos del responsable del tratamiento o del interesado en el ámbito del derecho laboral, de la seguridad y protección social. Asimismo, cuando el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento; o el tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicos. En suma, se refiera al elenco de supuestos de excepción establecidos en el artículo 9.2 RGPD.

Por último, respecto de los tratamientos biométricos que se realicen bajo toma de decisiones automatizadas (ADM), el artículo 11 Directiva 2016/680 exige medidas especiales y adecuadas para salvaguardar los derechos y libertades del interesado. En particular, el derecho a la doble instancia, es decir a obtener la intervención humana en la toma de decisión.

Además, se prohíbe la elaboración de perfiles que conduzcan a la discriminación de personas físicas sobre la base de datos sensibles, es decir que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o a la vida sexual o las orientaciones sexuales de una persona (artículos 10 y 11.3 Directiva 2016/680).

Por su parte, la Propuesta de Reglamento en materia de IA en el artículo 5.1.d establece la prohibición del uso de sistemas de identificación biométrica remota en tiempo real en espacios de acceso público con fines de aplicación de la ley, salvo para: a) la búsqueda selectiva de posibles víctimas concretas de un delito, incluidos menores desaparecidos; b) la prevención de una amenaza específica, importante e inminente para la vida o la seguridad física de las personas o de un atentado terrorista; y c) la detección, la localización, la identificación o el enjuiciamiento de la persona que ha cometido o se sospecha que ha cometido alguno de los delitos como terrorismo, trata de humanos, explotación infantil, entre otros.

Por último, es necesario recordar que *"*el principio de transparencia de protección de datos exige toda una serie de información sobre la existencia del sistema de reconocimiento, elementos básicos de funcionamiento y recepción de datos y destino de los mismos" (Cotino Hueso, 2022).

Así, la Propuesta de Reglamento establece que se aplicarán obligaciones de transparencia a los sistemas de IA que se utilicen para detectar emociones o determinar la asociación a categorías (sociales) concretas a partir de datos biométricos, entre ellos los sistemas de reconocimiento facial automatizado. Cuando una persona interactúe con un sistema de IA

cuyas emociones sean reconocidas por medios automatizados es preciso notificarla de tal circunstancia.

3. RECONOCIMIENTO FACIAL AUTOMATIZADO Y MARKETING

Históricamente, cuando de publicidad se trata, el legislador ha intentado su regulación en atención a la vulnerabilidad de los consumidores y usuarios. Lo cierto es que los consumidores se encuentran expuestos al bombardeo constante de mensajes tendientes a inducir la compra de un producto y/o servicios.

Así, en la Directiva 2006/114/CE sobre publicidad engañosa y publicidad comparativa del Parlamento Europeo y del Consejo de la Unión Europea se ha definido a la publicidad como "toda forma de comunicación realizada en el marco de una actividad comercial, industrial, artesanal o liberal con el fin de promover el suministro de bienes o la prestación de servicios, incluidos los bienes inmuebles, los derechos y las obligaciones" (2006, artículo 2.A).

En Argentina, la doctrina distingue entre publicidad lícita e ilícita.

Dentro de la publicidad ilícita se distingue entre engañosa y abusiva. La publicidad comparativa solo será ilícita si no cumple con determinados requisitos (Chamatropulos, 2019). Si bien el artículo 8 de la Ley de Consumo[10] regula sobre publicidad lícita, no define ni específica sobre publicidad ilícita.

Con la irrupción de las nuevas tecnologías la publicidad ha entrado en un giro vertiginoso, la exposición de los consumidores y usuarios a la publicidad se da a niveles nunca vistos.

La publicidad tradicional ha dado paso a la publicidad *online* que no solo se despliega a través de sitios *web* sino, también, mediante *apps*, motores de búsqueda, redes sociales, dispositivos electrónicos y *wearables*[11], etc. A través de ellos los proveedores ofrecen sus productos y servicios luego de prolijo perfilamiento de nuestras preferencias, pautas de consumo y comportamiento en línea.

Actualmente, con cada *me gusta* en nuestras redes sociales, cada interacción, cada búsqueda en los diferentes motores de búsqueda, cada s*crolleo*[12] inocente en una tarde aburrida, cada una de las aplicaciones existentes en nuestro móvil, los seres humanos emitimos valiosos datos que pueden ser utilizados para nuestra huella digital.

[10] En adelante, Ley de Consumidor, ley de consumo, LDC indistintamente.

[11] Los dispositivos *wearables* son aquellos que pasan desapercibidos como accesorios o en el vestuario del usuario, por ejemplo, un reloj inteligente, pulseras, etc.

[12] Se denomina *scrollear* al desplazamiento que hacemos a lo largo de la pantalla de cualquier dispositivo táctil.

No solo conformamos este rastro digital con interacciones en las redes sino con los datos emanados por nuestros dispositivos electrónicos interconectados, los *wearables*, sensores telemáticos, etc.

La denominada huella digital no es otra cosa que la traza que dejamos a nuestro paso con cada interacción digital.

A través de nuestra huella digital es que las empresas obtienen una información precisa acerca de nuestras preferencias, hábitos, opiniones, patrones de conducta y consumo. Las empresas se sirven de estas técnicas para predecir el arribo de nuevos clientes y el patrón de aumento de los ingresos, anticipar la demanda de productos o servicios, prevenir la tasa de abandono, y trabajar no solo en la incorporación de clientes sino, fundamentalmente, en la retención de los considerados buenos clientes.

Al elaborar el perfil del cliente deseado pueden establecer comparaciones con los perfiles de clientes potenciales y concentrarse en la captación de aquellos que encuadren en el ideal seleccionado. Asimismo, segmentar clientes por categorías, nivel adquisitivo, preferencias de consumo, etc.

Ahora bien, ¿qué es un perfil digital?

Se define como *perfil* a "un conjunto de datos que caracterizan a una categoría de personas y que está destinado a ser aplicado a una persona"[13].

Asimismo, se denomina *perfilado* a la "técnica de procesamiento automático de datos que consiste en aplicar un 'perfil' a un individuo, particularmente para tomar decisiones que le conciernen o para analizar o predecir sus preferencias, comportamientos y actitudes personales"[14].

En consonancia con lo expuesto, podemos señalar que el RGPD establece que perfilamiento digital es

> toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias

[13] Definición receptada en el apartado 1-D del anexo a la Recomendación CM/Rec (2010) 13 del Comité de Ministros de los Estados Miembros sobre la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal en el contexto de la creación de perfiles.

[14] Definición receptada en el apartado 1-E del anexo a la Recomendación CM/Rec (2010) 13 del Comité de Ministros de los Estados Miembros sobre la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal en el contexto de la creación de perfiles.

> personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física (Artículo 4, apartado 4, del RGPD).

Así, es clave entender que la publicidad tradicional tiene los días contados.

Las nuevas tecnologías, la elaboración de perfiles digitales, y el aprovechamiento de los datos personales a través sistemas de IA impactan en la gestión y desarrollo de la publicidad.

En la actualidad se hace preciso hablar de la denominada publicidad dirigida o conductual[15] (*online behavioral advertising*). "Este tipo de publicidad es el que utiliza cookies o tecnología similar para rastrear (*tracking*[16]) al usuario de internet en su navegación" (Navas Navarro, 2015).

El objetivo principal de este tipo de publicidad es ofrecer anuncios dirigidos a los segmentos del mercado que por su comportamiento en línea tienen más probabilidades de estar interesados en la adquisición del producto y/o servicio. A modo de ejemplo: en IG cuando se trackea el *scrolleo* del usuario que visita determinadas cuentas vinculadas a consejos sobre cuidado facial, la red social asume que el consumidor está interesado en este tipo de temática por lo que muestra no solo cuentas afines, sino también anuncios publicitarios relacionados.

Entendemos que se puede señalar a la publicidad online dirigida como el género, y como especies se hace preciso diferenciar entre la publicidad conductual, de la publicidad contextual, la segmentada y publicidad social.

La *publicidad conductual* es aquella "basada en la observación continuada del comportamiento de los individuos. La publicidad comportamental busca estudiar las características de dicho comportamiento a través de sus acciones (visitas repetidas a un sitio concreto, interacciones, palabras clave, producción de contenidos en línea, etc.) para desarrollar un perfil específico y proporcionar así a los usuarios anuncios a medida de los intereses inferidos de su comportamiento" (Grupo de Trabajo de Protección de Datos del Artículo 29, 2010, p. 5). Cómo se podrá advertir el eje de este tipo de publicidad está en el *trackeo* en línea del consumidor para elaborar un perfil tendiente a proporcionar publicidad a medida de sus preferencias y pautas de comportamiento.

[15] Algunos autores la denominan *publicidad comportamental,* pero nos parece más apropiado la denominación *publicidad conductual.*

[16] *Tracking* es un término en inglés que significa rastrear. Este vocablo se ha vuelto moneda corriente y es adaptado al español como trackeo o trackear.

La *publicidad contextual*, en cambio, se basa en palabras claves –k*eywords*– que utiliza en plataformas de búsquedas el consumidor y/o usuario. A través de estas palabras claves se le ofrece al consumidor anuncios vinculados a dichas *keywords.* La diferencia está en que se refiere a un sitio concreto y determinado desde donde se proporciona publicidad acorde a las palabras claves previamente determinadas por el proveedor, y que son introducidas por el consumidor al interactuar con la plataforma.

La *publicidad segmentada* es aquella que se apoya en la segmentación derivada del perfilamiento previo de los consumidores y usuarios, es decir en las características proporcionadas por el usuario al registrarse. Por ejemplo: edad, sexo, ubicación, preferencias, etc.

Por último, la *publicidad social –social advertising–* es la publicidad que se genera a consecuencia de las interacciones de un usuario determinado en una red social. El *quid* en este tipo de publicidad es que se circunscribe a la interacción del individuo con otros en una red social a la que se ha inscripto. Utiliza la información y contactos que el propio consumidor ha suministrado al registrarse en la red, pero no lo *trackea* por fuera de ella (Pérez Bes, 2012).

En la práctica toda esta metodología empleada por las empresas proveedoras no se manifiestan por separado, sino que se utilizan de manera combinada según las necesidades del proveedor.

En trabajo nos detendremos en analizar la *publicidad conductual*, pues entendemos que existe una estrecha vinculación entre esta y el tema objeto de investigación.

A partir de la utilización de sistemas de IA con reconocimiento facial los proveedores están desplegando lo que denominamos el *marketing 4.0*.

El *marketing 4.0* es el desarrollo y aprovechamiento de la publicidad conductual en su máxima expresión, ya que el *trackeo* a los consumidores y usuarios no solo se despliega a su *huella digital,* sino que, además, pone énfasis en las emociones que expresan los consumidores al momento de ser expuestos no solo a publicidad sino a eventos, situaciones, productos y/o servicios para luego ser analizados a los fines de elaborar nuevas estrategias publicitarias.

El uso de sistemas de IA para la identificación de rostros permite el reconocimiento de emociones, categorizar a las personas, identificar rasgos basados en la personalidad, lectura de lenguaje corporal a los fines de detectar y/o predecir comportamiento.

Así, un sistema de reconocimiento facial automatizado desplegado en tiendas comerciales podría reconocer emociones en clientes para sugerir productos o servicios basándose en

emociones predominantes en un momento dado, en su historial de compras, preferencias y pautas de consumo. Y en función de los datos obtenidos, inducirlos a comprar de determinada manera a través de publicidad personalizada.

El *marketing 4.0* no es solo una posibilidad futura sino una inquietante realidad.

Cuando de emociones se trata todos nos acordamos de Riley y sus emociones en *Inside Out*[17]. Paul Ekman elaboró una teoría que señalaba que el ser humano presentaba seis emociones básicas: ira, alegría, miedo, asco/desprecio, tristeza y sorpresa. Estas emociones poseen la característica de ser universales por lo que pueden verse reflejadas en el rostro de cada ser humano y, por ende, ser distinguibles una de otra. Así, por ejemplo: cuando uno está enojado frunce el entrecejo, cuando está alegre eleva las mejillas, etc. (Sarrió, 2013).

A partir de esta teoría es que muchos ven como propicia la posibilidad de entrenar sistemas de IA para que detecten estas variaciones faciales con el objetivo de predecir el estado de ánimo de una persona. Es lo que se denomina *detección de emociones*.

Así, se ha desarrollado un sistema de reconocimiento de emociones en tiempo real utilizando expresiones faciales y señales. Funciona eficazmente aún con rotación de la cabeza del sujeto y con diferentes tonos de piel. El sistema tiene como objetivo ayudar a las personas con discapacidad física (sordomudas, por ejemplo), y a niños con autismo para enseñarles a reconocer sentimientos de terceros. Sin embargo, también puede ser utilizado como herramienta de *marketing* (Yang et al., 2018).

Actualmente en el campo del marketing y la publicidad, el reconocimiento facial se utiliza para estudiar las emociones de los consumidores de dos formas: emociones positivas y negativas. Tal como lo señalamos anteriormente, muchas de nuestras expresiones faciales de las emociones ya tienen un significado adaptativo que sirve para comunicar cierto tipo de emoción universal.

Los sistemas de reconocimiento facial automatizado aprovechan de las expresiones faciales que transmiten emociones para reconocerlas. De esta manera, ante un producto o servicio determinado pueden analizarse el rostro del cliente para predecir qué tipo de emoción lo atraviesa en ese momento determinado.

El reconocimiento facial automatizado tiene tres fases, a saber: a) obtención de la imagen en tiempo real; b) análisis de las expresiones y la conversión de estas en caracteres geométricos (curvas, distancia entre ojos, eje de la nariz, altura de los pómulos, etc.). El objetivo es establecer patrones que permita vincular una expresión con emoción y/o

[17] En español Intensamente es una película de Disney lanzada en el 2015.

satisfacción del cliente. Y c) clasificación de las emociones de un cliente hacia un producto en tres tipos: positiva, negativa o neutral. Una vez analizados los rostros de los consumidores, con un sistema se podría comprender cómo los clientes perciben el producto y/o servicio (Hassouneh et al., 2020).

En la era del *marketing 4.0* la publicidad conductual pivotea en los sistemas de reconocimiento facial automatizado a los fines del perfilamiento digital preciso de cada consumidor y/o usuario en tiempo real.

Asistimos a panóptico a cielo abierto donde la huella digital de cada uno de los consumidores puede ser rastreada para establecer pautas de consumo, preferencias y hábitos que permitan desplegar una publicidad personalizada según el tipo de cliente que se trate.

En la actualidad, en diversos lugares del planeta los proveedores han intentado utilizar estos sistemas de reconocimiento facial automatizado para desplegar publicidad conductual.

En Brasil, más precisamente San Pablo, la concesionaria del Metro de esa ciudad puso en marcha el denominado *Sistema Digital Interactivo de Puertas* (DID), este sistema utilizaba reconocimiento facial automatizado para inferir emociones según género, etnia y edad de las personas, con el objetivo principal de personalizar la publicidad en el ámbito del metro.

Este caso fue llevado a la justicia[18] ya que se consideró que violentaba los derechos de los consumidores y usuarios. En efecto pudo determinarse que existían equipos de grabación de imágenes de usuarios con fines publicitarios y estadísticos en las estaciones del subte, esas imágenes eran tomadas sin consentimiento expreso de los usuarios y se registraban con el objeto de ser analizadas por sistemas de reconocimiento facial.

La empresa concesionaria admitió que el objeto de estos equipos era obtener un análisis de las emociones de los usuarios frente a la publicidad que se desplegaba en el metro con fines estrictamente comerciales.

La justicia condenó a la prestataria ya que se infringió la ley de consumo brasilera y de protección de datos personales al no requerir el consentimiento previo para la recolección de imágenes. Asimismo, se violó el deber de información al no poner en conocimiento de los usuarios de la recopilación de imágenes faciales a los fines de analizar sus emociones frente a la publicidad existente en el ámbito del subte.

[18] Cfr. Tribunal de Justicia del Estado de San Pablo, "IDEC v. Concesionaria de la línea 4 del metro de San Pablo (ViaQuatro)". 7/5/2021, disponible en el boletín "La judicialización de los Sistemas de Reconocimiento Facial" elaborado por la Escuela de la defensa pública del MPD junto al Observatorio de Derecho Informático Argentino (O.D.I.A.).

Así, el tribunal estableció que conducta del demandado viola patentemente el derecho a la imagen de los consumidores que utilizan el servicio público, las disposiciones relativas a la protección especial otorgada a los datos personales sensibles recabados, además de la violación de derechos básicos de los consumidores, en particular la información y protección en relación con prácticas comerciales abusivas. Por otro lado, la utilización de sistemas de reconocimiento facial automatizado en el subte excede los fines y objetivos previstos en el contrato de concesión otorgado por el Estado.

La demanda interpuesta fue considerada admisible, la empresa no podrá utilizar datos biométricos o cualquier otro tipo de identificación de los consumidores y usuarios del transporte público sin acreditar el debido consentimiento del consumidor. Recordemos que el objetivo de la actora era en principio detener la recopilación de datos biométricos de los pasajeros de manera inmediata. Asimismo, se impuso una indemnización por daño moral colectivo.

La empresa recurre el fallo de primera instancia que es confirmado en mayo de este año por la alzada quién, además, elevó el monto otorgado en primera instancia en concepto de daño moral colectivo.[19]

4. IMPLICANCIAS DEL USO DE RECONOCIMIENTO FACIAL AUTOMATIZADO EN CONSUMIDORES

En nuestros días, la utilización de técnicas de vigilancia y análisis de datos biométricos han dejado de ser patrimonio de las principales agencias de inteligencia, tampoco están reservadas al control del tráfico migratorio en las fronteras.

Hoy en día el reconocimiento facial automatizado poco a poco está reconfigurando la manera en la que se hace publicidad. Las estrategias de marketing de las grandes empresas ponen foco principalmente en el comportamiento en línea de los consumidores, es a través del *trackeo* de sus interacciones en el mundo digital que desarrollar publicidad personalizada.

La denominada *online behavioral advertising* no es otra cosa que la materialización del Gran Hermano 4.0 ya que los proveedores monitorean día y noche el comportamiento *online* de los consumidores para definir la próxima estrategia publicitaria.

En materia de publicidad se perpetúa como mantra

[19] Tribunal de Justicia de San Pablo- Sala 8ª de Derecho Público- Recurso de Apelación- "IDEC V. CONCESIONARIA DE LA LÍNEA 4 DEL METRO DE SAN PABLO (VIAQUATRO)"- 10/05/2023- Apelación Civil: AC 1090663-42.2018.8.26.0100 São Paulo.

> el argumento de que es la emoción, y no la razón, el factor predominante a la hora de tomar las decisiones de compra. Bombardear una y otra vez a los consumidores con el mismo mensaje comercial no es suficiente. Crear anuncios basados en el viejo modelo de construir conciencia, despertar interés, generar deseo y orientar/provocar una acción ha quedado obsoleto. Los métodos tradicionales no son suficientes para desbloquear los secretos enterrados en el inconsciente del ser humano (Castellanos Quintana, 2013, p. 52).

Las grandes empresas han encontrado la manera de obtener de nosotros nuestros secretos más profundos. Aún no pueden leernos la mente, pero pueden leer nuestros rostros y su expresividad. Nos delatamos a través de nuestras reacciones ante los estímulos y nuestras facciones pueden demostrar interés, desagrado, felicidad, etc.

La implementación generalizada del reconocimiento facial y los sistemas de identificación biométrica en consumidores y usuarios abre caminos para desentrañar aquello que no decimos verbalmente, lo que sumado al análisis de nuestro comportamiento en línea nos expone como individuos de una manera formidable.

De más está decir que este tipo de tecnología si bien importa innovaciones significativas, también presenta una serie de problemáticas complejas. Los principales desafíos se plantean en torno a la privacidad, el consentimiento, discriminación algorítmica, y que la potencial vigilancia masiva degenere en manipulación algorítmica.

En innumerables situaciones, las personas pueden no ser conscientes de que sus datos biométricos están siendo recopilados, procesados y almacenados, lo que viola los principios fundamentales de consentimiento informado, autodeterminación informativa y autonomía de la voluntad. Asimismo, la recopilación de datos biométricos a gran escala presenta un importante punto de dolor en términos de seguridad de los datos, ya que el proveedor podría sufrir una fuga de información y/o hackeo.

Por otro lado, la discriminación algorítmica es un problema serio cuando de sistemas de IA hablamos ya que, si las bases de datos de entrenamiento no son lo suficientemente diversos o contienen sesgos preexistentes, pueden mostrar tasas de error desproporcionadamente altas para ciertos grupos demográficos provocando discriminación en grupos de por si vulnerables.

La colocación de cámaras de reconocimiento facial automatizado en anuncios de productos para recopilar información personal como edad, género e indicadores emocionales potenciales pueden impactar en un reconocimiento erróneo dando lugar a malentendidos

que importen asumir por ejemplo preferencias sexuales no reconocidas por la propia persona.

Finalmente, el uso de tecnologías de reconocimiento facial por parte de empresas genera alguna preocupación ya que puede erosionar las libertades civiles a través de la manipulación algorítmica.

La publicidad conductual apunta a la vigilancia exhaustiva del comportamiento en línea del consumidor con el fin de anticipar, de predecir, patrones de consumo a los fines de ofrecer nuevos productos y servicios.

El *trackeo* constante de los consumidores y usuarios importa una vigilancia exacerbada sobre todo tipo de información, preferencias, productos y/o servicios correspondientes a nuestro historial de consumo. Esto empuja a los sistemas de IA a envolvernos en una especie de halo o efecto burbuja que diseña una realidad paralela conformada por todo aquello que consumimos históricamente. Así, todo aquello que no se ajusta a los parámetros establecidos por ese filtro de búsqueda será apartado.

La publicidad conductual puede reducir nuestra esfera de autonomía de la voluntad al influir en nuestros comportamientos analógicos, más aún inducir a grupos sociales a desplegar determinada conducta alentados por lo que se convierte en *tendencia* en un momento dado.

Asimismo, esta personalización de la información realizada por los algoritmos está basada en nuestro perfil digital. Cada uno de nosotros tiene una burbuja particular, es decir un universo personal y único de información basado en nuestra experiencia en línea. Dicho de otro modo, lo que hay en nuestra *filter bubble* depende de quiénes somos y qué hacemos al interactuar virtualmente. Justamente es aquello de lo cual aprovecha la publicidad conductual.

Lo cierto es que los algoritmos y el efecto burbuja que crean entorno a cada uno de nosotros puede interferir en nuestras preferencias y pautas de consumo en beneficio de quienes diseñan y se aprovechan de los algoritmos de filtro, es decir empresas proveedoras de bienes y servicios de todo tipo. Lo que nos lleva a plantearnos si no es una forma de manipulación, lo que denominamos manipulación algorítmica.

Si a ello le sumamos los sistemas de reconocimiento facial automático se forma la tormenta perfecta, ya que los algoritmos nos inducirán a consumir todo aquello que consideren se corresponden con nuestra preferencia y/o que sea apropiado según la emoción que nos invada en ese momento.

Así, finalmente los algoritmos editarán el contenido/información que consumimos por lo que nuestro derecho a buscar, elegir y consumir libremente se convertirá en la expresión de deseo del proveedor de turno. De esta manera, los proveedores usando sistemas de IA se aprovecharán de nuestros sesgos y vulnerabilidades cognitivas al incentivarnos a consumir solamente la información, producto y/o servicio que se viraliza o se convierte en tendencia (Colombo, 2023).

En suma, "no hacen falta excesivas explicaciones de por qué queda amedrentada la sociedad democrática y lo difícil que es vivir una vida digna si por el mero hecho de ir a comprar el pan es posible que controlen nuestros movimientos, identifiquen si somos una persona buscada por cualquier motivo, y capten datos para evaluar nuestro comportamiento o lo predigan" (Cotino Hueso, 2023, pág. 71).

Ante este panorama, ¿qué esperar?

En primer lugar, es necesario establecer como requisito innegociable la exigencia de consentimiento explicito para la utilización de este tipo de tecnología en consumidores. Asimismo, para toda aquella tecnología que involucre publicidad conductual.

Esto está íntimamente vinculado al deber de información exigido por los artículos 42 de la Constitución Nacional, artículo 1100 del Código Civil y comercial y el artículo 4 de la ley 24.240.

En consecuencia, para dar cumplimiento a lo dispuesto por los artículo 42 de la Constitución Nacional, artículo 1100 del Código Civil y Comercial y artículo 4 de la Ley De Defensa del Consumidor, los proveedores que utilizan sistemas de IA que despliegan publicidad conductual y sistemas de reconocimiento facial automático, para inferir o no emociones, deberían brindar una información cierta, adecuada y detallada de qué objetivos y finalidad persiguen con la utilización de determinado algoritmo. Asimismo, qué datos se recolectan, cómo es su tratamiento y quienes tienen acceso a la información recopilada.

El artículo 1100 del Código Civil y Comercial cuando señala que debe informarse "toda otra circunstancia relevante del contrato", lo que resulta vital para proteger los intereses de los consumidores y usuarios.

¿Y qué circunstancias son relevantes para el consumidor con relación a este tipo de publicidad y sistema de reconocimiento biométrico?

Entendemos que se trata de toda aquella información que permita conocer si el consumidor está siendo perfilado. Asimismo, es necesario informar qué tipo de decisiones automatizadas se toman en base a dicho perfil, y con quienes el proveedor comparte la información recolectada a través de sus sistemas reconocimiento facial automatizado.

Entendemos que, en materia de derecho a la información, cuando se utiliza sistemas de reconocimiento facial automatizado y se despliega publicidad conductual deberían establecerse una serie de pautas mínimas, saber: a) notificación de la intervención de cámaras con reconocimiento facial automatizado; b) advertencia sobre la utilización de estos sistemas para analizar emociones y desarrollar publicidad conductual; y c) información clara y detallada del tipo de algoritmos utilizados, su finalidad prevista, riesgos y consecuencias negativas.

Asimismo, aun cuando el consumidor haya prestado consentimiento para la utilización de sistemas de reconocimiento facial automatizado debe tener la posibilidad de ejercer *el derecho de arrepentimiento*. Es decir, de retirar el consentimiento otorgado en cualquier momento, y cuando así lo desee.

La problemática regulatoria que de por si presentan los sistemas de IA en la actualidad, debe sumarse un tipo de tecnología considerada por muchos de alto riesgo.

Sin embargo, en el ámbito europeo, la propuesta de Reglamento en materia de IA solo prohíbe los sistemas de reconocimiento facial automatizado en tiempo real en espacios de acceso público y con fines policiales.

Los sistemas de reconocimiento facial automatizado de categorización de emociones no están prohibidos ni son de alto riesgo, sino que serán sometidos a una obligación de transparencia que consiste en una garantía de que estarán diseñados y desarrollados de forma que los consumidores sean informados de que están interactuando con este tipo de sistemas, excepto en las situaciones en las que esto resulte evidente debido a las circunstancias y al contexto de utilización (artículo 52). En este punto, es importante destacar, que la advertencia o señalización de en un espacio determinado sobre el despliegue de este tipo de tecnología no debería considerarse deber de información satisfecho, ni la permanencia en el lugar como un consentimiento implícito.

Para finalizar, en materia de consumo, entendemos que los sistemas de reconocimiento facial automatizado solo deberían emplearse como método de autenticación o verificación. Consideramos que en espacios como metros, centros comerciales, empresas proveedoras de bienes y servicios deberían tener prohibido el uso de sistemas de reconocimiento facial automatizado con el objeto de analizar emociones para desarrollar estrategias de marketing, o bien a los fines de seguridad privada.

5. **CONCLUSIONES**

El Gran Hermano 4.0 está con nosotros, a través de los perfiles digitales las empresas pueden predecir y entender el comportamiento de sus eventuales clientes en la red, identificarlos y redirigir sus campañas de marketing de manera personalizada.

Las tecnologías de la IA aplicadas al marketing transforman la manera que tienen las empresas de interactuar con sus clientes, el marketing 4.0 apunta desarrollar nuevos productos y servicios ajustados a medida del consumidor.

Asimismo, brinda la oportunidad de comercializar de manera más efectiva productos que no tienen tanta aceptación al establecer estrategias de ventas capaces de captar la atención del consumidor a través *trackeo* de sus emociones.

El reconocimiento facial automatizado poco a poco está irrumpiendo en nuestras vidas, basta con solo mirar nuestro móvil para advertir que tenemos descargada una aplicación que utiliza este tipo de tecnología.

El uso de reconocimiento facial automatizado para el reconocimiento de emociones sumado a la posibilidad de utilizar sus resultados para desarrollar publicidad conductual requiere poner énfasis en la posible afectación de derechos fundamentales como la libertad de expresión, la dignidad humana, la privacidad, la ausencia de discriminación por razón de sexo, raza u origen étnico, religión o credo, u orientación sexual. Asimismo, una tutela judicial efectiva no solo de los datos personales sino también del derecho de los consumidores y usuarios.

En tiempos donde todo está bajo el escrutinio de los algoritmos es crucial abordar de manera proactiva los desafíos éticos, legales y técnicos que imponen los sistemas de reconocimiento facial automatizado. Esto requiere un enfoque multidisciplinario que equilibre la innovación tecnológica con el respeto a los derechos fundamentales y la dignidad humana.

BIBLIOGRAFÍA

Castellanos Quintana, Juan V; González Vilalta, Daniel. 2013. “¿Qué puede aportar la neurociencia al marketing y a la investigación de mercados?”, *Revista de Estudios de Juventud*, *103*, 51-68.

Cheradi, Ana. 2020. “Face Recognition”, *Towards Data Science*, cita online: https://towardsdatascience.com/face-recognition-using-deep-learning-b9be73689a23.

Colombo, María C. 2023. “La manipulación algorítmica: una problemática de la Revolución 4.0 que colisiona con el derecho a la libertad de expresión y el derecho a la información”, *Suplemento Innovación y* Derecho, cita online: TR LALEY AR/DOC/1806/2023.

Consejo de Europa. 2010. *Recomendación CM/Rec. (2010) 13 del Comité de Ministros de los Estados Miembros sobre la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal en el contexto de la creación de perfiles*, cita online: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016805cdd2a.

Cotino Hueso, Lorenzo. 2022. "Reconocimiento facial automatizado y sistemas de identificación Biométrica bajo la regulación superpuesta de Inteligencia Artificial y Protección de Datos", *Derecho Público de la Inteligencia Artificial*, cita online: https://www.fundacionmgimenezabad.es/sites/default/files/Publicar/publicaciones/documentos/oc27_13_lorenzo_cotino_es_o.pdf.

Cotino Hueso, Lorenzo. 2022. "Sistemas de inteligencia artificial con reconocimiento facial y datos biométricos. Mejor regular bien que prohibir mal", *El Cronista del Estado Social y Democrático de Derecho*, *100*, 68-79.

Grupo de Trabajo de Protección de Datos del Artículo 29. 2010. *Dictamen 2/2010 sobre publicidad comportamental en línea*, cita online: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp171_es.pdf.

Gallego Rodríguez, Pablo. 2022. "Los registros biométricos y su aplicación al proceso penal desde una perspectiva constitucional". En Calaza López, Sonia; Llorente Sánchez-Arjona, Mercedes (Dirs.), *Inteligencia artificial legal y administración de justicia*, Thomson Reuters Aranzadi.

Parlamento Europeo y Consejo de la Unión Europea. 2006. *Directiva 2006/114/CE sobre publicidad engañosa y publicidad comparativa*, cita online: https://www.boe.es/doue/2006/376/L00021-00027.pdf.

Muditt, Jessica. 2022. "The nation where your 'faceprint' is already being tracked", *Future now. Technology*, *BBC.com*, cita online: https://www.bbc.com/future/article/20220616-the-nation-where-your-faceprint-is-already-being-tracked.

Navas Navarro, Susana. 2015. *La personalidad virtual del usuario de internet*. Tirant lo Blanch.

Parlamento Europeo y Consejo de la Unión Europea. 2016. *Reglamento (UE) 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE*, cita online: https://www.boe.es/doue/2016/119/L00001-00088.pdf.

Pérez Bes, Francisco. 2012. *La publicidad comportamental online*. Editorial UOC.

Pérez y Madrid, Aniceto. 2021. *El reconocimiento facial es superpoder. Cómo te afecta y por qué deberías conocerlo*. Dykinson.

Parlamento Europeo y Consejo de la Unión Europea. 2023. *Propuesta de Reglamento en materia de Inteligencia Artificial (Ley de Inteligencia Artificial)*, cita online: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52021PC0206.

Santisteban Galarza, Mario. 2021. "Reconocimiento facial y protección de datos: una respuesta provisional a un problema pendiente", *Revista de Derecho de la UNED (RDUNED)*, 28, 499–526, cita online: https://doi.org/10.5944/rduned.28.2021.32887.

Sarrió, Clotilde. 2013. "Emociones y Expresiones Faciales Universales". *Psyciencia*, cita online: https://www.psyciencia.com/emociones-y-expresiones-faciales-universales/.

Yang, D; Abeer Alsadoon; Prasad; Singh; Elchouemi. 2017. "An Emotion Recognition Model Based on Facial Recognition in Virtual Learning Environment", cita online: https://www.sciencedirect.com/science/article/pii/S1877050917327679.

Chamatropulos, Demetrio A. 2019. *Estatuto del Consumidor. Comentado*, Thomson Reuters.

Hassouneh, Aya; Mutawa, A. M.; Murugappan, M. 2020. "Development of a Real-Time Emotion Recognition System Using Facial Expressions and EEG based on machine learning and deep neural network methods", *Informatics in Medicine Unlocked*, *20*, cita online: https://www.sciencedirect.com/science/article/pii/S235291482030201X.