Discriminación 4.0: una aproximación a los problemas que suscitan la biometría y los sistemas de reconocimiento facial[1]

Discrimination 4.0: An approach to the Issues Raised by Biometrics and Facial Recognition Systems

GABRIELA COMMATTEO[2] Y PILAR MOREYRA[3]

Resumen: Los sistemas biométricos de reconocimiento facial se enmarcan en las nuevas tecnologías que afectan nuestros derechos fundamentales. En este trabajo, analizamos el derecho a la igualdad ante las discriminaciones que pueden producir la biometría y los sistemas de reconocimiento facial. Para comprender de qué hablamos cuando nos referimos a la biométrica, primero examinaremos los conceptos de algoritmo e inteligencia artificial (IA) como dos áreas vinculadas al funcionamiento de los sistemas biométricos. Este primer paso es relevante para comprender de qué

[1] Este trabajo de investigación fue llevado a cabo en el marco del Proyecto IUS 0800 2019 01 00017 CT, "Los derechos fundamentales ante los desafíos de la era digital: Una búsqueda de soluciones para Argentina en un contexto global", de la Facultad de Derecho de la Universidad Católica Argentina.

[2] Coordinadora del Proyecto IUS. Abogada y Traductora Pública en Inglés por la Universidad Católica Argentina. Becaria Chevening, cursando Master of Laws (LL.M.) in Information Technology and Intellectual Property en King's College London.

[3] Integrante del equipo IUS. Alumna de grado de la carrera de Abogacía en la Facultad de Derecho de la Universidad Católica Argentina (UCA). Ganadora del concurso "Mi Primera Publicación", organizado por la Facultad de Derecho de la UCA, en el año 2021. Paralegal en Marval, O'Farrell & Mairal.

forma discrimina la biometría a través de IA y algoritmos parciales. Luego, reseñamos el marco normativo argentino en materia de protección de datos personales y actos discriminatorios, con la finalidad de determinar si la legislación vigente es suficiente para enfrentar los riesgos de la discriminación 4.0 y resguardar nuestros derechos en la era digital.

Palabras claves: Algoritmos, Inteligencia Artificial, Biometría, Datos Personales, Reconocimiento Facial, Igualdad.

Abstract: Biometric facial recognition systems are part of the new technologies that affect our fundamental rights. In this paper, we analyze the right to equality in the face of the discrimination that biometrics and facial recognition systems can produce. To understand what we are talking about when we refer to biometrics, we will first examine the concepts of algorithm and artificial intelligence (AI) as two areas linked to the operation of biometric systems. This first step is relevant to understand how biometrics discriminates through AI and partial algorithms. Then, we review the Argentine regulatory framework on personal data protection and discriminatory acts, in order to determine whether the current legislation is sufficient to address the risks of discrimination 4.0 and safeguard our rights in the digital era.

Keywords: Algorithms, Artificial Intelligence, Biometrics, Personal Data, Facial Recognition, Equality.

Recibido: 27.10.2021 Aceptado: 16.12.2021

Sumario

1. Introducción

En octubre de 2018 Amazon, el rey de los asistentes personales virtuales —creador de "Alexa", una de las asistentes de voz más utilizadas en el mundo[4]— decidió dejar la contratación de sus empleados en manos de un sistema de inteligencia artificial (IA). La

[4] O'Brien, 29 de julio de 2019, "*Could Alexa Become Your Next Executive Asisstant?*", TheInnovator. https://innovator.news/could-alexa-become-your-next-executive-assistant-eda21786920e

empresa esperaba, por un lado, optimizar recursos, ahorrar tiempo y mano de obra; y, por otro lado, lograr mayor productividad. Sumado a ello, celebraba encontrar un "nuevo reclutador", un sistema *neutral* para contratar personal, dado que la mirada humana siempre es *parcial* (*biased*, en inglés) o cargada de sesgos que muchas veces son inconscientes y difíciles de superar. Este sistema se entrenó sobre la base de información sobre solicitantes de empleo en Amazon durante un período de diez años. Fue entrenado para observar patrones. Sin embargo, la gran sorpresa se dio cuando la empresa tuvo que "despedir" a su "nuevo reclutador", artificial y supuestamente neutral, porque resultó ser sexista. En este sentido, el algoritmo a través del cual funciona este "nuevo reclutador" arrojaba resultados con una preferencia por candidatos masculinos, dado que los reclutamientos anteriores y *curriculum vitae* (CV) oportunamente enviados a la empresa provenían, en su gran mayoría, de hombres; lo que evidencia un reflejo del dominio masculino en la industria tecnológica.[5]

Este es tan solo un ejemplo de las dificultades que puede suscitar la aplicación de tecnologías como la IA, la biometría y los sistemas de reconocimiento facial por parte de compañías —y también, como se verá, gobiernos—. Entre otras, surgen las siguientes preguntas: ¿los algoritmos discriminan?, ¿generan desigualdad?, ¿evidencian las prácticas discriminatorias existentes?, ¿afectan nuestro derecho a la igualdad?

Este ensayo tiene por objeto dar respuesta a algunas de estas preguntas. Primero, se sentarán algunas bases conceptuales y se reseñará brevemente qué son los algoritmos, la IA, el *machine learning* y la biometría. Segundo, se analizará la "parcialidad

[5] Dastin, 10 de octubre de 2018, "*Amazon scraps secret AI recruiting tool that showed bias against women*", Reuters. https://www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G

algorítmica",[6] para entender si los algoritmos discriminan y distinguir los tipos de discriminación que podrían surgir de su aplicación. Además, se describirán casos específicos donde se produce discriminación en la aplicación de estas tecnologías. Tercero, se profundizará sobre el uso de la biometría en el campo del reconocimiento facial. Finalmente, se describirán algunos puntos básicos de la regulación argentina en materia de datos personales y discriminación, y se analizará si lo actualmente regulado es suficiente para defender nuestros derechos frente al avance de estas tecnologías en la era digital.

2. Una aproximación conceptual a la inteligencia artificial, los algoritmos y la biometría

En primer lugar, debemos aclarar que resulta difícil proporcionar una definición concreta de IA, porque todavía ni siquiera existe consenso sobre qué es la inteligencia en general.[7] Sin embargo, aquí abordaremos una idea aproximada, lo cual nos lleva a explorar diferentes conceptos.

Por ello, analizaremos qué son los algoritmos, como base de funcionamiento de cualquier tecnología —entre ellas, la IA—. La IA está diseñada para imitar comportamientos inteligentes. Para lograrlo, se necesita programar tareas en un lenguaje que las computadoras logren procesar. Los programadores deben convertir

[6] En este trabajo, entendemos por "parcialidad algorítmica" al algoritmo que está entrenado sobre la base de un conjunto de datos incompleto o que contienen un sesgo. Este tipo de algoritmo podría tomar decisiones o predecir resultados que resulten en la discriminación de un determinado grupo.

[7] Otra dificultad para lograr definir la IA es que se trata de una disciplina de inspiración biológica —porque intenta imitar comportamientos que requieren inteligencia (García, 2019, p. 9)— e interdisciplinaria —pues involucra conocimientos de ingeniería en informática, matemática, y neurociencia, entre otras disciplinas—. Además, la IA abarca diversos campos, porque los comportamientos inteligentes que busca imitar son varios, y cada uno de ellos cuenta con su propio objeto y método de investigación.

las cosas que hacemos en una secuencia de instrucciones que una máquina pueda procesar. Es decir, un algoritmo funciona como una suerte de traductor entre la lógica humana y la lógica de programación.

Sin embargo, los algoritmos por sí mismos no tienen impacto. Son instrucciones, pero un uso imprudente a través de tecnologías como la IA sí puede producir daños. La IA es una tecnología que se subdivide en varias ramas y ámbitos de aplicación, desde el reconocimiento facial hasta la robótica. Los algoritmos tienen a su cargo su debido funcionamiento, pues un algoritmo entrenado sobre datos parciales generará una IA parcial.

A su vez, dentro del vasto campo de la IA podemos encontrar a las tecnologías biométricas, que basan sus sistemas automáticos en sensores de IA.[8] ¿Por qué? Porque la IA busca imitar capacidades cognitivas y el reconocimiento facial es una tarea cognitiva. De esta manera, la IA sirve a la biometría al entablar entornos de interacción inteligente que perciban los rasgos, datos y emociones del usuario necesarios para el funcionamiento del sistema (Fernández *et al*, 2019, p. 36). Nuevamente, si la IA basa su funcionamiento en algoritmos parciales y esta deviene en parcial, el error se arrastra a los sistemas biométricos que utilizan esta tecnología en sus sensores para el reconocimiento facial.

a. Algoritmo

En términos generales, podríamos decir que un algoritmo es una especie de receta con instrucciones para llegar a un resultado determinado. Shanker entiende que es una "secuencia definida de reglas (operaciones) que especifica cómo producir un resultado [*output*] a partir de cierto valor [*input*] dado en un número finito de

[8] No siempre la biometría se sirve de IA para el funcionamiento de sus sensores; sin embargo, a los fines de este trabajo desarrollaremos aquellos que sí lo hacen.

pasos" (Shanker, 1987, p. 632 citado en Mota, 2015, p. 324). Por este motivo, al hablar de algoritmos es importante entender cuál es la información sobre la que se cementa su funcionamiento, de la cual se alimentan, dado que esto será crucial a la hora de analizar los resultados (*outputs*). En el campo de estudio de la IA existen diferentes tipos de algoritmos. Sin embargo, dado que el objetivo de este trabajo no es ahondar en sus detalles, solo se proporcionará una aproximación a su esencia.[9]

b. Inteligencia artificial

Como mencionamos, no existe una definición universalmente aceptada de IA. Una primera aproximación a la IA sería describirla en simples palabras como una tecnología o técnica que busca que las máquinas reproduzcan capacidades cognitivas similares a las de los seres humanos. La Organización para la Cooperación y el Desarrollo Económico ("OCDE" por sus siglas en español), por su parte, la denomina una "tecnología multipropósito".[10] El Grupo de Expertos de Alto Nivel en Inteligencia Artificial designado por la Unión Europea define a la IA del siguiente modo:

> *[L]os sistemas de inteligencia artificial (IA) son programas informáticos —software— (y posiblemente también equipos informáticos —hardware—) diseñados por seres humanos que, dado un objetivo complejo, actúan en la dimensión física o digital mediante la percepción de su entorno mediante la adquisición de datos, la interpretación de los datos estructurados o no estructurados, el razonamiento sobre el conocimiento o el tratamiento de la información, fruto de estos datos y la decisión de las mejores acciones que se llevarán a cabo para alcanzar el objetivo fijado* (Comisión Europea, 2020, p.65).

[9] Para más detalles sobre este tema, véase Alfonso Mancilla Herrera *et al*, 2015.

[10] Resolución OECD/LEGAL/0049

Por su parte, Richard Susskind entiende que la IA involucra "el diseño, el desarrollo y la implementación de sistemas informáticos capaces de desarrollar una tarea y resolver problemas del tipo que usualmente requeriría inteligencia humana" (Susskind, 1990, p. 105). Sin embargo, por el momento, lo que se ha logrado en materia de IA es la realización de tareas específicas. Por ejemplo, llevar a cabo un proceso de reconocimiento facial, aprender a jugar un juego, responder a ciertas ordenes o pedidos interactuando con su entorno y manejar un auto. Eso la distingue de lo que se conoce como Inteligencia Artificial General (IAG), cuyo fin sería superar a los seres humanos en múltiples campos.[11] Aún no hemos llegado al punto de desarrollar tales tecnologías.

c. Machine learning

Una de las ramas de la IA es el *machine learning*, que permite no solo que las máquinas sean programadas para *realizar* comportamientos que simulan ser "inteligentes", sino también para que puedan aprender *a realizar* comportamientos que se caracterizarían como inteligentes. En este sentido, para crear este tipo de sistemas deben identificarse: la clase de tarea a realizar (T), la medida de rendimiento a mejorar (P), y la fuente de experiencia (E). Tom Mitchell define el *machine learning* como "un programa de computación que aprende de experiencia E en relación con ciertos tipos de tareas T y evaluación del rendimiento P, si su rendimiento respecto a ciertos tipos de tareas T, evaluadas por P, mejoran con la experiencia E" (Mitchell M. T. 1997, p. 1). Por ejemplo, tomemos el caso de Amazon que busca que un algoritmo cumpla la tarea de un empleado de recursos humanos para reclutar personal. El problema a aprender será el reclutamiento de personas; la clase de tarea a realizar (T) será leer, clasificar, y seleccionar los mejores CV que ingresen a la plataforma de la empresa; la medida de rendimiento (P) será el

[11] Resolución 2018/2088 (INI).

número de puestos que logre cubrir, de acuerdo a los requisitos solicitados en la búsqueda, de manera satisfactoria sin cometer un error (ello evaluado por un humano que lo supervise), y la fuente de experiencia (E) que servirá de entrenamiento serán datos e información de procesos de reclutamiento anteriores de la empresa, . Mediante la repetición, el algoritmo "aprende" sobre la base de los datos que se brindan como la fuente de experiencia para poder realizar esa tarea en forma automatizada o autónoma.

d. Biometría

Los conceptos explorados sirven para determinar dónde posicionamos a la biometría en este mundo tan vasto que gobierna la IA. Según explican Wayman y otros, las "tecnologías biométricas son métodos automatizados de verificación o reconocimiento de identidad de una persona con vida basado en características físicas o conductuales" (Wayman *et al*, 2005, p. 1). Un ejemplo de tecnología biométrica es la forma en que desbloqueamos nuestros celulares a partir del reconocimiento facial o por huellas dactilares. Las tecnologías biométricas no determinan la verdadera identidad de la persona, sino que se enfocan en vincular patrones a atributos personales. Es decir, existen diferentes tipos de características biométricas que se analizan que pueden dividirse en características biológicas (cara, mano, retina, iris, huellas dactilares, etc.) y de comportamiento (firma, tipificación, voz, etc.). El reconocimiento facial se encuentra dentro de la primera categoría.

La biometría ha mejorado exponencialmente gracias a la aplicación de técnicas de *deep learning*. Así, su uso se ha expandido a diversos campos, incluidas las áreas de seguridad, defensa y vigilancia en general. Por ejemplo, según determinó un estudio de la universidad de Georgetown, la mitad de la población adulta estadounidense se encuentra registrada en bases de datos

biométricas para reconocimiento facial.[12] Los departamentos de policía en distintos estados utilizan software de reconocimiento facial para comparar imágenes de vigilancia con bases de datos de fotos de identificación (como la licencia de conducir o el pasaporte), no solamente para confirmar la identidad de un sospechoso detenido, sino también para determinar a través de cámaras de vigilancia los movimientos particulares de una persona (Asociación por los Derechos Civiles, 2017, p.15).

A pesar de su uso cada vez más extendido, los sistemas biométricos han suscitado diversas controversias. Por ejemplo, empresas como FaceFirst han llegado a publicitar porcentajes de 95% de efectividad en sus métodos (Garvie *et al*, 2016, p. 7). Sin embargo, estos porcentajes son dudosos cuando se analiza la verdadera efectividad de los sistemas biométricos en diversos grupos sociales. En la próxima sección, exploraremos algunos de los problemas que suscitan la aplicación de estos sistemas.

3. Los problemas que suscita la "parcialidad algorítmica"

a. ¿De qué maneras discriminan los algoritmos?

Algunos sistemas de IA presentan lo que se ha llamado "caja negra" (*black box*, en inglés) (Pasquale, 2015). Esto quiere decir que la forma en que operan algunos de estos sistemas nos impide comprender por qué el algoritmo toma ciertas decisiones respecto a ciertas personas. En otras palabras, conocemos la información (*inputs*) dada a la IA para operar, pero no sabemos cuál es el proceso que el algoritmo sigue para llegar a determinado resultado (*output*).

[12] Waddell, Kaveh, 9 de octubre de 2016, "Half of American Adults Are in Police Facial-Recognition Databases", The Atlantic. https://www.theatlantic.com/technology/archive/2016/10/half-of-american-adults-are-in-police-facial-recognition-databases/504560/

En consecuencia, su opacidad no permite determinar si la discriminación fue en base al sexo, etnia, raza, edad, religión, ideología, u otro factor. Esto vuelve difícil explicar cómo un algoritmo discrimina en algunas ocasiones.

Sin embargo, también existen sistemas de IA que no contienen una "caja negra". Aquí resulta más fácil ver cómo un algoritmo discrimina, y por lo general, se debe a que la información (los *inputs*) sobre la base de los cuales se entrenan los algoritmos son parciales, y como resultado traen criterios discriminatorios en su proceso de entrenamiento. Lo mismo aplica al *machine learning*, pues existen formas en que estos sistemas automatizados *aprenden* a ser parciales.

A fin de entender la razón de la parcialidad, debemos tener en cuenta diferentes cuestiones. Para empezar, tenemos las "metas variables" y las "clases de etiqueta". Las metas variables son aquello que el algoritmo busca alcanzar, mientras que las clases de etiqueta dividen a las metas variables en distintas categorías exclusivas (Barrocas & Selbst, 2016, p. 677). Por ejemplo, cuando se diseña un filtro de *spam,* la empresa alimenta al algoritmo con grandes cantidades de e-mails que son "*spam*" y otros que son "no *spam*", de acuerdo con lo que las personas suelen considerar que entra en cada categoría. Estos mensajes etiquetados como "spam" y "no spam" son llamados "datos de entrenamiento". Los mensajes que pertenezcan a la primera etiqueta, spam, contendrán frases como "ganaste un millón de dólares" o "pastillas mágicas para bajar de peso". Entonces, la meta variable para el algoritmo será aprender aquello que deberá considerar "spam" y "no spam" y, sobre la base de ello, lograr catalogar los e-mails correctamente.

Sin embargo, las metas variables pueden definirse con diferentes criterios. Al hilar fino, lo que una persona considera "spam" puede que otra lo considere "no spam". Este problema se presenta, naturalmente, en cualquier otro caso donde debamos encontrar criterios para crear definiciones. Por ejemplo, una empresa quiere

diseñar un algoritmo para reclutar "buenos empleados". ¿Cómo se define qué es un buen empleado?, ¿un buen empleado es quien más ventas alcanza o quién llega más veces puntual al trabajo? Veamos el siguiente ejemplo: las personas que deben viajar más distancia para llegar al trabajo, están expuestas al tráfico, o paros de transporte público, entre otros factores, lo cual a la larga afecta su puntualidad. La empresa podría elegir como clase de etiqueta que un "buen empleado" llega siempre a tiempo, o bien que un "buen empleado" pocas o rara vez llega tarde. Entonces, el algoritmo no consideraría a los trabajadores que viven lejos del puesto de empleo como "buenos empleados", inclusive cuando estos tuvieren mejor desempeño que otros en sus tareas (Barrocas & Selbst, 2016, p. 679). Por lo tanto, una de las formas en que la IA y los algoritmos aprenden a ser parciales es a partir de la forma en que las empresas u organizaciones definen las metas variables y las clases de etiqueta.

Otra forma de parcialidad algorítmica surge cuando el sistema basa su operatoria o aprende de bases de datos que acarrean sesgos. Esto sucede cuando la IA se entrena sobre datos parciales o aprende de una muestra parcial, por lo que luego va a reproducir esa parcialidad. Lamentablemente, este suele ser el caso, pues los datos con que se alimenta a los sistemas de IA suelen ser parciales, porque reproducen los sesgos discriminatorios humanos preexistentes. Así, una facultad de medicina inglesa, en 1980, recibía más solicitudes de ingreso de las que podía evaluar. En consecuencia, desarrolló un programa para que eligiera entre las numerosas solicitudes. Los datos de entrenamiento del programa fueron los archivos de admisión de años anteriores, cuando las autoridades de la facultad elegían a los candidatos que podían ingresar. De esos archivos (*input*) el programa aprendió cuáles eran los perfiles deseados que debía buscar (*output*). La computadora reprodujo el sistema de selección, y resultó que el programa discriminaba a mujeres y a inmigrantes. La IA no introdujo la discriminación al programa de selección, sino que más bien la ratificó (Ibídem, p. 682).

Otro ejemplo son las muestras parciales cuando se recopilan datos en materia criminal (Asociación por los Derechos Civiles, 2017, p. 15). En consecuencia, si la policía pone su atención en ciertos grupos étnicos, de origen nacional o ciertos barrios, no debería sorprender que sus archivos sistemáticamente sobrerrepresenten a estos grupos más que otros. Y si un programa de computación se entrenara bajo esos archivos, eventualmente reproducirá el mismo sistema de investigación parcial. Aún más, no solo se limitará a reproducir, sino que *amplificará* la discriminación en el supuesto que más de una comisaría decidiera adoptar ese programa (Ibídem, p. 690).

Finalmente, otro elemento problemático en materia de parcialidad de los sistemas de IA es el anonimato, que en muchos casos es necesario para proteger nuestra información. Esto está relacionado con la diferencia entre datos personales y datos sensibles. De acuerdo con la Ley Nro. 25.326 de Argentina,

- los *datos personales* son información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables (art. 2), y

- los *datos sensibles* son aquellos que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual (art. 2). Estos datos gozan de una protección especial, dado que "ninguna persona puede ser obligada a proporcionar datos sensibles" (art. 7).

Sin embargo, si un algoritmo intenta tomar decisiones en base a información que ha sido anonimizada, muchas veces esta mirada incompleta puede resultar en decisiones discriminatorias. Tomemos como ejemplo el caso de un banco que utiliza IA para decidir a qué clientes otorgará o rechazará un crédito. Supongamos que el banco entrena al algoritmo sobre la base de datos y registros del trabajo de

los últimos veinte años, y la información que se le proporciona al algoritmo en relación con los clientes es meramente numérica. Datos relevantes como el sexo, la etnia o la raza no están registrados. Sin embargo, en el entrenamiento, el sistema aprende que las personas de determinado código postal muestran una tendencia a no pagar sus préstamos. En el caso de que se corresponda con un barrio marginado, nos encontraríamos una vez más frente a un algoritmo que discrimina.

En consecuencia, la falta de información respecto de datos sensibles, en ciertos supuestos, podría derivar en la discriminación de minorías (Ibídem, p. 681). Puede ser, entonces, que en determinados contextos esta información sensible sea necesaria para hacer distinciones justas que eviten tratos inequitativos. Por ejemplo, conocer las situaciones económicas que enfrentan ciertos barrios marginados permite brindar un trato distintivo a comparación de otras zonas urbanas en las cuales las condiciones sean diferentes. En otras palabras, en algunas ocasiones pareciera que se requeriría de una discriminación positiva para impedir que un trato igualitario entre desiguales homogenice personalidades que merecen un trato distintivo y equitativo.

Por el contrario, el procesamiento de datos y el estudio de las categorías de la IA muchas veces permiten deducir, a partir de datos personales que han sido proporcionados, datos sensibles que no han sido proporcionados. Por ejemplo, en un estudio del año 2009 se probó que Facebook podía conocer la orientación sexual de una persona en base a sus relaciones y amistades.[13] Esto demuestra que inevitablemente existen datos personales (las amistades públicas de un usuario) íntimamente relacionados con características propias de una persona (su orientación sexual) que hacen a sus datos sensibles.

[13] Behram, Carter, 5 de octubre de 2009, "*Facebook Friendships Expose Sexual Orientation*", First Monday. https://firstmonday.org/article/view/2611/2302#:~:text=After%20analyzing%204%2C080%20Facebook%20profiles,classifier%20with%20strong%20predictive%20power.

La seguridad y confidencialidad de datos sensibles no se ve lograda por las normas que actualmente regulan la materia dado que en algunos supuestos los datos sensibles pueden deducirse a partir de datos personales ya otorgados.

b. Algunos casos de parcialidad algorítmica en los ámbitos público y privado

La creciente utilización de algoritmos en los ámbitos público y privado, entonces, podría dar lugar a discriminaciones. Veamos algunos ejemplos.

En el ámbito privado, nos encontramos con empresas como Google, Facebook, Amazon, Rolls Royce, Spotify, Airbnb y Uber, que marcan el paso en el *capitalismo de plataformas*[14] (Srnicek, 2016). El uso de algoritmos para estas compañías es moneda corriente, y nosotros —como sus consumidores, sus usuarios o sus trabajadores— nos encontramos a merced de sus fallas. Ya mencionamos el caso de Amazon y el uso de algoritmos como reclutadores de personal. Sin embargo, vale la pena ahondar en el mundo de las plataformas publicitarias de Facebook y Google.

La publicidad online (conocida como la industria del *AdTech)* es la principal fuente de ingresos de empresas como Facebook y Google. El uso de algoritmos en buscadores o redes sociales es útil para recolectar y analizar datos de los usuarios. Cuanto más se sabe del usuario, mejor se le pueden dirigir ofertas especializadas de productos y servicios, y por ende mayor será la ganancia. De esta manera, los usuarios son agrupados por sus intereses; en base a ello, están expuestos a ciertas publicidades online, por lo que ser parte de

[14] Según explica Srnicek, con una prolongada caída de la rentabilidad de la manufactura, el capitalismo se volcó hacia los datos como modo de mantener el crecimiento económico y la vitalidad, de cara al inerte sector de producción (Srnicek, 2018, p. 13).

un grupo que define qué información se recibe o no.[15] Las categorías son infinitas y van, en el caso de Facebook, desde "*gamers*" hasta "adolescentes deprimidos".[16] Un problema que genera la publicidad personalizada (*targeted advertising*, en inglés) es que los usuarios quedan aislados en "burbujas digitales" o "burbujas de publicidad digital". Además, las compañías ocultan las categorías en las que agrupan a los usuarios —es decir, los propios usuarios no saben que están siendo catalogados de tal o cual modo—.

Una dificultad adicional es que los comercios online publicitados en Google son capaces de determinar los antecedentes que tiene un comprador en su tienda. En consecuencia, las empresas ofrecen precios diferenciados para cada cliente, dependiendo de su historial. La Universidad de Princeton descubrió que los precios diferenciados de una compañía, establecidos por un algoritmo, resultaban en precios más altos para los clientes de origen asiático, por lo que un grupo étnico pagaba precios más altos en comparación a otros grupos (Watcher, 2020, p. 7).

Dentro del ámbito público, nos encontramos principalmente con casos relacionados con el actuar de la policía en la prevención del crimen. En Estados Unidos, el sistema COMPAS se utiliza para predecir si los acusados muestran tendencia a reincidir. La idea del programa es ayudar a los jueces a determinar si corresponde o no otorgarles a los acusados el beneficio de la *probation*. Si bien COMPAS lograba predecir efectivamente el 61% de los reincidentes, los acusados de origen afroamericano eran etiquetados el doble de veces como reincidentes en comparación con los acusados no

[15] White, 2017, "*When Algorithms Don't Account for Civil Rights: Do lucrative deals with advertisers have to come at the expense of users civil rights?*", The Atlantic. https://www.theatlantic.com/business/archive/2017/03/facebook-ad-discrimination/518718/

[16] Reilly, 1 de mayo de 2017, "*Is Facebook targeting advertising at depressed teens?*", MIT Technology Review. https://www.technologyreview.com/2017/05/01/105987/is-facebook-targeting-ads-at-sad-teens/

afroamericanos, cuando en realidad los no afroamericanos mostraban, a la larga, una tendencia mayor a reincidir. Además, los acusados afroamericanos tenían el doble de probabilidades de ser calificados por el sistema de manera errónea (Zuiderveen, 2018, p. 24).

Lo mismo ocurre en otras áreas, como el otorgamiento de planes de salud o beneficios sociales, o hasta la entrega de un documento de viaje o una visa.[17] Por lo tanto, cualquier tarea que pueda realizar un algoritmo puede ser objeto de actos discriminatorios que pasan inadvertidos detrás de una pantalla. El individuo siempre ha necesitado garantías frente al Estado y las empresas, pero pareciera que en tiempos modernos las necesitará más que nunca. El panorama se complejiza aún más con el creciente uso de sistemas de reconocimiento facial.

4. Las dificultades que generan los sistemas de reconocimiento facial

a. El creciente uso de los sistemas de reconocimiento facial

Como se ha mencionado, la biometría es el proceso por el cual se busca reconocer, autenticar e identificar a una persona, con base en sus características físicas o en su comportamiento. Dentro de sus dos categorías —biológicas y de comportamiento—, el reconocimiento facial pertenece a la primera. Es una práctica que ha despertado un gran interés entre gobiernos y empresas alrededor del mundo.

Como menciona Deibert, "uno de los mercados más lucrativos, y potencialmente el más preocupante para la privacidad, es el de la biometría y los sistemas de reconocimiento facial. Aunque desarrollado para fines militares, fuerzas de seguridad y de inteligencia —aproximadamente el 70% de los gastos actuales—, el

[17] Véase, en general, Asociación por los Derechos Civiles, 2017.

mercado de consumidores más amplio [doméstico/civil] está creciendo rápidamente. Muchas plataformas móviles y de *social media* utilizan la tecnología de reconocimiento facial en sus aplicaciones de fotos digitales para que los usuarios puedan etiquetar, categorizar y verificar sus identidades y las de sus amigos" (Deibert, 2013, p. 67, citado en Asociación por los Derechos Civiles, 2017, p.6).

La fuente de información biométrica es nuestro cuerpo. Desbloquear el celular con nuestra huella digital o a partir del reconocimiento facial hace a lo que se conoce como una *contraseña biológica*. Nuestra información biométrica es mayormente pública y de fácil acceso, considerando que no solo por su naturaleza carece de secretismo, sino que también datos como nuestros rasgos faciales se ven expuestos a diario con cada foto que publicamos en las redes.

Las empresas privadas, además, hacen un gran esfuerzo por ganar acceso a nuestros datos biométricos.[18] En enero de 2019, Facebook inició un desafío llamado "*Ten year challenge*". Los usuarios debían subir una foto actual y una foto con diez años de antigüedad, en principio "solo por diversión". Como profesa el mantra de la religión dataísta: "si vives algo fílmalo, si filmas algo súbelo, si subes algo compártelo" (Harari, 2016, p. 448). Sin embargo, lo que se convirtió rápidamente en una tendencia, presuntamente indefensa, dejó un gusto amargo cuando Kate O'Neill salió de la burbuja y cuestionó si en verdad este *challenge* no era en realidad ideal para que Facebook recolectara toneladas de datos de personas provenientes de diversas partes del mundo. Estos datos, sobre los rasgos faciales de esas personas en distintas edades,[19] podrían

[18] Hao, 17 de junio de 2020, "*La presión pública obliga a Amazon a paralizar el reconocimiento facial*", MIT Technology Review. https://www.technologyreview.es/s/12332/la-presion-publica-obliga-amazon-paralizar-el-reconocimiento-facial

[19] O'Neill, 15 de enero de 2019, "*Facebook's 10-year challenge Is Just a Harmless Meme—Right?*", Wired. https://www.wired.com/story/facebook-10-year-meme-challenge/

utilizarse para entrenar algoritmos que se aplican durante un proceso de reconocimiento facial, práctica que se ubica dentro del campo de la biometría.

En Argentina, se ha expandido el uso de tecnologías de biometría por parte del sector público y el sector privado. Los ámbitos en los que dichas herramientas son aplicadas son amplísimos, y abarcan desde bancos hasta centros educativos, pasando por estadios de fútbol y sistemas de seguridad social[20] y tributarios. Las personas que viven en Argentina están constantemente expuestas a la posibilidad de otorgar sus datos biométricos a entidades públicas y privadas.[21] El ámbito público es de particular importancia dado que cada vez más el Estado se apodera de datos biométricos muchas veces sin garantizar su cuidado, para citar algunos ejemplos:

- En abril de 2010, la Administración Federal de Ingresos Públicos (AFIP) emitió la Resolución General 2811/10, que creó el Registro Tributario. Ahora, las personas que deseen solicitar la inscripción y obtener la Clave Única de Identificación Tributaria (CUIT), además de la Clave Fiscal con Nivel de Seguridad 3, deben registrar digitalmente la fotografía de su rostro, su firma y su huella dactilar.

- En 2011, mediante el Decreto Nro. 1766, se creó el Sistema Federal de Identificación Biométrica para la Seguridad (SIBIOS), bajo la autoridad del Ministerio de Seguridad de la Nación y la administración de la Policía Federal Argentina (a través de la Superintendencia de Policía Científica). SIBOS es una base de datos utilizada para identificación de personas a través de su información biológica, por ejemplo, su rostro. Cada usuario de SIBIOS

[20] Bronstein, 2020, "*Rights group blasts Argentina for using face recognition tech on kids*", Reuters. https://www.reuters.com/article/argentina-rights-idUSL1N2GZ23N

[21] Véase, en general, Asociación por los Derechos Civiles, 2017.

tiene instalado en sus oficinas una computadora que está configurada para poder ingresar al Sistema y acceder a los servidores, donde se encuentra la base de datos, a través de una Red Privada Virtual. La Asociación por los Derechos Civiles ("ADC") ha descripto su funcionamiento de la siguiente manera: "todo comienza con la adquisición de la imagen del rostro (sea por una cámara de video 'en vivo' o mediante el archivo de una foto JPG, por ejemplo), para luego proceder a determinar dónde se encuentra ubicado el rostro dentro de la imagen y señalar el centro de los ojos, a partir de la cual se extrae una plantilla o modela, esta es una representación de la imagen que es adecuada para ser comparada (la plantilla puede representar tanto rasgos físicos visibles, como la ubicación de la nariz y las cejas, o pura información matemática). A medida que se analizan las imágenes se realiza un control de calidad, en el cual se determina si una imagen es de baja o alta calidad, en el caso de ser de baja calidad un operador puede confirmar la ubicación de los rasgos faciales para asegurar la exactitud del sistema" (Asociación por los Derechos Civiles, 2017, p. 27). Finalizado el proceso para la carga de imágenes en la base de datos, se puede realizar la comparativa de rostros, por ejemplo, para la búsqueda de una persona que ha cometido un crimen.

- En diciembre del 2014, la Administración Nacional de la Seguridad Social (ANSES) comenzó el proceso de enrolamiento del programa "Mi Huella",[22] mediante el cual procura que los jubilados, pensionados y sus apoderados registren sus huellas dactilares en el Sistema

[22] Una versión archivada del sitio web de ANSES en octubre del 2016 puede consultarse en <https://web.archive.org/web/20161011030812/http://www.anses.gob.ar/prestacion/mi-huella-201>.

de Identificación Biométrica,[23] con el objetivo de dar fe de vida y poder cobrar sus haberes previsionales. Esta información es registrada por la ANSES en una base de datos centralizada bajo la administración de la Dirección General de Diseño de Normas y Procesos.

b. Los problemas jurídicos que genera el uso de estos sistemas

Estos sistemas presentan un riesgo para nuestra privacidad, pues en el marco de las nuevas tecnologías, se reconoce el derecho a que toda información sobre la vida privada de una persona poseída por terceros –entre ellos, los gobiernos y las empresas– sea utilizada de una manera que no perjudique los intereses del titular. Asimismo, generan un riesgo para el acceso a derechos en condiciones de igualdad. El objetivo de este trabajo es interiorizar sobre esta problemática.

Otro de los principales riesgos que esconde el reconocimiento facial es el llamado *chilling effect*, que es "un efecto desalentador o disuasorio, especialmente uno resultante de una ley o reglamento restrictivo" (Eide, 2019, p. 228). El uso de este concepto está íntimamente relacionado con el derecho de libertad de expresión y la libre asociación, dado que leyes o acciones gubernamentales pueden provocar la disuasión de su ejercicio (Penney, 2017, p. 1). Por ejemplo, si se utiliza el reconocimiento facial como una herramienta de vigilancia social en una manifestación, se podría producir el *chilling effect* de que la vigilancia afecte el comportamiento de los individuos (Cushing, 2016, p. 47). Así, alguien con el derecho a la libertad de manifestarse podría no hacerlo por temor a enfrentar represalias o

[23] "*Los jubilados y pensionados tendrán que registrar sus huellas digitales para cobrar sus haberes*", 30 de diciembre de 2014, La Nación. https://www.lanacion.com.ar/economia/jubilados-y-pensionados-huellas-dactilares-anses-nid1756361/

sufrir consecuencias inesperadas. Por ejemplo, en Hong Kong, donde la ciber vigilancia es diaria, los civiles han diseñado tácticas para asegurar que sistemas biométricos no registren sus rostros durante las manifestaciones.[24]

Según determinó un estudio de la universidad de Georgetown, la mitad de la población adulta estadounidense se encuentra registrada en bases de datos biométricos para reconocimiento facial.[25] Varios estados del país utilizan los sistemas biométricos para comparar imágenes de vigilancia con bases de datos de fotos de identificación, por ejemplo, una licencia de conducir o un pasaporte. Estas tecnologías permiten no solo confirmar la identidad de un sospechoso detenido, sino también determinar a través de cámaras de vigilancia los movimientos particulares de una persona.

Sin embargo, estos sistemas presentan fallas que afectan negativamente el derecho a la igualdad y pueden llevar a la criminalización de personas incorrectamente identificadas. En particular, muestran un sesgo racial con personas afroamericanas, de origen asiático y caucásicas. El reconocimiento facial ha fallado 11% de las veces en identificar personas caucásicas y un 19% de las veces cuando el sujeto a identificar era afroamericano (Whitman, 2016, p. 59). En suma, se "determinó que los algoritmos utilizados para identificar a las personas son inexactos aproximadamente en un 15% de oportunidades y son más propensos a identificar erróneamente a los afroamericanos, a lo cual se suma que organismos como el FBI no realizan pruebas de sus sistemas por falsos positivos ni por sesgos

[24] Cid, 9 de agosto de 2019, "*¿Las protestas del futuro? Así "hackean" en Hong Kong al "Gran Hermano" chino*", El Confidencial.
https://www.elconfidencial.com/tecnologia/2019-08-09/protestas-hong-kong-hackear-inteligencia-artificial_2169083/

[25] Wadddel, 19 de octubre de 2016, "*Half of American Adults Are in Police Facial-Recognition Databases*", The Atlantic.
https://www.theatlantic.com/technology/archive/2016/10/half-of-american-adults-are-in-police-facial-recognition-databases/504560/

raciales, ya que para el FBI el sistema es 'ciego a la raza' lo cual ha preocupado al CPT debido a que el FBI no sabe con qué frecuencia el sistema identifica incorrectamente al sujeto incorrecto" (Asociación por los Derechos Civiles, 2017, p.15).

Por lo tanto, cuando instituciones como las fuerzas de seguridad hacen uso de estos sistemas para reconocer personas humanas o intentar encontrar sospechosos en una investigación criminal, debe tenerse presente que no solo existe la probabilidad de errar, sino también de afectar garantías fundamentales como el principio de inocencia, la libertad de expresión, el derecho de protesta ante las autoridades y el derecho a la igualdad.

A los fines de este trabajo se entiende que el derecho a la igualdad se conforma a partir de dos concepciones: (i) igualdad jurídica o formal e (ii) igualdad material. La primera refiere al reconocimiento de la igualdad "ante la ley" (Constitución Nacional, art. 16). En este caso, la igualdad queda satisfecha con el reconocimiento implícito de libertad jurídica a todos los hombres y con la abolición expresa de la esclavitud. No obstante, un segundo aspecto de la igualdad implica no solo el reconocimiento uniforme de este derecho sino también realizar acciones positivas, es decir, prestaciones de dar y de hacer en favor de la igualdad, como por ejemplo, promover y adoptar políticas activas que den impulso al acceso a la igualdad real y efectiva (Campos, 1998, p.268-271).

En suma, la Declaración Universal de Derechos Humanos, en su Artículo 7, describe al derecho a la igualdad como el reconocimiento de que "todos son iguales ante la ley y tienen, sin distinción, derecho a igual protección de la ley. Todos tienen derecho a igual protección contra toda discriminación en contravención a esta Declaración y contra toda provocación a tal discriminación". En el caso de las nuevas tecnologías es claro que existe una afectación a este derecho, pues la falta de una regulación específica al respecto da lugar a una falta de igualdad formal, y, a su vez, esto deviene en una afectación en

el plano material. Sin embargo, tampoco es cierto que la regulación desde el plano formal garantice la igualdad material, dado que sin políticas prácticas que fomenten los derechos, son solo palabras. Es por ello que el trabajo no solo ahonda en el impacto de las normas, sino también las políticas estatales responsables por el uso de estas tecnologías en diferentes áreas.

Por último, en el supuesto que otorgar un beneficio social dependiera de una huella dactilar o del reconocimiento facial, una mínima falla podría dejar a alguien sin la asistencia social necesaria para subsistir, o bien discriminar a los sectores más vulnerables económicamente que no tienen acceso a internet o a una computadora. La política y científica Virginia Eubanks ha definido a este fenómeno como *the digital poorhouse*, pues en su misión por digitalizar todo, los gobiernos olvidan que la digitalización, sin las medidas necesarias, podría significar una propagación de la desigualdad y la discriminación. La autora escribe en uno de sus trabajos que "los sistemas automatizados de toma de decisiones, los algoritmos de emparejamiento y los modelos de riesgo predictivo tienen el potencial de extenderse rápidamente. El estado de Indiana denegó más de un millón de solicitudes de asistencia pública en menos de tres años después de cambiar a centros de llamadas privados y procesamiento de documentos automatizado".[26] En consecuencia, Eubanks argumenta que no toda innovación significa progreso.

Los riesgos detrás de estas tecnologías son reales y una falla podría hasta tomar una vida inocente. La historia más inquietante proviene de Dumka, en la India, donde familias enteras han sufrido como resultado de *Aadhaar*, un número de identificación único de doce dígitos que el gobierno de la India ha emitido a todos los residentes en el experimento biométrico más grande del mundo. Motka Manjhi pagó el precio máximo cuando la computadora falló y

[26] Disponible en https://harpers.org/archive/2018/01/the-digital-poorhouse/

su huella digital —su clave en *Aadhaar*— no fue reconocida. Sus raciones de subsistencia se interrumpieron y se vio obligado a saltarse las comidas. Finalmente, el 22 de mayo de 2019 se derrumbó frente a su casa y murió. Su familia está convencida de que fue por hambruna.[27]

5. El marco regulatorio en Argentina

¿Cuáles son las salvaguardas que se toman para evitar la manipulación y adulteración de nuestros datos biométricos?, ¿qué tipo de garantías se deben establecer para asegurar la integridad de los datos obtenidos?, ¿cómo ampara la legislación argentina nuestros derechos frente la discriminación de algoritmos parciales y el reconocimiento facial deficiente?

La Constitución Nacional de la República Argentina contiene diversos artículos mediante los cuales reconoce el derecho a la igualdad (arts. 16, 37 y 75 inc. 17, 19, 22 y 23). Este derecho también se encuentra previsto en tratados de derechos humanos con jerarquía constitucional (art. 75 inc. 22).[28]

---

[27] Pilkington, 14 de octubre 2019, "*Digital dystopia: How algorithms punish the poor*", The Guardian. https://www.theguardian.com/technology/2019/oct/14/automating-poverty-algorithms-punish-poor

[28] Entre los instrumentos de protección de derechos humanos vigentes en nuestro país podemos mencionar la Declaración Universal de Derechos Humanos (artículo 2), la Declaración Americana de Derechos y Deberes del Hombre (artículo 2), la Convención Americana sobre Derechos Humanos (CADH) (artículos 1, 13.5, 17.4 y 24), el Pacto Internacional de Derechos Civiles y Políticos (PIDCP) (artículos 2 .1, 3, 20.2, 23.4, 24.1, 26), el Pacto Internacional de Derechos Económicos, Sociales y Culturales (PIDESC) (artículos 2.2 y 3); la Convención sobre los Derechos del Niño (CDN) (artículo 2); la Convención sobre los Derechos de las Personas con Discapacidad (CDPD) (artículos 3.b, 4.1.b, 5, 6, 7 y 12); la Convención Internacional sobre la Eliminación de Todas las Formas de Discriminación Racial (CERD) (artículos 2 y ss.), la Convención sobre la Eliminación de Todas las Formas de Discriminación contra la Mujer (CEDAW) (artículos 2 y ss.) y la Convención Internacional sobre la Protección de los Derechos de todos los Trabajadores Migratorios y de sus Familiares (artículo 1.1).

El derecho a la igualdad se traduce en no brindar tratos discriminatorios a personas en igualdad de condiciones. La ley 23.592, conocida también como ley antidiscriminatoria, describe un acto discriminatorio como aquel que impide, obstruye, restringe o de algún modo menoscaba el pleno ejercicio sobre bases igualitarias de los derechos y garantías fundamentales reconocidos en la Constitución Nacional (art. 1). A su vez, considera actos u omisiones discriminatorios "aquellos determinados por *motivos tales como* raza, religión, nacionalidad, ideología, opinión política o gremial, sexo, posición económica, condición social o caracteres físicos" (art. 1). El énfasis agregado es importante, porque denota que la enumeración no es taxativa. Por lo tanto, toda nueva forma de discriminación podría ser rechazada por la ley a pesar de no estar expresamente mencionada en su articulado.

Como se ha mencionado, las tecnologías de reconocimiento facial como forma de vigilancia masiva acarrean el peligro de discriminar a personas de ciertos grupos (como personas afroamericanas, o de origen asiático), por lo que su uso podría desembocar en el peligro de inculpar a personas inocentes acusándolas de haber cometido un determinado delito erróneamente. Ante esta situación, no solo se estaría violando el derecho a la igualdad, sino también la presunción de inocencia. Varias organizaciones, tales como Amnistía Internacional, reconocen los peligros que suscitan los sistemas de reconocimiento facial para la vigilancia masiva, y han llamado a que se prohíba su utilización ("*Amnistía Internacional reclama que se prohíba el uso de tecnología de reconocimiento facial*", 26 de enero de 2021).

Asimismo, uno de los grandes problemas que acarrea la utilización de las tecnologías biométricas, y especialmente de reconocimiento facial, es la afectación al derecho a la privacidad y la protección de los datos personales. Ya se ha mencionado que esta tecnología procesa datos personales de carácter sensible. La Ley Nro. 25.326, también conocida como ley de protección de datos

personales, tiene por objeto la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre estas se registre, de conformidad a lo establecido en el artículo 43, párrafo tercero de la Constitución Nacional.

En su artículo 5, la Ley Nro. 25.326 determina como lícita toda recolección de datos efectuada con el consentimiento libre, expreso e informado del titular. Sin embargo, hace tiempo que el consentimiento informado, en materia de datos personales, es un mecanismo endeble para regular las formas en que tanto empresas como gobiernos adquieren nuestra información. La razón es que muchas veces dependerá de ese consentimiento el acceso a servicios esenciales para la vida ciudadana; por ejemplo, como lo sería en Argentina el programa "Mi Huella" para los jubilados, pensionados y apoderados, o bien el Registro Tributario de la AFIP. Entonces, el consentimiento ya no resulta efectivo para proteger esos datos, porque se encuentra condicionado: si no se brinda, no se puede acceder a un servicio esencial.

El criterio jurídico sobre el que se fundamenta el procesamiento de los datos es fundamental para proteger nuestros datos biométricos y otros datos personales. Al sancionar la ley de protección de datos personales en el año 2000, Argentina siguió el modelo europeo. En efecto, en ese momento se redactó la ley de acuerdo con los lineamientos sentados en la Directiva de Protección de Datos (Directiva 95/46/CE), adoptada en 1995 por la Unión Europea. En Europa se utiliza el término "protección de datos personales" para designar un derecho fundamental autónomo, teniendo en cuenta el artículo 8 de la Carta de los Derechos Fundamentales de la Unión, aunque sin dejar de reconocer su fuerte vínculo con la privacidad —tanto por su relación con el artículo 7 de la Carta, como por la

interpretación del artículo 8 del Convenio Europeo de Derechos Humanos en la jurisprudencia del Tribunal Europeo de Derechos Humanos—.

Sin embargo, mientras en nuestro país no se ha vuelto sobre el tema mediante una reforma integral, el sistema jurídico europeo ha avanzado en la legislación en forma detallada. Conforme a la sanción del Reglamento General de Protección de Datos (RGDP), que entró en vigor en 2018, el reconocimiento expreso del derecho a la privacidad y del derecho a la protección de los datos personales ha llegado a su punto culmine en el ámbito europeo. En lo que respecta al tema de este trabajo, el RGPD establece tres disposiciones importantes, que se analizarán a continuación: a) el reconocimiento de los datos biométricos como datos sensibles y la expresa prohibición de su tratamiento; b) excepciones taxativas para el tratamiento de esos datos; c) evaluaciones de impacto ante el tratamiento de los datos mediante el uso de nuevas tecnologías.

En su artículo 9, el RGPD establece que "está prohibido el tratamiento de datos personales que revelen el origen étnico, o racial (…) datos genéticos, *datos biométricos* dirigidos a identificar de manera unívoca a una persona física (…)". Por el contrario, en ningún artículo de la ley 25326 se reconoce a los datos biométricos como datos sensibles, lo que ya brinda indicios de que la ley debería revisarse en su integralidad para adaptarse a las exigencias de la era digital.

El RGDP también establece diferentes excepciones que posibilitan el tratamiento de los datos sensibles. En primer lugar, el art. 9 inc. 2 establece que se podrá dar tratamiento a estos datos siempre que el interesado haya otorgado su consentimiento explícito. Como se ha mencionado, el consentimiento no resulta efectivo para la protección de los datos personales en la mayoría de las circunstancias. Además, en este caso en particular resultaría imposible utilizar el consentimiento como fundamento para la

recolección masiva de datos biométricos, dado que las personas no brindan su consentimiento para su uso por parte de fuerzas policiales. Por lo tanto, en este caso, debemos buscar otro criterio sobre el cual se fundamentar la recolección legal de estos datos. Así es que el RGPD establece que podrían recolectarse "por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado" (art. 9 inc. 2(g)). De esta forma, la Unión Europea busca que el tratamiento de estos datos se base específicamente en leyes dictadas a tal fin; a modo de ejemplo, puede mencionarse la Directiva 2016/680 sobre el tratamiento de los datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales.

Mientras tanto, el artículo 5 inc. 2(b) de la Ley Nro. 25.326 establece que "no será necesario el consentimiento cuando se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal". Sin embargo, como nuestra legislación no considera a los datos biométricos como una categoría de datos sensibles, existe un vacío legal al respecto difícil de llenar sin una reforma integral. Por lo tanto, aunque no existan leyes que autoricen el uso de sistemas de reconocimiento facial de vigilancia masiva con fines determinados, de todas formas, técnicamente no se estaría violando la ley con el tratamiento de estos datos, dado que no se reconocen como una categoría de datos sensibles.

Podría decirse que ley argentina intenta posicionar varios principios que buscan limitar la recolección y el tratamiento de datos de la misma forma en que lo hace el RGDP, aunque como se ha mencionado, este lo hace con más detalles y basándose en un sistema donde los principios, sobre todo de necesidad y proporcionalidad,

cumplen un rol central. Por ejemplo, en su artículo 4, la ley argentina describe cómo debe ser la calidad de los datos, y sostiene que a los efectos de su tratamiento deben ser "ciertos, adecuados, pertinentes y *no excesivos en relación al ámbito y finalidad para los que se hubieren obtenido*". El tratamiento de los datos, entonces, debe ser *limitado* a los fines por los que se los obtuvo. El artículo es acertado, pues si se permitiera la libre acumulación de datos se estaría otorgando a las empresas y a los gobiernos una fuente ilimitada de poder sobre los individuos. Sin embargo, surgen dos problemas. En primer lugar, la ley argentina falla en el adecuado reconocimiento de las categorías de datos sensibles, así como la identificación taxativa y explícita de excepciones, como sí lo hace el RGDP. En segundo lugar, aún cuando la norma con sus defectos tímidamente establece disposiciones que podrían aplicarse, estas no se traducen en la práctica.

Por último, y en lo que respecta a la utilización de sistemas de reconocimiento facial o el tratamiento de datos biométricos, el RGDP establece un mecanismo interesante en su sección 3: la evaluación de impacto relativa a la protección de datos (DPIA, por sus siglas en inglés). Aquellas organizaciones que realicen el tratamiento de datos mediante la implementación de nuevas tecnologías, que pueda significar un alto riesgo para los derechos y libertades de las personas físicas, deben llevar adelante esta evaluación. En contraste, si bien la Agencia de Acceso a la Información Púbica de Argentina, en trabajo conjunto con la Unidad Reguladora y de Control de Datos Personales de Uruguay, publicó en 2020 una "Guía de evaluación de impacto en el tratamiento de datos personales", la ley argentina no ha receptado aún la obligatoriedad de esta evaluación. Nuevamente vemos la inminente necesidad de que el Congreso revise la normativa vigente y la adapte a las circunstancias actuales, sobre todo teniendo en cuenta las exigencias de la Unión Europea en materia de transferencia de datos, así como el hecho de que la Argentina es un Estado parte del

Convenio 108 para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personales.[29]

Entendemos que la Argentina debe tomar este Reglamento como fuente de inspiración para modernizar su legislación, y no solamente "emparchar" la legislación vigente mediante guías con recomendaciones específicas que no se traducen en normas de carácter obligatorio. Dado el colosal avance tecnológico que se ha producido en las últimas dos décadas —en particular el indiscriminado aumento del uso de tecnologías biométricas y de reconocimiento facial—, es momento de revisar nuestra legislación en materia de privacidad y protección de datos personales, siguiendo el ejemplo de la Unión Europea que ya han tomado otros países de Latinoamérica.

6. Conclusión

En un mundo donde el desarrollo tecnológico se desenvuelve a una velocidad exponencial, se requiere de un gran esfuerzo para asimilar y entender lo que ocurre en el mundo y formular propuestas para mejorarlo. Sin embargo, ese esfuerzo es necesario si procuramos construir un futuro en el que la tecnología se utilice para promover el desarrollo sustentable, la innovación y el bienestar general, la igualdad y la no discriminación, con un enfoque respetuoso de los derechos humanos. Este trabajo ha procurado ser una contribución a esa búsqueda.

La IA, los algoritmos y la biometría, en especial su aplicación en materia de reconocimiento facial, se presentan como herramientas útiles a la hora de llevar a cabo numerosas tareas. Sin embargo, se ha visto que la tecnología no es ajena a los errores y puede presentar

[29] IAPP (2020) Argentina y Uruguay aprueban Guía de Evaluación de Impacto en la Protección de Datos https://iapp.org/news/a/argentina-y-uruguay-aprueban-guia-de-evaluacion-de-impacto-en-la-proteccion-de-datos/

tantas imperfecciones como sus creadores. Como se ha examinado, los algoritmos pueden entrenarse tanto sobre la base de datos o muestras parciales, que llevan a que se reproduzcan —e incluso profundicen— sesgos y patrones discriminatorios. ¿Qué pensarían nuestros antecesores de nuestra nueva "religión de datos"? ¿Qué pensarán los venideros sobre lo que hicimos con tanta información y conectividad? ¿Estamos usando los avances tecnológicos para mejorar las instituciones y afianzar nuestros derechos, o acaso estamos permitiendo que el avance sin reglas definidas atropelle nuestros derechos y garantías fundamentales?

Los rasgos faciales son fácilmente accesibles a través de fotografías que cada día subimos públicamente a internet, o incluso pueden ser analizados a partir de fotografías que nos toman a diario sin tener conocimiento de ello. Además, las huellas dactilares pueden ser capturadas de una infinidad de elementos que tocamos en nuestro camino a diario, e incluso ser utilizadas sin nuestro consentimiento. Por lo tanto, cuando el Estado o personas jurídicas se encargan de la recolección masiva de los datos biométricos de sus ciudadanos corresponde preguntarnos, ¿qué tipo de garantías se deben establecer para asegurar la integridad de nuestros derechos fundamentales a raíz de los datos obtenidos?

La normativa argentina pareciera cubrir aspectos básicos, pero no los suficientes como para cubrir todos los problemas que se suscitan con la aplicación cada vez más indiscriminada de las tecnologías de reconocimiento facial, especialmente mediante el uso de algoritmos automatizados y de sistemas de IA. Es imperioso que tanto el ámbito publico como en el privado se realice una revisión exhaustiva de los mecanismos existentes para proteger los derechos fundamentales frente a la aplicación de estas tecnologías, y que se avance en el desarrollo de legislación especifica que provea mejores soluciones frente a los problemas que estas pueden traer. También es elemental supervisar la aplicación de estas tecnologías, especialmente para garantizar que su aplicación no sea

discriminatoria, y conseguir que su uso en el ámbito privado o gubernamental sea de público conocimiento a los usuarios o civiles. Debe informarse sobre estas prácticas y concientizarse sobre la otra cara que esconden estas tecnologías. A su vez, es indispensable fomentar la investigación en la materia para así lograr que se legisle a favor de la protección de nuestros derechos en la era digital sobre la base de la evidencia.

Para finalizar, es importante destacar que, a pesar de todo el avance en la legislación vigente, en Europa autoridades en materia de protección de datos han instado a que se prohíba totalmente el uso de la IA para reconocer automáticamente a las personas. Aunque consideramos poco probable que esto ocurra, sí debería ser un llamado de atención para establecer mecanismos jurídicos y extrajurídicos robustos que pongan la protección de los derechos fundamentales de las personas en el centro. En este momento, Argentina tiene una seria deuda pendiente en esta materia.

Referencias

Alfonso Mancilla Herrera et al., "Diseño y Construcción de Algoritmos", 2015, https://elibro.net/en/ereader/sibuca/69931

Amba Kak, ed., "Regulating Biometrics: Global Approaches and Urgent Questions" AI Now Institute, September 1 2020, https://ainowinstitute.org/regulatingbiometrics.html.

Asociación por los Derechos Civiles. *Desafíos de la biometría para la protección de los datos personales. Reflexiones sobre el caso SIBIOS*. Mayo 2017. https://adcdigital.org.ar

Asociación por los Derechos Civiles. *Cuantificando identidades en América Latina. Un breve repaso acerca de cómo las sociedades latinoamericanas se enfrentan a la implementación de las tecnologías biométricas*. Mayo 2017. https://adcdigital.org.ar

Asociación por los Derechos Civiles. *La identidad que no podemos cambiar. Cómo la biometría afecta nuestros derechos humanos*. Abril 2017. https://adcdigital.org.ar

Bonacorso. G. *Machine Learning Algorithms*. (2017). Birmingham. Packt Publishing.

Bo Cowgill and Catherine Tucker. *Algorithmic Bias: A Counterfactual Perspective*. Working Paper: NSF Trustworthy Algorithms, December 2017, Arlington, VA.

Bronstein, Hugh. "Rights group blasts Argentina for using face recognition tech on kids". Reuters. 2020. https://uk.reuters.com/article/argentina-rights/rights-group-blasts-argentina-for-using-face-recogn ition-tech-on-kids-idUSL1N2GZ23N

Comisión Europea (2020) *Libro Blanco sobre la inteligencia artificial - un enfoque europeo orientado a la excelencia y la confianza*. Bruselas, 19.2.2020 COM(2020) 65 final https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_es.pdf

Council of Europe. *Study on the human rights dimensions of automated data processing techniques (in particular algorithms) and possible regulatory implications*. Prepared by the committee of experts on internet intermediaries (MSI-NET). DGI(2017)12.

Dastin Jeffrey. (2018) "Amazon scraps secret AI recruiting tool that showed bias against women".

https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G

David Danks and Alex John London. *Algorithmic Bias in Autonomous Systems*. Proceedings of the Twenty-Sixth International Joint Conference on Artificial Intelligence (IJCAI-17).

Deibert, Ronald J. "Black Code: Surveillance, Privacy, and The Dark Side of the Internet", 2013.

Dr. Philipp Hacker, LL.M. (Yale). *Teaching Fairness to Artificial Intelligence: Existing and Novel Strategies against Algorithmic Discrimination under EU Law*. Common Market Law Review. https://ssrn.com/abstract=3164973

Ed Pilkington. *Digital dystopia: how algorithms punish the poor*. The Guardian. 2019. https://www.theguardian.com/technology/2019/oct/14/automating-poverty-algorithms-punish-poor

European Parliament (2019). *A comprehensive European industrial policy on artificial intelligence and robotics*. 12.2.2019. (2018/2088(INI)). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52019IP0081&from=EN

Georgetown Law. Center of Privacy and Technology (2016). *The perpetual line-up. Unregulated police face recognition in America*. www.perpetuallineup.org

Gillian. B. White. "When Algorithms Don't Account for Civil Rights. Do lucrative deals with advertisers have to come at the expense of users' civil rights?". The Atlantic. 2017. https://www.theatlantic.com/business/archive/2017/03/facebook-ad-discrimination/518718/

Hao, Karen. “La presión pública obliga a Amazon a paralizar el reconocimiento facial”. MIT Technology Review. 2020.

https://www.technologyreview.es/s/12332/la-presion-publica-obliga-amazon-paralizar-el-reconoc imiento-facial

Harari. Y. N. (2016). *Homo Deus*. Londres. Penguin Random House UK.

Ignacio Serna, Aythami Morales, Julian Fierrez, Manuel Cebrian, Nick Obradovich, Iyad Rahwan. (2020). Algorithmic Discrimination: Formulation and Exploration in Deep Learning-based Face Biometrics. Universidad Autónoma de Madrid, Madrid, Spain. https://github.com/BiDAlab/DiveFace

Jon Kleinberg, Jens Ludwig, Sendhil Mullainathany and Cass R. Sunstein. (2019). *Discrimination in the age of algorithms*. Published by Oxford University Press on behalf of The John M. Olin Center for Law, Economics and Business at Harvard Law School. http://creativecommons.org/licenses/by-nc/4.0/

La Nación. (2014). "Los jubilados y pensionados tendrán que registrar sus huellas digitales para cobrar sus haberes". http://www.lanacion.com.ar/1756361-jubilados-y-pensionados-huellas-dactilares-anses

Latanya Sweeney. *Discrimination in Online Ad Delivery. Google ads, black names and white names, racial discrimination, and click advertising*. 2013 ACM.

López de Mántaras Badía. R. Meseguer González. P. (2017) *Inteligencia artificial*. Madrid. Ed. CSIC.

Lucas D. Introna and David Wood. (2004). *Picturing Algorithmic Surveillance: The Politics of Facial Recognition Systems. Surveillance & Society*. CCTV Special (eds. Norris, McCahill and Wood) 2(2/3): 177-198 http://www.surveillance-and-society.org/cctv.htm

Meiling Fang, Naser Damer, Florian Kirchbuchner, Arjan Kuijper. *Demographic Bias in Presentation Attack Detection of Iris Recognition Systems*. Fraunhofer Institute for Computer Graphics Research IGD. Darmstadt. Germany Mathematical and Applied Visual Computing. TU Darmstadt. Darmstadt. Germany.

Michael Reilly. "Is Facebook targeting advertising at depressed teens?". MIT Technology Review. https://www.technologyreview.com/s/604307/is- facebook-targeting-ads-at-sad-teens/.

Mitchell M. T. *Machine Learning*. (1997). New York. McGraw-Hill.

Mota S. (2015) "What is an algorithm? A response based on Wittgeinstein's work". Madrid, ÉNDOXA: Series Filosóficas, n.o 36, p.317-328.

Nick Srnicek. (2016). *Capitalismo de plataformas*. Caja Negra Editora. CABA.

Pasquale Frank (2015). *The Black Box Society. The Secret Algorithms That Control Money and Information*. Harvard College.

Pawel Drozdowski, Christian Rathgeb, Antitza Dantcheva, Naser Damer, and Christoph Busch. (2020). *Demographic Bias in Biometrics: A Survey on an Emerging Challenge*. IEEE Transactions on Technology and Society. Vol.1. N.2.

Philipp Terho, Jan Niklas Kolf, Naser Damer, Florian Kirchbuchner, Arjan Kuijper. (2002). *Post-comparison mitigation of demographic bias in face recognition using fair score normalization*. Fraunhofer Institute for Computer Graphics Research IGD, Darmstadt, Germany. Technical University of Darmstadt, Darmstadt, Germany.

Sandra Wachter. *Affinity Profiling and Discrimination by Association in Online Behavioural Advertising*. Oxford Internet Institute, University of Oxford, 1 St. Giles, Oxford, OX1 3JS, UK; the Alan Turing Institute, British Library, 96 Euston Road, London, NW1 2DB, UK. https://ssrn.com/abstract=3560645

Sarah Valentine. *Impoverished Algorithms: Misguided Governments, Flawed Technologies, and Social Control*. 46 Fordham Urb. L.J. 364 (2019). Puede consultarse en: https://ir.lawnet.fordham.edu/ulj/vol46/iss2/4

Solon Barocas and Andrew D. Selbst (2016). *Big Data's Disparate Impact*. California. Law Review. Vol. 104, No. 3, pp. 671-732 (62 pages).

Stuart Summer. (2016). *You: For Sale: Protecting Your Personal Data and Privacy Online*. Elsevier. USA.

Venditti, Lydia F.; Fleming, Jim; and Kugelmeyer, Kara, "Algorithmic Surveillance: A Hidden Danger in Recognizing Faces" (2019). Honors Theses. Paper 932.

https://digitalcommons.colby.edu/honorstheses/932Wayman, James; Jain, Anil; Maltoni, Davide, Maio, Dario; "Biometric Systems: Technology, Design and Performance Evaluation", Springer, London, 2005.

Wired, "Facebook's '10 Year Challenge' Is Just a Harmless Meme—Right?", 15 de enero de 2019, visitar en: https://www.wired.com/story/facebook-10-year-meme-challenge/

Zuiderveen Borgesius, F. (2018). *Discrimination, artificial intelligence, and algorithmic decision-making*. Council of Europe, Directorate General of Democracy. https://rm.coe.int/discrimination-artificial-intelligence-and-algorithmic-decision-making/1680925 d73