LA RECOPILACIÓN DE DATOS BIOMÉTRICOS EN COSTA RICA: CONTROVERSIAS ÉTICAS A PARTIR DEL PROYECTO DE LEY Nº 21321

THE COLLECTION OF BIOMETRIC DATA IN COSTA RICA: ETHICAL CONTROVERSIES BASED ON BILL NO. 21.321

Jonathan Piedra Alegría[1]

Resumen: El artículo abordará desde la ética los principales desafíos, así como los retos del manejo y utilización de los datos biométricos. Para esto se tomará como material inicial de reflexión el Proyecto de Ley/expediente Nº 21321, presentado el 27 de marzo de 2019 en Costa Rica. Dicha propuesta busca crear una base única de datos biométricos para la verificación de identidad de personas en Costa Rica. Teniendo como base el documento anterior, se analizarán las implicaciones éticas-filosóficas del Proyecto de Ley (expediente N° 21321), con tal de que sirvan como ejemplo para los desafíos presentes a la hora de recopilar y manejar los datos biométricos.

Palabras clave: Datos biométricos, recopilación, gestión, privacidad, sesgo algorítmico, ética.

Abstract: The article will address the main challenges of ethics and the challenges of handling and using biometric data. For this, the Bill of Law/file No. 21321, presented on March 27, 2019, in Costa Rica, will be taken as initial material for reflection. This proposal seeks to create a unique biometric database for the identity verification of people in Costa Rica. Based on the previous document, the ethical-philosophical implications of the Bill (File 21321) will be analyzed, provided that they serve as an example

1 Afiliación: Universidad Nacional (Costa Rica). jonathan.piedra.alegria@una.cr. Grados: Doctor en Filosofía. Máster en Filosofía Contemporánea, Máster en Derechos Humanos. Licenciado en Filosofía. Licenciado en Derecho. ID ORCID: 0000-0003-4532-4415.

of the present challenges when collecting and managing biometric data.
Keywords: Biometric data, collection, management, privacy, algorithmic bias, ethics.

Introducción

El uso de la tecnología biométrica ha experimentado un aumento significativo en los últimos años. Ya sea a través de sistemas de reconocimiento facial en aeropuertos o dispositivos de control y autenticación de datos biométricos en fronteras, estas tecnologías son comunes en la actualidad. No solo presentan grandes posibilidades para los Estados en términos de seguridad y autenticación de personas, sino que también han sido aprovechadas por empresas privadas. La demanda de tecnologías biométricas ha aumentado tanto que el tamaño del mercado global se espera que crezca de USD 42.9 mil millones en el 2022 a USD 82.9 mil millones en el 2027, con un aumento anual del 14.1%[2].

La pandemia de SARS-CoV-2 impulsó la demanda de sistemas sin contacto de reconocimiento e identificación por motivos de higiene, pero estos sistemas ya eran considerados prometedores antes de la pandemia. Desde una perspectiva comercial, estos sistemas pueden brindar mayor comodidad para el control de acceso o el comercio móvil para los usuarios, aumentando la eficiencia, personalización y seguridad. Por ejemplo, en los teléfonos móviles, se utiliza tecnología de reconocimiento de huellas dactilares, rostro, voz e iris. Estos sistemas suelen ser rápidos, precisos, estables y no invasivos, y pueden hacer más intuitivas y amigables con el usuario las aplicaciones comerciales.

Desde un punto de vista gubernamental, la tecnología biométrica ofrece una *autenticación transparente*. Normalmente, para identificarnos en un servicio en línea, adquirir un producto o identificarnos ante una institución pública, es necesario introducir una serie de datos o una contraseña. La autenticación transparente permite verificar la identidad del usuario sin la necesidad de ingresar manualmente una contraseña, ya que los rasgos biométricos son más difíciles de falsificar o replicar que el nombre de usuario o las contraseñas tradicionales. Estas tecnologías se pueden utilizar para el control de acceso, alertas de amenazas, prevención de fraudes, identificación de personas en servicios públicos, reconocimiento de delitos, búsqueda de personas desaparecidas o

2 Véase en: Marketresearch.com

secuestradas, entre otros. Sin embargo, su campo de aplicación es mucho más amplio y no se limita a cuestiones económicas.

Tanto para la empresa privada, como para los servicios públicos, la implementación y utilización de este tipo de tecnologías plantea muchos riesgos y dilemas. Dentro de sus principales desafíos se incluyen el tema de la confiabilidad, desconfianza de los usuarios respecto a la entrega de información personal, la forma en cómo se conservan los datos biométricos o quién puede acceder a ellos. También es importante el tema de la discriminación y la justicia. Así, por ejemplo, Coeckelbergh nos indica:

> "En todo el mundo, la tecnología de reconocimiento facial y otras tecnologías biométricas, como las huellas dactilares y los escaneos de iris, se emplean en aeropuertos y otros puntos de cruce fronterizo. Así como incurrir en el riesgo y discriminación (…) y amenazas a la privacidad[3]."

Con respecto a la utilización de las tecnologías de identificación biométrica por parte de los gobiernos, el principal debate es el uso adecuado de esas tecnologías. Uno de los principales temores es que los Estados o regímenes autocráticos utilicen estas tecnologías para fines poco democráticos. Como ejemplo de esta situación, se menciona con frecuencia la vigilancia biométrica en China por medio del uso de tecnología de reconocimiento facial para identificar a las personas en lugares públicos (Feng, 2019). Esta tecnología se utiliza en una variedad de aplicaciones, incluida la seguridad, el cumplimiento de la ley o el transporte. Es habitual que las cámaras de reconocimiento facial se utilicen en los centros de transporte, como aeropuertos y estaciones de tren, para identificar a las personas y verificar sus identidades (Feng, 2019).

También, existen otras formas de vigilancia biométrica que incluyen el uso de escáneres de huellas dactilares, escáneres de iris y tecnología de reconocimiento de voz. Estas tecnologías a menudo se usan en combinación con otras formas de vigilancia, como cámaras de circuito cerrado de televisión, para rastrear y monitorear a las personas en tiempo real. La mayoría de estos usos se encuentra legitimado bajo la premisa de una mayor seguridad pública. Todos estos usos generan

3 "Across the world, facial recognition technology and other biometrics technologies such as fingerprints and iris scans are being employed un airports and other border crossing sites. As well as incurring the risk and discrimination (…) and threats to privacy" (Coeckelbergh, 2022, p.12).

preocupaciones sobre la intrusión desmesurada a la privacidad o las limitaciones a las libertades civiles. Desde hace varios años existen reportes que indican que China ha empleado la vigilancia biométrica para monitorear a comunidades étnicas minoritarias en la Región Autónoma Uigur de Xinjiang con tal de controlarlos geográficamente y así facilitar su detención e internamiento en centros de reeducación. (CRS, 2021, p. 1). Pero este tipo de control social y represión no es único de este país asiático. En Irán, desde el año 2015, el gobierno comenzó a utilizar una tarjeta de identidad nacional biométrica (la tarjeta posee "chip" inteligente y almacena datos biométricos).

Sin embargo, su uso se ha vuelto discriminatorio, debido a que a partir del año 2020 el gobierno iraní dejó de permitir que los solicitantes de la tarjeta eligieran la opción "Otro" en el campo de religión del formulario de solicitud, que anteriormente era una de las opciones disponibles (Grant, 2020). Esto ha provocado que los actuales solicitantes deban elegir obligatoriamente una de las cuatro religiones reconocidas oficialmente que figuran en el formulario (islamismo, cristianismo, judaísmo o zoroastrismo). Ante esto, a las personas de minorías religiosas no les queda más que mentir sobre su identidad religiosa o no obtener la tarjeta. Pero no solo esto sucede en la actualidad. Existe un serio riesgo de que la información biométrica obtenida se utilice con tecnología de reconocimiento facial para identificar a las personas que violan el código de vestimenta obligatorio. Tanto así que, recientemente salió a luz un plan del gobierno iraní para utilizar el reconocimiento facial para hacer cumplir la nueva ley sobre el hiyab, principalmente para reprimir más aún a las mujeres en los espacios públicos (Strzyżyńska, 2022).

Pero los usos de las tecnologías de reconocimiento biométrico pueden ser mucho más perturbadores. En el año 2021, debido a la retirada de las tropas de estadounidenses de Afganistán, los talibanes se adueñaron de las bases de datos biométricos de la población, así como de muchos de los sistemas necesarios para el reconocimiento de estos datos. Existen muchas sospechas con respecto a que estos datos hayan sido utilizados para la eliminación de aquellas personas que se les opongan. "Los talibanes podrían usarlos para atacar a los opositores percibidos, y la investigación de Human Rights Watch sugiere que es posible que ya hayan usado los datos en algunos casos"[4] (HRW, 2022).

Pero este tipo de cosas no sucede únicamente en regímenes totalitarios. Algunos países democráticos también están tomando medidas con ciertas similitudes. *Verbigracia*, en el Estado de New York en

4 "The Taliban could use them to target perceived opponents, and Human Rights Watch research suggests that they may have already used the data in some cases" (HRW, 2022).

los Estados Unidos, un reciente estudio demostró que el uso de tecnologías de reconocimiento facial reforzó prácticas policiales racistas. "Nuestro análisis demuestra que el uso de la tecnología de reconocimiento facial por la policía de Nueva York contribuye a reforzar una actuación policial discriminatoria contra las comunidades minoritarias de la ciudad" (Amnistía Internacional, 2022).

Como vemos, el uso negativo de la tecnología biométrica ha generado serios debates sobre los Derechos Humanos y el potencial de abuso de poder. Todo este tipo de situaciones hacen necesaria una reflexión desde un punto de vista ético con el cual se puedan analizar y desplegar los aspectos filosóficos, sociales y culturales de la utilización de estas tecnologías en una escala como la que se está viendo.

El Proyecto de Ley Nº 21.321

América Latina no se encuentra exenta de estos desafíos. En Costa Rica se presentó en el año 2020 el proyecto de *Ley de repositorio único nacional para fortalecer las capacidades de rastreo e identificación de personas* (Proyecto Nº 21.321) en Costa Rica. El proyecto, como su nombre lo indica, busca crear un repositorio único o una base de datos centralizados que recopile los datos de todos los costarricenses y extranjeros (mayores de 12 años) que ingresen al país latinoamericano. Este proyecto tiene como objetivo lograr una verificación inequívoca de la identidad de personas. La creación de esta base de datos pretende complementar el trabajo que el Tribunal Supremo de Elecciones (TSE) ha venido desarrollando, desde hace más de veinte años, en lo concerniente a un sistema de identificación basado en la huella dactilar. Esto implica pasar de un sistema bidactilar (dos huellas) a uno decadactilar (diez huellas) con tal de aumentar el nivel de seguridad y precisión en cuanto a la identificación de una persona. A esta transición, que en principio debía ocurrir en el año 2020, se le iba a sumar la incorporación de sistemas para el reconocimiento facial[5]. Esta incorporación parecía una transición lógica ya que la recopilación de estos datos biométricos ya se venía realizando sin un debido marco regulatorio que definiera adecuadamente los límites o las protecciones pertinentes a para este tipo de datos. No obstante, esta situación no fue la que finalmente dio paso a la propuesta. De hecho, en el

5 A pesar de que para esa fecha y hasta ahora tampoco existe una regulación adecuada para la implementación o el uso de estas tecnologías. La regulación local es insuficiente y no contempla normas específicas para el uso de la biometría en campos como la seguridad, por ejemplo.

texto base del Proyecto Nº 21.321 se encuentra una justificación distinta. En dicho documento se menciona que la principal intención de esta base de datos centralizada es evitar la criminalidad y aumentar la seguridad (un *topoi* muy utilizado por los gobiernos). Es precisamente para esto que, según el Proyecto Nº 21.321,

> se deben tomar todas las medidas urgentes y necesarias para atacar la criminalidad y proveer a las autoridades policiales y de investigación judicial de las herramientas posibles para que puedan cumplir con su responsabilidad de mantener la paz y la seguridad a lo largo y ancho del país (Ley 21.321, 2020, p.2).

Ciertamente, la propuesta en cuestión se encuentra en consonancia con las tendencias tecnológicas y políticas más actuales sobre estos asuntos. La tecnología de identificación biométrica es tan eficiente para fines relacionados con la seguridad (Woodward et al., 2003; Bowyer et al., 2004) que las fuerzas policiales en todo el mundo la están adoptando sin mayores cuestionamientos[6]. Estas tecnologías por lo general se basan en el análisis de características fisiológicas, elementos comportamentales o también por combinación de ambas. Los registros más habituales son las huellas dactilares, el iris ocular, el reconocimiento facial y el reconocimiento de la voz. La rápida implementación de la biometría ha provocado una revolución dentro de la industria de la seguridad y el cumplimiento de la ley a nivel mundial. Esta revolución es la que se quiere llevar al Poder Judicial costarricense al actualizar las herramientas con las cuales pueden prevenir y sancionar los delitos. Por eso se necesita

> procurar una revisión de nuestra legislación en esta materia, que le permita al país contar con tecnología de última generación, no solo para el registro dactilar, sino incluso biométrico, que venga a facilitar el trabajo de identificación de sujetos que pudieran estar relacionados con hechos delictivos, que vengan a robustecer el registro de las personas extranjeras que ingresan al país y sus movimientos migratorios, y que logremos ser más eficientes con el uso de los recursos públicos, de manera tal que no repliquemos esfuerzos y malgastemos el dinero de todos los costarricenses. (Ley 21.321, 2020, p.4)

Es así, como la creación de ese repositorio único de información biométrica tiene como principales metas: 1) Una mejora en la prevención en la comisión de delitos, así como una mayor seguridad a la hora del cumplimiento de las normas legales, y 2) una optimización de los recursos públicos en vista de que el sistema biométrico es más confiable (y, por lo tanto, existe una reducción de tiempo y dinero).

6 Por ejemplo, el caso de la tecnología *Rekognition* de Amazon en los Estados Unidos de América (Piedra, 2021).

Una serie de propósitos bastante loables que, sin embargo, se encuentran carentes de un análisis sobre los desafíos éticos relacionados con la implementación y utilización de una tecnología como esta. Aspectos que, como veremos más adelante, plantean importantes retos para la creación de esta base unificada.

Controversias éticas

Violación a la privacidad informacional

A pesar de su aplicación generalizada, los sistemas de reconocimiento biométrico plantean muchos desafíos. Un reto importante se encuentra en la intrusión a la privacidad y a la intimidad. De hecho, posiblemente el tema de la privacidad sea uno de los temas éticos centrales, relacionados con las tecnologías de reconocimiento biométrico.

Según la Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales (N° 8.968) en Costa Rica, hay dos categorías principales de datos personales: (1) Datos personales en sentido general, que incluyen cualquier información que permita identificar a una persona física, ya sea directa o indirectamente. Por ejemplo, el nombre, la dirección y el número de teléfono. Estos se subdividen en: (1.1) Datos personales de acceso irrestricto, que se encuentran en bases de datos públicas y son accesibles para cualquier persona, y (1.2) Datos personales de acceso restringido, que pueden estar en algunas bases de datos públicas, pero solo son relevantes para la persona titular o, en algunos casos, para la Administración Pública. (2) Los datos sensibles, que son aquellos que pueden ser utilizados para discriminar o excluir a una persona, como la orientación sexual, la opinión política o las características socioeconómicas.

Es necesario recordar que "Los datos biométricos son aquellos que pertenecen puramente a los orgánicos (los vivos) y son métricos (medibles), por ejemplo: contorno o forma de la mano, de los dedos, huellas dactilares digitales, venas, su temperatura, forma facial, imagen del iris, latido del corazón, su ritmo, etc."[7] (Paret y Crégo, 2019, p. 60). De manera similar, el Reglamento General de Datos de la Unión Europea

7 "Biometric data are those that belong purely to organics (the living) and are metric (measurable), for example: outline or shape of the hand, of fingers, digital fingerprints, veins, their temperature, facial shape, image of the iris, heartbeat, its rhythm, etc" (Paret y Crégo, 2019, p. 60).

define a los datos biométricos: como "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" (GDPR, Art.4).

Si relacionamos ambos elementos, se puede inferir que en Costa Rica los datos biométricos son datos personales que, por su naturaleza sensible (ya que puede ser utilizada para discriminar o excluir a una persona), son de acceso restringido y solo podrían ser accedidos o verificados en casos muy específicos (que se deberían indicar expresamente) por la Administración Pública.

El artículo inicial del Proyecto Nº 21.321 señala que:

> ARTÍCULO 1: El Tribunal Supremo de Elecciones tendrá la responsabilidad de crear, como reserva de Estado, una Plataforma Nacional de Identificación Biométrica, la cual almacenará en un único repositorio nacional información biométrica de todos los costarricenses mayores de doce años, sin perjuicio de que se pueda adquirir nueva tecnología que permita ampliar la identificación de personas a través de la incorporación de más rasgos biométricos que se consideren necesarios. (Proyecto Ley 21.321, 2020, art. 1)

Además:

> ARTÍCULO 4: Los Poderes de la República, los órganos del Poder Legislativo, los ministerios y sus órganos adscritos que requieran verificar la identidad de las personas, utilizarán la Plataforma Nacional de Identificación Biométrica del Tribunal Supremo de Elecciones para el cumplimiento de sus fines y quedarán exentos de los cargos a los cuales se refiere el artículo 24 del Código Electoral.
> Las instituciones descentralizadas que conforman el sector público costarricense y el sector privado en general, que requieran verificar la identidad de las personas por medio de la citada plataforma nacional, podrán adquirir los servicios correspondientes de conformidad con lo que establece el artículo 24 del Código Electoral. (Proyecto Ley 21.321, 2020, art. 4).

La base de datos unificada estaría inscrita en el Tribunal Supremo de Elecciones (a través de la Dirección General de Estrategia Tecnológica). En los artículos siguientes se menciona que instituciones como el Organismo de Investigación Judicial, el Ministerio de Seguridad (y todos los cuerpos policiales adscritos) o la Dirección de Migración del país, tendrían acceso irrestricto a los datos que se encuentren en este repositorio. En el documento también se señala que otras instituciones públicas y empresas privadas podrán acceder a los sistemas que permiten la verificación, siempre y cuando realicen el pago estipulado para estos fines.

Todas estas situaciones nos plantean escenarios problemáticos relacionados con la privacidad que debemos considerar. La privacidad es un aspecto fundamental en las sociedades pluralistas y democráticas. Como indica Lukács (2016),

"La importancia de la privacidad puede relacionarse con el hecho de que la privacidad tiene una conexión muy estrecha con la dignidad humana, la libertad y la independencia del individuo, y es cada vez más cuestionada en la era del rápido desarrollo tecnológico de la sociedad de la información"[8].(p. 256).

Es relevante tener esto en cuenta, ya que por lo general el tema de la privacidad se aborda exclusivamente desde un marco exclusivamente individual.

No obstante, nuestra argumentación busca indicar que la privacidad no solo implica una visión individual relacionada con aspectos de la personalidad y la intimidad (como el caso que estamos analizando), sino que además envuelve una visión global de la sociedad, las relaciones entre sus miembros y la intervención del Estado. Según (Korja, 2006)

La privacidad física se puede definir como el derecho a estar libre de registros indeseables, intrusiones irrazonables o registros del propio cuerpo. La privacidad física se relaciona con la integridad corporal y está indirectamente relacionada con la integridad emocional junto con la dignidad humana (p.209).

Desde este punto de vista, la esfera de la privacidad implica un dominio íntimo que no solo involucra aspectos físicos. "La construcción individual de un dominio personal de elección y privacidad se generaliza a través de las culturas y no se restringe a las personas que viven dentro de las sociedades occidentales o 'modernas'" [9](Nucci en Trina, 2011, p.191).

8 "The importance of privacy can be related to the fact that privacy has a very close connection with human dignity, freedom and independence of the individual, and it is more and more challenged in the age of the rapid technological development of the information society."

9 The individual construction of a personal domain of choice and privacy generalizes across

Según un informe del 2006 de la *National Science and Technology Council* de los Estados Unidos, la privacidad incluye al menos dos aspectos diferentes: 1) Un espacio vital de las personas para tomar decisiones sobre los elementos que afectan su vida y su cuerpo. Por ejemplo, elegir con quién formamos una relación afectiva, la ropa que queremos, los lugares a los que deseamos ir, a quiénes les permitimos o no entrar a nuestros hogares, la comida con la que nos alimentamos, etc. Incluso aspectos relacionados con nuestro deseo (o no) de utilizar un tratamiento médico o temas relacionados con el final de la vida. 2) En un segundo lugar, también se encuentra un espacio intencional (*intentional)* que se relaciona con aspectos relativos a la comunicación (o transmisión) de actividades íntimas o de naturaleza personal. Algunos ejemplos serían: la publicación de fotografías, la grabación de conversaciones o la divulgación de vídeos íntimos. Finalmente, también existe un espacio informativo que se relaciona directamente con mi información personal y el uso concreto que quiero darle a esta.

La perspectiva de privacidad que más se adecua a los sistemas de información biométrica es esta última: la privacidad informacional. Precisamente este punto es el que más origina preocupaciones sobre cómo se generan y almacenan los datos biométricos, así como quién puede tener acceso a los sistemas de verificación de estos repositorios. Estas inquietudes se dirigen principalmente a los usos por parte de los Estados (en el caso en cuestión del Proyecto Nº 21.321), pero tampoco se resumen a ellos. También es habitual encontrar debates sobre la adecuada formulación de políticas que puedan garantizar un equilibrio entre los derechos de las personas y algunos intereses privados o comerciales.

Este es un tema muy problemático en el Proyecto Nº 21.321 ya que como se ha podido observar, se encuentra la posibilidad de la comercialización de los datos biométricos de la población nacional y extranjera que ingrese al país, sin ningún tipo de consentimiento. Esto, sin lugar a duda, plantea graves roces de inconstitucionalidad, pero además genera un escenario en el cual las personas no tienen claridad del propósito con el cual se están recopilando sus datos, ni qué tipos de usos pueden darle. No se indica en ninguna parte del proyecto la necesidad del consentimiento de la persona para la utilización de fines distintos a los policiales o de seguridad (según se desprende de la justificación del proyecto)[10].

cultures, and is not restricted to persons who live within Western or 'modern' societies" (Nucci en Trina, 2011, p.191).

10 De hecho, Costa Rica se encuentra en el *Top Ten* de los peores países en cuanto a recolección y protección de datos biométricos (Bischoff, 2019). El país se ubica en el noveno puesto

Existen varios principios importantes a la hora de recopilar, almacenar y gestionar datos biométricos. Según el artículo 40 del Reglamento a la Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales, existen ciertos elementos indispensables para la transferencia de datos:

> Condiciones para la transferencia. La transferencia requerirá siempre el consentimiento inequívoco del titular. La transferencia implica la cesión de datos personales por parte, única y exclusivamente, del responsable que transfiere al responsable receptor de los datos personales. Dicha transferencia de datos personales requerirá siempre del consentimiento informado del titular, salvo disposición legal en sentido contrario, asimismo que los datos a transferir hayan sido recabados o recolectados de forma lícita y según los criterios que la Ley y el presente Reglamento dispone. No se considera trasferencia el traslado de datos personales del responsable de una base de datos a un encargado, proveedor de servicios o intermediario tecnológico o las empresas del mismo grupo de interés económico. (Decreto Ejecutivo n°375543-JP, Año 2012)

Ninguna de estas situaciones se presenta en el Proyecto Nº 21.321. De hecho, parece un asunto discrecional del Tribunal Supremo de Elecciones sobre a quién venderle los servicios de verificación biométrica. Incluso, a partir del mismo documento, se puede suponer razonablemente que la comercialización de los datos es necesaria para la instrumentalización de todo el repositorio, así como para el mantenimiento y la gestión de esta base de datos.

Así las cosas, uno de los aspectos que genera más dudas tiene que ver con el consentimiento. En ninguna parte del Proyecto Nº 21.321 se observa la necesidad de un consentimiento informado, ni para la recopilación de los datos biométricos, ni menos aún para su transferencia. Situación que se agrava mucho más aún en el caso de las personas extranjeras o de los niños, niñas y adolescentes. Personas, que en este último caso, debido a su situación de vulnerabilidad, necesitan mayor protección en todas las esferas. Como si esto fuera poco, en una modificación que se realizó al Proyecto Nº 21.321, conocida como *Texto Sustitutivo*, se pretende crear

(Bischoff, 2019) de este deshonroso ranking internacional. Solo para tener una idea sobre lo que esto significa, algunos países que están peor que Costa Rica son Irán, China, Pakistán, Uganda, Guatemala o Bangladesh, lo cual nos puede servir para dimensionar el fenómeno.

un artículo 24 bis adicional al Código Electoral para que no sea necesario el consentimiento informado. El artículo en cuestión dice:

> Artículo 24 bis.– Repositorio Único de Identificación Biométrica
> La información recopilada y contenida en las bases de datos del Tribunal Supremo de Elecciones, para identificación de personas costarricenses, entre estos los necesarios para el funcionamiento y utilización del Repositorio Único de Identificación Biométrica que utilizará la Plataforma Nacional de Identificación Biométrica del Tribunal Supremo de Elecciones, no estarán sujetos al principio de consentimiento informado que establece la legislación nacional en materia de protección de datos, cuando sean para fines electorales, de identificación o de verificación de identidad. (Texto sustitutivo, Expediente N°, 21.321, LEY DE REPOSITORIO ÚNICO NACIONAL PARA FORTALECER LAS CAPACIDADES DE RASTREO E IDENTIFICACIÓN DE PERSONAS)

Es decir, existiría un servicio de comercialización de los datos biométricos de todos los ciudadanos costarricenses, así como de los extranjeros que ingresen al país, que no necesitan ningún tipo de consentimiento. El Estado estaría facultado legalmente para lucrar con información biométrica, sin ningún tipo de limitación. Por lo demás, no existe siquiera una "limitación del propósito" clara que pudiera servir como referente en el documento. Según el Artículo 5(1)(b) del Reglamento General de Protección de Datos de la Unión Europea, la limitación del propósito implica una razón específica y legítima para que sea recopilado cualquier tipo de dato personal. Consecuentemente los datos personales recopilados solo se podrían utilizar en los casos especificados. En el Proyecto Nº 21.321 no aparece ninguna razón concreta al respecto, más allá de la exposición general de motivos que hacen "necesario" el uso de este tipo de tecnologías: los fines policiales y de prevención del delito, que como hemos visto no parecen nada compatibles con la comercialización de los datos o con el contenido real del documento. Tampoco existe una limitación sobre qué datos biométricos (dactilares, rasgos faciales, iris ocular, la voz, los patrones de las venas, etc.) incluirá esta base de datos, dejando –según el Proyecto Nº 21.321– abierta la posibilidad "de que se pueda adquirir nueva tecnología que permita ampliar la identificación de personas a través de la incorporación de más rasgos biométricos que

se consideren necesarios" (Ley 21.321, 2020, p. 8). Todo esto genera un problema adicional conocido como una recolección innecesaria. "Un principio central de las reglas basadas en la privacidad de la información es que la recopilación de la información personal debe limitarse a aquellos datos que son necesarios y relevantes para un propósito legítimo" (Korja, 2006, p.205). Así las cosas, los riesgos de algo como esto son demasiado altos como para que no sean tomados en cuenta o simplemente omitidos.

Esto nos lleva directamente a un escenario conocido como Desplazamiento de funciones (*Funtion creep*), el cual "se puede definir como la ampliación gradual del uso de una tecnología o sistema más allá del propósito para el que se diseñó originalmente, especialmente cuando esto conduce a una posible invasión de la privacidad" (Korja, 2006, p.207). Es claro que la situación que plantea este repositorio es una clara violación al principio de limitación del propósito, ya que crea grandes riesgos para la privacidad de las personas. Sin embargo, al no existir una delimitación clara, no se puede prever el alcance de estos riesgos, ya que no es para nada obvio si este *Repositorio único nacional para fortalecer las capacidades de rastreo e identificación de personas* se limita a uno o a varios propósitos más allá de la seguridad o es un asunto económico (tampoco nada claro). No hay un contexto real que pueda sugerir las nuevas oportunidades producto de la comercialización de los datos o cómo las diferentes entidades públicas pueden vincular los datos para darle un "uso adecuado".

Podría decirse que este desplazamiento de funciones es una situación que puede presentarse con el uso de cualquier tecnología. No obstante, en este caso, sus consecuencias pueden ser mucho mayores ya que no existe ningún elemento que pueda precisar para qué se pueden usar o se van a utilizar los datos biométricos. Aun en el caso de que sean para evitar la criminalidad, surgen muchas dudas no resueltas, como por ejemplo: ¿cómo se utilizarán los datos biométricos?, ¿como prueba en juicios penales?, ¿para el reconocimiento de sospechosos?, ¿se utilizarán solo en investigaciones judiciales? Y de ser así, ¿es necesario que la investigación se encuentre activa? Respuestas que no se encuentran en ninguna parte. Obviamente el deslizamiento de funciones es muy problemático, porque puede llevar a las entidades públicas o a las empresas privadas a usar información personal de maneras que no cumplen con los requisitos mínimos de seguridad o con propósitos nada éticos.

En un contexto como este, el tema de identificación puede convertirse en un problema grave. Un elemento básico para proteger la privacidad de las personas que tengan sus datos biométricos en estos repositorios es el anonimato. El anonimato "se refiere al estado de

la identidad personal de un individuo o, en el caso de la biometría, la información de identificación personal, que se desconoce públicamente" (Korja, 2006, p.209), pero al tener las características que acabamos de mencionar, la base de datos que se pretende crear no puede garantizar esto. Pongamos un ejemplo: las imágenes faciales recopiladas a través de la tecnología de reconocimiento facial son datos personales que sirven para identificar a personas en ciertos contextos o situaciones (es decir, alguien secuestrado, una persona extraviada en el bosque o un delincuente requerido por la justicia). Sin embargo, como los rasgos faciales son necesarios para la comparación, no se puede anonimizar los datos relevantes con tal de evitar violaciones a la privacidad. Por lo tanto, las bases de datos biométricas basadas en el reconocimiento facial (como la que se pretende crear en el proyecto de ley), ponen en riesgo la privacidad de las personas usuarias desde su misma constitución, aun cuando su creación y utilización tuvieran un propósito expresamente delimitado. Esto sin contar el tema de la precisión de las tecnologías biométricas y el potencial de falsos positivos y errores.

Sesgo algorítmico y discriminación

Los riesgos para la privacidad aumentan si se utilizan sistemas para el reconocimiento facial en vivo, en el que la mayoría de las veces los datos de las personas se recopilan sin su conocimiento. Aunque los problemas siguen siendo los mismos. A pesar de que la precisión y los sistemas de reconocimiento facial han mejorado en pruebas de laboratorio, su precisión en la práctica es cuestionable (Grother et al., 2019). Por lo general, esta depende de la estabilidad de equipos muy potentes y de muchos datos de entrenamiento (Liu et al., 2015). Existen muchos casos que pueden ayudarnos a mostrar estos puntos.

En el año 2018, la prensa estadounidense sacó un reportaje en el que mostraba cómo la empresa Amazon había vendido un sistema llamado *Rekognition* a una serie de departamentos policiales en Estados Unidos (Brandon, 2018). *Rekognition* es un servicio de análisis de imágenes y videos basado en la nube que utiliza el aprendizaje automático para identificar objetos, personas, texto, escenas y actividades en imágenes y videos. Su utilización ha sido objeto de múltiples debates éticos, debido a su potencial para ser utilizado para la vigilancia y el reconocimiento facial, lo que ha suscitado preocupaciones sobre la privacidad y las libertades civiles (Piedra, 2021). Este software posee la capacidad de

analizar repositorios biométricos con millones de imágenes e identificar a cien personas con una sola toma (Ng, 2018).

Una de las principales preocupaciones sobre *Rekognition* es su uso potencial en la vigilancia (Piedra, 2021). El servicio se puede usar para rastrear a las personas mientras se mueven por espacios públicos, y también se puede usar para identificar a las personas en tiempo real a partir de una transmisión de video. Esto generó inquietudes sobre el potencial de abuso por parte de los gobiernos u otras organizaciones que buscan monitorear y controlar los movimientos y acciones de las personas. Finalmente, resultó que todas estas alarmas se encontraban justificadas, ya que este sistema estaba siendo utilizado desde el 2016 por una serie de fuerzas policiales estadounidenses (Brandon, 2018).

Ese mismo año (2018), la *American Civil Liberties Union Foundations of California* mostró la falta de precisión de los sistemas de reconocimiento facial de *Rekognition*, particularmente cuando se trata de identificar a personas afrodescendientes, las cuales tienen muchas más probabilidades de ser identificadas errónea o falsamente. Es decir, el sistema de reconocimiento posee un sesgo discriminatorio. En una prueba realizada para establecer la precisión del sistema, se comprobó que *Rekognition* identificaba incorrectamente los rostros de varios miembros del Congreso de los Estados Unidos, con diferentes tonalidades de piel morena, con los datos de delincuentes que habían sido condenados (Armasu, 2018). En un estudio posterior también se demostró como este sistema identificó de manera errónea a mujeres de piel oscura (*darker-skinned women*) con hombres, en el 31 por ciento de las veces (Singer, 2018).

Como se observa en estos casos, la tecnología no solo no es precisa, sino además posee un sesgo racial. Grother et al. 2019 han mostrado, lo que aparece claramente en el caso del sistema *Rekognition*, que existen diferencias demográficas en las tasas rechazo de una coincidencia correcta (falsos negativos) así como en las tasas de coincidencia con la persona equivocada (falsos positivos). Es decir, los algoritmos tienen sesgos de género, raciales, basados en la edad, la apariencia, etc. Es claro que existe poca diversidad en los datos de entrenamiento de los algoritmos. Los datos no solo son inadecuados, sino que además reflejan los mismos prejuicios y elementos discriminatorios que muestran los resultados de estos sistemas. Estos resultados discriminatorios y sesgados que no representan adecuadamente a la realidad afectan a las minorías, a las poblaciones vulnerables o a grupos que han sufrido discriminaciones históricas. En un famoso caso, sucedido también en Amazon, la empresa estadounidense "descubrió" que un algoritmo que reclutaba empleados

tenía un sesgo a favor de los hombres. Es decir, discriminaba a las mujeres. Desde el 2014 se habían construido una serie de programas que mecanizaban la selección de personal, categorizando los currículos de los solicitantes de empleo en la empresa. El algoritmo le otorgaba un puntaje basado en estrellas (de la misma manera que los compradores califican a vendedores o a los productos en la tienda de Amazon). Sin embargo, en el 2015 descubrieron que

> (…) la empresa se dio cuenta de que su nuevo sistema no calificaba a los candidatos para trabajos de desarrollo de software y otros puestos técnicos de manera neutral en cuanto al género. Esto se debe a que los modelos informáticos de Amazon fueron entrenados para examinar a los solicitantes mediante la observación de patrones en los currículos enviados a la empresa durante un período de 10 años. La mayoría provino de hombres, un reflejo del dominio masculino en la industria tecnológica [11].(Dastin, 2018).

Wang et al. (2019) comprobaron cómo un algoritmo de búsqueda asociaba imágenes de ejercicio físico a los hombres, mientras que las mujeres eran referidas a una imagen de elementos relacionados con la cocina o las compras. Este tipo de problemas aumentan debido al uso generalizado y masivo de los datos, lo que en algunos casos impide una revisión profunda en la recolección de los mismos. Este tipo de sesgos puede tener graves implicaciones en la vida de las personas. Si muchos de estos sistemas de reconocimiento algorítmicos poseen datos sesgados y basados en prejuicios, es razonable pensar que ciertos grupos están sobrerrepresentados en las bases de datos. En situaciones así, el algoritmo de reconocimiento va a "identificar" con mucha más frecuencia a personas de ese grupo. Esto es precisamente lo que pasó en New York, ya que según un estudio de Amnistía Internacional (2022) "(…) sabemos que la práctica de dar el alto y registrar es una táctica racista de control policial en Nueva York. Ahora también sabemos que las comunidades que más sufren esta práctica también están más expuestas a una actuación policial discriminatoria a través de la vigilancia invasiva"

11 "(…) the company realized its new system was not rating candidates for software developer jobs and other technical posts in a gender-neutral way. That is because Amazon's computer models were trained to vet applicants by observing patterns in resumes submitted to the company over a 10-year period. Most came from men, a reflection of male dominance across the tech industry" (Dastin, 2018).

(Amnistía Internacional, 2022). Esto se debe a los barrios donde hay más cámaras de videovigilancia con reconocimiento facial, son los barrios con población afrodescendiente como Brooklyn, Queen y el Bronx.

Algunos autores consideran que esto incluso podría ser mucho peor. *Verbigracia*, Schindel (2017) parte desde el contexto de la Unión Europea para analizar el uso de sistemas biométricos en las fronteras. Su análisis va más allá de las críticas a la privacidad o manejo de datos. La autora plantea una hipótesis según la cual los registros biométricos van construyendo un "cuerpo normalizado", según estándares tecnológicos. Esta normalización responde a criterios eurocéntricos con los cuales se busca la identificación de la población inmigrante, al tiempo que discrimina cuerpos que se alejan de este imaginario. La biometría se convertiría de este modo en una herramienta de dominación que, bajo la supuesta neutralidad tecnológica, pretende imponer modelos "naturales" (biológicos) que homogenizan a los seres humanos en patrones.

En general, los debates éticos en torno a *Rekognition* (de Amazon), así como a otras tecnologías de reconocimiento facial, giran en torno a cuestiones de privacidad, libertades civiles y el potencial de abuso por parte de gobiernos u otras organizaciones (Piedra, 2021). Es importante que la sociedad considere detenidamente las posibles consecuencias del uso de estas tecnologías y establezca medidas de seguridad para garantizar que se utilicen de manera ética y responsable.

Asimetrías de poder: población indígena

Es ampliamente conocido que los pueblos indígenas históricamente han sido objeto de investigaciones extractivas que han producido poco o ningún beneficio para estas comunidades (Smith, 2013; TallBear, 2013; Cram, 2017). Muchas de estas investigaciones exponen a los pueblos indígenas a ciertos riesgos (Carroll et al., 2022), debido al uso incorrecto de la información obtenida (es decir, como la generación de estereotipos). También, es normal que los beneficios potenciales de estas investigaciones nunca lleguen a la población indígena. Como resultado de estas prácticas indebidas y poco éticas, la población indígena ha desarrollado una desconfianza (más que justificada) frente las instituciones de investigación y, en general, hacia las propuestas de los gobiernos.

La redacción del Proyecto Nº 21.321 omite detalles esenciales sobre el tratamiento de los datos biométricos de las poblaciones vulnerables[12].

12 En el plano teórico, se suele decir que la Ley (en sentido general) aplica para todas las

Por ejemplo, no se proporciona ninguna indicación específica sobre cómo se manejará la información perteneciente a la población indígena. La privacidad de los datos es un tema crítico para las poblaciones indígenas, ya que su información personal a menudo se recopila y utiliza sin su total comprensión o consentimiento. Esto puede conducir a una variedad de consecuencias negativas, que incluyen discriminación, explotación y pérdida de control sobre sus propias vidas. Sobre este último punto, existen varias consideraciones éticas en torno al uso de datos biométricos en poblaciones indígenas. En primer lugar, entra en juego el tema de la autonomía. Los pueblos indígenas tienen derecho a la libre autodeterminación y deberían poder decidir si quieren o no compartir sus datos biométricos. La forma tradicional para definir esto sería por medio de un consentimiento informado[13]. Es importante que los pueblos indígenas comprendan completamente el propósito y los posibles riesgos y beneficios de la recopilación de datos, y den su consentimiento explícito antes de recopilar sus datos. Pero, como ya vimos, el Proyecto Nº 21.321 crea una situación jurídica en la que el consentimiento no es necesario. Todo esto es un obvio problema, por los argumentos que ya hemos mencionado, pero el caso de la población indígena plantea inconvenientes adicionales ya que la recopilación y el uso de datos biométricos pueden generar preocupaciones culturales y éticas, especialmente si no se hace de una manera que respete sus tradiciones y valores. Esto plantea lo que se conoce como "Soberanía de los datos indígenas" (*Indigenous Data Sovereignty*). Una propuesta novedosa que recién apareció en el 2016 (Kukutai & Taylor, 2016). De manera resumida, lo que implica es el derecho de los pueblos indígenas en la toma de decisiones, así como en la forma en cómo se recopilan, almacenan y gestionan sus datos, a través de sus valores, tradiciones, formas de conocimiento, cosmovisiones y, en definitiva, según sus propios intereses. Por ejemplo, ¿la comercialización de sus datos (sin su permiso) servirá como un medio para preservar el patrimonio cultural de los pueblos indígenas? Es plausible pensar que no será así. De hecho, también es razonable suponer que, por el contrario, será un medio más de denominación y control, puesto que se puede

personas, sin discriminar o diferenciar entre la población. No obstante, en el plano práctico, es posible que una ley o norma pueda legitimar discriminaciones históricas. Lo que hace necesario que deban crearse protecciones concretas explícitas o acciones reivindicativas claras que permitan superar o eliminar estas asimetrías. Este tipo de protecciones no se presentan en el Expediente Nº 21.321.

13 El tema del consentimiento informado en las poblaciones indígenas tampoco se encuentra exento de serios cuestionamientos. Por ejemplo, en cuanto a temas como la reciprocidad o la creación conjunta del consentimiento informado. Sin embargo, esos temas exceden las intenciones de este artículo.

generar un acceso desigual a los "supuestos" beneficios de la recopilación y el uso de datos biométricos, particularmente si algunos grupos están en desventaja o quedan fuera del proceso, por ejemplo, aquellos de zonas muy alejadas[14].

Incluso lo que se entiende por privacidad (Piedra, 2022) o la propiedad de los datos, muchas veces son ideas incompatibles con los derechos colectivos o con las culturas y tradiciones indígenas, lo que plantea retos adicionales en vista de que la mayoría de los datos personales de los indígenas se encuentra en posesión de los gobiernos, agencias o instituciones que no son indígenas. Así las cosas, resulta totalmente necesario aumentar la participación de la población indígena en todos los procesos relacionados con la recopilación, gestión y gobernanza de los datos, especialmente si son datos biométricos. (Kukutai y Taylor 2016; Ranie et al., 2019).

Esto genera desafíos que van más allá de los tradicionales debates sobre la protección y la privacidad. Se necesitan crear nuevos marcos teóricos y normativos que permitan reflejar las necesidades y los intereses de los grupos indígenas, pero siempre desde un esquema que respete su sensibilidad cultural, no como un simple aspecto formal, sino como una forma de empoderamiento. Para esta finalidad, en el año 2020 el *Native Nations Institute* de la Universidad de Arizona publicó los Principios CARE (*CARE principles*). Una pequeña lista de postulados mínimos para la gobernanza de datos indígenas. Si bien esta lista estaba pensada originalmente para el uso y la protección en investigaciones científicas, podría *mutatis mutandis* utilizarse de manera análoga con tal de proteger los datos biométricos. En primer lugar, se menciona la idea del (1) *Beneficio colectivo:* el ecosistema de datos debería tener un diseño y funcionamiento que permita a los grupos indígenas beneficiarse de los datos. Situación que como ya hemos visto, es del todo omisa en el Proyecto Nº 21.321, tanto para la población indígena, como para quienes no lo son. Por el contrario, la comercialización de los datos implica un claro perjuicio para las personas. Esto nos lleva a un segundo punto (2) *Autoridad de control:* debería existir una clara autoridad de los pueblos indígenas sobre sus datos biométricos con tal de que puedan controlar su uso, de forma tal que les permita pasar de una *dependencia de los datos* hacia una *soberanía de los datos.* De modo que tecnologías como estas,

14 Solo por mencionar algunos ejemplos; las regiones Brunca y Chorotega (regiones en donde existen reservas indígenas) presentan los índices más altos de desigualdad de todo Costa Rica (INEC, 2015). Asimismo, datos oficiales de la ONU (2022) mostraron que en los pueblos indígenas de Costa Rica existen grandes rezagos en prácticamente todas las áreas en comparación con el resto de la población costarricense.

les permitan un empoderamiento acorde con sus propios intereses y conocimientos. El Proyecto Nº 21.321 continúa una línea extractivista de datos, en la que se mantienen tal cual los procesos de colonización que han sufrido estas poblaciones a lo largo de la historia. En este sentido, debería existir como mínimo (3) una *responsabilidad* en dar a conocer la manera cómo estos datos promueven la libre determinación y el beneficio colectivo de los pueblos indígenas. Aspectos que como ya hemos señalado, no se presentan por ninguna parte. Todo esto se traduce, en lo que se conoce en la literatura como (4) *Explicabilidad*: ser transparente sobre cómo se recopilan, usan y comparten los datos biométricos. Dar explicaciones claras a las personas sobre el propósito de la recopilación y cómo se usarán sus datos. Esto puede ayudar a generar confianza y garantizar que las personas comprendan y se sientan cómodas con el proceso de recopilación de datos.

Conclusiones

Hemos mostrado cómo el repositorio que se pretende crear carece de las medidas de seguridad fundamentales para proteger los datos personales. Dado el carácter permanente de los datos biométricos y su difícil cambio, una violación de seguridad podría resultar en riesgos inalterables de privacidad. Nuestro análisis también ha identificado potenciales problemas de sesgo algorítmico y discriminación. Los datos biométricos, si se utilizan de manera inadecuada o abusiva, pueden ser herramientas de robo de identidad o discriminación basada en características individuales. La falta de transparencia y la ausencia de consentimiento informado agravan estos problemas, ya que obstaculizan la capacidad de los individuos para tomar decisiones informadas sobre la recopilación y el uso de sus datos biométricos. Esto, sin dejar de lado las graves asimetrías de poder que podrían surgir, particularmente en relación con las poblaciones indígenas.

Como vemos, es claro que este tipo de repositorio no cuenta con las normas técnicas de seguridad elementales para la protección de los datos de ninguna persona. El riesgo de ciberdelincuencia o robo de información es particularmente grave en este contexto, debido a la naturaleza de los datos biométricos. Estos datos son permanentes y extremadamente difíciles de cambiar, por lo que, si son falsificados o se filtran, no se pueden restablecer. Además, en este caso, son visibles para cualquiera que pague por ellos. Esto significa que cualquier violación de seguridad o invasión a la privacidad resultante de la falsificación o filtración de estos datos no podría ser corregida, lo cual incrementa enormemente el riesgo

de seguridad. Propuestas como estas deberían ser consideradas a la luz de un enfoque basado en derechos humanos, así como dentro de un marco reflexivo de naturaleza ética. Se debería realizar un debate público en el cual todas las partes involucradas, así como la sociedad civil, tuvieran voz a la hora de considerar, no únicamente, la creación de este repositorio, sino además los riesgos derivados de su utilización. Lo más importante de este proyecto de ley no son los aspectos técnicos, sino las profundas implicaciones éticas.

Ahora bien, un análisis de este tipo no solo es necesario *a posteriori,* sino que se hace completamente necesaria una amplia reflexión ética desde el origen mismo de la propuesta. La reflexión ética no se debe dar como resultado de una situación gravosa, sino que, por el contrario, debería presentarse como el primer paso para reflexionar sobre las posibilidades (y las implicaciones sociales) de propuestas tan controvertidas y problemáticas como las que acabamos de analizar. Un gran desafío ético es el tema sobre cómo proteger la privacidad. Los datos biométricos son extremadamente personales y confidenciales, su recopilación y uso pueden infringir el derecho a la privacidad de las personas. Existen preocupaciones sobre la posibilidad de que los datos biométricos se utilicen indebidamente o se abuse de ellos. Por ejemplo, los datos biométricos podrían usarse para el robo de identidad o para discriminar a ciertas personas en función de sus características. Además, existe el riesgo de que terceros no autorizados accedan a los datos biométricos, ya sea mediante piratería informática u otras formas de violación de datos. Otro gran desafío ético relacionado con los datos biométricos es la cuestión del consentimiento. En muchos casos, es posible que las personas no sean plenamente conscientes de hasta qué punto se recopilan sus datos biométricos o cómo se utilizan. Esta falta de transparencia puede dificultar que las personas tomen decisiones informadas sobre si permitir que se recopilen y utilicen sus datos biométricos. También hay dudas sobre la justicia y equidad de la recopilación de datos biométricos, particularmente cuando se trata de grupos marginados o desfavorecidos.

Una forma de abordar estos desafíos éticos es mediante la implementación de leyes y regulaciones sólidas que rijan la recopilación y el uso de datos biométricos. Esto podría incluir medidas como exigir el consentimiento explícito para la recopilación de datos biométricos, establecer pautas claras sobre cómo se pueden usar los datos biométricos y crear sanciones por uso indebido o abuso de datos biométricos. Es muy importante que las organizaciones que recopilan y utilizan datos biométricos sean transparentes en sus prácticas y proporcionen a las personas información sobre cómo se recopilan y utilizan sus datos. Esto

puede ayudar a garantizar que las personas conozcan sus derechos y puedan tomar decisiones informadas sobre si permitir que se recopilen y utilicen sus datos biométricos.

En general, los desafíos éticos de la recopilación de datos biométricos son complejos y multifacéticos. Es importante que tanto los formuladores de políticas como las organizaciones consideren cuidadosamente los impactos potenciales de la recopilación de datos biométricos y tomen medidas para abordar cualquier posible inquietud ética. Al hacerlo, se podría favorecer los beneficios del uso de los datos biométricos y, al mismo tiempo, minimizar cualquier impacto negativo en las personas y la sociedad.

Referencias

Asamblea Legislativa de Costa Rica. (2019). Proyecto de ley. Ley de repositorio único nacional para fortalecer las capacidades de rastreo e identificación de personas. Expediente n.º 21.321

Asamblea Legislativa de Costa Rica. (s, f). Texto sustitutivo. Expediente n.º 21.321. Ley de repositorio único nacional para fortalecer las capacidades de rastreo e identificación de personas

AI Global Surveillance (AIGS) Index. *Biometric System Market with COVID-19 Impact Analysis by Authentication Type, Type, Offering Type, Mobility, Vertical & Region - Global Forecast to 2027*. MarketsandMarkets.

Amnistía Internacional. (2022). *Estados Unidos: Nueva investigación revela que la tecnología de reconocimiento facial refuerza la práctica policial racista de dar el alto y registrar en Nueva York*. Noticia. Retrieved 25 June 2022, from https://www.amnesty.org/es/latest/news/2022/02/usa-facial-recognition-technology-reinforcing-racist-stop-and-frisk-policing-in-new-york-new-research/

Armasu, L. (2018). *Amazon 'Rekognition' Falsely Identifies 28 Congress Members as Criminals (Updated) | Tom's Hardware. (2021)*. Noticia. Retrieved 8 June 2021, from https://www.tomshardware.com/news/amazon-rekognition-congress-members criminals, 37515.html

Bischoff, P. (2019). *Biometric data collection by country: What's collected, how is it used?*. Noticia. Retrieved 18 December 2022, from https://www.comparitech.com/blog/vpn-privacy/biometric-data study/#The_worst_countries_for_biometric_data_collection_and_use

Bowyer, K. W., Flynn, P. J., & Jain, A. K. (2004). *Biometric identification. Communications of the ACM*, 47(2), 96-103.

Brandon, R. (2018). *Amazon is selling police departments a real-time facial recognition system.* Noticia. https://www.theverge.com/2018/5/22/17379968/amazon-rekognition-facial-recognition-surveillance-aclu

Carroll, SR., Plevel, R., Jennings, LL., Garba, I., Sterling, R., Cordova-Marks, FM., Hiratsuka, V., Hudson, M., Garrison, N.A. (2022). Biometric Technologies and Global Security. *Congressional Research Service. https://crsreports.congress.gov/product/pdf/IF/IF11783*

Cram, F. (2017). Lessons on decolonizing evaluation from Kaupapa Māori evaluation. In F. Cram, K. A. Tibbetts, & J. LaFrance (Eds.), *Indigenous evaluation*, 173-199.

Dastin, J (2018). Amazon scraps secret AI recruiting tool that showed bias against women. Reuters. Noticia. Retrieved, 20 de marzo, 2022, from https://www.reuters.com/article/us-amazon-com-jobs-automation-

insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G

Devanesan, J. (2021). Ranking the countries with the best (and worst) biometric data security. Noticia. Retrieved 8 May 2022, from https://techhq.com/2021/01/ranking-the-countries-with-the-best-and-worst-biometric-data-security/

Faundez-Zanuy, M. (2006). *Biometric security technology. IEEE Aerospace and Electronic Systems Magazine,* 21(6), 15–26.

Feng, E. (2019). How China Is Using Facial Recognition Technology. Noticia. Retrieved 16 March 2023, from https://www.npr.org/2019/12/16/788597818/how-china-is-using-facial-recognition-technology

Grant, P. (2020). *Minority and Indigenous Trends 2020: Focus on Technology*.

Grother, P., Ngan, M., & Hanaoka, K. (2019). Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects. *NISTIR 8280*. 1-82.

Gupta, B. (2008). Biometrics: Enhancing Security in Organizations. IBM Center for The Business of Government.

Human Right Watch /HRW (2022). New Evidence that Biometric Data Systems Imperil Afghans. Noticia. Retrieved 25 June 2022, from https://www.hrw.org/news/2022/03/30/new-evidence-biometric-data-systems-imperil-afghans

INEC. (2015). Regiones Chorotega y Brunca muestran mayor desigualdad. Noticia. Retrieved 10 November 2022, from https://inec.cr/noticias/regiones-chorotega-brunca-muestran-mayor-desigualdad

Korja, J. (2006). The privacy risks of biometric identification. En Ahti Saarenpää y Aleksander Wiarowski (editores), *Society trapped in the network, does it have a future?* Rovaniemi: University of Lapland.

Kukutai, T & Taylor, J, (2016) Indigenous data sovereignty: Toward an agenda. Canberra: ANU Press.

Liu, W., Wen, Y., Yu, Z., & Yang, M. (2015). Large-Margin Softmax Loss for Convolutional Neural Networks. *Proceedings of the 34th International Conference on Machine Learning*, 48, 507-516.

Lucero M., Boris A., Saracini, Chiara., Mora, Marco., Muñoz-Quezada, María Teresa (2020): Aspectos éticos del uso de identificadores biométricos. En: *Acta bioeth.* 26 (1), 43–50.

Lukács, A. (2016) *The History and Definition of Privacy*. Tavaszi Szél. Tanulmánykötet. I. kötet: Agrártudomány, állam- és jogtudomány, föld- és fizikatudomány, had- és rendészettudomány, 256–265. https://publicatio.bibl.u-szeged.hu/10794/

Market Research.(2022). Media, T., Computing, S., & Privacy, S. (2022). Biometric System Market with COVID-19 Impact Analysis by

Authentication Type (Single Factor, Fingerprint, Iris, Face, Voice; Multi-factor), Type (Contact-based, Contactless, Hybrid), Offering Type, Mobility, Vertical & Region - Global Forecast to 2027. https://www.marketresearch.com/MarketsandMarkets-v3719/Biometric-System-COVID-Impact-Authentication-31021036/ Grant, p.2020

National Science and Technology Council. (2006) *Privacy & Biometrics*. America: National Science and TechnologyCouncil (NSTC)

Ng, A. (2018). Amazon is selling facial recognition technology to law enforcement. Noticia. Retrieved 6 June 2021, from https://www.cnet.com/news/amazon-is-selling-facial-recognition-technology-to-law-enforcement/

ONU.(2022) Necesitamos priorizar el derecho de los pueblos indígenas a poseer, utilizar y manejar sus tierras en Costa Rica. Comunicado de prensa. Retrieved 25 November 2022, from https://costarica.un.org/es/125221-onu-necesitamos-priorizar-el-derecho-de-los-pueblos-indigenas-poseer-utilizar-y-manejar-sus

Parlamento Europeo y Consejo de la Unión Europea. (2016). Reglamento 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. (GDPR). https://gdpr-info.eu/

Paret, D. & Crégo, P. (2019). Aspects to Take into Consideration for Wearables. *Smart Textiles and Smart Apparel,* Elsevier (pp. 39-98). https://doi.org/10.1016/B978-1-78548-293-9.50006-4.

Piedra, J. (2021). Venditio fumi: Autorregulación Empresarial e Inteligencia Artificial. *Sincronía*. Año XXVI (81)DOI: 10.32870/sincronia.axxvi.n81.12a22

Piedra, J. (2022). Decolonizando la Ética de la IA. Dilemata. 38, 247-258.

Quintanilla, G (2020). Legislación, riesgos y retos de los sistemas biométricos. *Rev. chil. derecho tecnol.,* 9 (1), 63. DOI: 10.5354/0719-2584.2020.53965.

Rainie, SC., Kukutai, T. Walter, M. Figueroa-Rodriguez, OL. Walker, J., Axelsson, P. (2019). Issues in Open Data: Indigenous Data Sovereignty. En Davies, T, Walker, S, Rubinstein, M and Perini, F (Eds.) *The State of Open Data: Histories and Horizons*. Cape Town and Ottawa: African Minds and International Development Research Centre (pp. 300–319).

Trader, John. (2016). The Top 5 Uses of Biometrics Applications across the Globe. Noticia. https://www.m2sys.com/blog/biometric-hardware/top-5-uses-biometrics-across-globe/

Shindel, Estela. (2018). Biometrics, body normalization, and EU border control. *ATHENEAD,* 18 (1), 11. Doi: 10.5565/rev/athenea.2267.

Smith, L. T. (2013). *Decolonizing Methodologies: Research and Indigenous Peoples*. Zed Books Ltd.

Strzyżyńska, W. (2022) Iranian authorities plan to use facial recognition to enforce new hijab law. Noticia. Retrieved 5 January 2023, from https://www.theguardian.com/global-development/2022/sep/05/iran-government-facial-recognition-technology-hijab-law-crackdown

TallBear, K. (2013). *Native American DNA: Tribal Belonging and the False Promise of Genetic Science*. University of Minnesota Press.

Tianlu, Wang. Jieyu, Zhao. Mark, Yatskar. Kai-Wei, Chang. Ordonez, Vicente. (2019). Balanced Datasets Are Not Enough: Estimating and Mitigating Gender Bias in Deep Image Representations. Proceedings of the IEEE/CVF international conference on computer vision, 5310-5319.

Trina, M. (2011). Fourteen Reasons Privacy Matters: A Multidisciplinary Review of Scholarly. *The Library Quarterly*. 81(2), 187–209.

Wang, L. L. (2021). Face Recognition in Law Enforcement: A Comparative Analysis of China and the United States. *Open Journal of Social Sciences*, 9, 498-506.

Woodward Jr., J. D., Horn, C., Gatune, J., Thomas, A. (2003). *Biometrics: A Look at Facial Recognition*. RAND Corporation.