SE PRESENTA Y MANIFIESTA
COMO "AMIGO DEL TRIBUNAL"

xxxxxxxx:

**********, DNI ***** en mi carácter de CO - DIRECTORA DE LEGALTECH SEED SIMPLE ASOCIACIÓN, constituyendo domicilio en calle ****, de la Ciudad de Mendoza, denunciando como **domicilio electrónico** *****, xxxxxx – Usuario: xxxxx, presentándome en los **Autos 182908/2020-0 relativo al Sistema de Reconocimiento de Prófugos (SRFP) de la Ciudad Autónoma de Buenos Aires,** ante V.S. me presento y respetuosamente digo:

I. OBJETO

Vengo por este medio a solicitar a V.S, ser tenido como "Amigo del Tribunal" para someter a su consideración argumentos de relevancia pública para la decisión de la cuestión planteada en los derechos afectados por el Sistema de Reconocimiento Facial de Prófugos.

II. QUIENES SOMOS

Legaltech Seed es un semillero de ideas constituido como Asociación Civil Simple con más de 60 miembros de todo el país y del exterior dedicado al Derecho y la Tecnología que articula la participación interdisciplinaria de estudiantes, docentes y profesionales en el análisis, difusión y producción de conocimientos. Se trata de acompañar, entender y ser parte de las transformaciones generadas día a día por las Nuevas Tecnologías en nuestra sociedad desde el rol civil y profesional.

Desde la asociación se abordó el concepto de reconocimiento facial a través de diversas publicaciones como una temática de relevancia en la cuarta revolución industrial.

Para la realización de una de las publicaciones en redes algunos de los miembros experimentaron con el proyecto “HOW NORMAL AM I?” (algunos fueron reconocidos y otros no).

Dicho proyecto es un documental interactivo que permite explorar cómo se utiliza esta tecnología, probarla en tiempo real y observar cómo los algoritmos estiman edad, género, sexo, emociones, expectativas de vida, masa corporal, etcétera y en base a ello, clasifican.

Además, por un lado, mencionamos algunos riesgos que presentan, como la vulneración de datos y discriminación de las minorías; y por el otro, los beneficios. Como toda tecnología, no podemos clasificarla en buena o mala, sino que dependerá de su utilización.

III. CUESTIONES TÉCNICAS

Más de una vez cada uno de nosotros ha oído, o leído, acerca de la solicitud o la utilización de datos biométricos para completar condiciones que hacen a la seguridad de algún tipo de acto que efectuamos. Sin embargo, poco sabemos acerca de qué comprende el uso de este tipo de tecnología.

Para comenzar, cabe decir que la biométrica es un tipo de tecnología de la información que recaba datos biológicos para cuestiones atinentes a la seguridad. Si bien su aparición se centra en la segunda mitad del siglo XX, lo cierto es que luego de los atentados de septiembre de 2.001 su aceptación fue casi inobjetable como carta contra el terrorismo.

Como sus términos lo indican, los sistemas biométricos requieren de la recopilación y almacenamiento de ciertas características y referencias que son asociadas a un individuo determinado. En pocas palabras, para funcionar necesitan datos.

Teniendo en cuenta las características que pueden retener esta clase de sistemas, consideramos pertinente hacer foco en los derechos que por esas vías resultan afectados y en las condiciones técnicas y normativas que deben cumplimentar para funcionar.

Existen dos tipos de mediciones biométricas: fisiológica y de comportamiento. La medición fisiológica codifica las características físicas de los individuos. Ya sea a través de la morfología que estudia el organismo y sus características, como huella digital, forma de la mano, patrón venoso, iris y retina, forma de la oreja o forma de la cara; o a través de la biología, que analiza el origen, evolución y propiedades de los organismos, como su ADN, sangre, saliva u orina, características normalmente de uso forense o médico.

Estas mediciones por lo general son más confiables porque permanecen estables a lo largo de la vida del individuo. Sin embargo, solo tres son consideradas en verdad únicas y de precisión: retina, iris y huella digital (Woodward, 1997: 1.481, en Quintanilla Mendoza, p. 6).

La medición del comportamiento o conducta se orienta al reconocimiento de la voz, la dinámica de la firma (velocidad del movimiento de la pluma, aceleración, presión, inclinación), la pulsación de teclas, la forma de utilización de objetos, los gestos o la fuerza de la pisada, entre otros. Estas mediciones varían conforme el individuo se desarrolla y cambia su estado físico y social. (Quintanilla Mendoza, 2020, p. 7).

Entonces, centrándonos en el funcionamiento técnico de estos sistemas, y puntualmente del reconocimiento facial, que opera con un software no abierto, ¿cómo sabemos qué procesamiento hace de nuestros datos y qué uso se le da?

Sabemos que los sistemas de reconocimiento facial utilizan inteligencia artificial. Dentro de las técnicas de IA *machine learning* estos datos que son recolectados, se procesan por medio de uno o más algoritmos y, cómo resultado, se obtienen patrones o correlaciones entre esos datos que permiten identificar los rostros.

Ahora bien, ¿qué técnicas para reducción de riesgos se están aplicando en este sistema? Los sesgos son inherentes al ser humano, convivimos con ellos en el día a día

y, además, están presentes en los datos, pero la capacidad de procesamiento de un sistema de IA es mucho mayor que la de un ser humano, por ende, el daño del sesgo se puede ver aumentado exponencialmente.

A nivel mundial existen diversas legislaciones que regulan y protegen el tratamiento de datos biométricos. El problema se advierte en que si bien sancionan y establecen la forma y modo de recopilación y almacenamiento de datos —generalmente sin el consentimiento de los individuos—, las normas no establecen procesos claros y transparentes respecto del uso, control y destino de ellos. Esto pone en riesgo considerable la privacidad, libertad y seguridad de los individuos debido a que no es consultado ni solicitado acerca de su consentimiento. (Quintanilla Mendoza, 2020, p. 65).

Es decir, estas legislaciones no regulan ni protegen lo relativo al conocimiento y control del proceso por parte de los individuos. Debemos entender que, en materia de datos biométricos, el consentimiento es la base legal para el procesamiento de datos. Una legislación que no establece mecanismos claros sobre estos procesos, resultará violatoria de la libertad y privacidad.

No obstante, con el devenir de los años y el análisis de los datos obtenidos sobre aplicación de legislación deficiente, se han ido elaborando leyes que comienzan a receptar y proteger al individuo. Un ejemplo de ello es el Acta de Privacidad de Información Biométrica (740 ILCS 14/1), Illinois en 2008. Sobre esta ley, Quintanilla Mendoza (2020) comenta:

> "(...) esta Ley regula la información biométrica desde la manera en que es capturada, convertida, almacenada y compartida, para asegurar la protección, privacidad y seguridad de los individuos. Es la única ley americana que no solo permite protección a los individuos contra la violación de la privacidad de la información biométrica, sino que además les permite demandar a personas u organizaciones por no obtener autorización en la recopilación, uso y almacenamiento de la información biométrica. Características importantes son que prohíbe la recolección de datos biométricos sin consentimiento previo por

escrito y salvaguarda los datos biométricos, al prohibir a entidades comerciales el uso, intercambio, venta o préstamo de estos datos.” (p, 75).

Otro buen ejemplo sobre cómo legislación que comienza a dar lugar a la protección de los derechos de los individuos, especialmente relacionado al consentimiento, es el Reglamento General de Protección de Datos 2016/679 dictado por el Parlamento Europeo. Este establece que el procesamiento de datos biométricos y sensibles está prohibido a menos que la ley lo permita expresamente o el individuo haya sido dado el consentimiento expreso para ello (ibidem, p. 80).

Es importante destacar que el reglamento busca priorizar principios relacionados con la transparencia del procesamiento de datos, en especial el establecimiento de propósitos específicos y explícitos para el tratamiento de datos, requiriendo consentimiento expreso previo y estudio del impacto en la privacidad. (ibidem, Pp. 81-82). Así, Quintanilla Mendoza (2020) concluye que el reglamento posee un aspecto de gran importancia para el empoderamiento del individuo:

> “Un aspecto de gran importancia para el empoderamiento de los individuos sobre sus datos personales se encuentra referido en el artículo 13, el cual señala la necesidad de que el controlador,28 al obtener los datos, provea al sujeto de la siguiente información y le permita el ejercicio de sus derechos:
>
> • Identidad y detalles de contacto.
>
> • Detalles de contacto del oficial de protección de datos.
>
> • Propósitos del procesamiento y su base legal.
>
> • Beneficiarios de los datos personales.
>
> • Razones sobre la posible transferencia de datos personales.
>
> • Período de tiempo que esos datos serán guardados o el criterio utilizado para
>
> determinarlo.
>
> • Derecho a solicitar el acceso, rectificación” (p. 81)

Siguiendo a la Agencia Española de Protección de Datos, en su Modelo de Informe de Evaluación de Impacto en la Protección de Datos (EIPD) para Administraciones Públicas (2019), se deja en claro la necesidad de estudiar el tratamiento tanto interno, como externo de los datos cuando puedan verse afectados derechos de categoría constitucional. Análisis que deberá tener en cuenta, además, tipo de tratamiento, categoría de los datos recabados, responsables de su utilización, así como identificación de terceros que estén implicados en dicho tratamiento.

Luego, hace hincapié en la realización de un análisis sobre la necesidad del tratamiento, si es adecuado para perseguir los objetivos propuestos, y, por ende, si es necesario. Todo esto sobre la base de que los datos siempre deben ser optimizables, eliminando aquellos que no sean pertinentes.

Y tal como indica en uno de sus apartados preliminares, el modelo se basa "en las siguientes guías y normas:

- La Guía práctica para las Evaluaciones de Impacto en la Protección de los Datos sujetas al RGPD de la AEPD.
- Normas ISO-29134 "Directrices para la evaluación de impacto sobre la privacidad", ISO-31000 "Gestión del riesgo. Principios y directrices" e ISO-31010 "Gestión del riesgo. Técnicas de evaluación de riesgos".

Finalmente, el Ayuntamiento de Nueva York ha aprobado la llamada ley "Post" (Public Oversight of Surveillance Technology Act).

> "Se trata de un proyecto de ley para que las fuerzas de seguridad divulguen públicamente tanto las políticas de vigilancia que desarrollan como la tecnología que utilizan para garantizar el cumplimiento de dichas políticas.
>
> "Según esta nueva normativa, a partir de ahora se debe dar a conocer una descripción de las capacidades, las reglas, los procesos y las medidas de seguridad que se han establecido para proteger la información recopilada por drones, lectores de matrículas, cámaras y otros dispositivos de monitorización." (Innovadores, 2020).

A modo de observación, por medio de los antecedentes mundiales en la aplicación de legislaciones deficientes en cuanto a procesos claros de tratamiento de datos biométricos y la protección del individuo —en su privacidad, libertad y consentimiento—, y en las nuevas legislaciones, se han obtenidos importantes datos que permitirán mejorar legislaciones o dictar nuevas leyes que garanticen los derechos de los individuos. Por ello, resultará importante que los legisladores tomen en cuenta todos estos datos al momento de elaborar y aprobar nuevas leyes.

VI. CUESTIONES DE HECHO

En el marco del "Primer Congreso Internacional de Delito Transnacional" en la Legislatura Porteña, se anunció la implementación de un nuevo sistema de reconocimiento facial que funciona con Inteligencia Artificial, situación que originó diversos cuestionamientos por parte de distintas asociaciones en lo relativo a la protección de la privacidad, intimidad y datos personales. La puesta en marcha de manera intempestiva, sin el cumplimiento de procedimientos típicos, propios de esos sistemas tecnológicos, dio lugar al conflicto que nos convoca.

V. CUESTIONES DE DERECHO

En la causa por la cual tienen sentido estas palabras, se trata acerca de la irrupción en la intimidad, en la privacidad de los ciudadanos de la Ciudad Autónoma de Buenos Aires, por el uso de cámaras de seguridad con tecnología de reconocimiento facial, sin la debida evaluación de su impacto.

El conflicto que se plantea, es saber hasta qué punto la justificación que se asienta en términos de "seguridad" para tomar, tratar y almacenar información de tipo sensible, como es el rostro de una persona, ha sido debidamente planteada en pos de la protección de los derechos fundamentales de los ciudadanos que se ven involucrados.

Datos personales

Los datos biométricos son datos personales de carácter sensible según el encuadre normativo de la Ley 25.326 y la ampliación de dicho concepto mediante resolución 4/2019 emitida por la AAIP.

La consideración de dato sensible a priori impide generar base de datos, pero el presente caso encuadra en una excepción prevista en el artículo 7 de la ley 25.326 que permite recolectar y tratar esta información cuando medien razones de interés general autorizado por ley. Y los exime de cumplir los requisitos que brinda la ley según el artículo 23 por ser un caso especial destinado a fines de seguridad pública o defensa nacional.

No obstante, dicho artículo restringe de manera limitada el tratamiento a los estrictamente necesarios para cumplir su finalidad.

Asimismo, nuestro país ratificó el Convenio 108 en materia de datos personales con el fin de garantizar a cualquier persona física el respeto de sus derechos y libertades fundamentales, con respecto al tratamiento automatizado de los datos de carácter personal.

También es parte de los estados miembros de la OEA, cuyo comité jurídico, emitió en abril de 2021 los Principios Actualizados sobre la Privacidad y la Protección de Datos Personales.

En el principio doce mantiene esta excepción para los supuestos especiales con fines de seguridad pública con la salvaguarda de recomendar requisitos mínimos para el ejercicio de ello. Entre ellos menciona: fijar la finalidad del tratamiento; encuadrar la categoría de datos que trata; fijar las limitaciones; otorgar las garantías para evitar accesos o transferencias ilegítimas; determinar el responsable del tratamiento, la conservación de los datos, los riesgos para los derechos y libertades de los titulares; y el derecho de los titulares a ser informado sobre la limitación.

Intimidad

El derecho a la privacidad e intimidad, fundado en el artículo 19 de la Constitución Nacional, protege jurídicamente un ámbito de autonomía personal, así como acciones, hechos y datos que, conforme a las formas de vida acogidas por la sociedad, están reservadas al individuo, y cuyo conocimiento y divulgación por extraños implica peligro real o potencial para la misma intimidad.

El CCCN en sus artículos 1770 y 52 también protegen la vida privada y dignidad.

En virtud de estas normas existiría una función preventiva del daño, con lo que podría quedar habilitada una herramienta a los eventuales perjudicados por tales actos y manifestaciones, no solo a reclamar la reparación de los daños que sufrieran, sino también a ejercitar acciones de prevención para evitarlos, las que podrían llegar a un mandato inhibitorio en caso de que por los antecedentes fuera muy probable, al grado de cuasi certeza, que el denunciado vaya a atentar contra su derecho a la intimidad, su honra u otro derecho fundamental, de forma inminente.

Es que si una persona se enterara de que se van a difundir datos de su intimidad o que afecten su honra o reputación en un medio, o violatorios de su ámbito de intimidad o reserva, sin que existan motivos valederos para la divulgación, podría acudir a esta herramienta que brinda el art. 52 CCCN y pedirle a un juez que evite -preventivamente- la violación de su derecho a la intimidad, dictando un mandato inhibitorio y prohibiendo a ese medio que difunda tales datos.

Principio de inocencia

En nuestro sistema legal el principio de inocencia es una garantía constitucional —art. 18 de la Constitución Nacional y Tratados internacionales cfr. art. 75 inc 22—. Ello implica que toda legislación que violente este principio posee el germen del vicio de inconstitucionalidad.

Ya hemos observado que uno de los grandes conflictos que presentan las leyes de tratamiento de datos biométricos radica en la defectuosa o nula regulación de

estándares o protocolos sobre el tratamiento de dichos datos y, más preocupante, los procesos de protección y garantía de los derechos de los individuos.

El procedimiento de video vigilancia propuesto por la ley n° 6.339 —modificatoria de ley n° 5688— resulta altamente defectuoso en este sentido. En especial, respecto de los sistemas preventivo y forense se advierte una ausencia total de regulación acerca del tratamiento de los datos. Ni hablar de la consideración de los derechos de los individuos. Esto atenta contra derechos de privacidad, libertad e inocencia de los individuos.

La aplicación de procesos preventivos de video vigilancia mediante IA han demostrado graves inconvenientes en cuanto a la determinación concreta de comportamientos ambiguos, principalmente por la incorporación de datos sesgados por preconceptos sociales. Esta circunstancia, sumada con el análisis de patrones conductuales —e.g. etnia, *status* social, "zonas calientes"—, dará lugar a que los algoritmos arrojen resultados con una alta probabilidad de error. Por ello resulta importante un adecuado sistema de control. Circunstancia que no se corrobora cumplida.

Por ello, la aplicación ciega de estos procesos, sin el establecimiento de esquemas transparentes de control y garantía de los derechos de los individuos, implicará la remasterización de pensamientos superados por la dogmática penal. Es decir, existirá el peligro de retornar al positivismo criminológico donde se culpará previamente a un individuo porque el algoritmo así lo determinó.

Perfilamientos Niños, niñas y adolescentes

La Convención de los Derechos del Niño (CDN), sus principios y los derechos que consagra, forman parte del denominado "Bloque de Constitucionalidad Federal". Las Observaciones Generales constituyen una interpretación autorizada sobre aquello que se espera de los Estados partes cuando ponen en marcha las obligaciones que figuran en la CDN.

El compromiso del Estado argentino con la protección de la infancia, por fortuna, exige de un máximo compromiso de parte de todos actores sociales en la promoción y resguardo de sus derechos.

En Observación General N°25, el Comité de los Derechos del Niño explica la forma en que los Estados partes deben aplicar la Convención en relación con el entorno digital y ofrece orientación sobre las medidas legislativas, normativas y de otra índole pertinentes destinadas a garantizar el pleno cumplimiento de las obligaciones contraídas en virtud de la Convención.

El documento insta a interpretar el ejercicio de los derechos consagrados en la CDN a través de cuatro principios generales: no discriminación, interés superior del niño, Derecho a la vida, la supervivencia y el desarrollo y el respeto a las opiniones de lo NNA en relación a los asuntos que los afectan.

El documento es extenso y analiza los derechos consagrados por la CDN bajo la lupa de los principios antes mencionados y teniendo en cuenta la naturaleza de los servicios de información y comunicación y los modelos de negocio allí desarrollados.

En conexión con el tópico que nos atañe, el comité observa que la privacidad es vital para la autonomía, la dignidad, la seguridad de los niños y para el ejercicio de todos sus demás derechos. Además, resalta que la participación de NNA en entornos públicos debe ser segura, privada y libre de vigilancia por parte de entidades públicas o privadas.

En el apartado dedicado al Derecho a la privacidad, el documento reza:

"(…)Ciertas combinaciones de datos personales, como los datos biométricos, pueden identificar a un niño de forma determinante. Las prácticas digitales, como el procesamiento automatizado de datos, la elaboración de perfiles, la selección de comportamientos, la verificación obligatoria de la identidad, el filtrado de información y la vigilancia masiva, se están convirtiendo en procedimientos de rutina. Estas prácticas pueden dar lugar a una injerencia arbitraria o ilegal en el derecho de los niños a la

privacidad y pueden también tener consecuencias adversas para estos, cuyo efecto podría continuar en etapas posteriores de su vida."

En consonancia con lo anterior se advierte que "dada la existencia de motivaciones comerciales y políticas para promover determinadas visiones del mundo, los Estados partes deben garantizar que la utilización de los procesos automatizados de filtrado de información, elaboración de perfiles, comercialización y adopción de decisiones no suplanten, manipulen o inhiban la capacidad de los niños para formar y expresar sus opiniones en el entorno digital".

Siguiendo el espíritu de esta norma, que es Ley para la República, la utilización de los datos de NNA debe ser transparente, responsable y estar sujeta al consentimiento del niño o sus representantes.

Toda injerencia en su ámbito privado debe estar prevista por la ley, tener una finalidad legítima, respetar el principio de minimización de los datos, ser proporcionada, estar concebida en función del interés superior del niño y no debe entrar en conflicto con las disposiciones, los fines o los objetivos de la Convención. Sólo es admisible si no es arbitraria o ilegal.

El documento impone el deber de revisar periódicamente la legislación sobre privacidad y protección de datos y asegurarse de que los procedimientos y las prácticas impidan toda infracción deliberada o violación accidental de la privacidad de los niños. En el caso sub examine, entendemos que no se cumple con tal premisa.

En caso de que, excepcionalmente y siguiendo los principios mencionados ut supra "(…) Toda vigilancia digital de los niños, junto con cualquier procesamiento automatizado de datos personales conexo, debe respetar el derecho del niño a la privacidad y no debe realizarse de forma rutinaria, indiscriminada o sin el conocimiento del niño o, en el caso de niños de corta edad, de sus padres o cuidadores; tampoco debe efectuarse dicha vigilancia en entornos comerciales, educativos y asistenciales sin que exista el derecho a oponerse a ella, y siempre debe tenerse en cuenta el medio

disponible menos intrusivo para la privacidad que permita cumplir el propósito deseado.”

Los requisitos antes mencionados no son respetados en CABA y la empresa concesionaria del sistema de reconocimiento facial no puede brindar explicaciones respecto del tratamiento de datos de menores. Por lo tanto concluimos que su derecho a la privacidad está siendo vulnerado masivamente. Los efectos de la irresponsabilidad en el tratamiento de datos biométricos pueden tener innumerables efectos perjudiciales en la vida de millones de NNA.

VI.PETITORIO

Teniendo en cuenta lo expuesto, vengo a solicitar a V.S.

1. Que se me tenga por presentado en el carácter invocado de amigo del tribunal; y oportunamente se nos notifique de la resolución tomada al domicilio electrónico xxxxxxxxx.

2. Se consideren las cuestiones señaladas en ese carácter en oportunidad de resolver sobre este caso, decisión acerca de la cual solicitamos ser notificados.

3. Al resolver sobre el pedido xxxxxx, tenga V.E. en consideración el criterio de nuestro organismo.

Proveer de conformidad

SERA JUSTICIA

Referencias

Innovadores (1 de julio 2020). *La Policía de Nueva York tendrá que revelar la tecnología de vigilancia que usa* El Español. https://www.elespanol.com/invertia/disruptores-innovadores/innovadores/tecnologicas/20200701/policia-nueva-york-revelar-tecnologia-vigilancia-usa/501701517_0.html

Quintanilla Mendoza, G. (2020). Legislación, riesgos y retos de los sistemas biométricos. Revista Chilena de Derecho y Tecnología, 9(1), 63-91. https://rchdt.uchile.cl/index.php/RCHDT/article/view/53965/61673

Agencia Española de Protección de Datos (2019) *Modelo de Informe de Evaluación de Impacto en la Protección de Datos (EIPD) para Administraciones Públicas*. https://www.aepd.es/es/node/816