Datos sensibles, la biometría

Rosa Alicia Warlet

Paraná (E.R.)

Datos sensibles, la biometría

RESUMEN

Analizar la intersección entre inteligencia artificial y datos biométricos es un desafío importante en punto a la posible afectación al derecho a la privacidad. Luego de analizar esa problemática, se focaliza en los datos biométricos, sus riesgos y posibles soluciones

CONCLUSIONES PROPUESTAS

1. Es prioritario actualizar la LPDP continuando con la adaptación a estándares internacionales tales como la extraterritorialidad de sus normas, la definición de datos biométricos, adecuar los procesos de tratamiento de datos biométricos. En tal sentido podría ser útil seguir impulsando la propuesta del Proyecto de Actualización presentado por la Agencia de Acceso a la Información Pública en febrero/2023. Deberían ajustarse los procedimientos de recopilación, almacenamiento, uso de los datos biométricos con técnicas de cifrado sólidas; técnicas para prevenir accesos no autorizados; integrar medidas de privacidad y seguridad en todas las etapas del diseño y desarrollo del sistema, definir responsabilidades y establecer sanciones ejemplares en caso de incumplimiento provistas de celosos mecanismos de

control de su cumplimiento.

2. El consentimiento libre e informado es un baluarte que necesita ser fortalecido en pos de la seguridad y dificultar la suplantación, podría recurrirse a la combinación de la autenticación biométrica con otros factores, como contraseñas o tokens.

3. La educación y concientización de los usuarios sobre la importancia de proteger los datos biométricos es una medida necesaria a fin no sólo de prevenir ataques o minimizar sus consecuencias negativas sino también para impulsar un indispensable uso responsable de la tecnología biométrica.

Datos sensibles, la biometría

I.- Introducción

El cambio de paradigma que estamos viviendo debe ser sin dudas el más complejo de todos por la sumatoria de factores que confluyen y por la velocidad con la que se suceden los acontecimientos producidos por las innovaciones tecnológicas. Los cambios producidos y la digitalización han tenido un impacto significativo en la relación entre el Estado y los ciudadanos con referencia a la temática de protección de derechos y privacidad.

El análisis de grandes volúmenes de datos (big data) permite la recopilación, procesamiento y análisis de información proveniente de diversas fuentes, como redes sociales, registros públicos y sensores. La ventaja es que proporciona una visión más amplia y precisa de los problemas sociales, lo que podría generar políticas públicas beneficiosas tanto como contribuir con la planificación urbana y la toma de decisiones estratégicas.

El IoT[1] (internet de las cosas) permite entre otros, el monitoreo del tráfico, la recolección de datos ambientales y la optimización de los servicios públicos, cuestiones que necesariamente repercuten en el bienestar de la ciudadanía.

Resulta avasallante la transformación producida por la inteligencia artificial. la que puede colaborar para predecir y prevenir vulneraciones de derechos humanos. También es muy útil para el reconocimiento de patrones, la toma de decisiones y el procesamiento del lenguaje natural. Su aplicación permite automatizar procesos administrativos, mejorar la eficiencia en la toma de decisiones, contribuir a la detección de ilícitos, entre otras.

Pero no escapa al análisis que estas nuevas tecnologías pueden afectar derechos fundamentales de los ciudadanos como el derecho a la privacidad, la libertad de expresión, la igualdad, el debido proceso como consecuencia de lo cual es necesario tomar los recaudos que resulten necesarios a los fines de su adecuada protección.

El objeto de este trabajo es analizar un importante desafío que genera la inteligencia artificial, esto es la problemática que se presenta con relación a los datos biométricos.

---

[1] Consiste en la interconexión de objetos cotidianos a través de internet

II.- DESARROLLO

1.- Datos personales

Como consecuencia del avance tecnológico la protección de los datos personales es cada vez más difícil. Producimos datos constantemente. Nuestros datos están en archivos públicos, pero también al alcance de empresas privadas. Baste mencionar por ej., cuando la aplicación de música que utilizamos nos recomienda un listado musical preparado especialmente para nosotros. En ese caso, han encontrado un patrón para predecir nuestros gustos basado en la utilización que hemos realizado de la app.

En nuestro país, la protección de los datos personales encuentra fundamento en el art.43 de la Constitución Nacional y el plexo convencional incorporado al art.75 inc.22 del mismo cuerpo legal.

La Ley de Protección de Datos Personales (LPDP) N° 25326[2] considera que datos personales refiere a información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables. El Proyecto de Ley de Protección de Datos personales aclara el concepto expresando que se trata de *"información referida a personas humanas determinadas o determinables. Se entiende por determinable la persona que puede ser identificada directa o indirectamente por uno o varios elementos característicos de su identidad física, fisiológica, genética, biométrica, psíquica, económica, cultural, social o de otra índole"*.

La LPDP 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 de raigambre constitucional.

Los datos personales que se recojan 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.

La recolección de datos no puede hacerse por medios desleales, fraudulentos o en forma contraria a las disposiciones de la LPDP; no pueden ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención; deben ser exactos y actualizarse en el caso de que ello fuere necesario; los datos total o parcialmente inexactos, o que sean incompletos, deben ser suprimidos y sustituidos, o en su caso completados, por el responsable del archivo; deben almacenarse de modo que permitan el ejercicio del derecho de acceso de su titular;

---

[2] Publicada en el Boletín Oficial de la Nación de fecha 02/11/2000

deben ser destruidos cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubiesen sido recolectados.

Han transcurrido más de veinte años desde la sanción de la LPDP durante los cuales se ha producido un avance significativo del reconocimiento y protección de los datos, motivos que tornan imperioso transitar el camino de una actualización normativa. En efecto, así lo ponen de manifiesto la sanción de la Ley Nº 27.699[3] que aprueba el Protocolo Modificatorio del Convenio para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal (Convenio 108), el Reglamento Europeo de Protección de Datos Personales (RGPD); las Recomendaciones de Ética de Inteligencia Artificial de la UNESCO; amén de avances a nivel regional entre otros los “Estándares de Protección de Datos Personales para los Estados Iberoamericanos” de la Red Iberoamericana de Protección de Datos (RIPD); las legislaciones de Brasil y Ecuador; los proyectos de ley de Chile, Paraguay y Costa Rica, la reciente aprobación por el Parlamento Europeo de la regulación de la Inteligencia Artificial, sumado a proyectos en el orden nacional que han perdido estado parlamentario.

2.- Datos biométricos

Existen sistemas biométricos que permiten reconocer automáticamente a una persona por sus características fisiológicas o de comportamiento. El uso de éstas tecnologías implica la recolección de datos que permiten identificar a una persona. Estos sistemas utilizan la huella dactilar, reconocimiento facial que puede ser bi o tridimensional, reconocimiento de iris, reconocimiento de retina, reconocimiento vascular (autentifica la geometría de la mano), reconocimiento de voz. Datos biométricos son, por tanto, aquellos que posibiliten la identificación de una persona física a través de procesos técnicos, que recopilen información relativa al aspecto físico, corporal o conductual como su imagen facial, huella digital o similares. Para ser útiles, los datos biométricos deben ser únicos, permanentes y coleccionables.

En ese lineamiento, el Sistema Federal de Identificación Biométrica para la Seguridad (SIBIOS) ha obtenido buenos resultados tanto en la investigación criminal como en la identificación de personas desaparecidas, NN, víctimas de catástrofes, entre otros. Los datos biométricos también suelen utilizarse como control de acceso a empresas, en los aeropuertos para controlar los ingresos, la

A.F.I.P. valida con ellos la identidad de los contribuyentes; las entidades bancarias utilizan datos biométricos para proporcionar servicios de forma remota (abrir cuentas, tomar préstamos, etc.). En estos casos, su tratamiento debe regirse por las regulaciones en materia de protección de datos.

---

[3] Publicada en el Boletín Oficial de la Nación el 30/11/2022

Como contienen información única sobre características físicas o comportamientos humanos, están sujetos a riesgos tales como: a) suplantación cuando un individuo intenta hacerse pasar por otro utilizando características falsas o alteradas; b) robo de datos biométricos: cuando en caso de no contar con una debida protección podrían ser objeto de robo o acceso no autorizado; ataques de manipulación pretendiendo engañar al sistema por ej. alterando una imagen facial o modificar los patrones de voz para evadir la autenticación biométrica; c) ataques de interceptación: que podría darse cuando su transmisión no cuenta con una manera segura; d) ataques de ingeniería social que se da por ej cuando se engaña a una persona para que proporcione sus datos biométricos.

El art.2 de la LPDP, considera dato sensible los "*datos personales 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*". En base a ello puede inferirse que los datos biométricos son datos sensibles[4].

Los datos biométricos, al ser datos sensibles se rigen por la regla general de la prohibición de todo tipo de tratamiento. En tal sentido, nadie puede ser obligado a proporcionar datos sensibles y, por otro lado, se prohíbe la formación de archivos, bancos o registros que almacenen información que directa o indirectamente revele datos sensibles (cfr. art.7 inc.1 y 3 LPDP). Podrían admitirse excepciones. Así, ell art.7 inc.2 LPDP expresa que "*los datos sensibles sólo pueden ser recolectados y objeto de tratamiento cuando medien razones de interés general autorizadas por ley*".

La recolección y procesamiento de datos se fundamenta en la existencia de consentimiento libre e informado. El titular del dato que se recabe debe ser informado en forma clara y precisa sobre la finalidad de su tratamiento, quienes pueden ser sus destinatarios, la existencia de archivo, registro, banco de datos electrónico o de cualquier otro tipo, la identidad y domicilio de su responsable, el carácter obligatorio o facultativo de las respuestas al cuestionario que se le proponga, las consecuencias de proporcionar los datos, de la negativa hacerlo y de la inexactitud de los mismos, la posibilidad del interesado de ejercer los derechos de acceso, rectificación y supresión de datos.

El Proyecto de Actualización de LPDP presentado en febrero de 2023, expresa que

son *“aquellos que se refieren a la esfera íntima de su Titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen étnico; creencias o convicciones religiosas, filosóficas*

---

[4] A nivel comparado, el Reglamento General sobre Protección de Datos de la Unión Europea ubica los datos biométricos en categorías especiales de datos personales lo cual equivale a datos sensibles.

y morales; afiliación sindical u opiniones políticas; datos relativos a la salud, discapacidad, a la preferencia u orientación sexual, datos genéticos o biométricos cuando puedan revelar datos adicionales cuyo uso pueda resultar potencialmente discriminatorio para su Titular y que estén dirigidos a identificar de manera unívoca a una persona humana".

Es decir, aclara y amplía el concepto de Datos personales sensibles incluyendo expresamente a los datos biométricos, lo cual es positivo porque los datos biométricos constituyen un mecanismo de autenticación y verificación de identidad inequívoco. En consecuencia, la delimitación relativa a qué se debe entender por dato biométrico reviste importancia por la naturaleza misma de estos datos y por la protección jurídica que los mismos deben tener.

Sobre el consentimiento, el Proyecto señala que debe ser previo, libre, específico, informado e inequívoco.

La temática de consentimiento libre e informado es un importante baluarte para un uso responsable y ético de los datos biométricos. Pero, en la praxis resulta insuficiente ya que frente a la incidencia del big data puede resultar dificultoso determinar la existencia de consentimiento informado; podría ocurrir también que los datos aún obtenidos con consentimiento informado sean utilizados para otros fines violentando el principio de finalidad de tratamiento de datos consagrados en el art.4.1 y 4.3 de la LPDP. Consecuentemente, deberá en un futuro analizarse la posibilidad de reforzarlo.

III.- CONCLUSIÓN

A la expansión de utilización de los datos biométricos se le adicionan preocupaciones sobre su seguridad y privacidad. En ese contexto, los marcos legales y políticas existentes pueden quedar desactualizados, resultar insuficientes y también requerir nuevas normas tecnológicamente neutrales para abordar adecuadamente los problemas y desafíos que surgen con su uso.

Para optimizar el resultado es conveniente enfocar los datos biométricos desde distintos puntos de vista con un enfoque multidisciplinario pues la problemática que

plantea es compleja. Estando en pugna por un lado la seguridad de los datos biométricos y por otro el derecho a la privacidad debe encontrarse un delicado equilibrio entre ambos aspectos. Para ello podría ser necesaria una combinación de medidas normativas, técnicas y buenas prácticas.

En base a ello, se propone:

4. Es prioritario actualizar la LPDP continuando con la adaptación a estándares internacionales tales como la extraterritorialidad de sus normas, la definición

de datos biométricos, adecuar los procesos de tratamiento de datos biométricos. En tal sentido podría ser útil seguir impulsando la propuesta del Proyecto de Actualización presentado por la Agencia de Acceso a la Información Pública en febrero/2023. Deberían ajustarse los procedimientos de recopilación, almacenamiento, uso de los datos biométricos con técnicas de cifrado sólidas; técnicas para prevenir accesos no autorizados; integrar medidas de privacidad y seguridad en todas las etapas del diseño y desarrollo del sistema, definir responsabilidades y establecer sanciones ejemplares en caso de incumplimiento provistas de celosos mecanismos de control de su cumplimiento.

5. El consentimiento libre e informado es un baluarte que necesita ser fortalecido en pos de la seguridad y dificultar la suplantación, podría recurrirse a la combinación de la autenticación biométrica con otros factores, como contraseñas o tokens.

6. La educación y concientización de los usuarios sobre la importancia de proteger los datos biométricos es una medida necesaria a fin no sólo de prevenir ataques o minimizar sus consecuencias negativas sino también para impulsar un indispensable uso responsable de la tecnología biométrica.