



HIPERDERECHO

Tecnología como libertad

Escrito: 1

Sumilla: Denuncia

A LA DIRECCIÓN DE FISCALIZACIÓN E INSTRUCCIÓN DE LA DIRECCIÓN GENERAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN PÚBLICA Y PROTECCIÓN DE DATOS PERSONALES

HIPERDERECHO, asociación civil sin fines de lucro, debidamente representada por su Director Ejecutivo, DILMAR VILLENA FERNÁNDEZ BACA (Anexo 1-A), identificado con DNI No. 71250923 (Anexo 1-B) ambos domiciliados para este procedimiento administrativo en Av. Av. Santo Toribio 143, San Isidro, Lima, señalando correo electrónico para las correspondientes notificaciones dilmar@hiperderecho.org, (en adelante “El denunciante”) con el debido respeto me dirijo a usted a fin de presentar una denuncia por actos contrarios a la Ley de Protección de Datos Personales, Ley No. 29733, (en adelante, la “Ley”) y su Reglamento aprobado por Decreto Supremo No 003-2013-JUS (en adelante, el “Reglamento”) bajo el procedimiento reconocido en el artículo 37¹ de la referida Ley, contra la **MUNICIPALIDAD METROPOLITANA DE LIMA**, domiciliada en Jr. Rufino Torrico Nro. 1178, Cercado de Lima, Lima (en adelante “La denunciada”) y quienes resulten responsables en los siguientes términos.

I. FUNDAMENTOS DE HECHO

1. Con fecha 23 de junio de 2023, el Alcalde de Lima Rafael López Aliaga, [a través de su cuenta de TikTok](#), dió a conocer un video en el que mostraba el uso de cámaras de videovigilancia con tecnologías de reconocimiento facial a través de datos biométricos por parte de La Denunciada.

¹ **Ley No. 29733, Ley de Protección de Datos Personales, Artículo 37.- Procedimiento sancionador**

El procedimiento sancionador se inicia de oficio, por la Autoridad Nacional de Protección de Datos Personales o por denuncia de parte, ante la presunta comisión de actos contrarios a lo dispuesto en la presente Ley o en su reglamento, sin perjuicio del procedimiento seguido en el marco de lo dispuesto en el artículo 24. Las resoluciones de la Autoridad Nacional de Protección de Datos Personales agotan la vía administrativa. Contra las resoluciones de la Autoridad Nacional de Protección de Datos Personales procede la acción contencioso administrativa.



HIPER DERECHO

Tecnología como libertad



2. Esta situación también fue dada a conocer a través de distintos medios de comunicación² en los que se mencionaba que “la MML ha implementado el sistema de Inteligencia Artificial (IA), interconectando a las cámaras de videovigilancia que tiene la institución, para reconocer los rostros de los delincuentes más buscados por la policía”.
3. Posteriormente, con fecha 03 de julio de 2023, la Denunciada publicó, [a través de su red social en Twitter](https://panamericana.pe/locales/383731-mml-monitorea-ciudad-lima-4300-cameras-inteligencia-artificial-reconocimiento-facial), el mismo vídeo confirmando lo narrado previamente.

2

<https://panamericana.pe/locales/383731-mml-monitorea-ciudad-lima-4300-cameras-inteligencia-artificial-reconocimiento-facial>



HIPER DERECHO

Tecnología como libertad



Municipalidad de Lima
@MuniLima

...

¡Más de 4 mil cámaras con inteligencia artificial vigilando la ciudad! 📷
Gracias a la eficiente labor del Serenazgo Municipal junto a la PNP
venimos desarticulando presuntas bandas delincuenciales que alteran
el orden y seguridad de las calles de Lima.



4:15 p. m. · 3 jul. 2023 · 60,4 mil Reproducciones



4. Asimismo, a través de su página web, Iriarte & Asociados dio a conocer³ que habían presentado una solicitud de acceso a la información pública dirigida a La Denunciada en la que requerían la siguiente información:
 - a. Copia de los Protocolos de seguridad del sistema de cámaras de seguridad de reconocimiento facial.
 - b. Copia de las Auditorías al software del sistema de cámaras de seguridad de reconocimiento facial.
 - c. Copia de los contratos, órdenes de compra o de servicios de las contrataciones realizadas para la implementación y puesta en marcha del sistema de cámaras de seguridad de reconocimiento facial.
 - d. En caso de que el software haya sido desarrollado inhouse, copia de los contratos y curriculums de las personas que conformaron el equipo de programación del sistema de cámaras de seguridad de reconocimiento facial.
 - e. Copia de todos los informes u opiniones, técnicos o jurídicos, internos o externos, sobre la viabilidad e implementación del del sistema de cámaras de seguridad de reconocimiento facial.
 - f. Copia del Registro de base de datos ante la Autoridad Nacional de Protección de Datos personales del sistema de cámaras de seguridad de reconocimiento facial.

³ <https://www.iriartelaw.com/reconocimientofacialMUNILIMA>



HIPER DERECHO

Tecnología como libertad

- g. Protocolo, Manual, Directiva u documento análogo en el que se encuentren las políticas de uso y los mecanismos de control del sistema de cámaras de seguridad de reconocimiento facial.
5. Sin embargo, tal como se menciona en la publicación de Iriarte & Asociados, “La respuesta dada por la Municipalidad, detalla que no cuenta con ninguna de esta información necesaria para implementar un sistema de este tipo, habiendo señalado que sólo cuentan con un ‘acuerdo de intención’ firmado por el burgomaestre Rafael López Aliaga con la empresa AMERICA MOVIL PERU S.A.C. (Claro).”
6. Es decir, nos encontramos ante un supuesto en el que la Municipalidad Metropolitana de Lima ha implementado cámaras de vigilancia con tecnología de reconocimiento facial (y uso de “inteligencia artificial”, sin contar con ninguna documentación y/o directiva relacionada al tratamiento de datos personales.

II. FUNDAMENTOS DE DERECHO

A. El reconocimiento facial y los datos personales

- ¿Qué es el reconocimiento facial ?

5. Según la Opinión 02/2012 sobre reconocimiento facial en servicios en línea y móviles del Grupo de Trabajo del Artículo 29 de la Unión Europea, el reconocimiento facial es “el proceso automático de imágenes digitales que contienen rostros de personas para la identificación, autenticación/verificación o categorización de dichas personas”⁴.
6. Según la información brindada al público a través de notas y videos de prensa, la Municipalidad Metropolitana de Lima instaló cámaras con tecnología de reconocimiento facial para desarticular “presuntas bandas delincuenciales que alteran el orden y seguridad de las calles de Lim”. Ello quiere decir que el propósito del uso de esta tecnología es el de identificar personas y para ello la cámara captura una imagen, la procesa y la contrasta con una base de datos de rostros de dichos “delincuentes e infractores” en tiempo real.

- ¿Dónde se produce el tratamiento de datos personales ?

7. Los datos biométricos pueden ser definidos como las “propiedades biológicas, aspectos del comportamiento, características fisiológicas, rasgos de vida o acciones repetibles donde esas características y / o acciones son únicas para ese individuo y medibles,

⁴ https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp192_en.pdf p. 2.



HIPER DERECHO

Tecnología como libertad

incluso si los patrones utilizados en la práctica para medirlos técnicamente involucran un cierto grado de probabilidad”⁵. Así, la tecnología de reconocimiento facial emplea y procesa estos datos biométricos para poder realizar su tarea. En el caso de La Denuncia esta gira en torno a identificar a “posibles infractores” en tiempo real.

8. Este procesamiento de datos biométricos consta al menos de tres partes fundamentales. La primera de ellas es el **“registro de datos biométricos”** que se refiere a todos los subprocesos necesarios para obtener imágenes digitales, extraer los datos biométricos y vincularla con la identidad de una persona, que en el presente caso serían los “delincuentes e infractores”. Así el sistema obtiene un registro con el cual contrastar las imágenes de rostros que obtendrán con las cámaras. La segunda es el **almacenamiento de dichos datos biométricos**; y la tercera es **el contraste de los datos biométricos**. En esta última parte, se utilizan las cámaras para capturar imágenes de personas (en el caso en mención, de transeúntes), extraer la información biométrica y contrastar con el registro biométrico que se generó en la primera parte.⁶
9. De esta manera, el sistema responderá si la imagen recientemente capturada del transeúnte corresponde o no a alguna que está en el registro biométrico. Es decir, nos dirá si el transeúnte sería uno de los “delincuentes o infractores”. Esta tarea se realiza de inmediato y en tiempo real, por lo que se crea un contraste continuo de la identidad de los transeúntes.
10. Es decir, para realizar el proceso de identificación biométrica, se necesita una base de datos sobre la cual realizar una comparación sobre la información recogida por las cámaras de vigilancia. Sobre este punto no hay claridad respecto de cuál es y/o dónde se encuentra o qué entidad pública o privada proporciona la base de datos biométrica que utiliza la denunciada para realizar el proceso de identificación.
11. Hasta este punto, hemos detallado, de manera general, cómo funcionan los sistemas con cámaras con tecnología de reconocimiento facial para la identificación de personas. Cabe resaltar que más allá de si estos sistemas dan un resultado preciso, lo que nos importa es explicar donde existe tratamiento de datos personales sensibles y cuáles son los riesgos para las personas.
12. El tratamiento de datos personales implica toda captura, análisis, almacenamiento, transferencia y más. Así, cuando hablamos de el empleo de reconocimiento facial en todo momento se está procesando datos personales, que al ser biométricos son sensibles. De

⁵ https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf, pp. 3-4.

⁶ Ídem., p. 5.



HIPER DERECHO

Tecnología como libertad

este modo, encontramos que se tratan datos personales en el momento que se obtienen las imágenes, se extraen los datos biométricos, se les vincula con la identidad de una persona, se los almacena y luego se les contrasta con una segunda imagen (que a su vez es procesada). Toda esa captura, análisis y almacenamiento es tratamiento de datos personales sensibles.

13. El riesgo y las interferencias con los derechos de las personas comienza desde el proceso para la creación de un registro de datos biométricos. Al ser datos sensibles se esperaría que exista toma de consentimiento al titular de los datos de manera libre, informada y expresa o por lo menos que exista una norma con rango de ley que lo autorice a fin de evitar irregularidades en el registro. En la segunda parte, sobre el almacenamiento de los datos biométricos, es necesario que existan altos estándares en la custodia de este tipo de información, debido a que su robo o modificación llevaría a un daño grave para el titular de los datos. Cabe resaltar que la información biométrica es difícil, o hasta imposible, de ser reemplazada o modificada. Finalmente, el contraste de los datos biométricos también implica un riesgo para las personas en el sentido que crea un sistema de vigilancia masiva de todos los transeúntes quienes ven su identidad contrastada en tiempo real por sospecha de ser un “delincuente o infractor”, vulnerando así la presunción de inocencia y fundamentos del estado de derecho. Esta situación puede empeorar si el sistema no es preciso y los resultados obtenidos sobre si un transeúnte es o no un “delincuente o infractor” son erróneos. Esto claramente se agrava si no existen mecanismos de transparencia, apelación o reparación.

B. Normativa afectada

- Sobre la protección especial a los datos biométricos

13. Conforme al artículo 2 numeral 6 de la Constitución Política del Perú toda persona tiene derecho a la protección de los datos personales que le conciernen. Este derecho es desarrollado por la Ley de Protección de Datos Personales Ley N° 29733 (en adelante, “la Ley”) que define a los datos como “toda información sobre una persona natural que la identifica o la hace identificable” y que distingue a los datos biométricos como datos sensibles ya que por sí mismos pueden identificar al titular, por lo que merecen una protección especial (Art. 3 de la Ley).
14. Los datos biométricos merecen una protección tan especial que la misma ley señala la necesidad de la toma de consentimiento, por escrito, previo a su tratamiento o la existencia de una ley que lo autorice siempre que ello atienda a “motivos importantes de interés público” (Art 13.6 de la Ley) Asimismo, la ley dispone expresamente que de tratarse de este tipo de datos es especialmente necesario cumplir con el deber de



HIPER DERECHO

Tecnología como libertad

informar sobre el carácter obligatorio o facultativo del tratamiento de los datos. (Art 18 de la Ley).

15. Este marco especial para los datos biométricos también se pudo corroborar durante el proceso de consulta para la creación de la Directiva para el Tratamiento de Datos Personales mediante Sistema de Videovigilancia. En esta, la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales señaló que en el caso de reconocimiento facial se “necesita del consentimiento expreso y por escrito, salvo que una disposición normativa disponga lo contrario” ⁷.
16. Por consiguiente, se puede concluir que el marco legal peruano tiene una vocación expresa por proteger de manera especial a los datos biométricos que son, como explicamos, empleados en los sistemas de cámaras con tecnología de reconocimiento facial.

- Sobre la aplicación de la normativa de datos personales

17. La Autoridad de Protección de Datos Personales, a través de una nota de prensa publicada el 09 de setiembre del 2022⁸, dio a conocer que “las municipalidades, en mérito de su ley orgánica, tienen reconocidas competencias para resguardar la seguridad ciudadana y, en ese marco, videovigilar, pero no pueden por sí y ante sí utilizar datos biométricos con fines de identificación”. Esto debido a que dicho tratamiento se reserva “de manera exclusiva y excluyente a la Policía Nacional del Perú y/o al Ministerio Público, entidades que, caso a caso, y por su acceso privilegiado al Registro Nacional de Identificación y Estado Civil (RENIEC), pueden hacerlo”.
18. Asimismo, según MEMORANDO N.º 464-2022-JUS/DGTAIPD, la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, se indicó que dicha nota de prensa estaba sustentada en once [\(11\) opiniones consultivas sobre la materia](#).
19. Por lo tanto, la aplicabilidad de la Ley de Protección de Datos Personales, su Reglamento y las Directivas correspondientes no puede ser objetada. En este sentido, La Denunciada se encuentra en la obligación de cumplir el marco normativo peruano de protección de datos personales.

- Sobre los actos irresponsables (ilegales) de la denunciada

7

<https://www.minjus.gob.pe/wp-content/uploads/2020/01/Matriz-que-sistematiza-y-absuelve-los-comentarios-recibidos-al-proyecto-normativo-de-Directiva-de-Videovigilancia.pdf> p. 38

8

<https://web.archive.org/web/20220911155435/http://www.gob.pe/institucion/minjus/noticias/648855-autoridad-de-proteccion-de-datos-personales-insta-a-candidatos-a-conducir-campanas-con-apego-a-normas-de-proteccion-de-datos-personales>



HIPER DERECHO

Tecnología como libertad

20. De acuerdo a lo expuesto y aplicando la Ley de Protección de Datos Personales en especial lo referido por el artículo 4.2. del Reglamento del Decreto Legislativo 1218., encontramos que la denunciada viene incumpliendo diversos preceptos de la normativa.

- ***Sobre el principio de consentimiento:*** Como se vio al inicio, la protección de los datos biométricos, al ser datos sensibles, es especial. La normativa actual pide que previo a su tratamiento se obtenga el consentimiento expreso o que exista una ley que habilite el tratamiento de este tipo de datos biométricos. En el caso la denunciada no cuenta con el consentimiento ni de las personas que están en el registro biométrico por ser “delincuentes o infractoras” ni de los transeúntes. Tampoco existe una ley que habilite este tratamiento justificando que se atiende a motivos importantes de interés público. Por lo tanto, no existe una base legítima para que la denunciada trate los datos biométricos.
- ***Sobre el principio de finalidad:*** Todo tratamiento de datos personales, según la normativa nacional e internacional debe estar fundamentada en una finalidad. Sin embargo, más allá de los encabezados de las noticias donde se anuncia que la instalación de las 9 cámaras que cuentan con tecnología de reconocimiento facial ayudarán a identificar a posibles delincuentes e infractores, la denunciada no cuenta con documentación referida a qué finalidad tendrá el tratamiento de datos personales recogidos a través de las 09 cámaras que cuentan con tecnología de reconocimiento facial (en adelante, “Las cámaras”). Es necesario resaltar que un simple anuncio en medios de comunicación no basta para cumplir con este principio tan fundamental que implica una justificación fundamentada de la finalidad.
- ***Sobre el principio de seguridad:*** Como mencionamos anteriormente, el riesgo de robo o alteración de los datos biométricos es un daño grave para el titular de datos personales. Por ello, es imprescindible que el titular (en este caso el denunciado) y el encargado, de existir, deben tomar las medidas técnica organizativas y legales para garantizar la seguridad de los datos biométricos. Los cuales, deberían ser aún más rigurosos tratándose de datos sensibles. No obstante, la denunciada no cuenta con protocolos de seguridad y confidencialidad referidos al tratamiento de datos recopilados producto de las cámaras de reconocimiento facial; ni con protocolos para la supervisión y rendición de cuentas.



HIPER DERECHO

Tecnología como libertad

- ***Sobre el principio de disposición de recurso:*** Según este principio, el titular del banco de datos, en este caso la Municipalidad Metropolitana de Lima debe contar con un medio accesible para que el titular de los datos personales pueda hacer valer sus derechos, inclusive un simple pedido de acceso. Sin embargo, no es posible identificar ello. Asimismo, no cuenta con protocolos, directivas y/o similares en los que se detalle el procedimiento de borrado de las imágenes capturadas a través de las cámaras ni cuenta con auditorías para verificar que las imágenes fueron efectivamente eliminadas.
- ***Sobre el derecho de información del titular de los datos personales:*** Si bien la denunciada anunció la instalación de las cámaras con tecnología de reconocimiento facial en los medios de comunicación nacional, ello no es suficiente para que se cumpla con el deber de informar. El titular tiene derecho a ser informado de manera detallada, sencilla, expresa, inequívoca y de manera previa a la recopilación sobre la finalidad, destinatarios de los datos, la existencia del banco de datos, la identidad y domicilio del titular del banco de datos, el encargado, si lo hubiera, entre otros. Sin embargo, la denunciada no cuenta con documentación referida a la finalidad del tratamiento, ni protocolos que expliquen de qué manera se procesan las imágenes, cómo se supervisa o se rinde cuentas, cuánto y dónde tiempo se almacenan los datos biométricos, ni si estos datos son compartidos con terceros.
- ***Sobre la inscripción del sistema de videovigilancia ante la Dirección de Protección de Datos Personales:*** Según la ley de protección de datos personales constituye una infracción grave que el titular del banco de datos no inscriba dicho banco en el Registro Nacional de Protección de Datos Personales. Asimismo, se establece, como obligación, en el Reglamento del Decreto Legislativo N° 1218 la inscripción del sistema de videovigilancia ante la Dirección de Protección de Datos Personales. Luego de hacer una consulta en el Sistema de búsqueda de banco de datos del Registro Nacional de Protección de Datos Personales, no encontramos información alguna sobre el banco de datos que contiene datos biométricos que se emplean en el sistema de cámaras con tecnología de reconocimiento facial. Como comentamos, debe existir mínimamente un registro de datos biométricos con los cuales se contrasta las nuevas imágenes de rostros que captura la cámara y que podrían estar en otra base de datos. Nada de ello se encuentra registrado.



HIPER DERECHO

Tecnología como libertad

- ***Sobre las obligaciones y prohibiciones para el personal autorizado en sistemas de videovigilancia:*** Al tratarse de datos biométricos, se esperaría que existan protocolos, fichas, documentación en general sobre los procesos internos y responsables. Estos, además, deberían cumplir con la Directiva de Seguridad de la Autoridad Nacional de Protección de Datos Personales. Sin embargo, la Municipalidad Metropolitana de Lima no cuenta con documento que especifique las funciones y autorizaciones que tiene el personal que opera las cámaras con reconocimiento facial y softwares relacionados.

21. Por todo lo expuesto, cabe apreciar que la denunciada no estaría cumpliendo con la normativa relacionada a la protección de datos personales incumplimiento de manera general el principio de legalidad.

III. SOLICITUD

Por lo expuesto, solicitamos a su despacho admitir la presente denuncia y darle el trámite correspondiente conforme a ley.

IV. ANEXOS

Anexo 1-A: Partida Electrónica N° 12962448 del Registro de Personas Jurídicas de la Oficina Registral de LIMA

Anexo 1-B: Copia del Documento Nacional de Identidad de Dilmar Villena Fernández Baca

Lima, 04 de julio de 2023

Dilmar Villena Fernández Baca
Director Ejecutivo
Hiperderecho