FORMULARIO DE DENUNCIA POR ACTOS CONTRARIOS A LA LEY Nº 29733 Y SU REGLAMENTO APROBADO POR DECRETO SUPREMO N° 03-2013-JUS

Dirigido a la Dirección de Fiscalización e Instrucción

I. DATOS DEL DENUNCIANTE

Nombres: Miguel Enrique

Apellidos: Morachimo Rodríguez

Nº de Documento de Identidad

DNI [redacted] Pasaporte [ ] CE/CI [ ]

[redacted]

[redacted]

Distrito: [redacted] Provincia: Lima

Departamento: Lima

Referencia: –

Teléfono: [redacted]

Acepto que todo acto administrativo derivado del presente procedimiento se me notifique a mi correo electrónico (numeral 4 del artículo 20º del Texto Único Ordenado de la Ley Nº 27444).

SI (●) NO ( )

Si la respuesta es positiva, indicar dirección de correo electrónico:

dilmar@hiperderecho.org

II. DATOS DEL DENUNCIADO (TITULAR DEL BANCO DE DATOS PERSONALES O RESPONSABLE DEL TRATAMIENTO DE DATOS PERSONALES)

Titular del banco de datos personales [✔] Responsable del tratamiento [ ]

Nombres: Municipalidad Distrital de La Victoria

Apellidos: –

Razón Social: –

DNI [ ] Pasaporte [ ]

CE/CI [ ] RUC: 20131368071

Avenida

Av. Iquitos Nro. 500

Distrito: La Victoria Provincia: Lima Región: Lima

Otros datos para su ubicación:

-

III. DESCRIPCIÓN DE LOS HECHOS

Los hechos están descritos en el escrito parte integrante de la presente denuncia.

IV. DOCUMENTOS EN LOS QUE SE SUSTENTA LA DENUNCIA

Detalle la relación de documentos en los que sustenta la denuncia y adjunta al presente formulario:

1. Escrito N° 1
2. Anexo 1-A
3. Anexo 1-B
4. Anexo 1-C
5. Anexo 1-D, Anexo 1-E

CONDICIONES DEL TRATAMIENTO DE DATOS PERSONALES

En cumplimiento del artículo 18° de la Ley N° 29733, Ley de Protección de Datos Personales, se le informa que los datos personales proporcionados se incluirán en el banco de datos personales denominado "Expedientes de Fiscalización e Instrucción de la Dirección de Fiscalización e Instrucción", cuyo titular es el Ministerio de Justicia y Derechos Humanos, con domicilio en Scipión Llona 350, Miraflores, Lima- Perú. El banco de datos ha sido declarado ante la Autoridad Nacional de Protección de Datos Personales, mediante su inscripción en el Registro Nacional de Protección de Datos Personales con el código: RNPDP-EP N° 13431.

La finalidad del tratamiento de los datos es gestionar y tramitar los expedientes de la Dirección de Fiscalización e Instrucción y con fines estadísticos e históricos. Pueden ser destinatarios de la información los interesados en los procedimientos, los órganos jurisdiccionales, el Ministerio Público, la Defensoría del Pueblo, otras entidades de la Administración Pública. El plazo durante el cual se conservarán los datos será indeterminado conforme a Ley. El titular de los datos personales podrá ejercer los derechos de acceso, rectificación, cancelación y oposición ante el titular del banco de datos en la siguiente dirección: Calle Scipión Llona 350, Miraflores, Lima, o a la siguiente dirección de correo electrónico: protegetusdatos@minjus.gob.pe

Fecha: 16/10/2020

Firma: 

Nombre: Miguel Enrique Morachimo Rodrígez

DNI: Av. Iquitos Nro. 500

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, MIGUEL ENRIQUE MORACHIMO RODRÍGUEZ, según poderes inscritos en el Asiento A00003 de la Partida Electrónica No. 12962448 del Registro de Personas Jurídicas de la Oficina Registral de Lima (Anexo 1-A), identificado con DNI No. [redacted] (Anexo 1-B) y [redacted] **VERÓNICA ARROYO** [redacted], identificada con DNI N° [redacted] (Anexo 1-C), ambos domiciliados para este procedimiento administrativo en [redacted], Lima, señalando correos electrónicos para las correspondientes notificaciones dilmar@hiperderecho.org y veronica@accesonow.org respectivamente, (en adelante "Los denunciantes") con el debido respeto nos dirigimos 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 37[1] de la referida Ley, contra la **MUNICIPALIDAD DISTRITAL DE LA VICTORIA**, domiciliada en Av. Iquitos N° 500, La Victoria, Lima (en adelante "La denunciada") en los siguientes términos.

I. FUNDAMENTOS DE HECHO

1. Con fecha 12 de abril de 2019, el diario El Comercio publicó la nota titulada "Máxima vigilancia en Gamarra así funcionan las cámaras con reconocimiento facial"[2] mediante la cual tomamos conocimiento sobre la instalación de cámaras con reconocimiento facial en Gamarra y la inauguración del centro de monitoreo y control. Posteriormente, con fecha 31 de julio de 2019, el diario El Trome publicó nota periodística titulada "La

[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.

[2] https://elcomercio.pe/lima/seguridad/gamarra-vigilancia-extrema-funcionan-camaras-reconocimiento-facial-george-forstyh-victoria-noticia-ecpm-625744-noticia/

Victoria: George Forsyth anuncia la instalación de más de 160 cámaras con reconocimiento facial y de placas"[3] donde a su vez se informó del aumento del número de cámaras con tecnología de reconocimiento facial en todo el distrito de La Victoria.

2. Ante el conocimiento de dichos ellos y la falta de información adicional sobre el particular, el día 11 de Noviembre de 2019, presentamos una solicitud de acceso a la información pública dirigida a la Municipalidad de La Victoria (Anexo 1-D), solicitando información pública referida a las cámaras de videovigilancia con reconocimiento facial ubicadas en dicho distrito y el tratamiento de datos personales realizado en razón de dichas cámaras.

3. Ante la falta de respuesta presentamos un recurso de apelación ante el Tribunal de Transparencia y Acceso a la Información Pública el cual la declaró fundada (Resolución N° 010300612020, de 24 de enero de 2020) y ordenó a la denunciada la entrega de la información solicitada.

4. El 9 de marzo de 2020 la denunciada cumplió con lo ordenado a través de una carta de fecha 24 de diciembre de 2019 (Anexo 1-E) y brindó respuesta a la solicitud realizada el 11 de noviembre de 2019. De la información brindada por la propia denunciada, podemos afirmar lo siguiente:

    a. La Municipalidad de La Victoria 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").
    b. La Municipalidad de La Victoria no cuenta con protocolos para la supervisión y rendición de cuentas de las cámaras.
    c. La Municipalidad de La Victoria no cuenta con protocolos, directivas y/o similares que indiquen de qué manera se procesan las imágenes que son capturadas por las cámaras.
    d. La Municipalidad de La Victoria no cuenta con protocolos de seguridad y confidencialidad referidos al tratamiento de datos recopilados producto de las cámaras de reconocimiento facial.
    e. La Municipalidad de La Victoria no cuenta con documentos que detallen el tiempo por el cual son almacenadas las imágenes capturadas por la cámara de reconocimiento facial y procesadas por el sistema.
    f. La Municipalidad de La Victoria no cuenta con documentos que detallen en dónde se almacenan las imágenes capturadas por la cámaras de reconocimiento facial.

[3] https://trome.pe/actualidad/victoria-george-forsyth-anuncia-instalacion-160-camaras-reconocimiento-facial-placas-fotos-130985

g. La Municipalidad de La Victoria no cuenta con información referida sobre en qué servidores se almacenan los datos personales obtenidos por las cámaras.
h. La Municipalidad de La Victoria no cuenta con documentos que detallen qué autoridades o entidades públicas o privadas pueden tener acceso y/o procesar las imágenes capturadas por la cámaras de reconocimiento facial así como información relacionadas con este procesamiento.
i. La Municipalidad de La Victoria no cuenta con información referida a sobre si los datos recopilados por las cámaras son transferidos a terceros.
j. La Municipalidad de La Victoria 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.
k. La Municipalidad de La Victoria no cuenta con medidas de seguridad, privacidad y confidencialidad para asegurar el control e integridad de los datos personales recogidos a través de las cámaras.
l. La Municipalidad de La Victoria no cuenta con documento que especifique las funciones y autorizaciones que tiene el personal que opera las cámaras con reconocimiento facial y softwares relacionados.

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 de La Victoria instaló cámaras con tecnología de reconocimiento facial para “identificar a posibles delincuentes e infractores”[5]. 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.

[4] https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp192_en.pdf p. 2.
[5] https://elcomercio.pe/lima/seguridad/gamarra-vigilancia-extrema-funcionan-camaras-reconocimiento-facial-george-forstyh-victoria-noticia-ecpm-625744-noticia/

- **¿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, incluso si los patrones utilizados en la práctica para medirlos técnicamente involucran un cierto grado de probabilidad"[6]. Así, la tecnología de reconocimiento facial emplea y procesa estos datos biométricos para poder realizar su tarea. En el caso de la Municipalidad de La Victoria esta gira en torno a identificar a "delincuentes e 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 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. [7]

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. 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.

11. El tratamiento de datos personales implica toda captura, análisis, almacenamiento, transferencia y más. Así, cuando hablamos de el empleo de reconocimiento facial en todo

[6] https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf, pp. 3-4.
[7] Ídem., p. 5.

momento se está procesando datos personales, que al ser biométricos son sensibles. De 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.

12. 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 normas 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 Nº 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

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" [8].

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. En el caso particular de instalación de cámaras con tecnología de reconocimiento facial por parte de la Municipalidad de La Victoria encontramos una inconsistencia en la legislación actual que podría llevar a la desprotección de todos los transeúntes que pasan por el alcance de dichas cámaras, más aún teniendo en cuenta las respuestas brindadas por la denunciada que dan a conocer una actitud irresponsable en el procesamiento de datos biométricos.

18. Por un lado, la Ley excluye de su ámbito de aplicación a los datos contenidos o destinados a serlo en bancos de datos de administración pública en tanto resulte para el cumplimiento de competencias asignadas para la seguridad pública (Art 3). Esta misma idea es reafirmada en la Directiva para el Tratamiento de Datos Personales mediante Sistemas de Videovigilancia que igualmente excluye de su ámbito de aplicación a la situación mencionada (6.2.1.)[9]

19. La Municipalidad de La Victoria es un ente de la administración pública que según la Ley Orgánica de Municipalidades (Ley N° 27972) tiene entre sus competencias la seguridad ciudadana (arts. 73 numeral 2.5 y 85). Entonces, se entendería que la Ley de Protección de datos personales que incluye el reconocimiento de derechos, principios e imposición de obligaciones no es aplicable para el caso.

20. Sin embargo, el 2015 se aprobó el Decreto Legislativo N°1218 Decreto Legislativo que regula el uso de cámaras de videovigilancia, la cual regula el uso de cámaras de vigilancia y es de aplicación a personas públicas propietarias o poseedoras de cámaras de

[8] 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
[9] https://www.minjus.gob.pe/wp-content/uploads/2020/01/Directiva-N%C2%B0-01-2020-DGTAIPD-1.pdf

videovigilancia ubicadas en dominio público. Esta norma con rango de ley señala expresamente que:

> **Artículo 13.- Obligaciones en la captación y grabación de imágenes, videos o audios**
> Todas las personas naturales o jurídicas, entidades públicas o privadas propietarias o poseedoras de cámaras de videovigilancia que capten o graben imágenes, videos o audios deben observar lo siguiente:
> a. Cuando aparezcan personas identificables deben observar los principios y disposiciones de la normativa de protección de datos personales.

Asimismo, el reglamento del mencionado Decreto Legislativo N°1218 (Decreto Supremo N° 007-2020-IN) desarrolla en su Artículo 4 disposiciones referidas a la protección de datos personales en el ámbito del uso de las cámaras de videovigilancia con fines de seguridad ciudadana. Este artículo señala explícitamente:

> 4.2. Las disposiciones contempladas en la Ley N° 29733, Ley de Protección de Datos Personales, su Reglamento y normativa que se emita sobre la materia, se aplican principalmente para los siguientes aspectos:
>
> a) Respeto del derecho a la protección de datos personales cuando en las imágenes o videos de las cámaras de videovigilancia se presentan supuestos que identifican o hacen identificables a personas.
> b) Cumplimiento de los principios rectores de la protección de datos personales.
> c) Obligación de informar al público sobre la presencia de cámaras de videovigilancia y que está siendo grabado.
> d) Inscripción del sistema de videovigilancia ante la Dirección de Protección de Datos Personales.
> e) Formalidades por cumplir ante el encargo de la gestión del sistema de videovigilancia con utilización de los equipos o acceso a las imágenes o voces.
> f) Obligaciones y prohibiciones para el personal autorizado en sistemas de videovigilancia.
> g) Tratamiento específico con fines de seguridad para entidades financieras y escuelas.

21. Por consiguiente, esta norma dictamina que la instalación y uso de cámaras de videovigilancia por parte de una entidad pública debe cumplir con las obligaciones, principios y derechos propios del derecho fundamental a la protección de datos personales, los cuales se ven plasmados en la Ley de Protección de Datos Personales. Cabe resaltar que la norma menciona de manera general a las cámaras de videovigilancia las cuales pueden o no contener tecnología de reconocimiento facial, infrarroja, medición de distancia, entre otros. La preocupación por el cumplimiento de la normativa de datos personales se da por el riesgo que existe en la identificación de las personas transeúntes. Cuando se emplea tecnología de reconocimiento facial para acompañar a estas cámaras

de videovigilancia es justamente por que se desea identificar a personas, que en el caso de la denunciada es a “delincuentes o infractores”.

22. De esta manera, al tratarse del uso de cámaras con tecnología de reconocimiento facial que permiten la identificación de las personas, el Decreto Legislativo N° 1218 nos remite a la Ley N° 29733, la misma que señala que el caso en mención está fuera de su ámbito de aplicación. Esto crea una aparente inconsistencia en el marco jurídico: de un lado, la Ley de Protección de Datos Personales excluye de su ámbito de aplicación el cumplimiento de competencias asignadas por ley para la seguridad pública; y, de otro lado, el Decreto Legislativo N° 1218 establece que toda entidad pública que propietaria o poseedora de cámaras de videovigilancia debe observar los principios y disposiciones de la Ley de Protección de Datos Personales.

23. Dicha antinomia se salva interpretando dichas normas (ambas de rango de ley) de la siguiente manera: La normativa de protección de datos personales no es aplicable a los datos contenidos o destinados a ser contenidos en bancos de datos de administración pública para el cumplimiento de competencias referidas a la seguridad pública, **salvo que para cumplir dicha competencia se utilicen cámaras de videovigilancia, en cuyo caso será aplicable la Ley de protección de datos personales**. Esta interpretación es, además, conforme con el principio *pro persona* según el cual se debe brindar la interpretación normativa que privilegie la tutela de los derechos fundamentales, en este caso, el derecho fundamental a la protección de datos personales.

24. Además, no se puede objetar la aplicación de la normativa de protección de datos personales en función de la Segunda Disposición Complementaria Final del Decreto Legislativo N° 1218[10]. En efecto, esta disposición hace alusión al *vacatio legis* referido a estándares técnicos, mas no a la aplicación de principios, derechos u obligaciones de la Ley de Protección de Datos Personales. Similar regulación realiza lo dispuesto en la Primera Disposición Complementaria Final de su Reglamento[11], en donde no se establece *vacatio legis* específico para el artículo 4, referido a la Protección de Datos Personales. Por lo tanto, **la Municipalidad de la Victoria estaba en la obligación de cumplir**

---

[10] **SEGUNDA.- Adecuación de Estándares Técnicos de Cámaras de videovigilancia en bienes de dominio público**
A partir de la entrada en vigencia del reglamento del presente Decreto Legislativo, toda persona natural o jurídica, pública o privada que administre bienes de dominio público deberá adecuarse a los estándares técnicos definidos en dicho reglamento en un plazo no mayor a cinco (5) años. Los nuevos procesos de adquisición referidos a cámaras de videovigilancia deben cumplir los estándares técnicos.

[11] **Primera.- Vigencia**
La presente norma entra en vigencia al día siguiente de su publicación en el diario oficial El Peruano, con excepción de los artículos 7, 9, 10, 11, 14, 15, 20 y 22, cuya vigencia se da conforme a lo dispuesto en el Plan de Adecuación de los Sistema de Videovigilancia.

las disposiciones de la Ley de Protección de Datos Personales y sus normas de desarrollo al día siguiente de la publicación del Decreto Legislativo N° 1218, esto es, a partir del 25 de setiembre del 2015.

- **Sobre los actos irresponsables (ilegales) de la denunciada**

25. Como se comentó en los fundamento de hecho, la Municipalidad de La Victoria, luego de varios meses y la intervención de la Autoridad de Transparencia, la cual ordenó la entrega de la información, nos remitió la respuesta a nuestra preguntas sobre el sistema, los datos tratados, las especificaciones técnicas, los procesos internos y con terceros, y los procedimientos para la identificación y captura de sospechosos.

26. De acuerdo a las respuestas brindadas 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.

- ***Sobre el principio de disposición de recurso:*** Según este principio, el titular del banco de datos, en este caso la Municipalidad de La Victoria, debe disponer de vías para que la persona pueda reclamar y hacer valer sus derechos. La denunciada cuenta con un correo electrónico <fiscateescucha@munilavictoria.gob.pe > y una mesa de partes virtual para consulta de expedientes, pago de tributos y cuponera. No obstante, no cuenta de manera accesible con alguna herramienta para que el titular de los datos biométricos pueda reclamar o hacer valer sus derechos, inclusive un simple pedido de acceso. 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 la 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.

- ***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 Proteccíon de Datos Personales. Sin embargo, la Municipalidad de La Victoria no cuenta con documento que especifique las funciones y autorizaciones que tiene el personal que opera las cámaras con reconocimiento facial y softwares relacionados.

27. 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 Miguel Enrique Morachimo Rodríguez