Pontificia Universidad Católica del Perú
Facultad de Derecho

Programa de Segunda Especialidad en Derecho Administrativo

Tratamiento de datos personales sensibles en Perú en el contexto de Covid-19

Trabajo Académico para optar el título de Segunda Especialidad en Derecho Administrativo

AUTORA
Nataly Macutela Lavilla

ASESOR:

Diego Hernando Zegarra Valdivia

CÓDIGO DE LA ALUMNA:
20146551

2020

RESUMEN

La última década se caracteriza por el uso generalizado de tecnologías de información que son capaces de recopilar, almacenar, procesar, relacionar y transmitir gran cantidad información. Este contexto puso en evidencia riesgos derivados del tratamiento indiscriminado de información personal tales como el uso de información para finalidades no autorizadas por el titular de los datos personales; suplantación de identidad, elaboración de perfiles en el contexto de la toma de decisiones automatizadas; predicción del comportamiento o preferencias en una situación específica; entre otros. Por ello, el presente trabajo de investigación tiene como objetivo dar cuenta del desarrollo normativo y los aportes de la Autoridad Nacional de Protección de Datos Personales (en adelante, ANPDP) para la protección de datos personales de carácter sensible en Perú en el contexto de Covid-19. Para conseguir ello, se analiza el desarrollo doctrinario y jurisprudencial, así como la normativa comparada aplicable a los datos sensibles. Lo anterior permite arribar a las siguientes conclusiones: i) la Ley de Protección de Datos Personales (en adelante, LPDP) no contiene una definición acertada de datos biométricos como datos sensibles; ii) los datos relativos a salud de las personas son datos sensibles, cuyo tratamiento de encuentra exceptuado del consentimiento personal cuando tiene como finalidad la prevención, diagnóstico y tratamiento de una enfermedad o razones interés público o salud pública, no obstante, se deben observar los demás principios recogidos en la LPDP y adoptar medidas legales, técnicas y organizativas; y, iii) los aportes de la ANPDP no representan un avance significativo para la protección de datos sensibles.

CONTENIDO

I. Introducción

El derecho a la autodeterminación informativa o protección de datos personales recogido en el inciso 6 del artículo 2 de la Constitución Política del Perú (1993), cuyo bien jurídico es asegurar a las personas el control de su información personal y protegerlas de los perjuicios que puede causar el uso ilegítimo por parte de terceros, sean públicos o privados.

A partir de la Emergencia Sanitaria y Estado de Emergencia, declarados por el Decreto Supremo N° 008-2020-SA y el Decreto Supremo N° 044-2020-PCM publicados en el Diario Oficial El Peruano, en fechas 11 de marzo de 2020 y 15 de marzo de 2020, respectivamente, -y sus prórrogas- entidades públicas, privadas y medios de prensa empezaron a recopilar información concerniente a la salud de las personas, con la finalidad de evitar la propagación del Coronavirus SARS-CoV-2 (Covid-19); monitorear los síntomas de la enfermedad en las personas; informar sobre las estadísticas de casos (personas recuperadas y fallecidas): realizar investigaciones epidemiológicas para encontrar la vacuna; entre otras.

Para lograr tales finalidades, se ha recurrido al tratamiento de datos personales y datos sensibles a través de aplicativos móviles, redes sociales, sistemas biométricos; sin embargo, el uso de estos medios técnicos debe respetar el contenido del derecho a la protección de datos personales. Así, en el presente trabajo de investigación se examinará el uso de sistemas de geolocalización y cámaras de lecturas de temperatura, a la luz de la normativa peruana de protección de datos personales. Ello permite, posteriormente, explicar la aplicación de los principios de consentimiento, proporcionalidad y finalidad en el tratamiento de dichos datos personales de carácter sensible, así como la adopción de medidas legales, técnicas y organizativas.

II. Tratamiento de datos personales sensibles a través de sistemas biométricos

El derecho a la autodeterminación informativa o a la protección de datos personales, está reconocido en el inciso 6 del artículo 2 de la Constitución Política del Perú (1993) cuando señala que toda persona tiene derecho a que “los servicios informáticos, computarizados o

no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar".

El bien jurídico que subyace a este derecho "consiste en asegurar a las personas el control de la información –de los datos– que les es propia para ponerles al resguardo o, al menos permitirles protegerse de los perjuicios derivados, del uso por terceros, públicos o privados, de ese material" (Murillo de la Cueva & Piñar Mañas, 2009, pág. 18).

La normativa de protección de datos personales en nuestro país está conformada principalmente por la LPDP, ley 29733 (2011) que creó la ANPDP que es el Ministerio de Justicia y Derechos Humanos a través de la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (en adelante, DGTAIPD) y su Reglamento aprobado mediante decreto supremo 003-2013-JUS (2013).

Ahora bien, la referida normativa diferencia entre un dato personal que es "toda información sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados", de conformidad con la definición recogida en el numeral 4 del artículo 2 de la LPDP y un dato personal sensible, cuya definición abordaremos a continuación.

II.1. Datos personales sensibles

El Tribunal Constitucional mediante sentencia recaída en el Expediente N° 6164-2007-PHD/TC (2007, párrafo 2) hizo referencia a "dato sensible" cuando desarrolló el hábeas data supresorio incluido dentro del hábeas data manipulador como una de las tipologías de hábeas data[1]; no obstante, no brindó un concepto de dato sensible. Por ello, para comprender la *ratio legis* de la clasificación de datos sensibles, recurriremos a doctrina autorizada.

[1] El Tribunal Constitucional desarrolló los tipos de hábeas data, entre ellos se encuentra el hábeas data manipulador que a su vez contiene el hábeas data supresorio que busca eliminar la información sensible o datos que afectan la intimidad personal, familiar o cualquier otro derecho fundamental de la persona. También puede proceder cuando la información que se almacena no guarda relación con la finalidad para la cual ha sido creado el banco de datos.

La trascendencia de conceptualizar y diferenciar a los datos personales de los datos sensibles, radica en "la especial atención que le brinda el legislador desde el punto de vista de su protección" (Cristea Uivaru, 2018, pág. 44). Asimismo, la doctrina categoriza a los datos personales sensibles desde dos perspectivas: material y formal.

> "Los datos sensibles puede categorizarse desde un prisma material y un prisma formal. Desde un punto de vista material, son datos sensibles los que relevan o son susceptibles de poner de manifiesto datos que hacen referencia a las cualidades de la persona relacionadas con su dignidad, con aspectos que afectan su personalidad, que dibujan su forma de ser y de comportarse. Y desde un punto de vista formal, los datos que requieren unas especiales y reforzadas garantías de uso que alcanzan su recogida y tratamiento y que sopesan, en estas fases concretas de tratamiento, la voluntad de la persona" (Cristea Uivaru, 2018, pág. 44).

A su vez, Herrán hace una diferenciación entre los datos sensibles, distinguiendo entre un criterio referido al contenido de los datos y otro criterio referido al mayor o menor nivel de protección que ampara los mismos. Así, el primer grupo estaría constituido por informaciones referidas a la libertad ideológica; y, un segundo grupo involucra datos de origen racial, comportamiento social y salud (Herrán Ortiz, 1988, págs. 263-273).

De lo anterior podemos colegir que los datos sensibles –a diferencia de los datos personales- ameritan de una protección cualificada por parte de ordenamiento jurídico en atención a que, en caso de divulgarse de manera indebida, afectarían de manera más levisa al bien jurídico que subyace al derecho a la protección de datos personales.

El numeral 5 del artículo 2 de la LPDP recoge la siguiente definición de dato sensible "datos personales constituidos por los datos biométricos que por sí mismos pueden identificar al titular; datos referidos al origen racial y étnico; ingresos económicos; opiniones o convicciones políticas, religiosas, filosóficas o morales; afiliación sindical; e información relacionada a la salud o a la vida sexual".

Por ello, la ANPDP, mediante Oficio N° 213-2017-JUS/DGTAIPD "se consideran datos sensibles, entre otros, aquellos datos personales que cumplen con dos características: i) son datos biométricos; y, ii) dichos datos, por sí mismos, hacen posible la identificación del titular" (2017).

II.2. Biometría, datos biométricos y sistemas biométricos

Actualmente, la necesidad de contar con sistemas que permitan la identificación de las personas ha influenciado en el desarrollo de la biometría, que "como disciplina, ha sido definida como la ciencia para establecer la identidad de un individuo según atributos físicos, químicos o comportamentales" (Fraden, 2004). De manera que, la biometría "implica el manejo de datos característicos, ya sea de un individuo particular o de un grupo de individuos, los cuales son almacenados por quien maneja dichos datos como una representación de un perfil biológico" (Boris A, Chiara, Mora, & Muñoz-Quezada, 2020, pág. 44).

La normativa peruana de protección de datos personales no recoge una definición de datos biométricos, por lo que corresponde remitirnos al derecho comparado para dar contenido a este concepto, en particular al Reglamento General de Protección de Datos (en adelante, RGPDP), cuyo numeral 14 del artículo 4 define a los datos biométricos como "datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos" (2016).

Asimismo, el Dictamen 3/2012 del Grupo del Artículo 29[2] recoge la definición de dato biométrico definidos mediante el Dictamen 4/2007, donde los datos biométricos se definen de la siguiente manera:

[2] El Grupo de Trabajo del artículo 29 (GT Art. 29) es el grupo de trabajo europeo independiente que se ha ocupado de cuestiones relacionadas con la protección de la privacidad y los datos personales hasta el 25 de mayo de 2018 (entrada en aplicación del RGPD).
El Grupo se creó en virtud del artículo 29 de la Directiva 95/46/CE. Es un órgano consultivo europeo independiente en materia de protección de datos y derecho a la intimidad. Sus cometidos se describen en el artículo 30 de la Directiva 95/46/CE y en el artículo 15 de la Directiva 2002/58/CE.

> "(…) propiedades biológicas, características fisiológicas, rasgos de la personalidad o tics, que son, al mismo tiempo, atribuibles a una sola persona y mensurables, incluso si los modelos utilizados en la práctica para medirlos técnicamente implican un cierto grado de probabilidad" (2007, pág. 9).

Por su parte, el artículo 9.1. del RGPDP que regula el tratamiento de categorías especiales de datos personales señala que "quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física". De lo anterior, podría desprenderse que, los datos biométricos sólo constituirían una categoría especial de datos solamente en caso se sometan a un tratamiento técnico específico dirigido a identificar de manera unívoca a la persona.

La Agencia Española de Protección de Datos (en adelante, AEPDP), a través de un reciente pronunciamiento analizó si el tratamiento de datos biométricos incluye además de la identificación (artículo 4.14 y 9.1 del RGPDP) la verificación/autenticación (2020). Para ello, la AEPDP se remitió al Dictamen 3/2012 del Grupo del Artículo 29, que realiza la siguiente distinción entre identificación y verificación/autenticación biométrica:

> "Identificación biométrica: la identificación de un individuo por un sistema biométrico es normalmente el proceso de comparar sus datos biométricos (adquiridos en el momento de la identificación) con una serie de plantillas biométricas almacenadas en una base de datos (es decir, un proceso de búsqueda de correspondencias uno-a-varios).
>
> Verificación/autenticación biométrica: la verificación de un individuo por un sistema biométrico es normalmente el proceso de comparación entre sus datos biométricos (adquiridos en el momento de la verificación) con una única plantilla

> biométrica almacenada en un dispositivo (es decir, un proceso de búsqueda de correspondencias uno a-uno)" (2012, pág. 6).

Atendiendo a lo anterior, la AEPDP determinó que, puede interpretarse que de acuerdo con el artículo 4 del RGPD, el concepto de dato biométrico incluiría a ambos supuestos, tanto la identificación como la verificación/autenticación. De modo que, la AEPDP adopta una interpretación más favorable a los derechos de las personas, en tanto no haya un pronunciamiento al respecto por parte del Comité Europeo de Protección de Datos.

Ahora bien, el desarrollo acelerado de la tecnología también incentivó el diseño de diversos sistemas biométricos, que puede definirse del siguiente modo:

> "(…) aplicaciones de las tecnologías biométricas que permiten la identificación automática, y/o la autenticación/comprobación de una persona. Se suelen utilizar aplicaciones de autenticación/comprobación para diversas tareas en campos muy distintos y bajo la responsabilidad de una amplia gama de entidades diferentes" (2003, pág. 3).

De acuerdo al Dictamen 3/2012 del Grupo del Artículo 29, el tratamiento de datos biométricos a través de un sistema biométrico suele constar de tres procesos: registro, almacenamiento y correspondencia. En primer lugar, el registro abarca todos los procesos para extraer datos biométricos de una fuente biométrica y vincular estos datos a un individuo. En esta primera fase se requiere normalmente el contacto del individuo con un sistema biométrico -mediando o no su consentimiento- por ejemplo, sistemas de recojo de huellas dactilares o sistemas de circuito cerrado de televisión con funcionalidad de reconocimiento facial (2012, pág. 5).

En segundo lugar, los datos obtenidos pueden almacenarse en el lugar de registro (por ejemplo, un lector) o una tarjeta inteligente. Finalmente, la correspondencia implica el proceso de comparación de los datos o plantillas biométricas (capturados durante el registro) con los datos o plantillas biométricas recogidos en una nueva muestra a efectos de identificación, verificación y autenticación o categorización (2012, pág. 5).

Asimismo, de acuerdo al Documento de trabajo sobre biometría, se pueden distinguir dos categorías principales de principales de técnicas biométricas, en función de que se utilicen datos estables o datos dinámicos sobre el comportamiento, como se observa a continuación:

> "En primer lugar, existen técnicas basadas en aspectos físicos y fisiológicos que miden las características fisiológicas de una persona e incluyen: comprobación de las huellas digitales, análisis de la imagen del dedo, reconocimiento del iris, análisis de la retina, reconocimiento facial, resultados de muestras de las manos, reconocimiento de la forma de la oreja, detección del olor corporal, reconocimiento de la voz, análisis de muestras del ADN7 y análisis de los poros de la piel, etc. En segundo lugar, existen técnicas basadas en aspectos comportamentales, que miden el comportamiento de una persona e incluyen la comprobación de la firma manuscrita, el análisis de la pulsación sobre las teclas, el análisis de la forma de caminar, etc" (2003, págs. 3-4).

Algunos sistemas biométricos más usados son los sistemas de reconocimiento de huellas dactilares, reconocimiento del iris, sistemas de búsqueda de imágenes, entre otros, los cuales han ido mejorando significativamente a través del uso de tecnologías interdisciplinarias, conformando "sistemas biométricos interdisciplinarios" que usan diversos métodos como el método de patrones binarios locales -*Feature Local Binary Patterns (FLBP)*- o el método para el reconocimiento del color de la rostro -*Gabor-DCT Features (GDF)*, entre otros (Chengjun Liu, 2012).

Tomando en cuenta que, la fuente de los datos biométricos es el propio individuo y se requiere necesariamente de un procedimiento técnico para su recopilación y tratamiento, la utilización de tecnología biométrica conlleva el riesgo de que puedan revelarse datos sensibles de la persona.

En atención a ello, es posible afirmar que la definición de dato sensible contenida en el citado numeral 5 del artículo 2 de la LPDP no es precisa pues, ningún dato biométrico puede identificar *per se* a una persona, por el contrario, es imprescindible el uso de sistemas biométricos para el tratamiento de datos biométricos.

Esta definición puede llevar a equívocos y falta de tutela del derecho a la protección de datos personales por parte de la ANPDP, como es el caso de la Resolución N° 193-2019-JUS/DGTAIPD-DPDP (2019), procedimiento administrativo sancionador en contra de Sentinel Perú S.A. por recopilar y difundir la fotografía y fecha de nacimiento en sus reportes de crédito, donde la ANPDP no consideró que la fotografía es un medio que puede contener datos sensibles constituidos por datos sensibles como el origen racial o étnico y que para la recopilación de dichos datos debía mediar el consentimiento del titular, pues su tratamiento no se hallaba en alguna excepción al consentimiento prevista en el artículo 14 de la LPDP.

III. Tratamiento de datos personales sensibles y Covid-19

Como consecuencia de la pandemia ocasionada por el Coronavirus SARS-CoV-2 que causa el Covid-19, se ha implementado diversos mecanismos para evitar la propagación del virus y monitorear los síntomas de la enfermedad, para ello, se ha recurrido al tratamiento de diversos datos personales y datos sensibles a través de diversos aplicativos, redes sociales y sistemas biométricos. En el presente apartado examinaremos dos de ellos, a la luz de la normativa peruana de protección de datos personales y la normativa comparada.

III.1. Sistemas de geolocalización

El diccionario de la Real Academia Española no incluye la palabra “geolocalización” que está compuesta por el prefijo “geo” que significa perteneciente o relativo a la tierra y la palabra “localizar” como el lugar en que se halla alguien o algo (Real Academia Española , 2020), por lo que, geolocalización hace referencia a la ubicación o localización geográfica de algo o alguien.

Esta técnica consiste en que los operadores de telefonía móvil proporcionen información anonimizada de la ubicación de sus usuarios en las celdas de telefonía que definen sus antenas. Las operadoras recogen habitualmente datos de posición de sus abonados, que calculan en función de la fuerza con que les llegan las señales de cada móvil a las distintas antenas de una zona. Con esta información, que es necesaria para prestar el servicio, una

operadora es capaz de estimar qué números de teléfono hay en cada celda en un determinado momento, e incluso dar una ubicación aproximada de cualquier teléfono móvil activo en una celda (Agencia Española de Protección de Datos, 2020, pág. 4).

En el país contamos con una norma que regula el uso de los datos derivados de las telecomunicaciones para la identificación, localización y geolocalización de equipos de comunicación, en la lucha contra la delincuencia y el crimen organizado, decreto legislativo N° 1182 (2015), mediante la cual se regula -entre otros- la responsabilidad administrativa, civil o penal por parte de los concesionarios públicos de telecomunicaciones o en las entidades públicas relacionadas con estos servicios, así como los que participan en el proceso de acceso a los datos de localización y geolocalización ante la vulneración de la obligación de guardar reserva de dichos datos.

En Europa, durante la gestión del Covid-19, la Comisión Europea ha solicitado a las operadoras proporcionar este tipo de información anonimizada para ver los movimientos de la población (Agencia Española de Protección de Datos, 2020, pág. 4).

Por otro lado, geolocalización de los móviles a partir de los datos de redes sociales, opera a partir de las direcciones IP desde las que se accede a Internet y que pueden ser conocidas por los administradores de las páginas web. Algunos grandes proveedores como Facebook[3] o Google[4] han publicado recientemente los datos agregados en forma de grandes cuadros de mando (Agencia Española de Protección de Datos, 2020, pág. 5).

Al respecto, las Directrices 04/2020 sobre el uso de datos de localización y herramientas de rastreo de contactos en el contexto de la pandemia de Covid-19 precisó que "el seguimiento sistemático y masivo de la localización o los contactos de las personas físicas es una grave injerencia en su privacidad. Esta práctica solo puede legitimarse sobre la base de su adopción voluntaria por parte de los usuarios para cada uno de los fines respectivos, lo que implica, entre otras cosas, que las personas que decidan no utilizar esas aplicaciones, o no sepan

[3] Recuperado el 28 de noviembre de 2020 de https://dataforgood.facebook.com/covid-survey/?date=2020-11-25&dates=2020-09-26_2020-11-21&region=WORLD

[4] Recuperado el 28 de noviembre de 2020 de https://news.google.com/covid19/map?hl=es-419&gl=PE&ceid=PE%3Aes-419

hacerlo, no deben sufrir ninguna desventaja" (Comité Europeo de Protección de Datos, 2020, pág. 8).

III.2. Cámaras para lecturas de temperatura

Recientemente, las cámaras de videovigilancia con reconocimiento facial han añadido la capacidad de tomar la temperatura a los individuos que cruzan un área, sin requerir en muchos casos ninguna acción por su parte. Dichas cámaras identifican mediante algoritmos de inteligencia artificial los rostros humanos, los discriminan del resto de elementos que aparecen en la imagen y revelan la temperatura corporal aproximada de cada individuo. (Agencia Española de Protección de Datos, 2020, pág. 11). Al respecto, la AEPDP señaló lo siguiente:

> "Este tratamiento de toma de temperatura supone una injerencia particularmente intensa en los derechos de los afectados. Por una parte, porque afecta a datos relativos a la salud de las personas, no sólo porque el valor de la temperatura corporal es un dato de salud en sí mismo sino también porque, a partir de él, se asume que una persona padece o no una concreta enfermedad, como es en estos casos la infección por coronavirus.
>
> Por otro lado, los controles de temperatura se van a llevar a cabo con frecuencia en espacios públicos, de forma que una eventual denegación de acceso a un centro educativo, laboral o comercial estaría desvelando a terceros que no tienen ninguna justificación para conocerlo que la persona afectada tiene una temperatura por encima de lo que se considere no relevante y, sobre todo, que puede haber sido contagiada por el virus" (Agencia Española de Protección de Datos, 2020).

En el país, se ha generalizado el uso de termómetros por parte de entidad públicas o privadas para controlar la temperatura de manera previa al ingreso de las personas a un lugar. Por ello, la Dirección de Metrología del Instituto Nacional de Calidad elaboró una Guía para la selección y uso de termómetros de radiación infrarroja para la piel humana (medición de

temperatura sin contacto) (2020). Dicha guía deberá observarse al momento de elegir un termómetro a efectos medir la temperatura corporal de una persona.

Ahora bien, en la medida que se usen sistemas de videovigilancia que incorpore la capacidad de tomar la temperatura corporal de una persona, no debe dejar de observarse la Directiva de tratamiento de datos personales mediante sistemas de videovigilancia expedida por la ANPDP (2020).

IV. Aplicación de los principios de consentimiento, proporcionalidad y finalidad para el tratamiento de datos sensibles

El contenido del derecho a la autodeterminación informativa o protección de datos es delimitado a partir de sus principios rectores. La doctrina precisa que estos principios pueden reconducirse a los siguientes: consentimiento, información, finalidad, calidad de datos, proporcionalidad y seguridad. Estos principios alcanzan pleno significado desde el reconocimiento de que el derecho fundamental a la protección de datos se fundamenta en el poder de disposición de los datos personales por su titular, y en que tales datos son sometidos a tratamiento deben contar con la autorización del interesado, (Murillo de la Cueva & Piñar Mañas, 2009, págs. 101-102).

En primer lugar, el principio de consentimiento se encuentra recogido en el artículo 5 y el numeral 13.5. del artículo 13 de la LPDP que disponen que "para el tratamiento de los datos personales debe mediar el consentimiento de su titular" y que "los datos personales solo pueden ser objeto de tratamiento con consentimiento de su titular, salvo ley autoritativa al respecto. El consentimiento debe ser previo, informado, expreso e inequívoco", respectivamente.

El artículo 12 del Reglamento de la LPDP señala que las características del consentimiento son: i) libre, sin que medie error, mala fe, violencia o dolo que puedan afectar la manifestación de voluntad del titular de los datos personales; ii) previo, con anterioridad a la recopilación de los datos o en su caso, anterior al tratamiento distinto a aquel por el cual ya se recopilaron; iii) expreso e inequívoco, manifestado en condiciones que no admitan dudas

de su otorgamiento; e iv) informado, cuando se le informa sobre la identidad del titular de banco de datos; la finalidad, el banco de datos donde se almacenará, las consecuencias de proporcionar sus datos personales y de su negativa a hacerlo, entre otros.

Este principio se erige como "el pilar básico sobre el que gira toda la normativa de protección de datos de carácter personal. Todo tratamiento de este tipo de datos requiere, pues, el consentimiento inequívoco del afectado y, supone la expresión del derecho a la autodeterminación informativa" (Santamaría Ramos, 2012, pág. 6).

En segundo lugar, el principio de finalidad, se encuentra recogido en el artículo 6 de la LPDP que señala que "los datos personales deben ser recopilados para una finalidad determinada, explícita y lícita. El tratamiento de los datos personales no debe extenderse a otra finalidad que no haya sido la establecida de manera inequívoca como tal al momento de su recopilación, (...)". Asimismo, el artículo 8 del Reglamento de la LPDP establece que "una finalidad está determinada cuando haya sido expresada con claridad, sin lugar a confusión y cuando de manera objetiva se especifica el objeto que tendrá el tratamiento de los datos personales".

Zegarra afirma que, en la normativa peruana de protección de datos personales, como sistema formalista y de gestión, está prevista la obligación de inscribir los bancos de datos personales ante la autoridad administrativa. Así, los titulares de los bancos de datos personales están obligados a presentar al registro la denominación y ubicación del banco de datos, indicar la finalidad y los usos que le darán a los mismos (Zegarra Valdivia, 2019, pág. 184).

Asimismo, la doctrina apunta que "es esencial que la finalidad para la que el tratamiento de datos esté previsto sea una finalidad precisa y legítima, y que los datos recabados sean utilizados exclusivamente para esa finalidad y no para otra diferente" (Murillo de la Cueva & Piñar Mañas, 2009, pág. 157). En la misma línea Blasi señala que "el principio de limitación de finalidad consiste en recoger datos personales para finalidades específicas, explícitas y legitimadas, que no pueden ser tratados de manera incompatible con la finalidad original" (2015, pág. 144).

Finalmente, el principio de proporcionalidad se encuentra recogido en el artículo 7 de la LPDP que establece que "todo tratamiento de datos personales debe ser adecuado, relevante y no excesivo a la finalidad para la que éstos hubiesen sido recopilados".

Remolina-Angarita apunta que, este principio implica que la información recogida debe ser aquella estrictamente necesaria para el cumplimiento de los fines de la base de datos, estando prohibido el registro y divulgación de datos que no guarden relación con el objetivo de la base de datos (2013, pág. 70). Asimismo, la doctrina señala que "conforme al principio de proporcionalidad, siempre que resulte posible, deben preferirse otros medios menos agresivos para las personas a fin de prevenir interferencias injustificadas en los derechos y libertades fundamentales" (Murillo de la Cueva & Piñar Mañas, 2009, pág. 62).

En suma, el contenido del derecho a la protección de datos personales se configura a partir de sus principios rectores, entre ellos, el principio de consentimiento, finalidad y proporcionalidad. Por tanto, a fin de analizar si un determinado tratamiento es contrario a la normativa de protección de datos personales se deberá recurrir a analizar si facticiamente se observa los referidos principios rectores.

A fin de analizar los sistemas de tratamiento de datos personales sensibles señalados en el apartado anterior, se inexorable acudir a los principios rectores en materia de protección de datos. En este punto es preciso señalar que, como regla, para el tratamiento de datos personales relativos a la salud de las personas debe mediar consentimiento previo, informado, expreso e inequívoco (por escrito) por parte del titular de los mismos, de conformidad con lo establecido en los numerales 13.5 y 13.6 del artículo 13 de la LPDP.

Sin embargo, una excepción a dicha regla, es cuando el tratamiento ocurre en los siguientes supuestos: i) en circunstancia de riesgo para la prevención, diagnóstico y tratamiento médico del titular efectuado en establecimientos de salud y por profesionales en ciencias de la salud; o ii) cuando medien razones de interés público previstas por ley; o de salud pública, calificadas como tales por el Ministerio de Salud; o, iii) para la realización de estudios epidemiológicos o análogos, en tanto se apliquen procedimientos de disociación adecuados.

En consecuencia, solo el personal de salud que trabaja en hospitales, clínicas y postas médicas puede realizar tratamiento de datos personales sin solicitar el consentimiento del titular, siempre que este tratamiento tenga la finalidad de prevenir, diagnosticar y brindar tratamiento de las personas con Covid-19. (Macutela Lavilla, 2020).

La Emergencia Sanitaria no justifica el tratamiento indiscriminado de datos personales relacionados a la salud de las personas, en particular, de las personas con Covid-19. Las autoridades de salud no requieren solicitar el consentimiento de los pacientes con dicha enfermedad pues el tratamiento de sus datos personales se realiza al amparo de una excepción prevista en la normativa de datos personales; sin embargo, deben cumplir con adoptar las de seguridad suficientes y adecuadas para impedir que terceros accedan y difundan estos datos personales (Macutela Lavilla, 2020).

Por tanto, el hecho que los aplicativos de geolocalización o las cámaras para lecturas de temperatura y otras medidas adoptadas para la prevención y control del Covid-19 deben observar los principios de finalidad y proporcionalidad, debiendo guiar su uso para dos fines específicos, según las Directrices 04/2020 sobre el uso de datos de geolocalización y herramientas de rastreo de contactos en el contexto de la pandemia de Covid-19:

> "- el uso de datos de localización para apoyar la respuesta a la pandemia mediante la modelización de la propagación del virus, a fin de evaluar la eficacia global de las medidas de confinamiento.
> - el rastreo de contactos, cuyo objetivo es que las personas que hayan estado muy cerca de alguien que resulte ser un portador confirmado del virus sean informadas al respecto, a fin de romper las cadenas de transmisión lo antes posible". (Comité Europeo de Protección de Datos, 2020, págs. 4-5).

En cumplimiento del principio de proporcionalidad, el dato de la geolocalización de una persona deberá eliminarse una vez que se cumpla la finalidad para la cual se recopiló, toda vez que, este dato ya no sería necesario o pertinente para prevenir la propagación del Covid-19 o monitorear los síntomas de un paciente, cuando la Emergencia Sanitaria haya finalizado o cuando el paciente se ha recuperado.

Por otro lado, los datos obtenidos de proveedores de servicios de comunicaciones electrónicas se pueden transmitir a las autoridades o a terceros siempre y cuando medie un proceso de anonimización o disociación. El primero, es un procedimiento reversible que impide la identificación o que no hace identificable al titular; mientras que el segundo, es un procedimiento irreversible que impide la identificación o no hace identificable al titular, de acuerdo a lo establecido en los numerales 14 y 15 del artículo 2 de la LPDP, respectivamente.

La evaluación de la consistencia de la anonimización depende de tres criterios: i) singularización (identificación de una persona dentro de un grupo mayor sobre la base de los datos); ii) vinculación (vinculación de dos registros de datos sobre la misma persona); y iii) inferencia (deducción, con una probabilidad significativa, de información desconocida sobre una persona) (Comité Europeo de Protección de Datos, 2020, pág. 7).

En suma, el tratamiento de datos sensibles en el contexto ocasionado por el Covid-19 no debe dejar de observar el contenido del derecho a la protección de datos personales, es decir, los principios recogidos en la LPDP, en particular, el principio de finalidad y proporcionalidad.

IV. Medidas legales, técnicas y organizativas para el tratamiento de datos sensibles

En atención a lo señalado previamente, el tratamiento de datos sensibles por parte de entidades públicas y privadas debe observar las medidas legales, técnicas y organizativas establecidas en la Directiva de Seguridad de la ANPDP (2013), la cual orienta sobre las condiciones y medidas técnicas que deben tomar en cuenta para el cumplimiento de la LPDP y su Reglamento.

De manera que, corresponde observar las medidas legales técnicas y organizativas correspondientes a los bancos de datos que tengan la clasificación en alguna de las siguientes categorías señaladas en la referida Directiva: intermedio, complejo o crítico.

Finalmente, del análisis de los aportes de la ANPDP para la tutela de los datos sensibles se advierte que únicamente ha expedido una opinión consultiva relacionada tratamiento de

datos de salud durante la pandemia en el ámbito laboral (2020). A diferencia del rol activo y protagónico de la AEPDP en la protección de datos personales en el contexto de la Emergencia Sanitaria, la ANPDP tiene un rol pasivo en cuanto la tutela del derecho a la protección de datos personales pues aún cuando goza de potestad normativa, no ha expedido lineamientos o directrices para el tratamiento de datos personales sensibles, en particular, datos relativos a la salud de las personas, en el contexto de la pandemia de Covid-19.

V. Conclusiones

En primer lugar, la LPCP no contiene una definición acertada de datos biométricos como datos sensibles, lo cual puede llevar a equívocos y falta de tutela por parte de la ANPDP.

En segundo lugar, los datos relativos a salud de las personas son datos sensibles, cuyo tratamiento de encuentra exceptuado del consentimiento cuando tiene como finalidad la prevención, diagnóstico y tratamiento de una enfermedad como el Covid-19 o razones interés público o salud pública, no obstante, ello no implica que no se observen los demás principios recogidos en la LPDP y adoptar medidas legales, técnicas y organizativas establecidas en la Directiva de Seguridad expedida por la ANPDP.

Finalmente, los aportes de la ANPDP no representan un avance significativo para la protección de datos sensibles en el país.

VI. Bibliografía

Agencia Española de Protección de Datos. (30 de abril de 2020). Comunicado de la AEPD en relación con la toma de temperatura por parte de comercios, centros de trabajo y otros establecimientos. Recuperado el 15 de noviembre de 2020, de https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/comunicado-aepd-temperatura-establecimientos

Agencia Española de Protección de Datos. (mayo de 2020). Uso de las tecnologías en la lucha contra el Covid-19. Un análisis de costes y beneficios. Recuperado el 15 de noviembre de 2020, de https://www.aepd.es/sites/default/files/2020-05/analisis-

tecnologias-COVID19.pdf

Autoridad Nacional de Protección de Datos Personal. (noviembre de 2013). *Directiva de Seguridad.* Recuperado el 10 de octubre de 2020, de https://www.minjus.gob.pe/wp-content/uploads/2014/02/Cartilla-de-Directiva-de-Seguridad.pdf

Autoridad Nacional de Protección de Datos Personal. (enero de 2020). Directiva de tratamiento de datos personales mediante sistemas de videovigilancia, Directiva N° 01-2020-JUS/DGTAIPD. Recuperado el 29 de noviembre de 2020, de https://www.minjus.gob.pe/wp-content/uploads/2020/01/Directiva-N%C2%B0-01-2020-DGTAIPD-1.pdf

Blasi Casagran, C. (2015). Límites al derecho europeo de protección de ddatos en el control de fronteras de la UE. *Revista CIDOB d'Afers Internacionals*, 127-151. Recuperado el 10 de octubre de 2020, de http://search.ebscohost.com.ezproxybib.pucp.edu.pe:2048/login.aspx?direct=true&db=edsjsr&AN=edsjsr.43694844&lang=es&site=eds-live&scope=site

Boris A, L., Chiara, S., Mora, M., & Muñoz-Quezada, M. T. (1 de january de 2020). Aspectos éticos del uso de identificadores biométricos. *Acta Bioéthica*, 43-50. doi:https://doi-org.ezproxybib.pucp.edu.pe/10.4067/s1726-569x2020000100043

Chengjun Liu, V. K. (2012). *Cross disciplinary biometric systems.* Berlin: Springer Berlin Heidelberg. Recuperado el 12 de noviembre de 2020, de https://link-springer-com.ezproxybib.pucp.edu.pe/book/10.1007%2F978-3-642-28457-1

Comité Europeo de Protección de Datos. (21 de abril de 2020). Directrices 04/2020 sobre el uso de datos de localización y herramientas de rastreo de contactos en el contexto de la pandemia de COVID 19. Recuperado el 16 de noviembre de 2020, de https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_es.pdf

Congreso de la República del Perú. (02 de julio de 2011). Ley de Protección de Datos Personales, ley 29733. *Diario Oficial El Peruano*.

Congreso de la República del Perú. (21 de marzo de 2013). Reglamento de la Ley N°29733, Ley de protección de datos personales. *Diario Oficial El Peruano*.

Congreso de la República del Perú. (26 de julio de 2015). Decreto Legislativo que regula el uso de los datos derivados de las telecomunicaciones para la identificación, localización y geolocalización de equipos de comunicación, en la lucha contra la

delincuencia y el crimen organizado,Decreto Legislativo N° 1182. *Diario Oficial El Peruano*.

Constitución Política del Perú. (1993).

Cristea Uivaru, L. (2018). *La protección de datos de carácter sensible: historia clínica digital y big data en salud.* Barcelona: Bosch Editor. Recuperado el 20 de octubre de 2020, de https://books.google.com.pe/books?id=KDi3DwAAQBAJ&pg=PA189&lpg=PA189&dq=tc+%2B+dato+sensible&source=bl&ots=fwKF9rivsT&sig=ACfU3U0btFnsWK8qjUKAe95ROPuk6HRDIw&hl=es-419&sa=X&ved=2ahUKEwiSo92By6bqAhXSmOAKHfLPAtQ4ChDoATAAegQIChAB#v=onepage&q&f=false

Fraden, J. (2004). *Handbook of Modern Sensors: Physics, Designs, and Applications.* New York, USA: Springer Science & Business Media.

Grupo de Trabajo del Artículo 29. (1 de agosto de 2003). Documento de trabajo sobre biometría. Recuperado el 25 de octubre de 2020, de https://www.apda.ad/sites/default/files/2018-10/wp80_es.pdf

Grupo de Trabajo del Artículo 29. (20 de junio de 2007). Dictamen 4/2007 sobre el concepto de datos personales. Recuperado el 14 de octubre de 2020, de https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_es.pdf

Grupo de Trabajo del Artículo 29. (12 de abril de 2012). Dictamen 3/2012 sobre la evolución de tecnologías biométricas. Recuperado el 13 de octubre de 2020, de https://www.aepd.es/sites/default/files/2019-12/wp193_es.pdf

Herrán Ortiz, A. I. (1988). *La violación a la intimidad en la protección de datos personales.* Madrid: Dykinson.

Instituto Nacional de Calidad (INACAL). (mayo de 2020). Guia para la selección y uso de termómetros de radiación infrarroja para piel humana (medición de temperatura sin contacto). Recuperado el 01 de diciembre de 2020, de https://www.inacal.gob.pe/repositorioaps/data/1/1/2/jer/filehide/files/guia_termometro.pdf

Macutela Lavilla, N. (26 de mayo de 2020). Tratamiento de datos personales de pacientes con Covid-19. *Ius 360°*. Recuperado el 20 de noviembre de 2020, de

https://ius360.com/gideproc/tratamiento-de-datos-personales-de-pacientes-con-covid-19/#:~:text=Solo%20el%20personal%20de%20salud,las%20personas%20con%20COVID%2D19.

Murillo de la Cueva, P. L., & Piñar Mañas, J. L. (2009). *El derecho a la autodeterminación informativa.* Madrid: Fundación Coloquio Jurídico Europeo. Recuperado el 12 de octubre de 2020, de http://www.fcjuridicoeuropeo.org/wp-content/uploads/file/Libros_Publicados/Cuadernos_Fundacion/EL%20DERECHO%20A%20LA%20AUTODETERMINACION%20INFORMATIVA.pdf

Parlamento Europeo y Consejo de la Unión Europea. (27 de abril de 2016). Reglamento (UE) 2016/679. *Diario Oficial de la Unión Europea*. Obtenido de https://gdprinfo.eu/es

Real Academia Española . (25 de noviembre de 2020). Obtenido de https://dle.rae.es/localizar?m=form

Remolina-Angarita, N. (2013). *Tratamiento de datos personales: aproximación internacional y comentarios a la Ley 15181 de 2012.* Lima: Legis.

Santamaría Ramos, F. J. (2012). Principios básicos: calidad y consentimiento (I). *MK - Marketing más Ventas*. Recuperado el 17 de octubre de 2020, de http://web.a.ebscohost.com.ezproxybib.pucp.edu.pe:2048/ehost/detail/detail?vid=0&sid=65b8f039-178f-4606-9fc9-25907e79f4c5%40sessionmgr4006&bdata=Jmxhbmc9ZXMmc2l0ZT1laG9zdC1saXZl#AN=73812618&db=fua

Zegarra Valdivia, D. (2019). La normativa peruana de protección de datos personales frente al reto de pasar de un modelo de gestión de datos al uso responsable de la información. En D. Zegarra Valdivia, *La proyección del Derecho Administrativo Peruano Estudios por el Centenario de la Facultad de Derecho de la PUCP* (págs. 165-208). Lima: Palestra Editores.

Expediente N° 06164-2007-PHD/TC (Tribunal Constitucional 21 de diciembre de 2007). Recuperado el 15 de octubre de 2020, de http://justiciaytransparencia.pe/sentencias/des_buscador.php?ULTIMA_SECCION=252&SECCION_ID=252&ELEMENT_ID=774&BUSQUEDA=6164&ETIQUETAS=

Oficio N°213-2017-JUS/DGTAIPD (Dirección General de Transparencia, Acceso a la

Información Pública y Protección de Datos Personales del Ministerio de Justicia y Derechos Humanos 10 de octubre de 2017). Recuperado el 15 de octubre de 2020, de https://www.minjus.gob.pe/wp-content/uploads/2018/01/OFICIO-N%C2%B0-213-2017.pdf

Resolución Directoral N° 193-2019-JUS/DGTAIPD-DPDP (Autoridad Nacional de Protección de Datos Personales 22 de enero de 2019). Recuperado el 15 de noviembre de 2020, de https://cdn.www.gob.pe/uploads/document/file/1378486/RD-193-2019.pdf.pdf

N/REF: 0036/2020 (Agencia Española de Protección de Datos 8 de mayo de 2020). Recuperado el 2 de noviembre de 2020, de https://www.aepd.es/es/documento/2020-0036.pdf

Opinión Consultiva N° 32-2020-JUS/DGTAIPD (Autoridad Nacional de Protección de Datos 05 de mayo de 2020). Recuperado el 28 de noviembre de 2020, de https://www.minjus.gob.pe/wp-content/uploads/2020/05/OC-32.pdf