EL USO DE HERRAMIENTAS TECNOLÓGICAS EN LA LUCHA CONTRA EL COVID–19 Y SUS IMPLICANCIAS EN EL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS PERSONALES: UNA APROXIMACIÓN

THE USE OF TECHNOLOGICAL TOOLS IN THE FIGHT AGAINST COVID–19 AND ITS IMPLICATIONS ON THE FUNDAMENTAL RIGHT TO THE PROTECTION OF PERSONAL DATA: AN APPROXIMATION

DIEGO ZEGARRA VALDIVIA[1]

RESUMEN

El presente trabajo analiza algunos de los supuestos en que el uso variado de tecnologías para hacer frente a la propagación de la pandemia del COVID-19 y proteger la salud de las personas ha impactado en el derecho fundamental a la protección de datos personales; para ello, parte de la premisa de que la utilización de estas tecnologías no puede significar una afectación al referido derecho fundamental ni mucho menos un tratamiento indiscriminado de dichos datos sin control mínimo alguno.

PALABRAS CLAVE

Derecho Fundamental | Protección de datos personales | Pandemia | COVID-19 | Consentimiento | Salud Pública | Tecnología

ABSTRACT

This paper analyzes some of the cases in which the varied use of technologies to cope with the spread of the COVID-19 pandemic and protect people's health has impacted on the fundamental right to the protection of personal data; to this end, it starts from the premise that the use of these technologies cannot affect that fundamental right, much less an indiscriminate processing of said data without any minimum control.

KEYWORDS

Fundamental Right | Protection of personal data | Pandemic | COVID-19 | Consent | Public Health | Technology

CONTENIDO

1 Profesor Principal de Derecho Administrativo. Doctor en Derecho por la Universidad de Alicante, Master en Derecho de las Telecomunicaciones y de las Tecnologías de la Información por la Universidad Carlos III de Madrid, Director de la Maestría en Derecho Administrativo y del Programa de Segunda Especialidad en Derecho Administrativo en la Pontificia Universidad Católica del Perú. Jefe de la Oficia Académica de Internacionalización y Coordinador del Área de Derecho Administrativo en la Facultad de Derecho en la Pontificia Universidad Católica del Perú.

La presente investigación se enmarca dentro de las actividades de la Línea de Investigación de Protección de Datos Personales y Transparencia del Grupo de Investigación en Derecho Administrativo GIDA y su elaboración contó con la colaboración de Camila Chinchay, Ángela Casafranca, Christian Hernández, Alexandra Olivera, Piero Curi y Camila Atencio.

implementado herramientas tecnológicas: identificación de algunos riesgos y de posibles afectaciones al derecho fundamental a la protección de datos personales. **4.** A modo de conclusión.

SOBRE EL ARTÍCULO

El presente artículo fue recibido por la Comisión de Publicaciones el 8 de agosto de 2021 y aprobado para su publicación el 27 de octubre de 2021.

1. INTRODUCCIÓN

La pandemia del COVID-19 ha generado que en casi todos los países a nivel mundial adopten, de forma progresiva, diversos tipos de medidas con la finalidad de contener su propagación, proteger la salud pública y la vida de las personas (Gómez-Córdoba et al., 2020, p. 273). Entre dichas medidas, se identifican el aislamiento social obligatorio, el distanciamiento social, el control del aforo, el uso de herramientas tecnológicas para el procesamiento de datos y mitigación de contagios, el establecimiento de canales informativos sobre el COVID-19, la geolocalización de contagiados, los estudios de movilidad, rastreo y registro de contactos, control y medición de la temperatura corporal, entre otros.

Todas estas acciones de una u otra forma han limitado derechos y libertades fundamentales como la privacidad, la protección de datos personales, la libre circulación, la libertad de expresión, la libertad de reunión, entre otros derechos. De los mencionados, importa para los efectos del presente trabajo el derecho fundamental a la protección de datos personales, debido al tipo de información recogida y requerida para la implementación de los sistemas de vigilancia epidemiológica y de control de la propagación de la enfermedad (Gómez-Córdoba et al., 2020, p. 273).

En efecto, las medidas para mitigar el COVID-19 implican necesariamente el procesamiento de diferentes datos personales, con lo cual se debe garantizar un tratamiento adecuado y legal de los mismos. Si bien la gravedad de la actual crisis de salud permite el uso de poderes de emergencia en respuesta a amenazas importantes – como ha sido señalado por un grupo de expertos en derechos humanos de las Naciones Unidas el 16 de marzo de 2020 -, es indispensable que la respuesta a ser implementada por los Estados frente al COVID-19 sea proporcionada, necesaria y no discriminatoria (ONU, 2020).

Debe repararse entonces, que, en ninguna circunstancia, la declaración de emergencia sanitaria asumida globalmente por los países supone, ni expresa ni tácitamente la suspensión del derecho fundamental a la protección de datos personales, tan sólo implica adoptar determinadas medidas que traen consigo la limitación y no la suspensión en el ejercicio de derechos y libertades (Piñar, 2020). Sin embargo, como sostiene Arenas (2020), lo importante, es que las referidas limitaciones deben cumplir con una serie de requisitos y ofrecer una serie de garantías y responsabilidades en caso de incumplimiento: ser necesarias, apropiadas y proporcionales en una sociedad democrática (p. 10).

Cuestión distinta es que sea necesario adaptar este derecho fundamental para, conforme lo ha expresado la Agencia Española de Protección de Datos (en adelante, AEPD), "(…) permitir legítimamente los tratamientos de datos personales en situaciones, como la presente, en que existe emergencia sanitaria de alcance general" (2020, p.1). Esto último ha sido reiterado por el Comité Europeo de Protección de Datos Personales, al haber puesto énfasis en que el respeto a la privacidad de los individuos no constituye un escollo en la toma de decisiones que impliquen contener la pandemia actual, cuando se esté

hablando de datos sensibles como son los relativos a la salud de las personas (EDPB, 2020, p. 1).

En los meses en que lleva esta pandemia, han surgido voces para expresar si "la privacidad será una de las víctimas de la COVID-19" (Renda, 2020), se han acuñado expresiones como "a la muerte por protección de datos" (Martínez, 2020) o planteamientos respecto a si las concesiones y restricciones en materia de vigilancia, *tracing*, *traking* y seguridad de la ciudadanía pudieran llegar a ser permanentes (Calzada citado por Recuero Linares, 2020, p. 141), lo que hace manifiesta la incertidumbre respecto a las garantías que los ordenamientos jurídicos han establecido para el ejercicio de este derecho fundamental y de los derechos vinculados al mismo. Es por ello que autores como Andreu (2020) consideran problemática la aplicación de la normativa "en el uso de soluciones tecnológicas para la lucha contra la pandemia, lo que ha llevado a declaraciones restrictivas sobre su uso y a una gran confusión sobre su eficacia y seguridad" (p. 851).

En efecto, estas innovaciones han generado nuevas preocupaciones a nivel mundial sobre el uso inadecuado de determinados aplicativos que afectan el derecho fundamental a la protección de datos personales y la privacidad de los ciudadanos, lo que ha supuesto una tensión entre el derecho a la salud colectiva y los derechos individuales. Y es que, lamentablemente,

> Estas estrategias no siempre se contextualizan dentro de un régimen de protección de datos personales robusto, ni de instrumentos jurídicos que garanticen que en su desarrollo e implementación se protejan los derechos de las personas, se obtengan únicamente datos realmente necesarios, se evalúe el impacto en la salud humana que justifique las restricciones de libertades, o se garantice que la información obtenida no será empleada a largo plazo con otros fines estatales o privados (Gómez-Córdoba et al., 2020, pp. 274-275).

Es por estas consideraciones que el presente trabajo tiene como finalidad analizar que, si bien el contexto del COVID-19 requiere de medidas rápidas para hacer frente a su expansión y mitigar sus impactos, contando para ello con la tecnología como un medio idóneo y necesario para dicha finalidad accediendo a datos sensibles como la salud de las personas o datos personales y su geolocalización, existe una gran preocupación por el tratamiento y uso adecuado de estos datos personales recopilados en estas circunstancias debido a que el uso de estas tecnologías no puede significar una afectación del derecho fundamental a la protección de los datos personales ni mucho menos un tratamiento indiscriminado de dichos datos sin control mínimo alguno.

El tratamiento de datos personales en estas situaciones de emergencia sanitaria sigue realizándose de conformidad con la normativa de protección de datos personales, por lo que se aplican todos sus principios entre ellos el tratamiento de los datos personales con licitud, lealtad y transparencia, de limitación de la finalidad, principio de exactitud y minimización de datos (AEPD, 2020, pp. 6-7). Por ello, sin llegar al exceso alarmista de las citadas expresiones, bajo la premisa que los ordenamientos jurídicos legitiman los tratamientos de datos personales que sean imprescindibles para luchar contra la pandemia global del COVID-19, en el presente artículo se identifican los posibles riesgos y afectaciones al derecho fundamental a la protección de datos personales derivados de la implementación por parte de los Estados y los particulares de herramientas tecnológicas con motivo de controlar la propagación del virus, proteger la salud pública y la vida de las personas, y se formulan algunas reflexiones sobre el alcance de los mismos en la garantía del referido derecho fundamental.

2. LAS BASES DE LEGITIMACIÓN DEL TRATAMIENTO DE DATOS DE SALUD

La protección de datos personales es un derecho fundamental reconocido en diversos textos internacionales, en la legislación comparada, así como en el ordenamiento jurídico peruano. A nivel internacional, como señala Razquin, la protección de datos personales está prevista en:

> El art. 12 de la Declaración Universal de Derechos Humanos de 1948 y el art. 17 del Pacto Internacional de Derechos Civiles y Políticos de 1966, que se refieren a la protección de la vida privada y de la intimidad. También en el ámbito del Consejo de Europa, el art. 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales de 1950 establece el principio de protección de la intimidad; el Convenio nº 108 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal de 1981garantiza la protección de datos frente al tratamiento automatizado; y asimismo el Convenio del Consejo de Europa sobre el Acceso a los Documentos Públicos de 2009 recoge como uno de los límites del derecho de acceso a los documentos el de la protección de la intimidad (artículo 3.1.f). Los Tratados de la Unión Europea amparan asimismo la protección de los datos personales (art. 16 TFUE y art. 39 TUE). Y la Carta de los Derechos Fundamentales de la Unión Europea regula el derecho a la protección de datos de carácter personal (art. 8). (2019, p. 142).

Asimismo, a nivel europeo, en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (en adelante, RGPD), se encuentra regulado el tratamiento de los datos personales y la libre circulación de estos datos en una realidad asociada a la nueva sociedad digital, habiendo recogido para ello en su artículo 5 los principios básicos que deben regirlos, como son la licitud (cuyo alcance ha sido desarrollado en el artículo 6 del RGPD), lealtad y transparencia; limitación de la finalidad; minimización de datos; exactitud; limitación del plazo de conservación; e, integridad y confidencialidad.

Por su parte, en el ordenamiento jurídico peruano, el reconocimiento de la protección de datos personales como derecho fundamental ha sido recogida en el artículo 2, inciso 6 de la Constitución Política del Perú, al estipularse el derecho de toda persona a que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar.

El desarrollo normativo del citado precepto constitucional ha sido realizado en la Ley No. 29733 – Ley de Protección de Datos Personales (en adelante, LPDP), promulgada en el año 2011 y en plena vigencia desde el año 2013, y en su Reglamento aprobado por Decreto Supremo No. 003-2013-JUS (en adelante, RLPDP). A través de esta regulación se busca garantizar el derecho fundamental de los titulares de los datos personales, es decir, la capacidad de los mismos de controlar su tratamiento en el ámbito de Administración Pública como aquel que se da en el sector privado.

Durante esta pandemia es constante la recopilación y tratamiento de datos personales relativos a la salud, los mismos que son considerados como una categoría especial en la normativa de protección de datos personales cuya característica principal es el carácter sensible de mismos. Se trata de datos cuyo tratamiento puede suponer mayor riesgo de vulneración de los derechos y libertades del interesado y por ello son merecedores de

especial protección porque pueden afectar de manera significativa al individuo.

Los datos de salud consisten en aquellas informaciones "que se refieren a la salud pasada, presente o futura en personas sanas o enfermas, con enfermedades de carácter físico o psicológico, y que incluye la adicción al alcohol y a las drogas" (Cristea, 2018, p. 46). Los datos personales referidos a la salud, contienen, como señala Cristea, información de las personas que hace posible conocer las dolencias o enfermedades que han padecido, padecen o incluso podrán padecer (2018, p. 46). Solernou refiere además que el Grupo Europeo de Ética en la Ciencia y en las Nuevas Tecnologías considera que el dato personal de salud incluye la información relativa no sólo a las enfermedades, sino también a las intervenciones, medicamentos prescritos, diagnósticos, etc.; así como los datos administrativos sanitarios referidos al registro, y a las admisiones, a los seguros, etc. (2006, pp. 51-52).

> Se trata, en definitiva, de datos personales que forman parte de la esfera más íntima de la persona, que pueden estar revelando situaciones críticas relativas a determinadas enfermedades, a la aplicación de técnicas de reproducción asistida o relativa a información genética, cuyo potencial vulnerador de la intimidad personal nadie se atreve a poner en duda (Piñar, citado por Cristea, 2018, p. 46).

Es por el alcance que tiene la definición de los datos de salud que resulta indispensable analizar el marco de garantías de los principios de legalidad, consentimiento, finalidad, proporcionalidad, calidad, seguridad, disposición del recurso, y, nivel de protección adecuado, recogidos en la LPDP (Título I) y en el RLPDP (Título II) ya que delimitan el tratamiento de datos personales, tienen fuerza vinculante, aplicación práctica y definen si un tratamiento de datos se está o no realizando de manera leal, lícita, transparente y adecuada. No obstante, en la situación de emergencia sanitaria, los citados principios recogidos en la legislación peruana, al que es razonable sumarle - por su vinculación - los que han sido recogidos en el RGPD europeo, son de difícil cumplimiento para el tratamiento de datos de salud un entorno digital. Por ello,

> Existe una improrrogable necesidad de clarificar y precisar la aplicación de los principios de la protección de datos a las nuevas tecnologías, con el fin de garantizar una protección real y efectiva de los datos personales, cualquiera que sea la tecnología utilizada para tratar estos datos, y que los responsables del tratamiento de los datos tengan plena conciencia de las implicaciones de las nuevas tecnologías en la protección de datos personales (Cristea, 2018, p. 224).

Resulta entonces necesario identificar el alcance de los citados principios y los efectos derivados de la implementación de herramientas tecnológicas que involucran el tratamiento de datos de salud en el entendido de que se trata de una serie de reglas materiales concebidas para desarrollar y asegurar la consecución de los fines de la normativa de protección de datos personales.

2.1 EL CONSENTIMIENTO EN EL TRATAMIENTO DE DATOS DE SALUD

El principio de consentimiento implica que terceros podrán acceder a datos personales, siempre que exista consentimiento libre, expreso, inequívoco e informado por parte del titular. Este principio se encuentra recogido en el artículo 5[2] de la LPDP y los artículos 7, 11, 12 y 14 del RLPDP.

---

2 Ley N° 29733, Ley de Protección de Datos Personales
"Artículo 5. Principio de consentimiento

En concordancia con lo regulado en la LPDP, en el artículo 7[3] del RLPD, dispone que el consentimiento del interesado implica toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen. De esta forma, como sostiene Arias (2016. p. 122), el consentimiento tiene una forma propia de otorgarse:

- Mediante un acto afirmativo claro que refleja una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen. Puede ser una declaración por escrito, inclusive por medios electrónicos o una declaración verbal, si el consentimiento del interesado se ha de dar a raíz de una solicitud por medios electrónicos, la solicitud ha de ser clara, concisa y no perturbar y necesariamente el uso del servicio para el que se presta;

- Para todas las actividades de tratamientos realizados con el mismo o los mismos fines, es decir, cuando el tratamiento tenga varios fines, debe darse el consentimiento para cada uno de ellos;

- Mediante un medio que permita al responsable del tratamiento ser capaz de demostrar que aquel ha dado su consentimiento a la operación de tratamiento.

Asimismo, la LPDP ha previsto en el artículo 14[4] los supuestos en que es legítimo el tratamiento de los datos personales prescindiendo del consentimiento. Así, en el inciso 6 del citado artículo se dispone que no se requiere el consentimiento del titular de los datos personales, para los efectos de su tratamiento, *"cuando medien razones de interés público previstas por ley o cuando deban tratarse por razones de salud pública, ambas razones deben ser calificadas como tales por el Ministerio de Salud"*.

Para el tratamiento de los datos personales debe mediar el consentimiento de su titular".

3 Decreto Supremo No. 003-2013-JUS, Reglamento de la Ley 29733

"Artículo 7.- Principio de consentimiento.

En atención al principio de consentimiento, el tratamiento de los datos personales es lícito cuando el titular del dato personal hubiere prestado su consentimiento libre, previo, expreso, informado e inequívoco. No se admiten fórmulas de consentimiento en las que éste no sea expresado de forma directa, como aquellas en las que se requiere presumir, o asumir la existencia de una voluntad que no ha sido expresa. Incluso el consentimiento prestado con otras declaraciones, deberá manifestarse en forma expresa y clara".

4 Ley N° 29733, Ley de Protección de Datos Personales

"Artículo 14. Limitaciones al consentimiento para el tratamiento de datos personales

No se requiere el consentimiento del titular de datos personales, para los efectos de su tratamiento, en los siguientes casos:

(…)

6. Cuando se trate de datos personales relativos a la salud y sea necesario, en circunstancia de riesgo, para la prevención, diagnóstico y tratamiento médico o quirúrgico del titular, siempre que dicho tratamiento sea realizado en establecimientos de salud o por profesionales en ciencias de la salud, observando el secreto profesional; o cuando medien razones de interés público previstas por ley o cuando deban tratarse por razones de salud pública, ambas razones deben ser calificadas como tales por el Ministerio de Salud; o para la realización de estudios epidemiológicos o análogos, en tanto se apliquen procedimientos de disociación adecuados.

(…)".

El alcance de esta norma ha sido explicado en la Opinión Consultiva N° 07-2019-JUS/DGTAIPD-DPDP de la Autoridad Nacional de Protección de Datos Personales, según la cual, la excepción que regula el inciso 6 del artículo 14 de la Ley de Protección de Datos Personales *"refiere a situaciones específicas que implican una circunstancia de riesgo, como por ejemplo una epidemia, en la que se pone en peligro la vida o salud del titular del dato personal y de personas cercanas a él"* (2019). De esta forma, cuando medien razones de interés público o salud pública declaradas, como la Emergencia Sanitaria vigente en el Perú, se permite el tratamiento de datos personales sin que requiera para ello el consentimiento del titular de los datos personales con el objetivo de adoptar medidas de prevención frente a posibles contagios. Similar disposición ha sido prevista en el literal i del artículo 9[5] del RGPD europeo: *"sensitive data may be processed for reasons of public interest in the area of public health, such as protecting against threats to public health or ensuring medical device quality"* (Scheibner et al., 2020, p. 12).

Entonces, ante la necesidad de contar con información para el manejo adecuado de la pandemia, es admisible el tratamiento de datos personales de carácter general y aquellos que son relativos a la salud sin el consentimiento de los titulares. Sin embargo, este tratamiento debe ser justificado, necesario proporcional, razonable y eficaz como medida para contener la propagación, y se debe garantizar la seguridad en el tratamiento de los datos.

No debe perderse de vista además que es legitimo el tratamiento de datos de salud para la prevención o el diagnóstico médico, para la prestación de asistencia sanitaria y para la gestión de servicios sanitarios, siempre y cuando el tratamiento se realice por personas sujetas al deber de secreto (Solernou, 2006, p. 56). "Este tratamiento incluye la recogida, el almacenamiento y la comunicación de los datos y será legítimo siempre y cuando persiga el cumplimento de estos fines y lo lleven a cabo personas sujetas al secreto profesional" (Solernou, 2006, p. 56).

Con relación a las iniciativas que desde los Estados y el sector privado han supuesto la implementación de soluciones técnicas y aplicaciones móviles para la recopilación de datos de salud con el fin de mejorar la eficiencia operativa de los servicios sanitarios, así como para conseguir la mejor atención y la accesibilidad por parte de los ciudadanos, no se encuentran dentro de la excepción antes señalada ya que estamos frente a funcionalidades que se ponen a disposición de los ciudadanos y su uso es voluntario y requieren consentimiento expreso.

El uso de aplicaciones ("*app*") que le permitan al titular de los datos personales la autoevaluación en base a los síntomas médicos que comunique, de la probabilidad que esté infectado de COVID-19, de recibir información, consejos y recomendaciones, o de

---

5 Reglamento (UE) 2016/679

"Artículo 9. Tratamiento de categorías especiales de datos personales

(…)

2. El apartado 1 no será de aplicación cuando concurra una de las circunstancias siguientes:

(…)

i) el tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, sobre la base del derecho de la Unión o de los Estados miembros que establezcan medidas adecuadas y específicas para proteger los derechos y libertades del interesado en particular el secreto profesional.

(…)".

posibilitarle la geolocalización para verificar que se encuentra donde declara estar, debe ser enteramente voluntario, de manera que toda aquella persona que quiera someterse a ellas tendrá que prestar su consentimiento expreso, donde el responsable de tratamiento será la autoridad sanitaria estatal o la empresa privada que ponga a disposición la misma (Rodríguez, 2020, p. 143).

2.2 FINALIDAD, PROPORCIONALIDAD Y MINIMIZACIÓN DE DATOS

El tratamiento de los datos de salud que sean recopilados debe estar exclusivamente limitados a la finalidad pretendida, sin que pueda extender dicho tratamiento a cualesquiera otros datos personales no estrictamente necesarios para dicha finalidad, o que pueda confundirse conveniencia con necesidad, porque el derecho fundamental a la protección de datos debe seguir aplicándose sin perjuicio de las situaciones de emergencia establecidas en la normativa para la protección de intereses esenciales de salud pública (Piñar, 2020).

De acuerdo con esto último, la recopilación de datos personales debe ser mínima para el logro de objetivos de salud pública, estando ello acorde con el principio de proporcionalidad, cuya finalidad es "evitar que se recopilen información que no es razonablemente pertinente para cumplir la finalidad del tratamiento, lo que supone una limitación para cualquier forma de recopilación que no esté justificada" (Zegarra 2014, p. 631).

La garantía de que en el tratamiento de datos personales sea determinado, explícito, lícito y que el mismo no será incompatible para los fines para los que fueron recopilados; así como lo referido a que el tratamiento de los datos personales sea adecuado, relevante y no excesivo, todo ello con el propósito de lograr que las medidas de prevención en salud sean eficaces; se encuentran regulados en los artículos 6[6] y 7[7] de la LPDP, respectivamente. De acuerdo con las citadas normas, es necesario que se verifique el cumplimiento de la finalidad y la pertinencia de los datos personales solicitados con la normativa que las autoridades de salud han aprobado cuya finalidad es hacer frente al COVID-19 y disminuir su propagación.

Vinculado con el principio de proporcionalidad de la normativa peruana, se encuentra el principio de minimización de datos, recogido en el artículo 5[8] de la RGPD europeo, de acuerdo con el cual sólo pueden recopilarse datos personales estrictamente necesarios

---

6 Ley N° 29733, Ley de Protección de Datos Personales

"Artículo 6. Principio de finalidad

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, excluyendo los casos de actividades de valor histórico, estadístico o científico cuando se utilice un procedimiento de disociación o anonimización."

7 Ley N° 29733, Ley de Protección de Datos Personales

Artículo 7. Principio de proporcionalidad

Todo tratamiento de datos personales debe ser adecuado, relevante y no excesivo a la finalidad para la que estos hubiesen sido recopilados."

8 Reglamento (UE) 2016/679

"Artículo 5. Principios relativos al tratamiento

1. Los datos personales serán:

(…)

para el tratamiento y en la oportunidad que vayan a ser tratados no para usarlos tiempo después; asimismo, la solicitud de datos personales a sus titulares debe encontrarse plenamente justificada, en función a la finalidad que se persigue por dicho tratamiento (Puyol, 2017, p. 138).

Ante los nuevos desafíos en tiempos de pandemia, se deben reinterpretar los principios que sustentan el tratamiento de datos personales de manera que pueda contarse con un marco normativo que ofrezca seguridad jurídica, proteja los derechos de las personas y genere confianza en la sociedad (Gómez-Córdova et al., 2020, p. 285). Así, por ejemplo, el principio de finalidad del tratamiento de datos personales está vinculado con las recomendaciones éticas de la OMS en la pandemia de COVID-19 referidas a (i) la restricción de su uso; (ii) la proporcionalidad en la recolección de datos; y, (iii) la recolección mínima de datos para el logro de objetivos de salud pública (Gómez-Córdova et al., 2020, p. 286).

Es necesario reparar en que se tiende a recoger muchos datos de salud y en ello contribuye el uso de tecnologías de la información, afectando por tanto la eficacia de la prestación sanitaria (Souleron, 2006, p. 57). "El sistema debe asegurar que el personal sanitario dispone de información necesaria y relevante cuando ejerce sus funciones y eso implica decidir y, si cabe, cuestionar qué datos se introducen en el sistema y de qué forma". (Souleron, 2006, p. 57).

De lo expresado, resulta claro que, si bien estas consideraciones son previas a la emergencia sanitaria generada por el COVID-19, apuntan a advertir que el uso de tecnologías de la información en el tratamiento de datos de salud puede derivar en la inobservancia de los principios de finalidad, proporcionalidad y minimización de datos, lo que tiene un impacto significativo en caso se produzca el acceso a datos personales por terceros no autorizados, debido a que el mismo puede derivar en un tratamiento destinado a usos no autorizados o a tratamientos que limiten el ejercicio de los derechos del titular de los datos personales, de ahí la importancia de establecer mecanismos que garanticen el cumplimiento de los citados principios.

2.3 SEGURIDAD

El principio de seguridad implica que cualquier mecanismo de tratamiento de datos personales que se adopte debe garantizar la seguridad de los datos personales que eviten cualquier pérdida, desviación o adulteración de los datos personales obtenidos. En el caso específico de los datos de salud, las medidas de seguridad que se implementen son de nivel alto, atendiendo a la naturaleza de los referidos datos y en función a la mayor necesidad de garantizar la confidencialidad y la integridad de dicha información cuando es tratada (Cristea, 2018, p. 108).

La normativa peruana ha recogido dichos términos. Así, de conformidad con el artículo

c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados ("minimización de datos").

(...)"

9[9] de la LPDP y el artículo 10[10] del RLPD, el principio de seguridad garantiza que el titular del banco de datos personales y el encargado de su tratamiento deben adoptar medidas técnicas, organizativas y legales necesarias para salvaguardar la seguridad de los datos personales, evitando cualquier tratamiento contrario a la Ley o al Reglamento, incluyéndose la adulteración, pérdida, desviaciones de información, intencionales o no, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.

Por su parte, el artículo 4.12[11] del RGPD europeo establece que la violación de la seguridad de los datos personales implica toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos. Asimismo, el artículo 5[12] del RGPD garantiza la seguridad adecuada de los datos personales, lo cual implica la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas ("integridad y confidencialidad").

La garantía del principio de seguridad está directamente vinculada con el derecho a la confidencialidad de los datos personales. Sin embargo, al disponerse de medidas cuyo objetivo sea garantizar el derecho a la salud y que hagan posible que el suministro de la información sea oportuno y veraz, mejorando el acceso a los datos de salud con el uso de tecnologías de la información, no se está garantizando necesariamente la seguridad

---

9 Ley N° 29733, Ley de Protección de Datos Personales

"Artículo 9. Principio de seguridad

El titular del banco de datos personales y el encargado de su tratamiento deben adoptar las medidas técnicas, organizativas y legales necesarias para garantizar la seguridad de los datos personales. Las medidas de seguridad deben ser apropiadas y acordes con el tratamiento que se vaya a efectuar y con la categoría de datos personales de que se trate".

10 Decreto Supremo No. 003-2013-JUS, Reglamento de la Ley 29733

"Artículo 10.- Principio de seguridad

En atención al principio de seguridad, en el tratamiento de los datos personales deben adoptarse las medidas de seguridad que resulten necesarias a fin de evitar cualquier tratamiento contrario a la Ley o al presente reglamento, incluyéndose en ellos a la adulteración, la pérdida, las desviaciones de información, intencionales o no, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado".

11 Reglamento (UE) 2016/679

"Artículo 4. Definiciones

(…)

12. violación de la seguridad de los datos personales": toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o lícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos;

(…)".

12 Reglamento (UE) 2016/679

"Artículo 5. Principios relativos al tratamiento

1. Los datos serán:

(…)

f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas ("integridad y confidencialidad")

de los mismos.

Es necesario reparar en que la confianza del paciente sobre la confidencialidad depende de la seguridad del aparato técnico y la transparencia sobre el tratamiento de los datos personales en salud, tanto de médicos como no-médicos involucrados en las operaciones y procesos. (Almada & Maranhão, 2021) Por ello, el acceso no debe ser indiscriminado, incluso cuando el mismo se sustente en razones científicas, por lo que deben implementarse mecanismos que eviten afectar la seguridad de los datos de salud, es decir, su integridad y confidencialidad.

2.4 CALIDAD O ALMACENAMIENTO POR TIEMPO LIMITADO

El tratamiento de datos personales recopilados en el marco de la excepción de la obligación de del consentimiento por autoridades sanitarias o por empresas privadas, en el marco de la excepción de la obligación del consentimiento, deben limitarse, como sucede con cualquier tipo de tratamiento, al tiempo de duración de la situación de emergencia sanitaria, por ello debe garantizarse que la información obtenida no será empleada a largo plazo con otros fines estatales o privados.

Esta regla ha sido recogida en el artículo 8[13] de la LPDP, norma que dispone que los datos personales deben conservarse de forma tal que se garantice su seguridad y solo por el tiempo necesario para cumplir con la finalidad del tratamiento. Asimismo, en el artículo 28[14] de la LPDP se establece la obligación del responsable de tratamiento, cuando los datos hayan dejado de ser pertinentes, necesarios y adecuados para la finalidad establecida, de suprimirlos o anonimizarlos o deberá aplicarles un mecanismo de disociación o de seudonimización con código, permaneciendo los datos seguirán activos, pero sin poder identificar de manera sencilla al titular de los mismos, salvaguardando su derecho a la protección de los datos personales.

El RGPD europeo recoge un precepto cuyo contenido está en armonía con las citadas normas de la LPDP peruana. En su artículo 5[15], el RGPDP dispone que los datos personales

---

13 Ley N° 29733, Ley de Protección de Datos Personales

"Artículo 8. Principio de calidad

Los datos personales que vayan a ser tratados deben ser veraces, exactos y, en la medida de lo posible, actualizados, necesarios, pertinentes y adecuados respecto de la finalidad para la que fueron recopilados. Deben conservarse de forma tal que se garantice su seguridad y solo por el tiempo necesario para cumplir con la finalidad del tratamiento".

14 Ley N° 29733, Ley de Protección de Datos Personales

"Artículo 28. Obligaciones

(…)

7. Suprimir los datos personales objeto de tratamiento cuando hayan dejado de ser necesarios o pertinentes a la finalidad para la cual hubiesen sido recopilados o hubiese vencido el plazo para su tratamiento, salvo que medie procedimiento de anonimización o disociación.

(…)".

15 Reglamento (UE) 2016/679

"Artículo 5. Principios relativos al tratamiento

1. Los datos serán:

(…)

e) Mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del trata miento de los datos personales; los datos personales

deben mantenerse de forma que se permita la identificación de los interesados durante no más del tiempo necesario para los fines del tratamiento de los datos personales ("limitación del plazo de conservación").

> Superado ese tiempo sólo pueden conservarse durante períodos más largos con las finalidades de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, siendo en ocasiones preciso, en orden a salvaguardar el principio de minimización, proceder a la seudonimización de los datos (RGPD art. 89.1), y sin perjuicio de la aplicación de técnicas organizativas apropiadas que impone el RGPD para proteger los derechos del interesado (López, L.F., 2016, p. 61).

3. EL USO DE HERRAMIENTAS TECNOLÓGICAS SUSTENTADAS EN EL TRATAMIENTO DE DATOS PERSONALES PARA LUCHAR CONTRA LA PANDEMIA DEL COVID–19: IDENTIFICACIÓN DE ALGUNOS RIESGOS Y AFECTACIONES AL DERECHO FUNDAMENTAL DE PROTECCIÓN DE DATOS PERSONALES

Con la declaratoria de la pandemia por el COVID-19, diversas naciones del mundo han implementado numerosas iniciativas encaminadas a paliar los efectos nocivos del virus mediante el desarrollo de herramientas tecnológicas sustentadas en el tratamiento de datos de salud. La latente amenaza que para la vida humana representa el COVID-19 hace necesaria su contención a través de una gestión de datos personales correcta y medios idóneos que coadyuven a dicho fin.

Por ello, en los últimos meses diversos gobiernos y empresas privadas han implementado estrategias digitales que complementan los instrumentos de vigilancia epidemiológica para la detección de casos, el rastreo de contactos, el diagnóstico de la enfermedad, la documentación de lugares donde las personas han estado, la determinación de sitios y momentos de mayor afluencia, para así implementar medidas que limiten el contagio. Además, se han usado para comunicar y educar a la ciudadanía o darle atención sanitaria a través de telepresencia (Gómez-Córdoba et al., 2020, p. 274). Esto ha sido reconocido a nivel internacional en la Resolución No. 1/2020 de la Corte Interamericana de Derechos Humanos, titulada "Pandemia y Derechos Humanos en las Américas":

> En cuanto a las medidas de contención con el fin de enfrentar y prevenir los efectos de la pandemia, la CIDH ha observado que se han suspendido y restringido algunos derechos, y en otros casos se han declarado "estados de emergencia", "estados de excepción", "estados de catástrofe por calamidad pública", o "emergencia sanitaria", a través de decretos presidenciales y normativa de diversa naturaleza jurídica con el fin de proteger la salud pública y evitar el incremento de contagios. Asimismo, se han establecido medidas de distinta naturaleza que restringen los derechos de la libertad de expresión, el derecho de acceso a la información pública, la libertad personal, la inviolabilidad del domicilio, el derecho a la propiedad privada; y se ha recurrido al uso de tecnología de vigilancia para rastrear la propagación del coronavirus, y al almacenamiento de datos de forma masiva. (CIDH, 2020, p.4).

---

podrán conservarse durante períodos más largos siempre que se traten exclusiva mente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado («limitación del plazo de conservación»);"

En efecto, la llamada tecnología de vigilancia se ha materializado en aplicativos que tienen como principal intención informar sobre el virus y brindar un diagnóstico a partir de los datos ingresados en el aplicativo e identificar individuos contagiados, focos de contagio y permitir el rastreo del contagio (*tracking* y *tracing*). Asimismo, se han implementado herramientas tecnológicas que han permitido medición masiva de temperatura en espacios de uso público.

No existen dudas de que la implementación de nuevas tecnologías sustentadas en el tratamiento de datos personales, unido al uso de técnicas propias de la analítica de datos y la Inteligencia Artificial, comportan beneficios significativos y representan una importante oportunidad para detener la expansión del COVID–19, en tanto que permiten mejorar la capacidad de previsión y decisión de las autoridades sanitarias, contribuyen a fortalecer la eficacia de las medidas de distanciamiento social reduciendo con ello significativamente la propagación de la pandemia y minimizando el coste de vidas humanas (Domínguez, 2020, p. 610).

No obstante, como previamente se ha señalado, estas estrategias no siempre se configuran dentro de un régimen jurídico de protección de datos personales robusto y que garantice debidamente la protección de los datos personales y sus principios, lo que justifica identificar, para su prevención, los riesgos que se generan cuando se emplean herramientas tecnológicas que tratan datos personales y las posibles afectaciones al derecho fundamental a la protección de datos personales, máxime cuando su utilización ha hecho que los métodos de recopilación de datos personales sean cada vez más abundantes, complicados y se detecten con mayor dificultad (Cristea, 2018, p. 226).

Este contexto, plantea un necesario análisis de aquellas cuestiones que permitan alcanzar el difícil equilibrio entre el impulso de instrumentos tecnológicos que contribuyan a controlar los efectos del COVID–19 incrementando los recursos puestos a disposición de las autoridades sanitarias y la salvaguarda del derecho fundamental a la protección de datos personales.

3.1 INFORMACIÓN Y DIAGNÓSTICO DEL VIRUS

Contar con canales informativos que permanentemente sean actualizados sobre el COVID-19, sus síntomas, las medidas de prevención y diagnóstico es un asunto de interés para cualquier persona que tenga mínimamente algún síntoma o busque información que necesite compartir en su entorno familiar.

Ante el colapso de la atención telefónica para las consultas, los Estados, empresas privadas, organizaciones supranacionales desarrollaron *apps*, *webs*, *chatbots*, canales de *Telegram*, entre otros, a fin de que la ciudadanía obtenga información veraz y oficial o realice autoevaluaciones de forma sencilla, sin necesidad de hacer una llamada telefónica o acudir a la emergencia de un centro de salud pública o privada (Cascón-Katchadurian, 2020, p. 4).

En lo concerniente a las aplicaciones de autoevaluación, estás ofrecen recomendaciones sobre cómo actuar según los síntomas, llegando incluso a ponerse en contacto con los usuarios para realizarles *test* sobre el coronavirus o un seguimiento de la evolución de la enfermedad (Cascón-Katchadurian, 2020, p. 4). Todos estos datos se usan igualmente para hacer una representación aproximada del nivel posible de inmunidad de la población (Cascón-Katchadurian, 2020, p. 4).

En España, la Secretaría General de Administración Digital, dependiente de la Secretaría

de Estado de Digitalización e Inteligencia Artificial del Ministerio de Asuntos Económicos y Transformación Digital, desarrolló el aplicativo móvil *Radar COVID*. Con su descarga, los usuarios de esta *app* reciben una notificación en caso de que en los catorce días anteriores a la misma hayan estado expuestos a un contacto epidemiológico con otro usuario que haya declarado en la aplicación haber dado un resultado positivo en la prueba de COVID-19, previa acreditación por parte de las autoridades sanitarias correspondientes (Domínguez, 2020).

En Corea del Sur se desarrolló la *app Self-quarantine safety protection* con el objetivo de evitar el descontrol de la enfermedad y el colapso de los hospitales, para lo cual registra los datos de los usuarios y sus respuestas a preguntas sobre el estado de salud y con los mismos los médicos ofrecen un diagnóstico en remoto lo cual ayuda a la descongestión de los teléfonos (Cascón-Katchadurian, 2020, p. 5). "De esta forma se consigue un diagnóstico masivo y con esos datos se decide a quién debe realizarse el test" (Ruiz, 2020 citado en Cascón-Katchadurian, 2020, p. 5).

En el caso peruano, la *app* que se ha hecho cargo de proveer información actualizada sobre las zonas de contagio y brindar a los ciudadanos un pronóstico sobre su posible condición de portador del COVID-19 fue la llamada "*El Perú en tus manos*", la misma que "ofrece la opción «Mapa de zonas afectadas» (...) para acceder a un mapa de cercanías a él donde se marca la incidencia de contagios; así también, se dispone de la opción «Triaje» (...) mediante el cual, de acuerdo con los síntomas que consigne, podrá determinar si es o no un posible portador del mencionado virus." (Vásquez, 2020, p. 158).

Con respecto a los riesgos o posibles afectaciones al derecho a la protección de datos personales, que pueden derivarse de este tipo de *apps* deben considerarse aquellos vinculados al principio del consentimiento de las personas, puesto que existe el peligro que tanto los datos ingresados por las personas para recibir actualizaciones informativas sobre el virus como los datos ingresados para generar un autodiagnóstico de la *app* sean usados para una finalidad distinta a la que el usuario creía y consentía.

El análisis parte de considerar que cuando un usuario brinda sus datos identificativos y de salud para ser informado y/o autoevaluado por el aplicativo, su consentimiento girará en torno a la finalidad concreta del servicio; por tanto, el responsable del tratamiento que gestione la *app* no podría emplear los datos para una finalidad distinta a la de diagnosticar el virus con los datos del usuario.

Respecto a los aplicativos que son capaces de realizar un autodiagnóstico, se encuentran aquellos que lo logran en base a la grabación de voz de las personas. En España, por ejemplo, la empresa Biometric Vox viene desarrollando con ayuda de inteligencia artificial una *app* que será capaz de detectar un índice de contagio del COVID-19. Este sistema permitiría analizar - a distancia, sin contacto físico y en tiempo real - el estado del aparato fonador y, como consecuencia, poder aportar un índice de contagio y servir a las autoridades sanitarias como ayuda complementaria para el control de la propagación y cualquier otra gestión de datos (Biometric Vox, 2020, párr. 4).

En Brasil, SPIRA y SoundCov son dos aplicativos en los que los usuarios realizan una grabación de su voz que luego es analizada a través de algoritmos de aprendizaje automático dando lugar a un diagnóstico del COVID-19 (Almada & Maranhão, 2021, pp. 1-2).

> The SPIRA project, currently under development at the University of Sao Paulo, seeks to detect severe respiratory insufficiency associated with the SARS-COV-2

> virus, to indicate whether the user of the app must seek hospitalization. To obtain this diagnosis, the SPIRA app records the patient´s reading of a few pre-defined sentences. These recordings are analyze by a machine learning model trained to distinguish the voices of healthy persons from those of people afflicted with respiratory insufficiencies (Almada & Maranhão, 2021, p. 2).
>
> [El proyecto SPIRA, actualmente en desarrollo en la Universidad de Sao Paulo, pretende detectar la insuficiencia respiratoria grave asociada al virus SARS-COV-2, para indicar si el usuario de la aplicación debe ser hospitalizado. Para obtener este diagnóstico, la aplicación SPIRA registra la lectura del paciente de unas frases predefinidas. Estas grabaciones son analizadas por un modelo de aprendizaje automático entrenado para distinguir las voces de personas sanas de las de personas afectadas por insuficiencias respiratorias].
>
> SoundCov, an app developed by Fiocruz, Intel, and Instituto Butantan, trains a machine learning system to distinguish between the coughing sounds of a Covid-19-positive person and those of healthy people and people afflicted by other respiratory illnesses, such as pneumonia or tuberculosis. The application then combines the analysis of the coughing sounds with additional information about epidemiological variables and patient´s health history, thus producing a final diagnosis (Almada & Maranhão, 2021, p. 2).
>
> [SoundCov, una aplicación desarrollada por Fiocruz, Intel y el Instituto Butantan, entrena un sistema de aprendizaje automático para distinguir entre los sonidos de la tos de una persona que da positivo en el Covid-19 y los de personas sanas y los de personas afectadas por otras enfermedades respiratorias, como la neumonía o la tuberculosis. A continuación, la aplicación combina el análisis de los sonidos de la tos con información adicional sobre las variables epidemiológicas y el historial de salud del paciente, con lo que se obtiene un diagnóstico final].

Con este tipo de tecnología puede generarse una transgresión al principio de consentimiento ya que el mismo debe obtenerse brindando a los titulares de los datos de salud toda aquella información acerca de la forma y duración del tratamiento, de manera que, si ello no se produce, el consentimiento se considera inválido (Almada & Maranhão, 2021, p. 7). Vinculado a esto último, debe repararse en que las aplicaciones basadas en sistemas de aprendizaje automático son notoriamente opacas para los observadores externos, lo que plantea dificultades adicionales a la tarea de proporcionar a los usuarios la información que necesitan para dar su consentimiento informado (Almada & Maranhão, 2021, p. 7).

También se identifica la posibilidad de que se transgreda el principio de finalidad aplicable al tratamiento de los datos personales y, por tanto, se afecte al titular de los mismos, en razón a que

> Almacenar datos de voz, hace posible que entidades no autorizadas utilicen los datos para identificar a las personas, obtener acceso de manera malintencionada a los sistemas que implementan el reconocimiento de voz, o simplemente procesar datos y construir artefactos de voz que podrían utilizarse para personificar a los individuos creando escenarios que resultan problemáticos (Alva, 2020, p. 171).

Otra de las situaciones que pueden generar riesgos y afectaciones es la que se produce cuando los responsables de las *apps* mantienen datos de salud indefinidamente. Esto último está directamente relacionado con el principio de calidad e implica que los los responsables del tratamiento de los datos de salud deben garantizar que la información

obtenida no será empleada a largo plazo con otros fines estatales o privados, sino que deben limitarse al tiempo de duración de la pandemia.

De esta forma, la exposición que puede tener el titular de los datos de salud que accedan a este tipo de *app* a que la utilización de su información sea destinada para finalidad distintas es alta, por lo que resulta indispensable identificar cuál es la empresa que pone a disposición el aplicativo y revisar sus políticas de privacidad, de forma previa a consignar datos personales con el objetivo de obtener información y/o efectuar un autodiagnóstico.

3.2 GEOLOCALIZACIÓN Y SEGUIMIENTO DE CONTAGIADOS

Sobre este punto, es necesario realizar una precisión conceptual previa debido a que el frente al uso de los teléfonos móviles para ayudar a controlar la pandemia, se presentan dos posibilidades principales: una basada en el geoposicionamiento (o *tracking*) y otra basada en el seguimiento automatizado de contactos (o *tracing*) (Buchland, 2020).

De acuerdo con la distinción mientras que el *tracking* consiste en que la app instalada en un teléfono móvil va guardando en todo momento la posición de la persona que lo utiliza, el *tracing* busca realizar un seguimiento automatizado de contactos, lo cual, involucra que haya una comunicación directa entre el teléfono móvil de una persona con el de todas aquellas personas con las que quiere estar en contacto cercano (Buchland, 2020).

Lo cierto es que, como se verá a continuación ni las herramientas enfocadas en *tracking* ni las apps destinadas al *tracing* se libran de los grandes peligros que surgen en cuanto a datos personales se refiere.

A. GEOPOSICIONAMIENTO *(TRACKING)*

Frente al avance del COVID-19 los Estados han implementado iniciativas tecnológicas destinadas a conocer los movimientos de la población para que a través de su estudio cuenten con patrones de la movilidad de las personas alrededor de una ciudad, región o país, con el objetivo de registrar la localización de las de personas contagiadas (o no contagiadas, para que no eviten el confinamiento) para asistirlas en caso sea necesario. Entonces, el conocimiento de estos datos resulta beneficioso para que los entes de la Administración a cargo de salud, seguridad e infraestructura, a la hora de articular y dimensionar las acciones que mitiguen el virus, puedan hacerlo de la manera más adecuada (AEPD, 2020a, p. 5).

La herramienta que permite conocer estos datos es la geolocalización o geoposicionamiento, es decir, una *app* que hace uso del *Global Position System* o más comúnmente conocido como GPS. Lo que debe considerarse, es que este tipo de herramientas tienen algunos problemas prácticos, como la falta de exactitud en la geolocalización (sobre todo en espacios interiores), o que los teléfonos móviles sólo informan que los usuarios han estado cerca de una persona, entre otros. (Buchland, 2020).

No obstante, si bien son conocidas las limitaciones que acompañan a la tecnología, lo cierto es que el contexto de la pandemia ha involucrado una proliferación de soluciones tecnológicas que han tenido la intención de apoyar en la lucha contra la pandemia (Andreu, 2020, p. 851). Es el caso de la *app* HaMagen, la cual ha sido un ejemplo de cómo el *tracking* puede ser una herramienta interesante para que un gobierno emprenda acciones eficientes para con su población. Las funcionalidades de este aplicativo han sido explicadas por el Ministerio de Salud de Israel:

> HAMAGEN is an app that allows the identification of contacts between diagnosed patients and people who came in contact with them in the 14 days prior to the patient's diagnosis of the disease.
>
> Cross-referencing your location data with the corona patients' location is done on your device and as soon as a match is identified, you will be directed to a link to the Ministry of Health to let you know what steps to take and to report the match to The Ministry (Israel National Cyber Directorate, 2020, p. 1).
>
> [HAMAGEN es una app que permite identificar los contactos entre pacientes diagnosticados y las personas que estuvieron en contacto con ellos en los 14 días anteriores al diagnóstico de la enfermedad del paciente. El cruce de sus datos de localización (del usuario) con la ubicación de los pacientes de Corona se realiza en su dispositivo y, en cuanto se identifique una coincidencia, se le dirigirá a un enlace al Ministerio de Sanidad para informarle de los pasos que debe dar y para informar la coincidencia al Ministerio].

La geolocalización a través de dispositivos móviles puede operar de dos formas: por los operadores de telecomunicaciones y a partir de las redes sociales[16]. Sin embargo, ninguna de estas formas está privada de riesgos.

En el caso de la geolocalización realizada a través de los teléfonos móviles por los operadores de telecomunicaciones, esta 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" (AEPD, 2020a, p. 4). El riesgo que puede generarse es el de una anonimización incompleta, una subcontratación poco rigurosa o un ciberataque que ponga en manos de un tercero la localización de los teléfonos móviles de los usuarios.

Respecto a la geolocalización de los teléfonos móviles a partir de redes sociales, esta es una técnica utilizada antes de la pandemia ya que las direcciones IP de los usuarios pueden ser conocidas por los administradores de las páginas web y son utilizadas habitualmente con fines de publicidad. La información puede ser de ayuda para las autoridades sanitarias siempre que esté de acuerdo con un propósito y un fin previamente definido y sea aplicado a sus estrategias de prevención y control (AEPD, 2020a, p. 6).

La geolocalización puede brindar algunas tendencias y estadística de contagio a los operadores de los gobiernos para que haya más acción de su parte en las diferentes zonas. Sin embargo, como se ha visto en los anteriores párrafos, el geoposicionamiento hoy en día puede ser también una excusa para que se emprendan abusos contra el derecho fundamental a la protección de datos personales, incluso hay quienes consideran que "la inusitada expansión de la vigilancia y control estatal por medio de las tecnologías digitales para monitorear la posible transmisión del virus implica una importante regresión en materia de derechos humanos que será difícil de revertir en el escenario post-pandemia"(Bizberge y Segura, 2020, p. 71).

B. RASTREO Y SEGUIMIENTO DE CONTACTOS *(TRACING)*

El rastreo de contactos sigue la lógica de los servicios utilizada tradicionalmente por los servicios de salud: "se trata de cualquier registro de escrito que identifica a un paciente y sigue su historia clínica, la que es monitoreada por trabajadores de la salud, quienes a su vez pueden entregarle recomendaciones médicas personal o técnicamente" (Weidenslaufer, C. y Meza, M. 2020, p. 1).

16 Clasificación propuesta por la Agencia Española de Protección de datos.

Han surgido entonces en el medio nuevas formas para diseñar aplicativos, con la finalidad que los mismos colaboren más allá de una simple localización. Nos referimos a aquellos aplicativos que logran hacer una labor de *tracing* y no solo de *tracking*, previamente desarrollada. El objetivo al cual están orientadas, no sólo es el de hacer seguimiento de enfermos, sino también alertar a quienes hayan estado físicamente cerca de un paciente de COVID-19 adopten las medidas necesarias sanitarias pertinentes más adecuadas que permitan ayudar a contener la propagación del virus (Weidenslaufer, C. y Meza, M. 2020, p. 1).

> Es prácticamente imposible que un sujeto recuerde, y conozca, todos los contactos que haya podido tener a lo largo de un período de entre dos días o una semana desde que muestra síntomas. Lo importante es romper la cadena de transmisión de la infección de la forma más eficaz posible. Y esto lo pueden hacer las apps de rastreo de contactos (Arenas, M. 2020, p.3).

En las apps del tipo *tracing* cuya tecnología predominante es el *bluetooth*, lo que interesa no es tanto la localización exacta de la persona, sino registrar a las posibles personas con las que ha estado en contacto para que en el momento que alguien dé positivo se avise a todos los demás y de esa forma detectar a los asintomáticos (Cascón-Katchadurian, 2020, p. 10). Una de las ventajas de estos aplicativos que emplean el bluetooth es que son anónimas y descentralizadas por lo general, por lo que a los usuarios les indicaría que han estado en contacto con un paciente que ha dado positivo, pero no revelará la identidad de la persona (Cascón-Katchadurian, 2020, p. 15).

Se debe reparar en el hecho de que los Estados monitoreen a su población por su geolocalización coadyuva a que la asistencia en puntos geográficos específicos se brinde de una manera más pronta y eficaz; sin embargo, no hay que considerar que ello esté exento de afectaciones al derecho fundamental a la protección de datos personales debido a las prácticas que pueden derivarse del objetivo antes descrito. Esto último lo ha identificado Access Now[17], al señalar que "el rastreo de la ubicación geográfica de los teléfonos inteligentes proporciona información sobre el movimiento de los teléfonos de las personas y no del virus" (2020, p. 10), y que realizar seguimiento de cómo evoluciona el COVID – 19 mediante referencias cruzadas entre los datos geográficos de las personas con los casos de infección conlleva riesgos inherentes (2020, p. 10).

La referida organización refiere además que, si bien la información que se registra a través de la apps de rastreo y seguimiento es anónima dicha características puede revertirse de manera que la personas pueden ser reidentificadas fácilmente, y que la información puede resultar incompleta respecto del lugar en que la persona realiza sus actividades (Access Now, 2020, p. 10).

Los riesgos y la posible afectación al derecho a la protección de datos personales de este tipo de soluciones pueden producirse cuando se realizan mapas de relaciones entre personas, reidentificación por localización implícita de la fragilidad de los protocolos a la hora de configurar tarjetas casi anónimas, y al dispersarse las señales de los contagios de forma que no se identifique en ningún caso la identidad de los contagiados.

3.3 MEDICIÓN MASIVA DE TEMPERATURA EN ESPACIOS DE USO PÚBLICO

Al ser la fiebre el síntoma más recurrente en los infectados por el COVID-19, el escaneo de temperatura en las personas cumple una especial relevancia (Wilches-Visbal et al,

17 Access Now es una organización sin fines de lucro que viene funcionado desde el año 2009. Su misión es la defensa de los derechos digitales de los usuarios del mundo.

2021). Siendo así, una de las formas de medición masiva de temperatura en espacios de uso público ha sido a través de cámaras térmicas de reconocimiento facial.

Las cámaras térmicas son dispositivos que "detectan la radiación infrarroja emitida por cualquier cuerpo con temperatura superior al cero absoluto y la transforman en una señal eléctrica, que luego es procesada para obtener un valor o un mapa de temperaturas" (Wilches – Visbal et al, 2020, pp. 305-306). Como señala la AEPD, "(…) añaden la capacidad de tomar la temperatura a los individuos que cruzan un área, sin requerir en muchos casos ninguna acción por su parte" (2020a, p. 11).

Al respecto, si bien el uso de cámaras térmicas supone el empleo de una tecnología interesante para identificar el contagio, puede llegar a ser una práctica que comprometa los datos personales de las personas si es que va de la mano con el reconocimiento facial de las mismas, como lo ha sostenido Van Natta et al.: "In such exceptional times, one could argue that fever checks offer substantial population health benefits with limited long-term impacts on personal privacy. Yet, several private companies have integrated thermal imaging with facial recognition technology". [En tiempos tan excepcionales, se podría argumentar que los controles de fiebre ofrecen importantes beneficios para la salud de la población con un impacto limitado a largo plazo en la privacidad personal. Sin embargo, varias empresas privadas han integrado la imagen térmica con la tecnología de reconocimiento facial] (2020, p. 5).

En el ámbito laboral y, en concreto en la normativa de seguridad y salud en el trabajo, la toma de temperatura puede ser de utilidad, pero situada en un marco de tratamiento de datos más extenso del que formen parte otras comprobaciones y garantías adicionales en las que se respeten los derechos y libertades previstos en la normativa de protección de datos personales (AEPD, 2020a, p. 12).

En el Perú, la Ley No. 29783, Ley de Seguridad y Salud en el Trabajo, señala en el literal c) de su artículo 49 que es una obligación del empleador: "identificar las modificaciones que puedan darse en las condiciones de trabajo y disponer lo necesario para la adopción de medidas de prevención de los riesgos laborales". Esta obligación supone que el empleador preste particular atención a las medidas que toma para que sus trabajadores se encuentren en una situación de riesgo controlado en su centro de labores.

Respecto a los riesgos a la posible afectación al derecho a la protección de datos personales debe repararse en que la cámara térmica y la recopilación del dato solo puede entenderse como parte de un tratamiento mayor y no puede tomar un dato de salud a una persona y tratarlo espontáneamente por cualquier gestor de un lugar público simplemente porque crea que es lo mejor para sus clientes y usuarios (AEPD, 2020a, p. 12), lo que puede afectar directamente el principio de finalidad.

También resulta especialmente problemático no tener la posibilidad de conocer el alcance de la información que puede obtenerse utilizando los datos personales de salud recopilados mediante esta herramienta tecnológica, porque puede tratarse de información basada en la medición de temperatura que revele información reservada del estado de salud de la persona como puede ser el embarazo, la menopausia o el uso de fármacos, lo que supondría una afectación directa al principio de proporcionalidad en materia de protección de datos personales (Van Natta et al., 2020, p. 7).

En caso de no contar con una regulación adecuada, un monitoreo con tantas imprecisiones puede inadvertidamente generar un daño en los individuos que son etiquetados en un centro comercial, durante un viaje, sin que pueda tener una mínima posibilidad rectificación (Van Natta et al., 2020, p. 8), lo que supone una vulneración al principio

de calidad. Asimismo, se tendrá un riesgo de discriminación, estigmatización y tal vez difusión pública de datos de salud. Todo ello se puede agravar con el riesgo de fugas de información sensible si es que no se atiende al principio de seguridad en la protección de datos personales.

4. A MODO DE CONCLUSIÓN

Lo desarrollado en este trabajo conlleva una reflexión respecto del cuidado que los Estados y el sector privado deben tener al adoptar medidas para enfrentar la expansión del COVID-19, las cuales pueden tener consecuencias irreversibles en el derecho fundamental a la protección de datos personales y que pueden estar guiadas únicamente por la urgencia, el miedo y lo que es peor, por otros intereses.

Y es que, como consecuencia de la pandemia, los Estados y particulares han implementado distintas herramientas tecnológicas con la finalidad de proteger la salud pública y evitar la propagación de contagios. No obstante, en determinados casos, la implementación de estas herramientas conlleva a asumir riesgos y afectaciones al derecho a la protección de datos personales.

Comprobada la existencia de estos riesgos, resulta pertinente rescatar lo considerado por la antes citada Resolución de la CIDH, en tanto recomienda a los gobiernos de los Estados miembros que deben guiar su actuación de conformidad con dos obligaciones generales relacionadas a la protección de datos personales:

> 35. Proteger el derecho a la privacidad y los datos personales de la población, especialmente de la información personal sensible de los pacientes y personas sometidas a exámenes durante la pandemia. Los Estados, prestadores de salud, empresas y otros actores económicos involucrados en los esfuerzos de contención y tratamiento de la pandemia, deberán obtener el consentimiento al recabar y compartir datos sensibles de tales personas. Solo deben almacenar los datos personales recabados durante la emergencia con el fin limitado de combatir la pandemia, sin compartirlos con fines comerciales o de otra naturaleza. Las personas afectadas y pacientes conservarán el derecho a cancelación de sus datos sensibles.
>
> 36. Asegurar que, en caso de recurrir a herramientas de vigilancia digital para determinar, acompañar o contener la expansión de la epidemia y el seguimiento de personas afectadas, éstas deben ser estrictamente limitadas, tanto en términos de propósito como de tiempo, y proteger rigurosamente los derechos individuales, el principio de no discriminación y las libertades fundamentales. Los Estados deben transparentar las herramientas de vigilancia que están utilizando y su finalidad, así como poner en marcha mecanismos de supervisión independientes del uso de estas tecnologías de vigilancia, y los canales y mecanismos seguros para recepción de denuncias y reclamaciones.

Como se advierte, son diversos los riesgos asociados a los aplicativos que brindan información sobre el virus o facilitan al usuario un autodiagnóstico. No obstante, es responsabilidad de los Estados y de las empresas brindar gestión correcta de los datos personales de los usuarios de los aplicativos para lograr los objetivos de dar información y atención en la pandemia de forma eficiente y respetuosa de los principios del derecho fundamental a la protección de datos personales.

Es por esta razón que debe reforzarse la garantía del derecho fundamental a la protección de datos personales a través de un adecuado diseño de las herramientas tecnológicas y

de nuevos modelos de gestión de la información, lo que significa que en su desarrollo deben participar no solo expertos en sistemas de información, sino también científicos de datos, especialistas en inteligencia artificial, en bioética, bioderecho y en derechos humanos.

El tratamiento de datos personales en la actual emergencia sanitaria debe tener un objetivo general basado en evidencias científicas, en el que se haya evaluado su proporcionalidad en relación con su eficacia, eficiencia y teniendo en cuenta, de forma objetiva, los recursos organizativos que sean necesarios.

REFERENCIAS BIBLIOGRÁFICAS

Arias, M. (2016). Definiciones a efectos del Reglamento General de Protección de Datos. En J.L. Piñar (Dir.) *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad* (115-134). Reus.

Access Now. (2020). *Recomendaciones para la protección de la privacidad y los datos en la lucha contra el COVID-19*. 28. Disponible en: https://www.accessnow.org/cms/assets/uploads/2020/04/Recomendaciones-para-la-protección-de-la-privacidad-y-los-datos-en-la-lucha-contra-el-COVID-19.pdf

Agencia Española de Protección de Datos (AEPD). (2020). Informe N/Ref. 0017-2020 sobre el tratamiento de datos personales en relación a la extensión del virus COVID-19.

Agencia Española de Protección de Datos (AEPD). (2020a). Informe sobre el uso de las tecnologías en la lucha contra el COVID-19. Un análisis de costes y beneficios.

Agencia Española de Protección de Datos (AEPD). (2018). *Guía Práctica de Análisis de Riesgos en los Tratamientos de Datos Personales sujetos al RGPD* [Guía].

Almada, M., & Maranhão, J. (2021). Voice-based diagnosis of covid-19: Ethical and legal challenges. *International Data Privacy Law*, *11*(1), 63-75. Fecha de consulta: 15 de abril de 2021. Disponible en: https://doi.org/10.1093/idpl/ipab004

Alva, V. (2020). La pandemia COVID-19, distanciamiento social, el uso de tecnologías de la información y comunicación y la falta de la regulación internacional que proteja los datos personales. *Revista Académica de la Facultad de Derecho de la Universidad La Salle*. Fecha de consulta: 28 de junio de 2021. Disponible en: https://repositorio.lasalle.mx/handle/lasalle/1695

Andreu Martínez, B. (2020). Privacidad, geolocalización y aplicaciones de rastreo de contactos en la estrategia de salud pública generada por la COVID-19. *Actualidad Jurídica Iberoamericana* 12, pp. 848-859

Angarita, N. R. (2012). Aproximación constitucional de la protección de datos personales en Latinoamérica. *Revista Internacional de Protección de datos personales*, *13*.

Angarita, N. R. (2010). ¿Tiene Colombia un nivel adecuado de protección de datos personales a la luz del estándar europeo? *International Law: Revista Colombiana de Derecho Internacional*, *8*(16).

Arenas, M. (2020). ¿Testing, Tracing, Isolation? A propósito de las Directrices 04/2020 del Comité Europeo de Protección de Datos. *LA LEY Privacidad*, 4.

Arenas, M. (2020).¿Rastrear o no rastrear? He ahí la cuestión. Las apps de rastreo de contactos y la protección de datos personales. *LA LEY Privacidad*, 5.

Autoridad Nacional de Protección de Datos Personales. (2019). Opinión Consultiva No. 07-2019-JUS/DGTAIPD-DPDP. Limitaciones al consentimiento cuando se de tratamiento a datos relacionados a la salud, de conformidad al artículo 14, numeral 6, de la Ley No. 29733. 06 de febrero.

Biometrix Vox (2020). Biometric Vox inicia una investigación con inteligencia artificial para de tectar COVID19 a través la voz. Disponible en: https://biometricvox.com/blog/general/biometriricvox-inicia-investigacion-inteligencia-artificial-detectar-covid19-por-voz/

Bizberge, A. y Segura, M.S. (2020). Los derechos digitales durante la pandemia COVID-19 en Argentina, Brazil y México. *Revista de Comunicación*. 19 (2) pp. 61- 85.

Buchland Gidumal, J. (2020). ¿Son fiables las aplicaciones de geolocalización? The Conversation. Fecha de consulta: 23 de mayo de 2021. Disponible en: https://theconversation.com/son-fiables-las-aplicaciones-de-geolocalizacion-y-seguimiento-de-contactos-141069

Cascón-Katchadourian, Jesús-Daniel (2020). Tecnologías para luchar contra la pandemia Covid-19: geolocalización, rastreo, big data, SIG, inteligencia artificial y privacidad. Profesional de la información, v. 29, n. 4, e290429. https://doi.org/10.3145/epi.2020.jul.29

Cate, F. H., Cullen, P., & Mayer-Schonberger, V. (2013). Data protection principles for the 21st century.

Corredor, F. A., Suárez, J. C., & Patarroyo, L. J. (2020). Protección De Datos Personales en Sistemas De Monitorización y Vigilancia Masiva De Personas Ante La Pandemia De Covid-19.

Corte Interamericana de Derechos Humanos. (2020). Resolución 1/20: *Pandemia y Derechos Humanos en las Américas*.

Cristea, L. (2018). *La protección de datos de carácter sensible: Historia Clínica Digital y Big Data en Salud*. Bosch.

Cubillos Sánchez, M. C., y Restrepo Rojas, M. A. (2020, diciembre 7). La CoronAPP-Colombia y su política de tratamiento de datos. *Departamento de Derecho Informático*. https://derinformatico.uexternado.edu.co/coroappcolombia/

De', R., Pandey, N., & Pal, A. (2020). Impact of digital surge during Covid-19 pandemic: A viewpoint on research and practice. *International Journal of Information Management*, *55*, 102171. https://doi.org/10.1016/j.ijinfomgt.2020.102171

Domínguez, J. (2020). La necesaria protección de las categorías especiales de datos personales. Una reflexión sobre los datos relativos a la salud como axioma imprescindible para alcanzar el anhelado desarrollo tecnológico frente al COVID-19. *Revista de Comunicación y Salud*, 10(2), pp. 607-624.

European Data Protection Board (EDPB). (2020). Declaración sobre el tratamiento de datos personales en el contexto del brote de COVID-19. Adoptada el 19 de marzo de 2020. Fecha de consulta: 17 de mayo de 2021. Disponible en: https://edpb.

europa.eu/sites/default/files/files/file1/edpb_statement_art_23gdpr_20200602_es_1.pdf

Gómez-Córdoba, A., Arévalo-Leal, S., Bernal-Camargo, D., Rosero de los Ríos, D., Gómez-Córdoba, A., Arévalo-Leal, S., Bernal-Camargo, D., & Rosero de los Ríos, D. (2020). El derecho a la protección de datos personales, tecnologías digitales y pandemia por COVID-19 en Colombia. *Revista de Bioética y Derecho*, *50*, 271-294.

Herrera Bravo, R. (2011). Cloud computing y seguridad: Despejando nubes para proteger los datos personales. *Revista de derecho y ciencias penales: Ciencias Sociales y Políticas*, (17), 43-58.

Lopez, Luis Felipe (2016). *Protección de datos personales: adaptaciones necesarias al nuevo Reglamento europeo*. Francis Lefebvre.

Martinez, Ricard. (2020). A la muerte por protección de datos. Fecha de consulta: 20 de abril de 2021. Disponible en: http://lopdyseguridad.es/a-la-muerte-por-proteccion-de-datos/_

Mendoza Enríquez, O. A. (2018). Marco jurídico de la protección de datos personales en las empresas de servicios establecidas en México: desafíos y cumplimiento. *Revista IUS*, *12*(41), 267-291.

Naciones Unidas. Consejo de Derechos Humanos. (2020). Nota de prensa. COVID-19: los Estados no deben abusar de las medidas de emergencia para reprimir los DDHH. 16 de marzo. Fecha de consulta: 17 de mayo de 2021. Disponible en: https://www.ohchr.org/SP/HRBodies/HRC/Pages/NewsDetail.aspx?NewsID=25722&LangID=S_

Oliver, N., Lepri, B., Sterly, H., Lambiotte, R., Deletaille, S., De Nadai, M., ... & Vinck, P. (2020). Mobile phone data for informing public health actions across the COVID-19 pandemic life cycle. *Sci Adv* 6 (23) Fecha de consulta: 24 de mayo de 2021. Disponible en: https://advances.sciencemag.org/content/advances/6/23/eabc0764.full.pdf

Piñar, José Luis. (2020). La protección de datos durante la crisis del coronavirus. Consejo General de Abogacía Espñola. Fecha de consulta: 20 de abril de 2021. Disponible en: https://www.abogacia.es/actualidad/opinion-y-analisis/la-proteccion-de-datos-durante-la-crisis-del-coronavirus/

Puyol, J. (2016) XI. Los principios del Derecho a la Protección de. En José Luis Piñar (Dir.), *Reglamento General de Protección de Datos*. Madrid, pp. 135-150

Razquín, M. (2019). El necesario equilibrio entre transparencia y protección de datos personales. En Diego Zegarra Valdivia (Coord.), *La proyección del derecho administrativo peruano: estudios por el centenario de la Facultad de Derecho de la PUCP*. Lima, Palestra, pp. 137-164.

Recuero Linares, M. (2020). La compartición internacional de datos personales relativos a la salud en tiempos de la COVID-19: Aspectos éticos y legales para el impulso de la necesaria cooperación. *Revista de Bioética y Derecho*, *50*, 133-146.

Renda, A. (2020). Will privacy be one of the victims of COVID-19?. *Centre for European Policy Studies*. Publicado el 23 de marzo de 2020. Disponible en: https://www.

ceps.eu/will-privacy-be-one-of-the-victims-of-covid-19/

Scheibner, J., Ienca, M., Kechagia, S., Troncoso-Pastoriza, J.R., Raisaro, J.L., Hubaux, J.P:, Fellay, J., & Vayena E. (2020). Data protection and ethics requirements for multisite research with health data: a comoaratove examination of legislative povernance frameworks and the role of data protection technologies. *Journal of Law and the Biosciences, 1-30*. https://doi.org/10.1093/jlb/lsaa010

Van Natta, M., Chen, P., Herbek, S., Jain, R., Kastelic, N., Katz, E., Struble, M., Vanam, V., & Vattikonda, N. (2020). The rise and regulation of thermal facial recognition technology during the COVID-19 pandemic. *Journal of Law and the Biosciences*, 7. https://doi.org/10.1093/jlb/lsaa038

Vásquez Rodríguez, R. (2020). El consentimiento para tratamiento de datos personales de salud en tiempos del covid-19. Yachaq Revista De Derecho, (11), 145-164. https://Doi.Org/10.51343/Yq.Vi11.366

Visbal, J. H. W., Pedraza, M. C. C., & Veliz, D. G. A. (2021). Procedimiento para el uso de pirómetros durante la pandemia por COVID-19: Procedure for the usage of pyrometers during the COVID-19 pandemic. Archivos de Medicina (Manizales), 21(1), 305-308.

Weidenslaufer, C. y Meza, M. (2020). COVID – 19: Uso de apps con rastreo de contactos y respto de contactos y respecto a la privacidad. *Boletín* 10 Biblioteca del Congreso Nacional de Chile / BCN. Disponible en: https://obtienearchivo.bcn.cl/obtienearchivo?id=documentos/10221.1/79593/1/boletin_coronavirus_10.1_FINAL.pdf

Wilches-Visbal, Jorge-Homero, & Castillo-Pedraza, Midian-Clara, & Apaza-Veliz, Danny-Giancarlo (2021). Procedimiento para el uso de pirómetros durante la pandemia por COVID-19. Archivos de Medicina (Col), 21(1), 305-309.

Zegarra, D. (2014). Los principios de la protección de datos personales en el marco de la Ley No. 29733 y su Reglamento. En Jorge Danós Ordóñez y otros (Coords.), *Derecho Administrativo. Innovación, cambio y eficacia. Libro de ponencias del Sexto Congreso Nacional de Derecho Administrativo*. Lima, ECB Ediciones, pp. 623-635.

Zegarra, 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 Diego Zegarra Valdivia (Coord.), *La proyección del derecho administrativo peruano: estudios por el centenario de la Facultad de Derecho de la PUCP*. Lima, Palestra, pp. 165-208.