RECOMENDACIONES DE LA RED IBEROAMERICANA DE PROTECCIÓN DE DATOS (RIPD)

PARA EL TRATAMIENTO DE DATOS PERSONALES SOBRE LA SALUD EN TIEMPOS DE PANDEMIA

2021

Red Iberoamericana
Rede Ibero-Americana

RED IBEROAMERICANA DE PROTECCION DE DATOS

ÍNDICE

01.
GLOSARIO

Para los efectos del presente documento se entenderá por[1]:

- **Anonimización:** la aplicación de medidas de cualquier naturaleza dirigidas a impedir la identificación o reidentificación de una persona física sin esfuerzos desproporcionados.
- **Consentimiento:** manifestación de la voluntad, libre, específica, inequívoca e informada, del titular a través de la cual acepta y autoriza el tratamiento de los datos personales que le conciernen.
- **Coronavirus:** extensa familia de virus que pueden causar enfermedades tanto en animales como en humanos. En los humanos, se sabe que varios coronavirus causan infecciones respiratorias que pueden ir desde el resfriado común hasta enfermedades más graves como el síndrome respiratorio de Oriente Medio (MERS) y el síndrome respiratorio agudo severo (SRAS). El coronavirus que se ha descubierto más recientemente causa la enfermedad por coronavirus COVID-19.
- **COVID-19:** enfermedad infecciosa causada por el coronavirus que se ha descubierto más recientemente. Tanto este nuevo virus como la enfermedad que provoca eran desconocidos antes de que estallara el brote en Wuhan (China) en diciembre de 2019. Actualmente la COVID-19 es una pandemia que afecta a muchos países de todo el mundo.
- **Datos biométricos:** 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;
- **Datos genéticos:** datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona;
- **Datos Personales:** cualquier información concerniente a una persona física identificada o identificable, expresada en forma numérica, alfabética, gráfica, fotográfica, alfanumérica, acústica o de cualquier otro tipo. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente, siempre y cuando esto no requiera plazos o actividades desproporcionadas.
- **Datos personales sensibles:** aquellos que se refieran a la esfera íntima de su titular, o cuya utilización indebida puedan dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico; creencias o convicciones religiosas, filosóficas y morales; afiliación sindical; opiniones políticas; datos relativos a la salud, a la vida, preferencia u orientación sexual, datos genéticos o datos biométricos dirigidos a identificar de manera unívoca a una persona física.
- **Datos relativos a la salud:** datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud;
- **Elaboración de perfiles:** toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona

[1] Las definiciones sobre tratamiento de datos personales fueron tomadas de los Estándares de protección de datos personales para los Estados Iberoamericanos (RIPD) de 2017: https://www.redipd.org/es y 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 (Reglamento general de protección de datos): https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32016R0679#d1e4722-1-1 Los conceptos sobre COVID fueron tomado de la página web de la Organización Mundial de la Salud: https://www.who.int/es

física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física;

- **Encargado:** prestador de servicios, que con el carácter de persona física o jurídica o autoridad pública, ajena a la organización del responsable, trata datos personales a nombre y por cuenta de éste.
- **Exportador:** persona física o jurídica de carácter privado, autoridad pública, servicios, organismo o prestador de servicios situado en territorio de un Estado que efectúe transferencias internacionales de datos personales, conforme a lo dispuesto en los Estándares.
- **Pandemia:** Esla propagación mundial de una nueva enfermedad. Se produce una pandemia de gripe cuando surge un nuevo virus gripal que se propaga por el mundo y la mayoría de las personas no tienen inmunidad contra él. Por lo común, los virus que han causado pandemias con anterioridad han provenido de virus gripales que infectan a los animales.
- **Responsable:** persona física o jurídica de carácter privado, autoridad pública, servicios u organismo que, solo o en conjunto con otros, determina los fines, medios, alcance y demás cuestiones relacionadas con un tratamiento de datos personales.
- **Titular:** persona física a quien le conciernen los datos personales.
- **Tratamiento:** cualquier operación o conjunto de operaciones efectuadas mediante procedimientos físicos o automatizados realizadas sobre datos personales, relacionadas, de manera enunciativa más no limitativa, con la obtención, acceso, registro, organización, estructuración, adaptación, indexación, modificación, extracción, consulta, almacenamiento, conservación, elaboración, transferencia, difusión, posesión, aprovechamiento y en general cualquier uso o disposición de datos personales.
- **Seudonimización:** el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable;

02.
SIGLAS

APD	Autoridad de Protección de Datos
AEMPS	Agencia Española del Medicamento y Productos Sanitarios
Estándares	Estándares de Protección de Datos Personales para los Estados Iberoamericanos aprobados por la RIPD en 2017
Reglamento General de Protección de Datos o RGPD	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
RIPD o Red	Red Iberoamericana de Protección de Datos
TDP	Tratamiento de datos personales

03.
INTRODUCCIÓN

La pandemia de la COVID-19 ha generado mucha incertidumbre y retos a la sociedad. Los datos personales han sido relevantes para adoptar, entre otras, políticas para mitigar los efectos de dicho virus e implementar medidas de bioseguridad.

Los Estados y las empresas han adoptado protocolos de bioseguridad para mitigar, controlar y realizar el adecuado manejo del riesgo de la pandemia por el Coronavirus COVID-19 respecto de diversas actividades, servicios, sectores, procesos, establecimientos y lugares. La implementación de las medidas adoptadas implica la recolección y tratamiento de datos personales.

Dichas medidas no suspenden el derecho fundamental a la protección de datos personales, cuya normativa permanece plenamente vigente y es de obligatorio cumplimiento para los Responsables y Encargados del Tratamiento de Datos Personales.

Estas recomendaciones pretenden establecer los principales aspectos que deben tenerse presente cuando se tratan datos personales en épocas de pandemia. Como tal, presentan algunas orientaciones para que sean tenidas en cuenta por quienes recolectan o usan datos personales.

Para la elaboración de este documento se han tenido en cuenta los *Estándares de protección de datos personales para los Estados Iberoamericanos* de la RIPD[2] como el referente para establecer los principios, términos, definiciones, etc. No obstante, no se transcriben todos los aspectos de los mismos, sino que se hace alusión a algunos de ellos. Por lo tanto, este documento debe leerse de manera conjunta e integral con los citados estándares.

Este texto no es un concepto legal, ni un artículo académico, ni constituye asesoría jurídica. Tampoco pretende ser un listado exhaustivo de recomendaciones específicas porque ello es un asunto interno que corresponde decidir a cada organización a la luz de los objetivos y la magnitud de cada proyecto que implique el tratamiento de datos personales en épocas de pandemia.

[2] Cfr. Red Iberoamericana de Protección de Datos -RIPD- (2017). Estándares de protección de datos personales para los Estados Iberoamericanos. Disponibles en: https://www.redipd.org/sites/default/files/inline-files/Estandares_Esp_Con_logo_RIPD.pdf

04.

BASES JURÍDICOS DEL TRATAMIENTO DE DATOS PERSONALES

La emergencia sanitaria derivada de la pandemia del virus SARS-COV-2, que provoca la enfermedad de la COVID-19, ha generado la necesidad de emplear información personal para atender todo lo relacionado con la misma y, especialmente, mitigar sus efectos adversos sobre las personas y la sociedad.

El tratamiento de información personal se encuentra regulado por normas que reconocen el derecho a la Protección de Datos Personales como un derecho fundamental. Por ello, es imperioso realizar un uso responsable de dicha información, procurando alcanzar equilibrios con otros derechos.

En ese sentido, el tratamiento de los datos personales, realizados con motivo de la COVID-19 deberán observar las bases jurídicas de cada país en que son tratados los datos, conforme a las siguientes consideraciones:

- Tener la certeza de que se están tratando datos personales, es decir, información que hace a una persona física identificada o identificable. Lo anterior toda vez que, si se está frente a datos anónimos, que no permiten la identificación de una persona física, no aplicará la normativa sobre protección de datos personales.
- Se debe tener especial cuidado especial en los datos que han pasado por un tratamiento de seudonimización, ya que este procedimiento permite identificar a una persona mediante la suma de nuevos datos de forma razonable, por lo que es importante tomar en cuenta lo señalado al respecto en diversas normativas regionales[3].
- La mayoría de las legislaciones en la materia, consideran a los datos de salud como datos sensibles o con categorías especiales, por lo que su tratamiento requiere como principio, el cumplimiento de requisitos especiales, en particular, contar con el consentimiento previo, expreso, informado, específico, inequívoco y en su caso, escrito de los titulares de los datos.
- Se debe tener en cuenta que los responsables y encargados legítimos para el tratamiento de datos de salud, son los establecimientos sanitarios públicos o privados, los profesionales vinculados a las ciencias de la salud en cumplimiento de la Ley en la materia, y que de manera expresa se reconozca que la titularidad de la información sobre el estado de salud, corresponde al paciente.
- Se debe considerar que fuera los profesionales vinculados con las ciencias de la salud, el tratamiento y la comunicación de datos de salud deben hacerse con el consentimiento del titular, en las condiciones antes mencionadas o en el marco de alguna de las excepciones establecidas en las leyes de la materia, razones de interés general autorizadas por ley, cuando el organismo solicitante tenga mandato legal para hacerlo, o para finalidades estadísticas o científicas, en este último caso disociado de sus titulares.
- Se sugiere revisar en la legislación doméstica si se encuentra previsto el procedimiento de disociación, el cual consiste en hacer que la información no pueda vincularse a persona determinada o determinable, por lo que debe descartarse cualquier tratamiento con información que pueda volver a vincularse con una persona, salvo cuando la ley expresamente lo permita.
- En ningún caso, los responsables del tratamiento de datos quedan eximidos del cumplimiento de los demás principios generales de la Protección de Datos Personales. Así, los datos recolectados deben ser los mínimos necesarios para el cumplimiento de la finalidad informada y no emplearse para fines distintos o incompatibles con aquellos que motivaron su recolección. Deben adoptarse medidas para garantizar la seguridad y confidencialidad de los datos y otras medidas técnicas y organizativas

[3] RIPD (2017). Estándares de protección de datos personales para los Estados Iberoamericanos. Numeral 5.

comprobables para garantizar un tratamiento acorde a la legislación vigente[4].

- Es fundamental informar al personal del responsable de los datos recabados sobre el cuidado de la información personal y, en su caso, de las consecuencias penales asociadas a la revelación de dicha información. Resulta también conveniente estipular las condiciones para el tratamiento de la información en contratos que se suscriban con los encargados de tratamiento.
- El tratamiento adecuado de los datos personales requiere asegurar el cumplimiento de los derechos de los titulares de los datos, en la forma y en los plazos que prevé la legislación vigente. Debe cumplirse con el derecho a informar previamente del tratamiento a los titulares, con el derecho a la revocación del consentimiento ante el requerimiento del titular afectado y con los derechos previstos en el Capítulo III de los Estándares y los previstos en las respectivas legislaciones nacionales.
- Al momento de llevar a cabo el registro de datos personales, seleccionar las categorías de datos relevantes y adecuadas para el problema que se ha de abordar, vigilando que sean pertinentes, correctos y actualizados.
- Se deberá informar a los titulares de los datos sobre la información de identificación del responsable, qué datos se recaban y con qué fines a través de los medios que estén previstos por la legislación doméstica en la materia.
- El tratamiento deberá limitarse al cumplimiento de las finalidades previamente informado a los titulares de los datos personales.
- Persistentemente se debe velar por el cumplimiento de los principios de protección de datos personales, debiendo adoptar las medidas necesarias para su aplicación.
- Las instituciones y prestadores de servicios de salud públicos y privados deben recabar solamente los datos personales mínimos necesarios para lograr el propósito de implementar medidas para prevenir o contener la propagación de COVID-19 y, en su caso, brindar la atención, diagnóstico y tratamiento médico correspondiente.

[4] RIPD (2017). Op. cit. Capítulo III.

05.

RESPONSABLES Y ENCARGADOS DEL TRATAMIENTO DE DATOS PERSONALES

El tratamiento de datos personales derivado de la emergencia sanitaria por la COVID-19 obliga el establecimiento de las líneas generales para garantizar el debido uso de los mismos conforme a los principios de protección de datos, incluso frente a estas circunstancias excepcionales. Líneas que deberán seguir tanto los responsables como los encargados del tratamiento de los datos, sin que esto signifique una excusa para no realizar todas las medidas necesarias en la lucha contra la pandemia o en sentido contrario, se utilice la emergencia sanitaria para eliminar el derecho a la protección de los datos.

Los responsables y encargados del Sector Público y Privado que traten datos personales relacionados con casos de COVID-19, deberán:

- Contar con estrictas medidas de seguridad administrativas, físicas y técnicas para evitar cualquier pérdida, destrucción, robo, extravío, uso o acceso, daño, modificación o alteración no autorizada, tales como: generación de contraseñas, doble verificación, eliminación de virus, etc.
- Cumplir con los principios y obligaciones establecidos en las leyes en materia de protección de datos personales vigentes, salvo los casos de excepción previstos en las mismas.
- Garantizar la confidencialidad sobre cualquier dato personal o personal sensible relacionado con casos de COVID-19, para evitar daño o discriminación de la persona afectada.
- Adoptar las medidas que considere convenientes para procurar que los datos personales de casos de COVID-19, sean exactos, completos, pertinentes, actualizados y correctos. Toda comunicación que se realice en la organización sobre la posible presencia de la COVID-19 en el lugar de trabajo, no debe identificar a ningún colaborador de forma individual.
- El tratamiento de datos personales ante el COVID-19, debe ser informado y el titular debe conocer en todo momento las finalidades para las cuáles serán recabados y tratados sus datos personales.
- Los responsables podrán tratar, de acuerdo con la normativa aplicable, los datos personales de sus colaboradores que sean necesarios para garantizar la salud de todo su personal y evitar la propagación de COVID-19 en las instituciones y organizaciones.
- Limitar el periodo de tratamiento al tratarse de datos inherentes a la salud de un titular y por ser considerados datos personales sensibles de acuerdo con el marco legal en materia de protección de datos personales.
- Definir los plazos de conservación de los datos personales relacionados con casos de COVID-19, así como los mecanismos que se emplearán para eliminarlos de forma segura, tomando en consideración la normatividad sectorial en la materia.
- Notificar cualquier vulneración de seguridad de datos personales, a los titulares y cuando corresponda, a la Autoridad de Protección de Datos. Adicionalmente, el responsable deberá analizar las causas por las cuales se presentó la vulneración e implementar en su plan de trabajo las acciones preventivas y correctivas para adecuar las medidas de seguridad, en relación con el tratamiento de los datos personales, a efectos de prevenir futuras vulneraciones.
- Evitar la difusión pública no autorizada de información y datos personales de casos -posibles o confirmados- de COVID-19.
- Proteger y evitar la difusión de datos personales de niñas, niños y adolescentes en casos -posibles o confirmados- de COVID-19.
- Implementar medidas de seguridad físicas, técnicas y administrativas en aquellos dispositivos móviles, de almacenamiento, equipos de cómputo y sistemas informáticos que realicen tratamiento de datos personales de casos de COVID-19.
- No divulgar la identidad de los titulares sospechosos o afectados por el COVID-19, evitando la obtención y tratamiento

de información y datos personales que resulten innecesarios, no pertinentes o excesivos.

- Impedir que el tratamiento de los datos personales para brindar información a la sociedad en el ejercicio a la libertad de expresión genere discriminación o conlleve un riesgo grave para sus titulares.

06.

LAS “APPS DE AUTOEVALUACIÓN”

Existe una eclosión de uso de aplicaciones para dispositivos móviles (apps) para muchas finalidades dentro de la cuales se encuentran aquellas para mitigar o controlar la pandemia de la COVID-19. Sin perjuicio de los beneficios del uso de las apps, desde 2013 las autoridades de protección de datos mediante la Declaración de Varsovia sobre la appificación de la sociedad[5] plantearon lo siguiente:

- "Quienes desarrollan estas aplicaciones pocas veces están conscientes de las implicaciones que para la privacidad de las personas tiene su trabajo y no están familiarizados con conceptos tales como "privacidad desde el diseño" y "consecuencias al no optar".
- "Los principales sistemas operativos y las plataformas de las aplicaciones ofrecen algunas opciones de privacidad; pero, no permiten al usuario el control total para una adecuada protección de sus datos personales, tampoco posibilita el verificar qué información es recabada ni cuál el uso que habrá de dársele.

Adicionalmente, en dicha Declaración se manifestó que:

- Es fundamental que los usuarios de las apps estén y sigan estando en control de sus propios datos. Ellos deben ser capaces de decidir qué información compartir, con quién compartirla y para qué fines.
- Los usuarios deben tener la opción de permitir o no el acceso a información específica como los datos de localización o su libreta de direcciones.
- Las aplicaciones deberán desarrollarse conforme al principio de disminuir la aparición de sorpresas para el usuario: excluir características o propiedades ocultas, no recabar datos sin especificar el contexto del acopio.
- Los desarrolladores de las apps deben asegurarse de que sus proyectos propician el cumplimiento de la normativa en materia de protección de datos. Con el fin de lograr este objetivo, y al mismo tiempo mantener una experiencia positiva para el usuario, la privacidad debe tomarse en cuenta desde el inicio del diseño de una aplicación.
- Los desarrolladores necesitan tomar una clara decisión sobre qué información es necesaria para el funcionamiento de la aplicación y deben asegurarse que ninguna información adicional pueda ser recabada de no mediar el consentimiento del usuario. Esto también se aplica cuando el código de un tercero o plug in son utilizados por los desarrolladores de las aplicaciones, por ejemplo, los provenientes de anuncios en las redes.

A continuación, se señalarán los principales aspectos que deben tenerse presentes cuando se utilizan apps con ocasión de la pandemia de la COVID-19 desde la perspectiva de la regulación sobre tratamiento de datos personales. Asimismo, se presentan algunas orientaciones para que sean tomadas en consideración por quienes desarrollan estas aplicaciones.

Neutralidad tecnológica en el tratamiento de datos personales

La regulación sobre tratamiento de datos personales es neutral, tecnológica y temáticamente. Ello significa que aplica a cualquier tratamiento dato con independencia de las técnicas, procesos o tecnologías -actuales o futuras- que se utilicen para dicho efecto. En este sentido, el artículo 4.1 de los Estándares dice que los mismos son "aplicables al tratamiento de datos personales que obren en soportes físicos, automatizados total o parcialmente, o en ambos soportes, ***con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización***".

La neutralidad tecnológica es importante porque cualquier actividad que se realice con datos personales, a través de medios manuales o

[5] Cfr. ICDPPC (2013). "Declaración de Varsovia sobre la appification de la sociedad". En: http://globalprivacyassembly.org/wp-content/uploads/2015/02/Warsaw-declaration-on-Applification-of-society-ES.pdf (Varsovia, Polonia- 24 de septiembre de 2013)

automatizados, con o sin intervención humana, debe observar las reglas establecidas en las normas sobre protección de datos personales.

En suma, la regulación sobre tratamiento de datos personales debe aplicarse al margen de los procedimientos, metodologías o mecanismos que se utilicen para recolectar, usar o tratar ese tipo de información. Por ende, debe ser cumplida por quien realice tratamiento de datos mediante el uso de técnicas, herramientas como, entre otros, en internet de las cosas, las Apps, la inteligencia artificial, la robótica y la computación en la nube. El uso de esas innovaciones tecnológicas debe respetar la protección de datos y evitar convertirse en un instrumento para disminuir el nivel de protección de los derechos de las personas que es exigido por la regulación en comento.

Respetar las normas locales sobre Tratamiento de Datos Personales (TDP)

Los responsables o encargados que desarrollen apps deben tener presente que están obligados a cumplir las normas nacionales sobre tratamiento de datos personales. Lo anterior les permitirá definir una estrategia para, entre otros: (i) mitigar riesgos jurídicos; (ii) ganarganar y mantener la confianza de los titulares de los datos; (iii) no afectar la buena reputación de su organización y (iv) evitar eventuales investigaciones de las autoridades de protección de datos o de otras entidades.

Crear políticas de tratamiento de datos especiales para la pandemia del COVID-19

Por tratarse de un proyecto específico y excepcional que recolectará datos sensibles de millones de personas, se recomienda que se redacte una política de tratamiento de información (PTI) especial para los casos relacionados con el COVID-19.

Para el efecto, se deben tener presentes las exigencias de las regulaciones locales y las recomendaciones de organismos internacionales[6] respecto de la creación de aplicaciones móviles en general y de su uso durante la pandemia del COVID19. Esto redundará en beneficio de los ciudadanos y de las entidades que utilizan apps porque generará mayor confianza en sus usuarios y en el público en general.

Se sugiere que:

- Sean específicas las finalidades del tratamiento de datos;
- La recolección de datos debe limitarse a aquellos que sean pertinentes y adecuados para alcanzar la finalidad específica;
- El tratamiento de datos solo debe ser por el tiempo necesario y razonable para cumplir los objetivos de las apps para prevenir o mitigar la propagación de la COVID-19. Una vez cumplida la finalidad, se deben suprimir los datos. Es necesario documentar los procedimientos para el tratamiento, conservación y supresión de los datos.

Datos de geolocalización y tecnologías de detección de cercanía

Por defecto, los servicios, las tecnologías o infraestructuras[7] destinadas a prestar servicios de geolocalización, las conexiones a bluetooth o sensores de localización estarán desactivadas o desconectadas. Sólo se activarán cuando así lo deseen los usuarios y voluntariamente programe su equipo o dispositivo para dicho efecto. La misma regla se aplicará respecto del uso de tecnologías de detección de cercanía respecto de personas contagiadas con Covid-COVID-19.

[6] Cfr. (1) Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf; (2) Dictamen 02/2013 sobre las aplicaciones de los dispositivos inteligentes https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp202_es.pdf; (3) Dictamen 13/2011 sobre los servicios de geolocalización en los dispositivos móviles inteligentes: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp185_es.pdf ; (4) Buenas prácticas de privacidad para desarrollar aplicaciones móviles: https://www.priv.gc.ca/en/privacy-topics/technology/mobile-and-digital-devices/mobile-apps/gd_app_201210/

[7] Tales como, entre otras, GPS, estaciones de base GSM y WiFi.

No se recopilará información sobre los movimientos y actividades de un usuario mediante el uso de sensores de ubicación (tales como GPS), puntos de acceso WiFi y estaciones de base.

Anonimización de los datos

Una vez que se recolecten los datos personales, por regla general, se deberán utilizar herramientas de anonimización para que la información no esté asociada o vinculada a una persona en particular. En caso de ser necesario circular dicha información, sólo se deberán remitir los datos estrictamente necesarios y anonimizados de tal manera que no se pueda identificar al titular del dato.

Excepcionalmente se tratará la información de forma no anonimizada cuando sea rigurosamente necesario conocer la identidad del titular del dato.

Efectuar estudios de impacto de privacidad

Previo al diseño y desarrollo de las apps se debe efectuar una evaluación de impacto en la privacidad (*Privacy Impact Assessment - PIA* por sus siglas en inglés), con el fin de poner en funcionamiento un sistema efectivo de manejo de riesgos y controles internos, para garantizar que los datos se tratarán debidamente y conforme a la regulación existente aplicable. En este sentido, los Estándares disponen que "*cuando el responsable pretenda llevar a cabo un tipo de tratamiento de datos personales que, por su naturaleza, alcance, contexto o finalidades, sea probable que entrañe un alto riesgo de afectación del derecho a la protección de datos personales de los titulares, realizará, de manera previa, a la implementación del mismo una evaluación del impacto a la protección de los datos personales.*"[8]

Dicha evaluación debería incluir, como mínimo, lo siguiente:

- Una descripción detallada de las operaciones de tratamiento de datos personales que involucra el desarrollo de la app;
- Una evaluación de los riesgos específicos para los derechos y libertades de los titulares de los datos personales, y

Las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad, confidencialidad, diseño de software, tecnologías y mecanismos que garanticen la protección de datos personales, teniendo en cuenta los derechos e intereses legítimos de los titulares de los datos y de otras personas eventualmente afectadas. Los resultados de este estudio, junto con las medidas para mitigar los riesgos, hacen parte de la aplicación del principio de privacidad desde el diseño y por defecto.

Incorporar la privacidad, la ética y la seguridad desde el diseño y por defecto

La privacidad desde el diseño y por defecto (*Privacy by Design and by Default*) es considerada una medida proactiva para cumplir con el Principio de *Accountability*[9], como se observa en los numerales 1 y 2 del artículo 38 de los Estándares de la RIPD. Al incrustar la privacidad desde el diseño, se está buscando garantizar el correcto tratamiento de los datos a través de las apps, incluso antes de la materialización de los riesgos[10].

La Privacidad desde el Diseño "*promueve la visión de que el futuro de la privacidad no puede ser garantizada sólo por cumplir con los marcos regulatorios; más bien, idealmente el aseguramiento de la privacidad debe convertirse en el modo de operación predeterminado de una organización*"[11]. Por eso, desde antes que se

[8] RIPD (2017). Op. Cit. Numeral 41.1
[9] Cavoukian (2011)
[10] Gulbenkoglu (2018)
[11] Cfr. Cavoukia, Ann. Privacidad por Diseño: Los 7 principios fundamentales. Disponible en:

recolecte información y durante todo el ciclo de vida de la misma, se deberían adoptar medidas preventivas de diversa naturaleza (tecnológica, organizacional, humana, procedimental, entre otras) con el objeto de evitar vulneraciones al derecho a la privacidad o a la confidencialidad de la información. Así como fallas de seguridad o indebidos tratamientos de datos personales.

La ética desde el diseño y por defecto debe irradiar el esquema, desarrollo y uso de las apps debiendo ser parte del ADN de cualquier aspecto relacionado con la prestación de dichos servicios. Lo anterior también debe predicarse en la seguridad en el tratamiento de datos mediante la app. Sin seguridad no habrá debido tratamiento de los datos personales. Es fundamental adoptar medidas tecnológicas, humanas, administrativas, físicas, contractuales y de cualquier otra índole que cumplan los siguientes objetivos:

- Evitar accesos indebidos o no autorizados a la información;
- Evitar manipulación de la información;
- Evitar destrucción de la información;
- Evitar usos indebidos o no autorización de la información; y
- Evitar circular o suministrar la información a personas no autorizadas.

Las medidas de seguridad deben ser apropiadas considerando varios factores como entre otros, los siguientes: (i) los niveles de riesgos del tratamiento; (ii) la naturaleza de los datos; (iii) la magnitud del daño que se puede causar a los titulares y al responsable; (iv) la cantidad de información; (v) el tamaño de la organización; (vi) los recursos disponibles y (vii) el monitoreo y seguimiento a la confiabilidad de los servicios de la app. Todas estas deben ser objeto de revisión, evaluación y mejoras permanentes.

Materializar el principio de responsabilidad

Los diseñadores y creadores de productos y apps deben adoptar medidas útiles, apropiadas y efectivas para cumplir sus obligaciones legales. Adicionalmente, tendrán que evidenciar y demostrar el correcto cumplimiento de sus deberes. Dichas herramientas, deben ser objeto de revisión y evaluación permanente, a fin de determinar su nivel de eficacia en cuanto al cumplimiento y grado de protección de los datos personales.

El reto de las organizaciones frente al Principio de Responsabilidad va mucho más allá de la mera expedición de documentos o redacción de políticas. Se trata de una actividad constante, que exige demostrar un cumplimiento real y efectivo en la práctica de sus funciones. No basta hacer meras declaraciones simbólicas de buenas intenciones, sino que es necesario evidenciar resultados concretos respecto del debido tratamiento de los datos personales.

En este aspecto es esencial realizar entrenamientos periódicos y especializados al equipo humano de la organización para proveerles la experticia, guía y herramientas que requieren para el correcto desarrollo de su actividad.

La identificación y clasificación de riesgos, así como la adopción de medidas para mitigarlos, son elementos cardinales del principio de responsabilidad. Es fundamental que las organizaciones desarrollen y pongan en marcha, entre otros, un *"sistema de administración de riesgos asociados al tratamiento de datos personales"*[12] que les permita *"identificar, medir, controlar y monitorear todos aquellos hechos o situaciones que puedan incidir en la debida administración del riesgo a que están expuestos en desarrollo del cumplimiento de las normas de protección de datos personales"*[13].

Adoptar medidas para garantizar los principios sobre el Tratamiento de Datos Personales (TDP) mediante el uso de apps.

Es necesario que los responsables o encargados que desarrollen o usen alguna app (aplicación móvil), prevean estrategias pertinentes y eficientes para garantizar el cumplimiento de los principios sobre tratamiento de datos

[12] SIC (2015). *"Guía para implementación del principio de responsabilidad demostrada (accountability)"*. Págs 16-18.
[13] Ibid. P 16.

contenidos en el Capítulo II de los Estándares de Protección de Datos Personales para los Estados Iberoamericanos emitidos por la RIPD[14].

El alcance de cada principio está determinado en el texto de los "Estándares de Protección de Datos Personales para los Estados Iberoamericanos"[15] de la RIPDP, razón por la cual nos remitimos al mismo para no transcribirlos en este espacio.

Garantizar los derechos de los titulares de los datos e implementar mecanismos efectivos para el ejercicio de los mismos

Los responsables o encargados que desarrollen o contraten los servicios de app deben garantizar los derechos de los titulares de los datos.

El alcance de cada derecho está delineado en el texto de los "Estándares de Protección de Datos Personales para los Estados Iberoamericanos" de la RIPD, razón por la cual se hace una remisión expresa a dicho documento.

[14] Red Iberoamericana de Protección de Datos (2017)
[15] Cfr. RIPD (2017). Op. Cit.

07.

LA TOMA DE TEMPERATURA PARA EL CONTROL DE LA PANDEMIA

En el contexto de la pandemia de la COVID-19 y de la emergencia sanitaria global, la toma de temperatura corporal en los ingresos a edificios o en la vía pública es una medida que organismos públicos o privados de los Estados Iberoamericanos podrían implementar, con el fin de prevenir la propagación de la enfermedad.

Este tipo de control puede tener un impacto en la privacidad o la intimidad de las personas, por lo que es importante que los distintos actores involucrados se comprometan a proteger los datos personales, implementando salvaguardas adecuadas.

Alcance de las Recomendaciones

Cuando un establecimiento público o privado toma la temperatura de una persona, identificada o identificable, ya sea a través de termómetros tradicionales, digitales, cámaras térmicas u otros medios técnicos, está realizando una operación de tratamiento de datos personales que se encuentra alcanzada por los Estándares[16].

En consecuencia, estas Recomendaciones se aplican a toda instancia en que un responsable proceda a tomar la temperatura corporal de las personas.

Teniendo en cuenta que el registro de temperatura, de por sí, afecta a las personas que son objeto de dicho control, vale aclarar que las Recomendaciones aplican independientemente de si el responsable:

- Confecciona un registro de las personas a las que les tomó la temperatura;
- Requiere a las personas identificarse cuando procede a tomar su temperatura.

Dato sensible

La temperatura corporal es un dato de salud considerado sensible, por lo que merece una protección más rigurosa que otras categorías de datos, sobre todo en materia de seguridad de la información[17].

Es de notar que la utilización indebida del dato en cuestión puede dar origen a discriminación o aparejar otros riesgos graves para los derechos de las personas[18].

Por regla general, el responsable de tratamiento no podrá tomar la temperatura de las personas, salvo que se presente alguno de los siguientes supuestos:

- El tratamiento sea estrictamente necesario para el ejercicio y cumplimiento de las atribuciones y obligaciones expresamente previstas en las normas que regulan la actuación de entidades públicas o privadas;
- Se cuente con el consentimiento expreso y por escrito del titular de los datos; y
- El tratamiento se encuentre autorizado por razones de seguridad nacional, seguridad pública, orden público, salud pública o salvaguarda de derechos y libertades de terceros.

En particular, las emergencias sanitarias decretadas de forma local, relacionadas con el COVID-19, podrían autorizar la toma de temperatura en varias instancias con el fin de salvaguardar la salud pública.

La legislación nacional de los Estados Iberoamericanos aplicable en la materia podrá establecer excepciones, garantías y condiciones adicionales para asegurar el debido tratamiento de los datos personales sensibles, de conformidad con su derecho interno[19].

Comercios y establecimientos en la vía pública

En el caso de los comercios, locales y establecimientos en la vía pública, ellos podrían tomar la temperatura de los potenciales ingresantes, siempre y cuando lo hagan de conformidad con lo dispuesto por los protocolos

[16] RIPD (2017). Op. Cit. Literal i) del numeral 2.1.
[17] RIPD (2017). Op. Cit. Literal d) del numeral 2.1.
[18] Ibid.
[19] RIPD (2017). Op. cit. Numeral 9.2.

sanitarios correspondientes, que hayan sido dictados en el marco de la emergencia sanitaria.

Si detectaran que la temperatura corporal supera el umbral definido por las autoridades sanitarias, se podría denegar la entrada al titular de los datos. Ello a fines de garantizar la seguridad y proteger la salud de todos los ingresantes.

Empleadores

Tanto en el sector público como en el privado, los empleadores podrían tomar la temperatura de sus empleados en el ingreso. Si detectasen que la temperatura corporal supera el umbral definido por las autoridades sanitarias, el empleador podría denegarle la entrada al titular de los datos. Ello a fines de garantizar la seguridad y proteger la salud del resto de los trabajadores.

Organismos públicos que reciben visitantes

En el caso de los organismos públicos que reciben personas que desean realizar trámites o interponer denuncias, la toma de temperatura estará permitida en la medida en que esté debidamente reglamentada por protocolos sanitarios, en el marco de las leyes y decretos locales de la emergencia sanitaria.

El mismo criterio es aplicable a los controles en el transporte público, centros de transbordo, vía pública y espacios verdes.
Resulta recomendable que los organismos públicos en los que se interpongan denuncias relacionadas con la afectación de derechos fundamentales provean medios digitales alternativos al ciudadano para poder presentar sus reclamos y consultas.

Cámaras térmicas y otras herramientas de tratamiento automatizado

Cuando algún organismo público o privado planee utilizar cámaras térmicas u otras herramientas automatizadas que permitan detectar la temperatura corporal, deberá asegurar una instancia de revisión humana. Sobre todo, si el tratamiento automatizado apareja alguna consecuencia significativa para la persona cuya temperatura está siendo captada[20].

Asimismo, y con independencia de que el responsable sea un organismo público o privado, cuando se tomen decisiones basadas únicamente en el tratamiento automatizado de datos que perjudiquen a las personas o los afecten significativamente de forma negativa, las personas tendrán derecho a solicitar al responsable de la base de datos una explicación sobre la lógica aplicada en aquella decisión[21].

En todos los supuestos, el titular de datos podrá, en su caso, oponerse al tratamiento automatizado de su temperatura corporal cuando[22]:

- Tenga una razón legítima derivada de su situación particular.
- El tratamiento de sus datos personales tenga por objeto la mercadotecnia directa, incluida la elaboración de perfiles, en la medida que esté relacionada con dicha actividad.

En la medida en que sea viable, se recomienda al responsable de tratamiento de datos personales realizar una evaluación de impacto de manera previa a la implementación de la herramienta automatizada, con el fin de controlar y mitigar sus riesgos[23].

Dicha evaluación de impacto podría realizarse conforme otros documentos emanados de autoridades o especialistas en la materia[24].

Principios fundamentales de protección de datos personales

En todos los casos, se deben respetar los principios fundamentales en materia de

[20] RIPD (2017). Op. cit. Numerales 29.1 y 29.4
[21] RIPD (2017). Op. cit. Numeral es 29.2 y 25.1.
[22] RIPD (2017). Op. cit. Numeral 28.1
[23] RIPD (2017). Op. cit. Numeral 41.

protección de datos personales. En particular:

- El dato de temperatura corporal no puede ser utilizado para finalidades distintas o incompatibles con aquellas que motivaron su obtención[25].
- La toma de temperatura corporal debe ser pertinente y no excesiva en relación con el lugar y los fines para los que se realiza[26].
- Los datos deben ser destruidos cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubiesen sido recolectados[27].
- En el caso de los empleadores y los organismos públicos que reciben visitantes, puede ser necesario dejar asentado a qué persona se le denegó la entrada al establecimiento para justificar que no se ha interferido arbitrariamente con sus derechos.
- En el caso de los locales en la vía pública, la toma de temperatura corporal es inmediata y no es necesario que el dato quede guardado en un registro.
- En los casos en los que el responsable del tratamiento no almacene la información sobre los controles de temperatura, se deberá aclarar a través de cartelería[28]:

  - Quién es el responsable y cuál es su domicilio legal.
  - Por qué razones se realiza el control y cuáles son las consecuencias de la toma de temperatura.
  - Que la información referida al control de temperatura no será almacenada.
  - Qué normativa resulta de aplicación y ante qué autoridad pueden interponerse denuncias en caso de vulneración de los derechos de los titulares de datos.

- En los casos en los que el responsable del tratamiento sí almacene la información, se deberá informar lo siguiente a través de cartelería[29]:

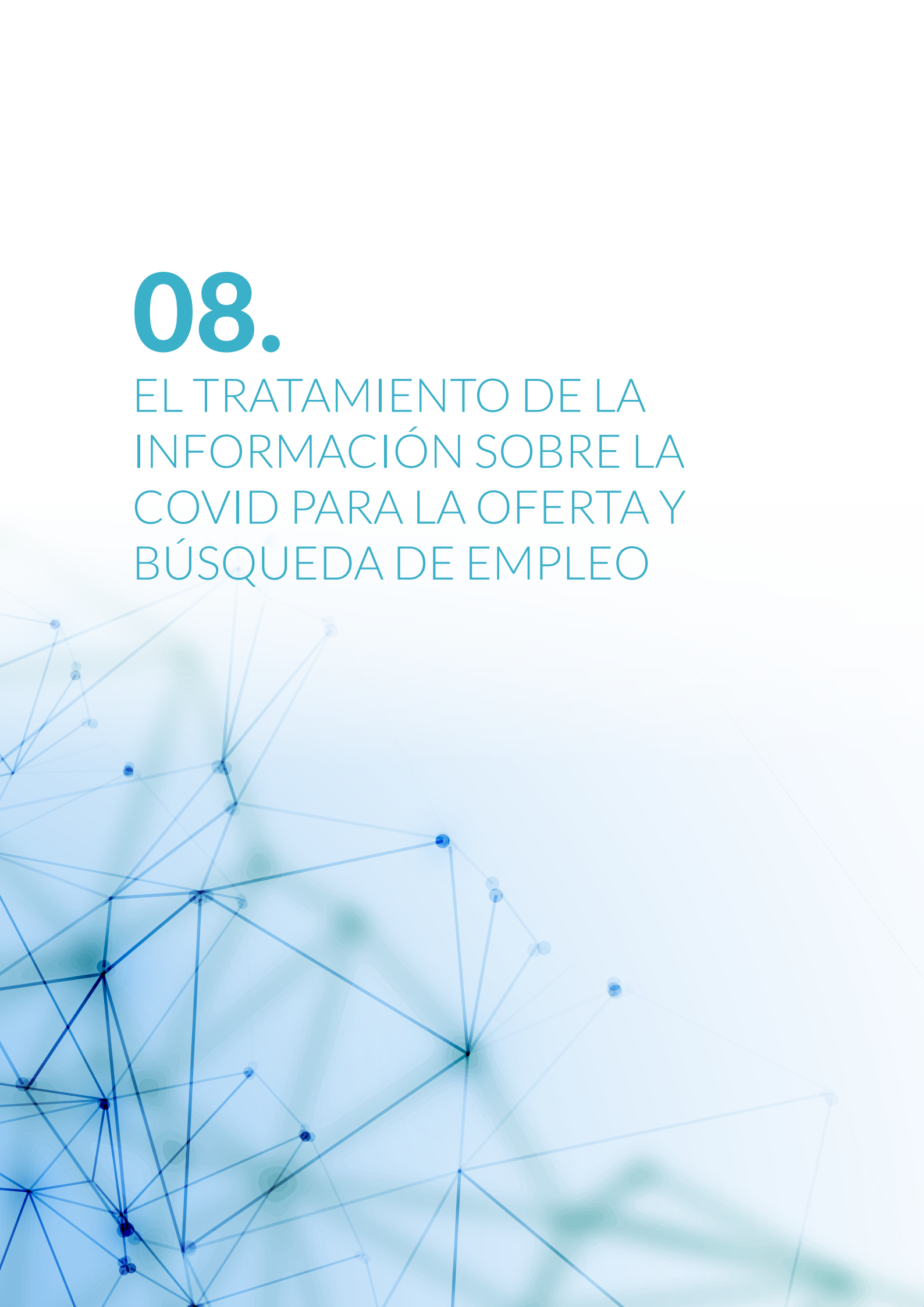
  - Quién es el responsable y cuál es su domicilio legal.
  - Por qué razones se realiza el control y cuáles son las consecuencias de la toma de temperatura.
  - Que la información referida al control de temperatura será almacenada, aclarando durante cuánto tiempo.
  - Si la información registrada será cedida a terceros y, en su caso, quienes son los posibles destinatarios.
  - Qué normativa resulta de aplicación, aclarando que el titular del dato puede ejercer sus derechos de acceso, rectificación y supresión, y que el responsable de tratamiento puede ser denunciado ante la autoridad competente.

- En el caso en que se forme un registro compuesto de datos de temperatura corporal, los datos total o parcialmente inexactos, o que sean incompletos, deben ser suprimidos y sustituidos, o en su caso completados, por el responsable del archivo o base de datos cuando se tenga conocimiento de la inexactitud o carácter incompleto de la información de que se trate[30].

[24] p. ej. la Guía de Evaluación de Impacto en la Protección de Datos elaborada de forma conjunta por la Agencia de Acceso a la Información Pública de Argentina y la Unidad Reguladora y de Control de Datos Personales de la República Oriental del Uruguay.
[25] RIPD (2017). Op. cit. Numeral 17
[26] RIPD (2017). Op. cit. Numeral 18
[27] RIPD (2017). Op. cit. Numeral 19.2.
[28] RIPD (2017). Op. cit. Numeral 16
[29] Loc. cit..
[30] RIPD (2017). Op. cit. Numeral 19.1

08.

EL TRATAMIENTO DE LA INFORMACIÓN SOBRE LA COVID PARA LA OFERTA Y BÚSQUEDA DE EMPLEO



La información sobre la COVID-19 y el desarrollo de anticuerpos es un dato de salud calificado en los Estándares, dentro de las categorías especiales de datos, cuyo tratamiento está prohibido, como regla general; prohibición que puede exceptuarse en algunos casos obteniendo el consentimiento del interesado o siendo necesario para la ejecución de un contrato o precontrato[31].

Sin embargo, la recogida del dato de salud y la utilización de dicha información por la empresa carece de base jurídica y es ilícita si no se observan las pautas previstas en los Estándares.

En relación con la base jurídica del consentimiento, hay que señalar que no sería libre, cuando no puede negarse o retirarse sin consecuencias negativas para la obtención del puesto de trabajo.

La relación contractual tampoco puede ser una base jurídica adecuada, ya que no se trata de un empleado y, aunque lo fuera, va más allá de los derechos y obligaciones de la normativa laboral.

Por otra parte, el tratamiento de datos no responde a una finalidad legítima, cuando esa información se utiliza para generar una diferencia de trato sin justificación objetiva y razonable.

[31] Consultar asimismo el numeral 9 de los Estándares.

09.

LA LEGITIMACIÓN PARA EL CONTROL POR LAS FUERZAS Y CUERPOS DE SEGURIDAD EN LAS SITUACIONES DE CONFINAMIETO OBLIGATORIO

La normativa aplicable a la pandemia de COVID-19 prevé medidas especiales en materia de salud pública, que legitima la adopción de medidas apropiadas por parte de las autoridades sanitarias para el control de enfermos o personas de contacto en caso de epidemia.

En consecuencia, la base jurídica de estas transferencias a las Fuerzas y Cuerpos de seguridad sería el interés público y la garantía de intereses vitales de los afectados y de terceros para permitir la adopción de medidas por las autoridades sanitarias.

No obstante, la transferencia debe cumplir los principios de minimización, proporcionalidad y finalidad, por lo que ha de limitarse a los datos necesarios para la identificación de los confinados y de su domicilio o lugar de residencia. No podría incluir otros datos de salud, como son los incorporados a la historia clínica.

Adicionalmente, las Fuerzas y Cuerpos de seguridad deben cumplir con las garantías de confidencialidad conlleva la obligación de guardar secreto respecto de los datos personales que son tratados a fin de evitar causar un daño a su titular por informar a terceros.
Y, una vez cumplida la finalidad del tratamiento, las Fuerzas y Cuerpos de seguridad no deben conservar los datos, salvo en la medida en que lo exija una obligación legal.

10.

EL USO DE LOS DATOS DE LOCALIZACIÓN Y LAS APPS DE SEGUIMIENTO Y RASTREO DE CONTACTOS EN EL CONTEXTO DE LA PANDEMIA

En lo que refiere al rastreo de contactos, se trata de sistemas incorporados en las aplicaciones móviles que permiten monitorear los movimientos de las personas según áreas geográficas y determinar vínculos de proximidad entre ellas. A través de este monitoreo, se procura, idealmente, realizar mediciones, predicciones y análisis en apoyo a la implementación de políticas públicas, con el objeto de evitar la propagación de la pandemia.

En el contexto de la pandemia, distintas autoridades sanitarias a nivel global plantearon la conveniencia de desarrollar aplicaciones que incluyan dichos sistemas para monitorear los movimientos de las personas según áreas geográficas y determinar vínculos de proximidad entre personas infectadas y personas sanas. En el primer caso con el fin de realizar predicciones y controlar la expansión, y en el segundo, para informar a potenciales infectados de forma que adopten las medidas necesarias para asegurar su salud.

En relación a las especificaciones técnicas vinculadas al almacenamiento de la información de contacto, se distinguen sistemas con almacenamiento centralizado y los que descentralizan su operación, almacenando la información de contacto en los propios dispositivos de los usuarios.

El informe del Comité Europeo de Protección de Datos N° 4/2020 señala que los datos de ubicación necesarios para el funcionamiento de los sistemas de rastreo de contactos pueden provenir de proveedores de servicios de comunicaciones electrónicas o de aplicaciones que requieren el uso de dichos datos, recolectados por proveedores de servicios de la sociedad de la información.

Las distintas aplicaciones móviles cuentan con otras funcionalidades vinculadas a la provisión de información general sobre la pandemia, el auto-monitoreo del estado de salud, y mecanismos de telemedicina, entre otras. Adicionalmente, dichas aplicaciones solicitan información personal de naturaleza sensible, por lo que se impone su uso responsable, adecuado y ponderado, atento a los riesgos que importan para la privacidad de las personas.

En cualquier caso, cabe precisar que la aplicación de sistemas de rastreo de contacto y su inclusión en otras aplicaciones en desarrollo requiere un análisis de ponderación entre el derecho y el deber a la salud y el derecho a la protección de datos personales.

En ese sentido, corresponde recordar que la comunicación de datos personales por razones sanitarias o de emergencia corresponde se efectúe, de principio en forma disociada, habilitando la identificación del titular del dato en circunstancias particulares, fuera de las cuales se requerirá el consentimiento del titular del dato. Si los datos son obtenidos de operadores de telecomunicaciones deberá tenerse presente la existencia de regímenes especiales para la salvaguarda de dichos datos que garanticen la privacidad y la protección de los datos en términos de las normas jurídicas de los países que lleven a cabo este tipo de procedimientos.

Por su parte, cabe destacar que el monitoreo a gran escala de los contactos de las personas no posee una base legal que lo habilite salvo el previo consentimiento informado. Además, el tratamiento de estos datos podrá realizarse exclusivamente por el período de duración de la emergencia sanitaria, en el marco de una política de mitigación de la pandemia, y bajo el estricto control y responsabilidad de la autoridad sanitaria, quien deberá actuar en el marco de sus funciones legalmente establecidas.

En ese sentido, deben tenerse presentes los principios de protección de datos personales contenidos en las legislaciones correspondientes, así como garantizar el efectivo ejercicio de los derechos de los titulares de los datos, explicitados en forma general en los Estándares de Protección de Datos para los Estados Iberoamericanos expedidos por la Red Iberoamericana de Protección de Datos (artículos 10 a 23 y 24 a 32 respectivamente).

Adicionalmente, el tipo de tratamiento realizado ameritará la adopción de medidas de responsabilidad proactiva específicas.

En función de lo expresado, pueden realizarse las siguientes recomendaciones:

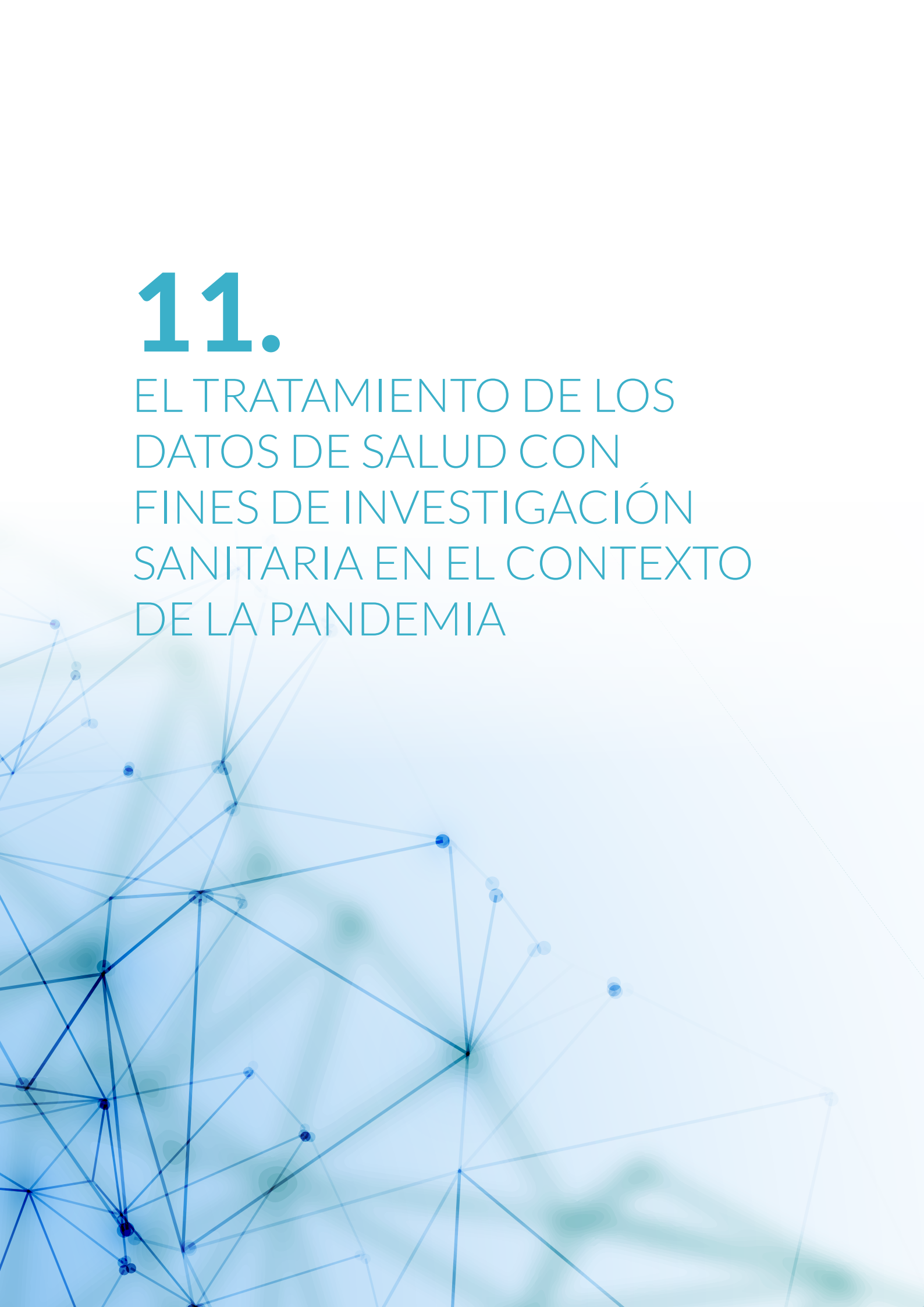
- En cuanto a los sistemas de rastreo de contactos, aconsejar los que implican un almacenamiento descentralizado de los datos por resultar menos invasivos para la privacidad de las personas.
- Señalar la pertinencia de realizar en forma previa una evaluación de impacto en protección de datos; el cumplimiento en su caso de deberes formales como -en los regímenes en que se encuentra previsto- la inscripción de la base de datos personales; y la suscripción de acuerdos que garanticen el cumplimiento de la normativa en caso en que se aplique sistemas provistos por terceros, así como analizar y evaluar especialmente los aspectos técnicos vinculados con seguridad.
- En caso de que el rastreo de contactos se adicione como funcionalidad a aplicaciones preexistentes que recolecten otro tipo de información, deberán extremarse las medidas de seguridad, atendiéndose otras alternativas en el marco de la necesaria evaluación de impacto a la protección de datos.
- Corresponde asegurarse la obtención del consentimiento previo y expreso de los usuarios mediante la descarga y aceptación de términos de la aplicación, o en caso de que se agregue como funcionalidad a aplicaciones pre-existentes, de las nuevas funcionalidades y actualizaciones que se propongan incluir en el sistema.
- Deberá establecerse una adecuada granularidad del consentimiento ante distintas acciones propuestas a los titulares de los datos, y prever la posibilidad que éstos puedan revocar su consentimiento para el uso del rastreo de contacto, aún sin tener que eliminar la aplicación.
- Procede asegurarse que el sistema sólo pueda ser aplicado por la Autoridad de salud pública en el marco de la emergencia sanitaria en calidad de responsable de tratamiento de datos, y con fines de alertar a potenciales contagiados, del contacto con una persona positiva por COVID-19. Adicionalmente, no debe emplearse para realizar un monitoreo individual de los usuarios.
- La información debe almacenarse en centros seguros. En casos debidamente justificados de transferencias internacionales, deberá cumplirse con los requisitos que prevea la normativa correspondiente al respecto. Los respaldos deberán cumplir con las recomendaciones indicadas y ser eliminados en las mismas condiciones que las bases originales.
- En caso de conservarse información en forma centralizada –fuera de los dispositivos de los usuarios- se debe contar con los mecanismos de seguridad pertinentes para evitar incidentes y ser eliminada una vez cumplida la función para la cual fue recolectada.
- En caso de que se agregue el rastreo de contacto a una aplicación preexistente, mantenerse independiente la información vinculada a éste de la que resulte de otras funcionalidades de la aplicación.
- No deberá proporcionarse información personal de casos positivos a potenciales contagiados por la enfermedad; tal información sólo puede remitirse a la autoridad de salud pública con el consentimiento expreso del titular del dato y a efectos del seguimiento de su situación de salud.
- Cuando el rastreo de contactos se adicione a una aplicación preexistente, la comunicación de confirmación de un caso positivo debe efectuarse con el consentimiento expreso del titular del dato.
- Deberán ponerse a disposición de los interesados las especificaciones de la aplicación a efectos de garantizar un tratamiento transparente de los datos y un eventual consentimiento informado. En particular, especificarse la forma de habilitar o deshabilitar el rastreo de

contactos y la información sobre el uso de bluetooth; si ésta se adiciona a una aplicación preexistente, deberá aclararse expresamente y en forma separada las condiciones de tratamiento de otras funcionalidades de la aplicación.

- Procede informarse expresamente a los titulares de los datos sobre situaciones de potencial contagio y los parámetros de tiempo y distancia, así como eventuales modificaciones, en el marco de la necesaria y permanente transparencia.
- Deberá minimizarse la recolección de información, en especial cuando refiere a informaciones de terceros; en su caso, estas sólo podrán remitirse a la autoridad de salud pública para su gestión conforme los protocolos que se elaboren al respecto, manteniéndose separadas de la información derivada del rastreo de contactos.
- Deberá eliminarse toda la información finalizada la emergencia sanitaria, salvo circunstancias especiales debidamente acreditadas.
- La información recolectada debe ser periódicamente revisada en función de los objetivos específicos considerando un

11.

EL TRATAMIENTO DE LOS DATOS DE SALUD CON FINES DE INVESTIGACIÓN SANITARIA EN EL CONTEXTO DE LA PANDEMIA



La pandemia de COVID-19 ha exigido grandes esfuerzos de investigación científica con el fin de hacer frente a la misma en diversos ámbitos, desde el epidemiológico hasta la obtención de vacunas que permitan hacer frente a la pandemia.

Ante esta situación, el Comité Europeo de Protección de Datos adoptó las Directrices 03 /2020, sobre el tratamiento de datos relativos a la salud con fines de investigación científica en el contexto del brote COVID-19.
Las directrices analizan las excepciones que serían aplicables respecto de la prohibición general de tratamiento de los datos de salud como categorías especiales de datos de conformidad con el Reglamento General de Protección de Datos (RGPD). En este marco, señala que serían de aplicación las excepciones relacionadas con el ámbito de la salud pública y con fines de investigación (artículo 9. 2. i) y j) RGPD), añadiendo que las legislaciones nacionales pueden adoptar disposiciones específicas con arreglo a estas bases jurídicas para legitimar el tratamiento de los datos.

Respecto de las bases jurídicas del tratamiento, las directrices señalan que, con carácter general, se encontrarán en los motivos de interés público y el ejercicio de poderes públicos sin necesidad de que concurra el consentimiento de los interesados. No obstante, el consentimiento sería una base jurídica adecuada en algunos casos (por ejemplo, para participar en una encuesta como parte de un estudio no intervencional sobre población, que busca detectar los síntomas de una enfermedad y determinar su evolución).

En todo caso, las directrices insisten reiteradamente en que debe garantizarse que el consentimiento sea libre y pueda revocarse en cualquier momento.

Adicionalmente destacan, en el marco del modelo de cumplimiento proactivo del RGPD, que debe analizarse la pertinencia de llevar a cabo una evaluación de impacto en la protección de datos personales teniendo en cuenta los riesgos que plantea el tratamiento de datos en el contexto de la pandemia.

Las directrices reiteran que debe cumplirse con el principio de transparencia y el derecho de información Informando individualmente a los interesados sobre el tratamiento de datos personales con fines científicos. Información qué debe facilitarse también cuando los datos no han sido obtenidos del interesado. En este último supuesto las directrices hacen referencia a las posibles exenciones al deber de informar analizando específicamente las relacionadas con el esfuerzo desproporcionado para facilitar la información y los casos en que esta exigencia pueda suponer un obstáculo grave para el logro de los objetivos de la investigación.

Para definir los periodos de conservación, las directrices indican que deben ser proporcionados teniendo en cuenta criterios, tales como la duración de la investigación y su finalidad. Pero admitiendo que las legislaciones nacionales puedan establecer normas específicas sobre el período de almacenamiento. En relación con los derechos de los interesados, las directrices parten de la afirmación de que no se suspenden ni restringen en la situación de la pandemia de COVID- 19, aunque admitiendo que puedan ser limitados por la legislación nacional siempre que se establezcan garantías adecuadas.

Por último, el Comité reconoce que en el contexto de la pandemia es probable que haya una necesidad de cooperación internacional que implique transferencias internacionales de datos sanitarios con fines de investigación científica fuera del espacio económico europeo, tanto a terceros países como a organizaciones internacionales. Y concluye que, en ausencia de una decisión de adecuación, podrán realizarse por ser necesarias por razones excepcionales de interés público en la perspectiva de que, tan pronto como sea posible, se adopten las cláusulas contractuales tipo.

En el caso de España, cabe destacar como realidades de investigación específicamente

relacionadas con la pandemia de COVID-19, la Orden SND/404/2020, de 11 de mayo, de medidas de vigilancia epidemiológica de la infección durante la fase de transición hacia la nueva normalidad. La Orden establece la obligación de cesión, así como la utilización posterior por el Ministerio de Sanidad, de datos de pruebas diagnósticas de PCR y de su resultado por todo tipo de laboratorios públicos y privados.

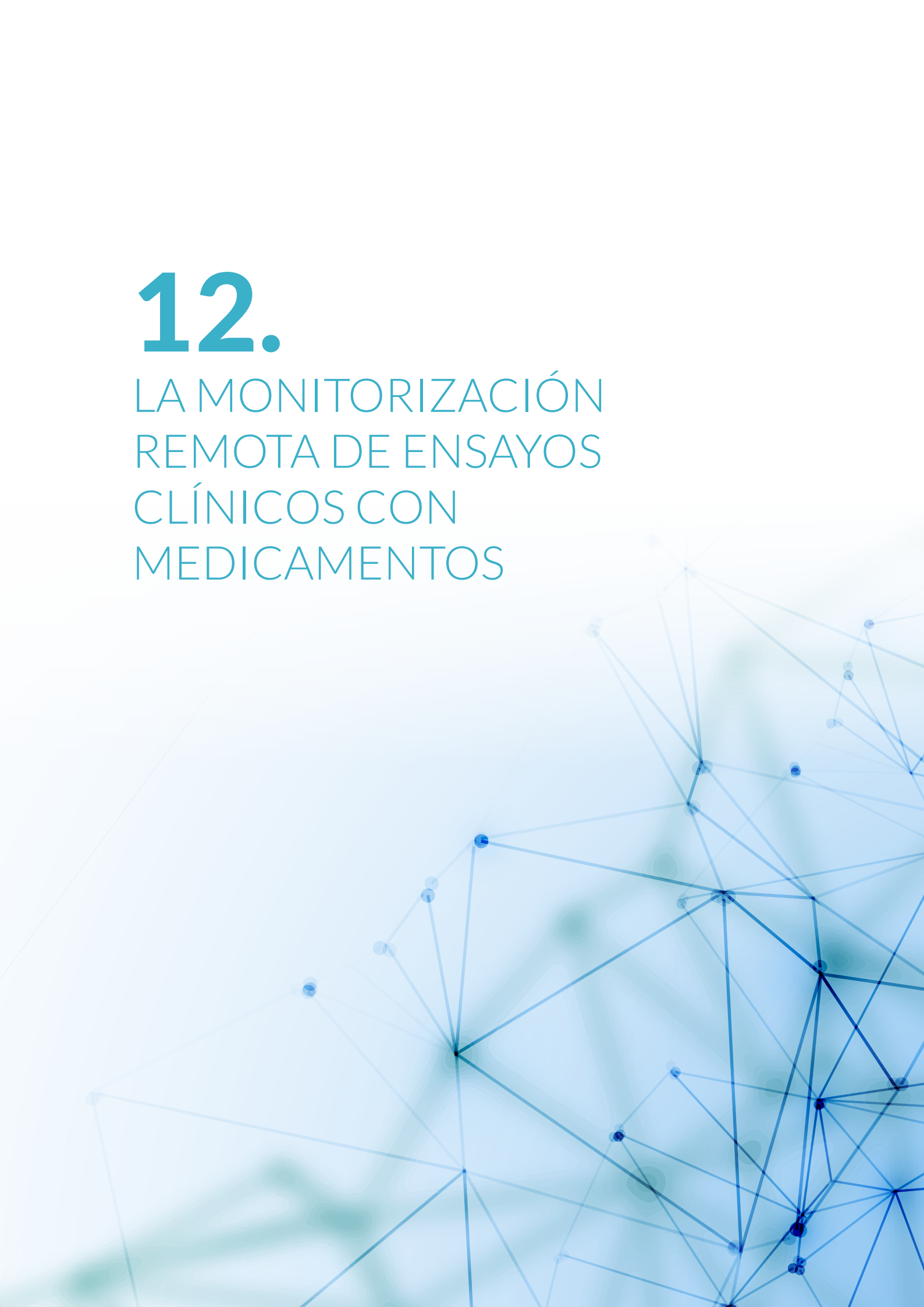
Y la Resolución de la Dirección General de Salud Pública de 16 de diciembre de 2020 por la que se establece el Sistema de Información para el seguimiento de la vacunación frente a la COVID-19. En ella se prevé la obligación de remitir al Ministerio de Sanidad diariamente los datos relativos a las vacunaciones administradas. El tratamiento de esta información será exclusivamente estadístico y de georreferenciación, previo proceso de seudonimización de los datos personales.

Adicionalmente, la resolución contempla la creación de un sistema de información separado con datos identificativos de los vacunados para la finalidad exclusiva de que, si cada interesado vacunado voluntariamente lo solicita, expresa e inequívocamente, pueda obtener un certificado de la vacunación. Este sistema de vacunación se custodiará, separado del anterior con las medidas de seguridad del Esquema Nacional de Seguridad.

La resolución incorpora garantías para el tratamiento ulterior por terceros de los datos del certificado señalando que, a fin de evitar usos indebidos y posibles situaciones de discriminación, el tratamiento se realizará de acuerdo con lo dispuesto en el RGPD, haciendo constar específicamente esta advertencia en los certificados emitidos.

12.

LA MONITORIZACIÓN REMOTA DE ENSAYOS CLÍNICOS CON MEDICAMENTOS



En respuesta a una consulta de Farmaindustria, la Agencia elaboró un informe admitiendo la posibilidad remota de ensayos clínicos con medicamentos durante la pandemia de COVID-19. Monitorización que responde a la necesidad de garantizar el desarrollo de determinados ensayos clínicos y, en todo caso, la salud de los sujetos participantes. El resultado final de la consulta se fundamenta en una novación del contrato inicial entre el promotor y el centro del ensayo y dos anexos: un compromiso de confidencialidad entre el promotor y el monitor y un protocolo de seguridad de conexión remota.

La monitorización remota se refiere únicamente a las circunstancias actuales de la COVID-19, siguiendo las directrices de la Agencia Española del Medicamento y Productos Sanitarios (AEMPS) para implementar la monitorización remota con verificación de datos fuente en las categorías de ensayos clínicos para los que se estén realizando.

Se acompaña una adenda al contrato firmado por el promotor con el centro donde se realiza la investigación, que incluye dos anexos:

- Anexo 1. Compromiso de confidencialidad del monitor.
- Anexo 2. Protocolo de seguridad de conexión remota.

Se describen la posición jurídica del promotor y del monitor, así como sus obligaciones conforme al Reglamento (UE) 536/2014, sobre ensayos clínicos de medicamentos de uso humano, así como del Real Decreto 1090/2015, de 4 de diciembre, por el que se regulan los ensayos clínicos con medicamentos.

El promotor es el responsable del tratamiento y el monitor un encargado del tratamiento debiéndose incorporar las garantías sobre protección de datos personales mediante un contrato u otro acto jurídico.

El primero de los documentos presentados es una adenda al contrato suscrito entre el promotor y el centro en el que se está realizando el ensayo clínico.

Se trata, por tanto, de una novación modificativa y no extintiva de un contrato preexistente en el que deben figurar todos los requisitos exigidos por la normativa de ensayos clínicos para la realización del mismo.

De ahí, que la valoración que ha realizado la Agencia Española de Protección de Datos se limite, exclusivamente, a las garantías aportadas para llevar a cabo la monitorización remota de los ensayos clínicos.

En la parte expositiva se destaca la habilitación por parte del centro para la utilización de un sistema de acceso remoto a la información necesaria para ejercer las labores de monitorización del ensayo.

Estas labores incluyen la verificación de datos fuente, como alternativa a la monitorización presencial, en el marco de un sistema que podrá ser utilizado para dicho ensayo en tanto la situación sanitaria derivada por la emergencia por la pandemia de la COVID-19 en España así lo requiera, conforme a los criterios de la AEMPS.

Adicionalmente, en dicha cláusula, el promotor garantiza, como responsable del tratamiento de los datos del ensayo clínico, que el monitor llevará a cabo sus funciones conforme a los procedimientos normalizados de trabajo, accediendo únicamente a la información estrictamente necesaria para la realización de sus funciones (principio de minimización). Y, a tal efecto, suscribe con el monitor, encargado del tratamiento de los datos, el acuerdo de confidencialidad que consta como Anexo I.

Asumiendo, la plena responsabilidad de las consecuencias que pudieran derivarse de dicho incumplimiento, entre las que estarían en su caso, las relacionadas con la normativa de protección de datos personales.

El compromiso de confidencialidad incluye,

sintéticamente, las siguientes obligaciones:

- El cumplimiento de la normativa de protección de datos personales.
- Actuar conforme a los procedimientos normalizados de trabajo establecidos por el promotor, accediendo únicamente a la información estrictamente necesaria (principio de minimización).
- Cumplir la totalidad de medidas establecidas en el protocolo de seguridad.
- Llevar a cabo la monitorización garantizando que no se produce el acceso por parte de terceros no autorizados a la información utilizada.
- Utilizar únicamente el dispositivo facilitado por el promotor, evitando la utilización de equipos informáticos de uso personal o a los que pudieran tener acceso a terceros.
- Cumplir las garantías que se detallan en relación con las redes y canales utilizados para la ejecución de las labores de monitorización.
- Tratar la información en nombre y por cuenta del promotor y de conformidad con sus instrucciones escritas, sin que pueda utilizarla para otras finalidades (encargado del tratamiento), evitando facilitar al promotor datos identificativos de los afectados.
- No conservar copia alguna en ningún soporte del material, información y/o documentación a la que tenga acceso en el marco de sus funciones.
- Notificar al centro y colaborar con él en la gestión de los incidentes de seguridad que pudieran producirse en el plazo de 24 horas siguientes a haber tenido constancia de ellos. Así como notificar al promotor la brecha de seguridad, si bien excluyendo datos personales de los afectados.
- Llevar a cabo personalmente labores de monitorización y si fuese necesaria la intervención de otro monitor o co-monitor, notificarlo al centro. El nuevo monitor o co-monitor deberán firmar, con carácter previo, idéntico compromiso de confidencialidad.
- Permitir que el centro pueda verificar en cualquier momento el cumplimiento de las obligaciones descritas, suspendiéndose automáticamente el acceso a la información en caso de incumplimiento.

Por su parte, el protocolo de seguridad de la conexión remota para el entorno de monitorización de los ensayos clínicos incluye garantías detalladas sobre los requerimientos de administración de acceso para el monitor; la arquitectura y conexión propuesta; el cifrado; la gestión de "Logs" y auditoría; la gestión de vulnerabilidades; los requerimientos sobre el equipo a utilizar que deberá ser únicamente el que se le hubiera facilitado, no permitiéndose la instalación de ningún componente de software y el entorno de trabajo.

13.
TRABAJO A DISTANCIA

Como parte de las medidas de control adoptadas, para evitar la propagación de COVID-19, las organizaciones e instituciones de los diversos sectores, en los casos que así lo permitan, han adoptado esquemas de trabajo a distancia también llamado teletrabajo.

Ante esta situación es importante considerar medidas para proteger la información y datos personales que serán tratados en este esquema temporal de trabajo, a continuación, algunas recomendaciones:

10.1. Personal / Trabajadores

- Concientizar al personal sobre la responsabilidad de proteger la integridad, confidencialidad y disponibilidad de la información y datos personales que tratarán para continuar con sus actividades en la modalidad de trabajo a distancia.
- Cumplir con las medidas de seguridad físicas y técnicas establecidas por la organización, para la protección de la información y datos personales.
- Cerrar la sesión del equipo de cómputo o sistemas de información cuando no se utilice, tanto en casa como en lugares públicos.
- Conocer los canales de comunicación en donde se podrá reportar cualquier incidente que comprometa o afecte la seguridad de la información y/o datos personales.
- Realizar respaldos de la información y/o datos personales de forma regular, para garantizar su disponibilidad.

10.2. Acceso a la red y servicios de nube

- Utilizar los servicios de nube y las redes de confianza de la organización.
- Cumplir con las políticas y procedimientos sobre acceso a la red, servicios de nube, usuarios, contraseñas, intercambio y respaldo de información.
- Usar un canal seguro siempre que se utilice una red pública para conectarse, por ejemplo, una VPN (Red Privada Virtual).
- En caso de requerir acceso a la red de la organización, para operar sistemas de información, administrar recursos tecnológicos de forma remota o consultar información de la intranet, se sugiere utilizar una VPN.
- Realizar una revisión física para verificar que los elementos de red funcionen correctamente (modem, cableado, corriente eléctrica, intensidad de la señal).

10.3. Correo electrónico

- Cumplir con las políticas de la organización relacionadas con el uso de correo electrónico.
- Usar las cuentas de correo electrónico de trabajo en lugar de cuentas personales para correos electrónicos relacionados con actividades laborales que traten datos personales.
- Si es estrictamente necesario utilizar cuentas de correo electrónico personales para enviar datos personales o información confidencial adjunta, ésta deberá estar cifrada.
- Evitar incluir datos personales o información confidencial en el asunto del correo electrónico.
- Antes de enviar un correo electrónico verificar que la dirección del destinatario sea correcta, especialmente en casos donde se envíen datos personales y/o sensibles.
- Verificar que el entorno donde se utilice el correo electrónico sea seguro, para evitar que personas no autorizadas tengan acceso a datos personales o información.

10.4. Dispositivos móviles (equipos de cómputo, tabletas electrónicas y smartphones).

- Instalar medidas de seguridad que protejan a los dispositivos móviles de cualquier software malicioso que pueda

comprometer la información y datos personales que éstos almacenan.
- Asegurarse que los dispositivos que se utilicen para tratar datos personales o información de la organización cuenten con las últimas actualizaciones instaladas.
- Verificar que el entorno donde se utilicen los dispositivos móviles sea seguro, para evitar su pérdida o extravío, así como la exposición de datos personales o información a personas no autorizadas.
- Establecer medidas para bloquear el acceso a los dispositivos en donde se realizará el tratamiento de datos personales o información, a través de un código, patrón o huella.
- Usar medidas para controlar el acceso a los dispositivos, aplicaciones o servicios, tales como contraseñas robustas, autenticación de múltiples factores y/o cifrado para restringir el acceso al dispositivo y reducir el riesgo de que se comprometa la seguridad de los datos personales o información.
- Implementar medidas para el borrado remoto de dispositivos en caso de pérdida, robo o extravío.
- Cumplir con las políticas de la organización relacionadas con el uso de dispositivos móviles (tabletas electrónicas, smartphones o laptop).

10.5. Empleadores

- Se recomienda definir las responsabilidades y obligaciones que asumirán las personas empleadas bajo la modalidad de teletrabajo.
- Contar con estrictas **medidas de seguridad administrativas, físicas y técnicas** para evitar cualquier pérdida, destrucción, robo, extravío, uso o acceso, daño, modificación o alteración no autorizada.
- Cumplir con los **principios, deberes y obligaciones** establecidos en las leyes en materia de protección de datos personales vigentes, salvo los casos de excepción previstos en las mismas.
- Proteger la **confidencialidad** sobre cualquier dato personal o personal sensible relacionado con cualquier caso de COVID-19, para evitar daño o discriminación de la persona afectada.
- Adoptar las medidas que considere convenientes para procurar que los datos personales de casos de COVID-19, sean **exactos, completos, pertinentes, actualizados y correctos**.
- Toda comunicación que se realice en la organización sobre la posible presencia de COVID-19 en el lugar de trabajo, **no debe identificar** a ningún colaborador de forma individual.
- El tratamiento de datos personales ante el COVID-19, debe **ser informado** y el titular debe conocer en todo momento las finalidades para las cuáles serán recabados y tratados sus datos personales. Previo al tratamiento, el responsable deberá poner a disposición del titular el **aviso de privacidad** correspondiente.
- Los responsables podrán tratar, de acuerdo con la normativa aplicable, los **datos personales de sus colaboradores** que sean necesarios para garantizar la salud de todo su personal y evitar la propagación de COVID-19 en las instituciones y organizaciones.
- Limitar el **periodo de tratamient**o al tratarse de datos inherentes a la salud de un titular y por ser considerados datos personales sensibles de acuerdo al marco legal en materia de protección de datos personales.
- Definir los plazos de **conservación de los datos personales** relacionados con casos de COVID-19, así como los mecanismos que se emplearán para eliminarlos de forma segura, tomando en consideración la normatividad sectorial en la materia.
- Notificar cualquier vulneración de seguridad de datos personales, a los titulares y de forma adicional para el Sector Público, a la Autoridad de Protección de Datos que corresponda.
- Implementar **medidas de seguridad físicas,**

técnicas y administrativas en aquellos dispositivos móviles, de almacenamiento, equipos de cómputo y sistemas informáticos que realicen tratamiento de datos personales de casos de COVID-19.

- Capacitar al personal sobre las principales amenazas y consecuencias a las que pueden verse afectados en caso de hacer mal uso del equipo o de la información que los empleados poseen.

Red Iberoamericana
Rede Ibero-Americana

RED IBEROAMERICANA DE PROTECCION DE DATOS