RUEDA ABADI PEREIRA
CONSULTORES

Dr. José Miguel Ordiozola Perrone -Delegado de Protección de Datos certificado en España de acuerdo al Esquema AEPD-DPD

¿Puede el derecho a la protección de datos personales significar un obstáculo a la adopción de medidas de excepción y de ciertas iniciativas tecnológicas gubernamentales para evitar la propagación y combatir el Virus COVID-19?

La respuesta en nuestra opinión, necesariamente debe ser negativa.

Uruguay es un país que en materia de protección de datos personales goza del mejor prestigio a nivel internacional. En el 2012 fue declarado "adecuado" en la Protección de Datos por la Unión Europea; fue el primer país no europeo que suscribió y ratificó el Convenio 108 del Consejo de Europa para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal y su Protocolo Adicional (Ley No. 19.030) y; tuvo una activa participación en la formulación y adopción de los Estándares de la Red Iberoamericana de Protección de Datos Personales (RIPD).

La limitación al derecho a la protección de datos en situaciones excepcionales como lo es la emergencia sanitaria declarada por el Virus COVID-19, no implica en medida alguna, la desaplicación de la normativa que regula ese derecho. Por el contrario, implica la necesidad de recurrir y considerar las previsiones ya existentes en la legislación y la Constitución para situaciones excepcionales como la que vivimos actualmente, especialmente, cuando los datos involucrados refieren a la salud de las personas, que son datos calificados como "sensibles" y que por tanto, requieren los más altos estándares de protección.

Nuestra ley de Protección de Datos Personales (No. 18.331), establece como principio general que ninguna persona puede ser obligada a proporcionar datos sensibles y que éstos sólo podrán ser objeto de tratamiento con el consentimiento expreso y escrito del titular (art. 18).

Esta regla reconoce sin embargo excepciones generales, tales como que los datos sensibles pueden ser recolectados y objeto de tratamiento cuando medien razones de interés general autorizadas por ley, o cuando el organismo solicitante tenga mandato legal para hacerlo, así como el tratamiento con finalidades estadísticas o científicas cuando se disocien de sus titulares (art. 18). También existen algunas excepciones particulares, por ejemplo, para los datos de salud, admitiéndose su comunicación sin consentimiento del titular cuando esa comunicación sea necesaria por razones sanitarias, de emergencia o para la realización de estudios epidemiológicos, preservando la identidad de los titulares de los datos mediante mecanismos de disociación adecuados cuando ello sea pertinente (arts. 17, lit.c).

En Uruguay, el 13/03/2020 el Poder Ejecutivo declaró por Decreto No. 93/020, el estado de emergencia nacional sanitaria como consecuencia de la pandemia originada por el Virus COVID-19.

En los días siguientes, las autoridades presentaron y disponibilizaron la aplicación **Coronavirus UY**, con funcionalidades que en una primera etapa permitirían detectar remotamente posibles casos de infectados con solo responder el usuario a un cuestionario, lo que evitaría que las personas que tengan dudas respecto de su estado de salud, concurran a los centros sanitarios. Se habló también de una segunda etapa de esta App con funciones más avanzadas, entre las que se mencionó - al menos en algún momento-, el empleo de la tecnología de geolocalización para el seguimiento y control de los pacientes que hayan sido confirmados como infectados.

También en estos días se conoció un **Proyecto de Ley que incluye la enfermedad Covid-19 en el listado de enfermedades profesionales de la Ley No. 16.074 para el personal sanitario del sector privado mientas dure la emergencia sanitaria**. Este proyecto - que ya cuenta con media sanción- prevé la formación en el Ministerio de Salud Pública (MSP) de un registro con datos personales de pacientes asistidos que hayan sido confirmados como infectados por el virus COVID-19 y del personal sanitario que estuvo en contacto con los mismos, a efectos de poder verificar el nexo causal y dar trámite a la prestación bajo cobertura del BSE. Por el inciso final del artículo 1ro. de este proyecto de ley, se obliga a los prestadores de salud del sector privado a transferir a dicho registro del MSP los datos sensibles referidos, tanto de sus pacientes como de sus dependientes.

Aun cuando en este trabajo no vamos a realizar un análisis exhaustivo acerca de si en estos dos ejemplos citados, los tratamientos de datos personales sensibles involucrados son legítimos, más adelante realizaremos algunas consideraciones puntuales sobre los mismos.

Interesa sí a estos efectos destacar que, con fecha 20 de marzo de 2020, la Unidad Reguladora y de Control de Protección de Datos (URCDP) emitió el Dictamen No. 2/2020, donde concluye que en la situación de emergencia sanitaria declarada por el Decreto No. 93/020, el tratamiento de datos de salud relacionados directamente con la misma, puede realizarse sin el consentimiento informado de los titulares en el marco de las excepciones previstas en la propia ley de protección de datos.

Con la consideración de esta opinión de nuestra autoridad de control reflejada en el dictamen antes citado y la de las experiencias de derecho comparado que se dirán, el abordaje de este trabajo tiene como objetivo plantear que en términos generales, una afectación del derecho a la protección de datos personales en tiempos de una situación de emergencia sanitaria como la que vivimos, es legítima.

En los análisis particulares, como señalamos, tal legitimidad dependerá de si la afectación concreta la privacidad que implica la medida dispuesta o la tecnología empleada, tanto en

forma como en sustancia, tiene cabida en nuestro derecho, considerando el contexto particular. En este sentido cabe tener presente que no basta con considerar la posibilidad de legitimar el tratamiento en otras bases jurídicas distintas al previo consentimiento informado, sino que hay que considerar como impacta la situación de excepción en los otros aspectos del tratamiento, teniendo en cuenta todos los principios y los derechos que confiere la protección de datos a los titulares, aspecto que también destaca la URCDP en el dictamen referido, con acertado enfoque.

La protección de datos personales es un derecho humano y por tanto, está comprendido en el art. 72 de la Constitución Uruguaya. Pero tanto este derecho como otros derechos humanos pueden ser limitados en su protección en determinadas condiciones, como lo establece la Constitución Nacional con carácter general y, en particular para este derecho en concreto, la propia ley de Protección de Datos Personales, No. 18.331.

Ha de verse que aun en los países con los sistemas de protección de datos más garantistas como es el caso de los nucleados en la Unión Europea, existe consenso general entre los distintos actores, que tales limitaciones son aceptables y que de hecho, ya están previstas en los ordenamientos jurídicos respectivos, tal como es el caso del propio Reglamento General de Protección de Datos (RGPD) de la UE.

Respecto al tema del tratamiento de los datos personales en tiempos del Virus COVID-19, la Agencia Española de Protección de Datos (AEPD) hizo público un informe de su Gabinete Jurídico (No. 0017/2020)[1] que – además de un riguroso análisis normativo – establece dos premisas generales que resumidamente señalan: a) que la normativa de protección de datos personales, en tanto dirigida a salvaguardar un derecho fundamental, se aplica en su integridad a la situación actual, dado que no existe razón alguna que determine la suspensión de derechos fundamentales y; b) que dicha normativa ya contiene las salvaguardas y reglas necesarias para permitir legítimamente los tratamientos de datos personales en situaciones, como la presente, en que existe una emergencia sanitaria de alcance general.

Con relación concretamente al empleo de Apps de autoevaluación y eventualmente, de seguimiento por geolocalización de infectados, la Agencia Española de Protección de Datos (AEPD) publicó el 26/03/2020 en redes y en su web un informe[2], del cual nos interesa destacar las siguientes afirmaciones:

a) "… las finalidades para las que pueden tratarse los datos son, únicamente, las relacionadas con el control de la epidemia, entre ellas, las de ofrecer información sobre el uso de las aplicaciones de autoevaluación realizadas por las administraciones públicas o la

1 https://www.aepd.es/es/documento/2020-0017.pdf
2https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/aepd-apps-webs-autoevaluacion-coronavirus-privacidad

obtención de estadísticas con datos de geolocalización agregados para ofrecer mapas que informen sobre áreas de mayor o menor riesgo…";

b) "… Únicamente podrán tratar dichos datos las autoridades públicas competentes para actuar conforme a la declaración del estado de alarma, es decir, el Ministerio de Sanidad y las Consejerías de Sanidad de las Comunidades Autónomas, que podrán cederse datos entre ellas, y a los profesionales sanitarios que traten a los pacientes o que intervengan en el control de la epidemia..."

c) "… En cuanto a la previsión de que todos aquellos ciudadanos que hayan dado positivo en la prueba del COVID-19 puedan ser geolocalizados a través del teléfono móvil que hayan facilitado previamente, de modo que se pueda llevar a cabo un seguimiento de su cuarentena, hay que partir de nuevo de las amplias competencias que en situaciones excepcionales, como sin duda lo es la presente epidemia, tienen las autoridades sanitarias, teniendo en cuenta, además, que una de las medidas excepcionales para la gestión de la situación de crisis sanitaria ocasionada por el COVID-19 es la de limitar la libertad de circulación de las personas…"

d) "… No obstante, el único dato que a los efectos de la geolocalización debería facilitarse a los operadores de telecomunicaciones, en su caso, sería el correspondiente al número de teléfono móvil que se tiene que geolocalizar, salvo que el Ministerio de Sanidad considerara que fuera imprescindible facilitar algún otro dato a los efectos del seguimiento de la enfermedad…."

También en España - como informa el Diario El País de Madrid del 21/03/2020 -, un grupo de 60 expertos que incluye abogados y especialistas en privacidad y en ética de datos, suscribieron recientemente una carta pública[3] al gobierno de ese país, apoyando el uso de tecnología durante la crisis del Virus COVID-19, aun cuando ello pueda afectar en alguna medida el derecho a la protección de datos personales.

Este grupo de expertos consideró que el tratamiento de datos personales aun en este contexto de excepción, debe cumplir al menos con tres requisitos: 1) que sea seguro y proporcional a la necesidad; 2) que la conservación de los datos en el periodo de crisis tenga un objetivo y un límite, por lo que deben ser eliminados cuando el peligro termine, con la sola excepción del aprovechamiento científico de su análisis para mejorar la respuesta en crisis futuras y; 3) que el desarrollo de las herramientas sea cuidadoso con los datos, estableciendo medidas garanticen que los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas.

En cuanto a la posibilidad de transpolar estas conclusiones al ordenamiento jurídico uruguayo, debe reconocerse que aun cuando éste fue inspirado en la normativa europea,

3 https://elpais.com/tecnologia/2020-03-21/expertos-en-privacidad-admiten-que-la-crisis-permite-un-uso-excepcional-de-datos-personales.html?prm

no son completamente coincidentes y existen previsiones muy importantes en el RGPD que no están expresamente recogidas en nuestro derecho y obligan en algún caso a esfuerzos interpretativos, para aplicar en Uruguay algunos de sus institutos por vía de los principios generales.

De cualquier forma, nosotros consideramos que en términos generales, las opiniones y los conceptos vertidos respecto del caso de España, son conceptualmente trasladables al caso de Uruguay, lo cual, coincide en lo sustancial con las conclusiones de nuestra autoridad de control (URCDP), vertidas en el Dictamen No. 2/2020.

En este sentido y con base en lo que dispone la propia Constitución y la Ley No. 18.331, cabe concluir que el derecho a la protección de datos personales en Uruguay no puede significar un obstáculo para que las autoridades competentes adopten las decisiones que la presente situación de emergencia sanitaria exige, siempre que tales medidas sean necesarias, proporcionadas, fundadas, transparentes y con la consideración de la privacidad - desde su diseño – como derecho humano.

Teniendo en cuenta esta premisa, la legitimidad de algunas medidas recientemente adoptadas en Uruguay no dependerá solamente de considerar que en la excepcionalidad de la situación – ya prevista en nuestra legislación – es posible realizar tratamientos incluso de datos personales sensibles, sin el consentimiento del titular de los datos. Hace falta más.

En el caso de la **APP Coronavirus UY**, el hecho de que su instalación dependa de la voluntad del usuario, implica un consentimiento y ello nos liberaría - en principio – de buscar otra base de legitimación para el tratamiento de datos que implica su uso.

Distinto es el caso del tratamiento de datos sensibles que implica la ejecución del mecanismo previsto en el **Proyecto de Ley que incluye temporalmente la enfermedad Covid-19 en el listado de enfermedades profesionales de la Ley No. 16.074 para el personal sanitario del sector privado**, donde si bien por las razones analizadas en este trabajo, podría admitirse el tratamiento de los datos de salud sin el consentimiento de los titulares, la legitimidad del mismo requeriría también de otras consideraciones.

Destacamos en primer lugar, considerar si es necesario realizar este tratamiento excepcional de datos de salud considerando su finalidad. Cierto es que la Ley No. 16.074 establece cierta rigideces, pero cabe preguntarse si en esta situación excepcional que considera el proyecto de ley: ¿es imprescindible identificar el paciente infectado atendido para establecer el “nexo causal” con el personal sanitario que contrajo la enfermedad a efectos de otorgarle la prestación por enfermedad profesional? o; ¿en la excepcionalidad de la situación, no bastaría con acreditar que en el período estimado de contagio el trabajador sanitario se encontraba prestando servicios en una entidad de salud privada donde se asistieron a pacientes contagiados?.

Como comentario general de las dos iniciativas en análisis, consideramos que existe cierta falta de transparencia en varios aspectos importantes de los tratamientos de datos personales que involucran, si bien ello podría tener alguna justificación en la urgencia con la que se adoptan las medidas en la situación actual.

En el caso de la App, para que el consentimiento sea válido es necesario que el usuario haya sido debidamente informado al momento de recolectar los datos (cumpliendo con lo previsto en el art. 13 de la Ley 18.331). Y en este sentido, es de destacar que el usuario al registrarse para utilizar la APP accede a unos términos y condiciones donde se informan los principales datos del tratamiento. Lo criticable es que a posteriori no hay ninguna opción de menú o link que permita al usuario acceder a esos términos nuevamente. La transparencia debe aplicarse durante todo el ciclo de vida de los datos.

Por otro lado, tampoco se establece al usuario una opción clara y accesible desde el menú de la App para darse de baja de dicho registro, aspecto que resulta fundamental cuando el tratamiento de datos está basado en el consentimiento.

Estos dos aspectos negativos mencionados de la App, sin duda que obstaculizan el ejercicio de los derechos de los titulares de los datos, quienes deberían en todo momento poder acceder a los términos de privacidad y también deberían desde el mismo menú de la aplicación, de una forma sencilla – tan sencilla como registrarse - poder darse de baja al registro.

En el caso del mecanismo previsto en el proyecto de ley que implica un tratamiento de datos personales de salud, sería recomendable que en la propia norma se establecieran algunas cuestiones fundamentales tales como una delimitación clara de la finalidad del uso de la información sensible, período de conservación, condiciones de destrucción o de archivo con valor de dicha información y referencias a la seguridad de todo el proceso, aportando la mayor transparencia al uso excepcional de datos sensibles previsto.

Y para ambas iniciativas hay también otras obligaciones que resultan exigibles a las entidades públicas responsables de los tratamientos que fueron impuestas por la reforma introducida en la materia por los artículos 39 y 40 de la ley 19.670, que no sabemos si fueron cumplidas.

En este sentido, cumpliendo con la obligación de practicar una “responsabilidad proactiva” es exigible a los responsables que hayan aplicado las medidas recomendadas en el estándar de “Privacidad desde el Diseño y Por Defecto” desde la concepción misma de los tratamientos y que en forma previa a su inicio hayan analizado los riesgos, así como realizado una evaluación de impacto en la protección de datos personales (EIPD), ya que conforme a lo recientemente reglamentado en el Decreto 64/020, las operaciones de tratamiento previstas en estas iniciativas, cumplen los requisitos que hacen obligatoria la realización de una EIPD (art. 6).

También por tratarse los responsables de entidades públicas, conforme a lo previsto en el art. 40 de la Ley 19.670, resulta obligatorio contar con el asesoramiento especializado de un Delegado de Protección de Datos (DPD)[4] tanto en el diseño de los tratamientos como en la EIPD que previamente debió realizarse, brindando el asesoramiento de su área de especialización.

Si bien puede pensarse que aplicar estas medidas de responsabilidad proactiva puede atentar contras las urgencias del caso, no necesariamente es así (ni por el factor tiempo ni por el factor complejidad) y la aplicación del estándar de la "Privacidad desde el Diseño y Por Defecto" así como la realización una EIPD, son herramientas realmente útiles a la hora de definir los controles para salvaguardar la privacidad en un justo equilibrio con la finalidad de estos tratamientos fundados en razones de interés general. Consideramos que en AGESIC y en la URCDP existen asesores muy calificados para apoyar estas iniciativas públicas aportando su conocimiento técnico para poder utilizar estas herramientas y dar mayores garantías, aun con la celeridad que amerita la situación.

En este sentido y como reflexión final, es necesario considerar que más allá de las urgencias que están justificadas por el estado de emergencia sanitaria, cuando el tratamiento de datos personales sensibles tiene legitimación en razones de interés general, es imprescindible que el Estado y las entidades públicas responsables apliquen la mayor transparencia en todos los aspectos del uso a los datos (lo cual ya es una obligación legal), asegurando a los ciudadanos que se hará un uso ético de su información personal, en la estricta medida de lo necesario para afrontar la situación excepcional y con garantías para los titulares de los datos.

0/0/0/0/0

4 Lo expuesto es sin perjuicio de que el art. 14 del Decreto 64/020 – reglamentario del art. 40 de la Ley 19.670 - confiere un plazo que vence el 21/05/2020 para designar el DPD a todas aquellas entidades que al momento de la entrada en vigencia de dicho decreto, ya cumplan las condiciones que las obligaban a tal designación. Si bien ese plazo se confiere sin distinción alguna, es de destacar que esta obligación rige desde enero de 2019, y en el caso de las entidades públicas la propia ley determinó con total claridad que estaban todas obligadas a designar un DPD (a diferencia de las entidades del sector privado donde podía haber alguna duda), por lo cual, no hay ninguna justificación para que las entidades del sector público no hubieran designado sus DPD aun antes de la reglamentación, cumpliendo el art. 40 de la Ley 19.670.