

LOS RETOS DE LA PROTECCIÓN DE DATOS PERSONALES ANTE LA PANDEMIA DEL CORONAVIRUS COVID 19 (SARS-COV2)

The challenges of the protection of personal data in the face of the pandemic of the Coronavirus Covid 19 (SARS-CoV2)

Omar Delgado Chávez¹

Recepción: 25 de mayo 2020
Aceptación: 29 de mayo de 2020
Pp: 85-106



Sumario: **1.** ¿Qué son los datos personales? **2.** La pandemia y la actuación de las instituciones de transparencia, acceso a la información y protección de datos. **3.** La pandemia y la nueva correlación de protección de datos personales. **4.** ¿Problemáticas futuras o correcciones oportunas? **5.** Panorama internacional respecto a la protección de datos y la pandemia. **6.** A manera de conclusión. **7.** Fuentes de información.

Resumen

El mundo se encuentra en plena contingencia. México no es la excepción. Muchos aspectos diarios han sufrido cambios y otros apenas se han acoplado. La protección de datos refleja el único espacio que trasciende fuera de los hogares y lugares de confinamiento, mucho derivado del Internet. ¿Qué se ha hecho? ¿Están seguros si antes, con el menor tráfico de datos en las redes cibernéticas, existían robos de identidad, suplantación o un uso malicioso de los mismos?

¹ Abogado por la Universidad de Guadalajara. Maestro en Derecho Electoral por el Instituto Prisciliano Sánchez del otrora Tribunal Electoral del Poder Judicial del Estado de Jalisco. Secretario de Estudio y Cuenta de la Sala Regional Guadalajara del Tribunal Electoral del Poder Judicial de la Federación. Correo electrónico: omar.delgado@te.gob.mx.

ENSAYOS

Los retos de la protección de datos personales ante la pandemia del coronavirus COVID-19-(SARS-CoV2)

La pandemia representa un reto nacional y global en garantizar este derecho humano de libre información y, a su vez, de protección de datos personales. Debemos saber qué se hace y si ello es suficiente, o bien habrá que mejorar. Estamos ante un nuevo panorama con viejas reglas. ¿Saldremos airosos?

Palabras claves

Pandemia, datos personales, protección, derechos humanos, riesgos

Abstract

The world is in full contingency. Mexico is not the exception. Many daily aspects have undergone changes and others have barely been coupled. Data protection reflects the only space that transcends outside of homes and places of confinement, much derived from the Internet. What has been done? Are you sure if before, with the least data traffic on cyber networks, there was identity theft, spoofing or malicious use of the same? The pandemic represents a national and global challenge in guaranteeing this human right to free information and, in turn, to the protection of personal data. We must know what to do and if it is enough, or we will have to improve. We are facing a new panorama with old rules. Will we succeed?

Keywords

Pandemic, personal data, protection, human rights, risks.

INTRODUCCIÓN

Más allá del derecho electoral, en estos tiempos en que estamos en pleno confinamiento ante la contingencia del Covid-19, se han tomado diversas medidas para garantizar la protección de datos personales, como el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), quien habilitó una sección especial en Internet para este tipo de casos, el cual brinda información y asesoría al respecto.

Va enfocado a los particulares pero también a los sujetos obligados en dicho tratamiento, como son las autoridades electorales.

Pero, ¿será todo lo que habrá de realizarse para que, ante la vorágine de avances tecnológicos y aplicaciones “app” garanticen nuestros datos? ¿Permaneceremos estáticos como se pide en esta autodenominada “cuarentena” o podrán reactivarse algunas actividades del Estado, principalmente de administración y procuración de justicia?

1. ¿QUÉ SON LOS DATOS PERSONALES?

Antes, quisiera exponer un tema relacionado a la protección de datos, consistente en la transparencia proactiva, la cual se contempla en la Ley General de Transparencia y Acceso a la Información Pública, al definirla como un conjunto de actividades que promueven la identificación, generación, publicación y difusión de información adicional o complementaria a la establecida con carácter obligatoria por dicha ley; y su objetivo es generar conocimiento público útil, con un objeto claro, enfocado en las necesidades de sectores de la sociedad, determinados o determinables (artículos 56, 57 y 58 de la Ley General)².

Dicha figura ha sido recogida en otras legislaciones, una de las cuales la define como aquella que, sin ser una obligación de ley, promueva, difunda y publique información útil para fomentar la calidad de vida, participación pública, toma de decisiones y el empoderamiento de las personas (siendo este un principio de apertura institucional previsto en los artículos 106 al 110 la Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México).

Entonces, en esta pandemia hay una obligación y potestad de las autoridades o sujetos obligados a brindar la mayor cantidad posible de información, dicho coloquialmente, ir más allá de su deber.

Esta información pudiera implicar obtenerla de los propios datos proporcionados por los particulares.

El derecho a la protección de los datos o derecho a la autodeterminación informativa, adquiere concreción jurisprudencial en la decisión conocida como “Censo de Población” del Tribunal Constitucional alemán: “...el libre desarrollo de la personalidad presupone, en las modernas condiciones para el procesamiento de datos, la protección de los individuos frente a la ilimitada recolección, archivo, empleo y retransmisión de sus datos personales... El derecho fundamental garantiza de esta manera la capacidad del individuo principalmente para determinar la transmisión y empleo de sus datos personales”³.

2 Véase <https://www.cinvestav.mx/Transparencia-y-RC/Transparencia-Proactiva>. El Instituto de Transparencia de la Ciudad de México refiere que “Un aspecto central en el diseño y gestión de estrategias de comunicación para prevención y emergencia es definir canales para hacer llegar a la población datos de interés, explicaciones confiables, instrucciones y avisos, todo ello en lenguaje sencillo. Así que si cuentas con información que pueda ser de utilidad para prevenir y/o contribuir a combatir la emergencia sanitaria de la pandemia COVID-19 aquí algunas recomendaciones de transparencia proactiva que te sugerimos implementar con la finalidad de llegar a todos los sectores de la población”. Véase <https://www.infocdmx.org.mx/covid19/transparencia/>.

3 Véase <https://bloqueconstitucional.com/el-derecho-a-la-proteccion-de-los-datos-personales-frente-a-la-pandemia-del-covid-19/>.

ENSAYOS

Los retos de la protección de datos personales ante la pandemia del coronavirus COVID-19-(SARS-CoV2)

Ahora, en la protección de datos personales también se ven involucrados los particulares como sujetos obligados al tenerlos o poseerlos en ciertos negocios o transacciones, que es cuando los recaban para sus propias actividades.

Entrando en materia, las personas tienen el aspecto doble, tanto como ejercicio y como derecho de solicitar información y proteger sus datos y sobre esto último nos referiremos.

Los datos personales son la información concerniente a una persona física identificada o identificable, directa o indirectamente. De esta definición existen algunos conocidos como “Datos Sensibles”, que son aquellos que se refieren a la esfera más íntima de su titular, cuya utilización indebida pueda generar discriminación o conlleve un riesgo grave para éste, como el origen racial o étnico, estado de salud presente o futuro, información genética, información biométrica, creencias religiosas, filosóficas, morales, opiniones políticas, preferencia sexual, etc.

Así, el derecho a la información encuentra un límite en la información reservada y confidencial, la cual procederá cuando la difusión pone en riesgo la vida, seguridad o salud de alguna persona⁴.

Una y otra tienen finalidades diversas, pues la información como reservada corresponde al desarrollo del límite previsto en el artículo 6o. constitucional referente a la protección del interés público, mientras que la categoría de información confidencial responde a la necesidad de proteger la vida privada de las personas y sus datos personales.

La Suprema Corte de Justicia de la Nación ha reconocido que la relación entre el derecho a la información y sus límites, en cuanto se fundamentan en otros bienes constitucionalmente tutelados, no se da en términos absolutos de todo o nada, sino que su interacción es de carácter ponderativo, en la medida en que la natural tensión que pueda existir entre ellos, requiere en su aplicación un equilibrio necesario entre el ejercicio efectivo del derecho a la información y la indebida afectación de otro tipo de bienes y valores constitucionales que están instituidos también en beneficio de las personas⁵.

Y la información se encuentra interrelacionada con la obtención y divulgación de datos, por lo cual es necesario vigilar que los límites, aunque no son absolutos tanto el acceso a la información como la protección de datos personales, sean demasiado flexibles porque estos tampoco

4 Tesis: 1a. VIII/2012 (10a.). “INFORMACIÓN RESERVADA. LÍMITE AL DERECHO DE ACCESO A LA INFORMACIÓN (LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA GUBERNAMENTAL)”. *Semanario Judicial de la Federación y su Gaceta*. Décima Época. Libro V, febrero de 2012, tomo 1, página 656, y número de registro digital en el Sistema de Compilación 2000234.

5 Tesis: P. II/2019 (10a.). “DERECHO A LA INFORMACIÓN. LA RELACIÓN CON SUS LÍMITES CONSTITUCIONALES NO DEBE PLANTEARSE EN TÉRMINOS ABSOLUTOS”. *Gaceta del Semanario Judicial de la Federación*. Libro 74, enero de 2020, tomo I, página 561, y número de registro digital en el Sistema de Compilación 2021411.

son de tal magnitud para aminorar el derecho de reserva o confidencialidad de la persona titular de ese derecho para que sean dados a conocer al público o entre particulares con finalidades no autorizadas por el mismo.

La protección de los datos se reconoce como un derecho humano consagrado en el artículo 6, apartado A, fracciones I y II de la Constitución Federal, vinculado a la protección de la privacidad y de los datos de las personas, con el propósito de impedir su uso ilícito y vulneración en perjuicio de la dignidad de las personas; para ello, la legislación secundaria⁶ prevé el ejercicio de este derecho mediante los denominados “Derechos ARCO” (Acceso, Rectificación, Cancelación y Oposición), mediante los cuales se puede:

- Conocer quién dispone de tus datos y para qué están siendo utilizados.
- Solicitar rectificación de tus datos en caso de que resulten incompletos o inexactos.
- Solicitar la cancelación de los mismos por no ajustarse a las disposiciones aplicables.
- Oponerse al uso de tus datos si es que los mismos fueron obtenidos sin tu consentimiento.

Dichos derechos constituyen un medio para garantizar el derecho de los individuos a decidir qué aspectos de su vida deben o no ser conocidos o reservados por el resto de la sociedad, y la posibilidad de exigir su cumplimiento a las autoridades y particulares que conocen, usan o difunden dicha información; y también un medio de salvaguarda de otros derechos fundamentales como la vida privada, el honor, la intimidad y la dignidad humana⁷.

Así, la protección de datos y la transparencia involucra más derechos constitucionales⁸.

6 Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (Sector Público) y Ley Federal de Protección de Datos Personales en Posesión de los Particulares (Sector Privado).

7 Tesis: I.10o.A.5 CS (10a.). “PROTECCIÓN DE DATOS PERSONALES. CONSTITUYE UN DERECHO VINCULADO CON LA SALVAGUARDA DE OTROS DERECHOS FUNDAMENTALES INHERENTES AL SER HUMANO”. *Gaceta del Semanario Judicial de la Federación*. Libro 70, septiembre de 2019, tomo III, página 2199, y número de registro digital en el Sistema de Compilación 2020563.

8 Tesis: I.2o.A.E.1 CS (10a.). “SISTEMAS DE PROTECCIÓN DE DATOS PERSONALES Y DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA. PRECEPTOS CONSTITUCIONALES QUE LOS REGULAN”. *Gaceta del Semanario Judicial de la Federación*. Libro 39, febrero de 2017, tomo III, página 2364, y número de registro digital en el Sistema de Compilación 2013674.

2. LA PANDEMIA Y LA ACTUACIÓN DE LAS INSTITUCIONES DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS

Y estos derechos, ¿se han visto afectados por los sucesos del COVID-19?, o más bien, su protección ¿ha sufrido adecuaciones?

El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), emitió una serie de acuerdos para adecuar su actuar ante las medidas de prevención dictadas por la autoridad sanitaria.

El primero de ellos fue publicado el 27 de marzo de 2020, en el Diario Oficial de la Federación (DOF), en el cual se decretó la suspensión de plazos y términos de los trámites y medios de impugnación, entre ellos los relativos a los derechos ARCO.

También se dispuso privilegiar la asistencia virtual o remota, así como la entrega electrónica de la documentación ya sea por correo electrónico o herramienta de comunicación con los sujetos obligados.

Se instruyó a las Secretarías de Acceso a la Información y de Protección de Datos Personales para que, por conducto de sus Direcciones Generales competentes, se trabaje en la implementación de una mesa de trabajo de transparencia proactiva con los diversos sujetos del sector salud, que permita detectar toda aquella información que resulte de interés de la sociedad y sea vital para la prevención y el combate de la pandemia del virus COVID-19, y así garantizar el debido tratamiento de los datos personales en posesión de sujetos obligados de todas aquellas personas que pudieran verse afectadas.

De igual manera, para interés en nuestro tema, se instruyó a la Secretaría de Protección de Datos Personales para que, a través de sus Direcciones Generales competentes, y como parte de las actividades de transparencia proactiva, establezca canales de comunicación con los diversos sujetos regulados del sector salud, a fin de garantizar el debido tratamiento de los datos personales de todas aquellas personas que pudieran verse afectadas por la pandemia del virus COVID-19.

Con posterioridad, otro de los acuerdos publicados en el DOF fue el del 22 de abril, el cual modificaba diversas actas de dicho Instituto.

Así, acorde a su considerando XII, atendiendo a las condiciones de distanciamiento social y reducción de la actividad en los sectores público, privado y social que se derivan de la situación de emergencia sanitaria, el Instituto no pretendió dejar a la ciudadanía sin la protección de los derechos fundamentales que tutela, por lo que se determinó mantener en operación aquellas

actividades con las que se puede garantizar de manera esencial, los derechos de las personas respecto del acceso a la información y a la protección de datos personales, exclusivamente, las que son directamente necesarias, ineludibles o prioritarias, para atender y entender la emergencia sanitaria generada por el virus SARS-CoV2.

En consecuencia, las solicitudes de acceso a la información pública que se reciban en el Instituto y guarden una estricta relación con información de la emergencia sanitaria generada por el virus SARS-CoV2 (COVID-19), serán atendidas mediante un ejercicio de transparencia proactiva.

Por ello, se establecieron 3 mesas de trabajo con sujetos obligados, con las temáticas siguientes:

- a) Coronavirus INAI/Secretaría de Salud: Con el cual se pone a disposición de la ciudadanía, de manera accesible, la información fundamental, relacionada con la emergencia sanitaria.
- b) Datos personales seguros COVID 19: es un micrositio para brindar información clara y precisa a los titulares sobre el derecho a la protección de sus datos personales que, en su caso, serán tratados en instituciones públicas o privadas a fin de otorgarles el diagnóstico, atención y seguimiento sobre Coronavirus, COVID-19; así como proporcionar recomendaciones para los responsables y encargados del Sector Público y Privado, sobre el adecuado tratamiento de datos personales que deberán realizar en las diversas actividades requeridas para la atención de casos de COVID-19, de forma que se cumpla con los principios, deberes y obligaciones que el marco legal en materia de protección de datos personales establece.
- c) #QuédateEnCasa sugerencias de actividades para realizar durante la contingencia sanitaria.

Sobre el punto **b**, dicho sitio <https://micrositios.inai.org.mx/covid-19/> contiene una serie de apartados para asesorar y orientar en materia de protección de datos personales, como derechos, quejas, tratamiento de datos y recomendaciones para tal fin, así como el trabajo a distancia.

Así, se encamina a los sujetos obligados para que garanticen la protección de los datos de las personas que acudan a sus servicios, aunque también brinda un esquema desarrollado de cómo puede desenvolverse el uso de esos datos en el manejo de las nuevas tecnologías.

Destaca como se aclara la regla de excepción en el otorgamiento de consentimiento, siempre que sean indispensables para atención médica, la prevención, diagnóstico, la prestación de asistencia sanitaria, tratamientos médicos o la gestión de servicios sanitarios, mientras el

ENSAYOS

Los retos de la protección de datos personales ante la pandemia del coronavirus COVID-19-(SARS-CoV2)

titular no esté en condiciones de otorgar el consentimiento o cuando exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona.

Por ello será indispensable que el responsable analice de forma específica los casos que pudieran ser sujetos de excepción y ante cualquier duda acudir con la autoridad federal (INAI) o local (Órganos Garantes).

Este tipo de microsítios se ha replicado por diversos institutos y comisiones de transparencia, bien sea como tales o como apartados especiales brindando información relativa sobre la pandemia y la protección de datos; por ejemplo el de la Ciudad de México⁹, Durango, Michoacán¹⁰, Jalisco¹¹, Guanajuato (en este anuncia recomendaciones a la ciudadanía para la protección de sus datos)¹², y Puebla¹³.

También, algunos municipios han instado este tipo de orientación como parte de la transparencia proactiva, tal es el caso del ayuntamiento de Oaxaca de Juárez, el cual lanzó un comunicado para la protección de datos en relación con el COVID-19¹⁴.

De esta forma, podemos hablar de una tendencia a divulgar la protección de datos por parte de los diversos organismos en la materia en cada entidad federativa, y por parte de los sujetos obligados del sector público.

3. LA PANDEMIA Y LA NUEVA CORRELACIÓN DE PROTECCIÓN DE DATOS PERSONALES

Prosiguiendo con el INAI, otro de los acuerdos se publicó en el DOF el 15 de mayo, en el cual se dispuso la admisión, trámite y resolución de los medios de impugnación, así como cualquier otro mecanismo legal o procedimiento, tendiente a verificar el cumplimiento de la

9 Véase <https://www.infocdmx.org.mx/covid19/inicio/>; y también <https://www.infocdmx.org.mx/covid19/proteccion/>.

10 Reyna Lizbeth Ortega Silva señaló la implementación de acciones por parte de su organismo de transparencia, consistente de carácter preventivo, de ejecución y operativas tecnológicas como la capacitación en línea. "Conversatorio de Acciones y Recomendaciones de Protección de Datos Personales ante el COVID-19", disponible en YouTube, canal "COTAINL".

11 Véase <https://www.itei.org.mx/v3/micrositios/covid19/index.php?seccion=datos>.

12 *Tus datos relacionados con tu estado de salud presente o futuro son considerados datos personales sensibles. * Las instituciones de salud te deben solicitar solamente los datos personales mínimos necesarios para prevenir o contener la propagación del COVID-19, mismos que no podrán utilizarse para fines distintos. * Tu identidad como persona afectada no debe divulgarse. * Cada que te recaben tus datos personales asegúrate de que pongan a tu disposición el aviso de privacidad donde se establezcan las finalidades para las cuales serán recabados y tratados tus datos personales, así como los casos en los que se realizarán transferencias de tus datos personales. * Recuerda, es obligación de todas las instituciones públicas establecer todas las medidas de seguridad necesarias para la protección de tus datos personales. Véase <http://covid19.iacip.org.mx/>.

13 Entre las recomendaciones realizadas por su Instituto de Transparencia se encuentra evitar la captura de imágenes o videograbaciones, proporción de los avisos de privacidad, medidas de seguridad eficaces que garanticen la confidencialidad, entre otros. Véase <https://itaipue.org.mx/portal/documentos/datosPersonales/RecomendacionesDP-C-19.pdf>.

14 Véase <https://www.municipiodeoaxaca.gob.mx/pdf/datos-personales-covid-19.pdf>.

Ley en dichas materias, relacionados con solicitudes de acceso a la información y de ejercicio de derechos ARCO sobre datos personales en posesión de sujetos obligados, incluyendo los procedimientos de investigación y verificación en el sector público en términos de la Ley General y demás normatividad aplicable; respecto de los diversos sujetos obligados precisados en dicha publicación (la mayoría del Poder Ejecutivo Federal).

Destaca como comienzan a activarse los mecanismos de protección por parte del INAI en la materia.

Esto encuentra una explicación en la Resolución No. 1/2020, adoptada por la Comisión Interamericana de Derechos Humanos, denominada PANDEMIA Y DERECHOS HUMANOS EN LAS AMÉRICAS, en la cual, en la parte resolutive recomendó¹⁵:

- a) *«Asegurar el derecho de acceso a la información pública en el marco de la emergencia generada por el COVID-19 y no establecer limitaciones generales basadas en razones de seguridad u orden público. Los órganos que garantizan este derecho y los sujetos obligados deben otorgar prioridad a las solicitudes de acceso a la información relacionadas con la emergencia de salud pública, así como informar proactivamente, en formatos abiertos y de manera accesible a todos los grupos en situación de vulnerabilidad, de forma desagregada sobre los impactos de la pandemia y los gastos de emergencia, desagregados de acuerdo con las mejores prácticas internacionales... y*
- b) *Proteger el derecho a la privacidad y los datos personales de la población, especialmente de la información personal sensible de los pacientes y personas sometidas a exámenes durante la pandemia. Los Estados, prestadores de salud, empresas y otros actores económicos involucrados en los esfuerzos de contención y tratamiento de la pandemia, deberán obtener el consentimiento al recabar y compartir datos sensibles de tales personas. Solo deben almacenar los datos personales recabados durante la emergencia con el fin limitado de combatir la pandemia, sin compartirlos con fines comerciales o de otra naturaleza. Las personas afectadas y pacientes conservarán el derecho a cancelación de sus datos sensibles.»*

Esto busca contrarrestar una preocupación ante el número creciente de casos COVID19 en los cuales es necesaria la atención de las personas que acuden a los servicios médicos, por lo cual se deben proporcionar datos para su diagnóstico o tratamiento médico, así como para otra serie de factores que pudieran presentarse, como el traslado a hospitales, servicios de atención o ayuda en el hogar, e incluso las llamadas citas a distancia para exámenes de laboratorio, por ejemplo.

15 Considerando XIX, véase https://www.dof.gob.mx/nota_detalle.php?codigo=5593419&fecha=15/05/2020.

ENSAYOS

Los retos de la protección de datos personales ante la pandemia del coronavirus COVID-19-(SARS-CoV2)

Ante ello, la habilitación del Instituto en sus actividades, con medidas proporcionales, buscan atender cualquier vulneración a los datos personales otorgados por sus titulares.

En este aspecto, por ejemplo, se deben tomar una serie de medidas tendientes a protegerlos, pues ante la urgencia de prevención o el nerviosismo provocado por un posible padecimiento, el titular de los derechos puede propiciar una falta de garantía en su protección.

Por ello se recomienda verificar quién solicita la información (sujeto obligado identificable y aviso de privacidad), se indique la finalidad para recabar dicha información, de preferencia debe hacerse de modo personal y no por medios electrónicos, mucho menos cuando no sea posible establecer la identidad del dueño del dominio de la *web* o de la aplicación “*app*”, ante el riesgo de que pueda tratarse de suplantadores de identidad, y toda tecnología o recopilación de información debe privilegiar la protección de datos.

Cabe indicar que ante la pandemia, existe la posibilidad de transferencia de información entre las diversas instituciones de salud, sin necesidad de requerir la autorización del particular.

Esto, claro, debe tener como finalidad para tomar las acciones sanitarias necesarias para enfrentar la pandemia. Un ejemplo de esta utilización lo tenemos en los informes estatales y nacionales sobre estadísticas de personas con COVID 19.

Lo anterior tiene sustento en el artículo 22, fracciones II, VI y VII, de la Ley General de Protección de Datos Personales en Posesión de Particulares, como casos de excepción para recabar el consentimiento del titular del derecho (persona física).

Entonces, si las acciones del Consejo Salubridad General tienen como finalidad controlar, mitigar y evitar la propagación del COVID-19, los sujetos obligados pueden proporcionar información, sin menoscabo de resguardar y proteger los datos personales con la finalidad de proporcionar información únicamente para realizar las acciones necesarias y pertinentes para la atención de la emergencia sanitaria.

No obstante, hay casos en los que puede suceder una posible vulneración a ese derecho. Por ejemplo, el gobierno de Morelos difundió datos personales de pacientes recuperados de COVID-19 en una conferencia de prensa, aunque con posterioridad aclaró que los propios pacientes autorizaron su difusión como un reconocimiento al personal médico que los atendió¹⁶.

El afán de divulgación de los logros o los riesgos por la pandemia no justifica vulnerar datos sensibles si estos tienen un objeto distinto a la prevención o combate médico.

16 Véase <https://aristeguinoticias.com/2504/mexico/el-gobierno-de-morelos-difunde-datos-personales-de-pacientes-recuperados-de-covid-19-video/>.

Incluso, el Primer Tribunal Colegiado en Materia Administrativa del Primer Circuito ha indicado que el expediente clínico¹⁷ de toda persona, independientemente del cargo público que ocupe en el sector público, constituye información personal de carácter confidencial, por tanto reservado¹⁸; por mayoría de razón, en saber el resultado de un examen médico de laboratorio a determinado funcionario, pues atendiendo a dicho criterio, ello también sería información contenida en parte de su expediente clínico y su ámbito personal o de intimidad.

Laura Sofía Gómez Madrigal, Directora de Seguridad de Datos Personales del INAI, expuso como en esta pandemia, “las instituciones pueden manejar nuestra información siempre y cuando sea la necesaria para el diagnóstico, la atención y gestión del servicio sanitario, cuando el titular no se encuentre en condiciones de otorgar su consentimiento”, pero resulta grave la existencia de aplicaciones en las cuales es posible obtener información de las personas contagiadas, constituyendo una invasión a la privacidad¹⁹.

Resumiendo, en principio la institución de salud (pública o privada) no puede usar los datos personales sin consentimiento, sin embargo hay excepciones, por ejemplo cuando el tratamiento de los datos sea indispensable para atención médica, la prevención, diagnóstico, la prestación de asistencia sanitaria, tratamiento médicos o la gestión de servicios sanitarios, cuando no se esté en condiciones de otorgar dicho consentimiento o cuando exista una situación de emergencia que potencialmente pueda dañarte en tu persona²⁰.

4. ¿PROBLEMÁTICAS FUTURAS O CORRECCIONES OPORTUNAS?

Ahora, hay otras situaciones un poco ajenas a lo médico, en estos tiempos sobre la obtención de datos personales, como lo sería el uso de la tecnología.

Seguramente varios han utilizado en últimas fechas programas de video llamadas o videoconferencias. Si bien los ponentes deben mostrarse ante el auditorio, ¿Cuántos de los que no son panelistas les han preguntado si puede salir su imagen en el video para ser subido a un portal como “YouTube”?

¿Cuántos de los que han disertado en zoom les han preguntado si autorizan que su imagen aparezca en un recuadro y sea subido a una red de videos pública?

¿Existió algún aviso de privacidad o de protección de datos, o solo cláusulas generales pero no específicas sobre el tratamiento de las imágenes?

17 La definición del mismo y su contenido se encuentra desarrollado en la NOM-004-SSA3-2012.

18 Tesis: I.1o.A.60 A (10a.). *Gaceta del Semanario Judicial de la Federación*. Libro 5, abril de 2014, tomo II, página 1523, y número de registro digital en el Sistema de Compilación 2006298.

19 Véase <https://www.afmedios.com/blog/2020/05/20/recomiendan-cuidar-uso-de-datos-personales-durante-crisis-sanitaria-por-covid-19/>.

20 Véase <https://updatemexico.com/destacadas/la-proteccion-de-datos-personales-frente-a-la-pandemia-covid-19/>.

ENSAYOS

Los retos de la protección de datos personales ante la pandemia del coronavirus COVID-19-(SARS-CoV2)

Y si me opongo a que mi imagen salga, ¿quedó excluido de las clases, charlas o videoconferencias?

Genera polémica este caso, pero dado el nuevo contexto no toda videoconferencia o video taller es público, sino que se encuentra sujeto a un limitado número de personas, y si bien el ponente, moderador o participantes en el panel son de interés para conocer sus puntos de vistas, ¿tenemos que ver en un recuadro a una persona sentada en una hamaca tomando esa conferencia? ¿Qué si de repente aparece un menor de edad o incluso, acompaña de forma permanente en la imagen a la persona adulta?

Actualmente es conocido que se brinda un enlace virtual de los pacientes COVID-19 con sus familiares, ¿cómo garantizar que dicha comunicación sea mediante un enlace confiable o cifrado para no ser hackeado?

Considero que estamos ante una “nueva realidad” en la que no se ha reparado del todo, y seguramente no teníamos en cuenta. Ante ello, deberíamos implementar no solo accesos exclusivos y controlados, sino otros mecanismos más cuando se trate de conferencias o talleres abiertos al público y a disposición del público general con posterioridad.

Así, debería proporcionarse un correo exclusivo para el evento, poner atención a las políticas de privacidad –ausente en modelos virtuales como **zoom**, **meet**, u otras similares por ejemplo–, solicitar autorización para que aparezcan en las imágenes o hacer la aclaración de que si participan con preguntas es una forma de consentimiento, hacerles del conocimiento que se grabará la sesión, y responsabilidades en caso de que se filtren las imágenes sin su consentimiento.

Ya no será solo grabar y subir, o llenar un formulario de inscripción. Debe implicar mayores acciones para resguardar la privacidad y los datos de las personas.

Esto muestra solo un aspecto, pues el uso creciente de “**app**” o programas cibernéticos acrecienta la posibilidad de delitos en este campo, por un mal empleo de los datos personales otorgados en direcciones o programas con cuentan con los mecanismos suficientes de seguridad para resguardarlos, o bien, ante fenómenos de suplantación.

Cristos Velasco expone como, ante la búsqueda masiva de curas o programas de compra o entrenamiento, así como de compras, incrementa la posibilidad de que las personas proporcionen datos que las haga sujeto a extorsiones o fraudes²¹.

21 Véase <http://protecciondatos.mx/>.

Aquí no podemos hablar, supongo, de una vulneración total a un derecho de protección de datos porque no son sujetos obligados sino ciber delincuentes o piratas informáticos quienes obtienen datos de forma irregular. Sin embargo, más allá de los engaños o tretas de programas maliciosos, la “fuga” de información puede provenir de sujetos obligados que deben cumplir con dicha regla, como *Zoom, Microsoft, Facebook, Webex, Hangout, Skype* o *Whatsapp*, por citar algunos.

Entonces, si estamos en presencia de un mecanismo deficiente que, lejos de proteger el derecho de los titulares de datos, los hacen vulnerables, tratando de escudarse en fallas del sistema o echándole la culpa al propio titular, ello significa un daño de las empresas al efectuarse un mal uso de los datos proporcionados.

Amnistía Internacional, en su informe de noviembre de 2019 titulado “Gigantes de la Vigilancia”, se refería no a los gobiernos sino a los grandes de la tecnología como *Google* y *Facebook*, indicando lo complicado que sería el uso del internet sin recurrir a estas dos multinacionales y ellas “se aprovechan de este poder para lucrarse con nuestros datos a cambio de ofrecernos esas plataformas y herramientas digitales gratis”²².

Imaginemos, atento a los datos proporcionados por “El Economista” en 2018, derivado de la Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (ENDUTIH) 2017, en México existen más de 71.3 millones de usuarios de Internet, quienes representan 63.9% de la población mayor a seis años. De ésta, 76.6% lo ha utilizado para acceder a redes sociales, 50.2% para descargar *software*, 47.7% para realizar compras o pagos y 15.7% para acceder a servicios en la nube (Instituto Nacional de Estadística y Geografía (INEGI) 2018. Dado que estas actividades se sujetan a la solicitud de información que permita la identificación del usuario, más de 75% de cibernautas mexicanos han dejado algún dato personal (de identificación, sensible, patrimonial o biométrico) en los sitios virtuales²³.

Definitivamente estos números se incrementaron en estos dos meses de pandemia, lo que implica un vasto universo de datos disponibles de empresas tecnológicas, cuyo botín para los ciber delincuentes es ambicioso.

Si bien México adoptó el Convenio 108 del Consejo de Europa, aprobado por decreto publicado el 12 de junio de 2018 en el DOF²⁴, el Estado debe implementar acciones tendientes a

22 Véase <https://bloqueconstitucional.com/el-derecho-a-la-proteccion-de-los-datos-personales-frente-a-la-pandemia-del-covid-19/>.

23 Véase <https://www.eleconomista.com.mx/gestion/Panorama-de-la-proteccion-de-datos-personales-en-Mexico-20180905-0112.html>.

24 Véase <https://www.dof.gob.mx/index.php?year=2018&month=06&day=12>. DECRETO por el que se aprueba el Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal y su Protocolo Adicional relativo a las Autoridades de Control y a los Flujos Transfronterizos de Datos, hechos en Estrasburgo, Francia, el 28 de enero de 1981, y el 8 de noviembre de 2001, respectivamente.

ENSAYOS

Los retos de la protección de datos personales ante la pandemia del coronavirus COVID-19-(SARS-CoV2)

proteger los datos, lo que necesariamente debe llevarse de la mano con las industrias tecnológicas²⁵.

Además de dicho instrumento, nuestro país forma parte de la Red Iberoamericana de Protección de Datos (RIPD), cuyo principal objetivo —previsto en el artículo primero de su Reglamento— es promover políticas, tecnologías y metodologías para garantizar el derecho a la protección de datos.

Estos ámbitos coadyuvan a la implementación de políticas públicas para, tomando la experiencia del ámbito supranacional, pueda mejorarse las acciones tendientes a la protección de datos, y más en los tiempos del COVID-19, considerando que la red de comunicación internacional el tráfico de datos, desconoce fronteras físicas.

Tanto el ámbito médico-salud como tecnológico no son obstáculo para desatender la protección de datos, pues el deber del Estado frente al derecho de los gobernados a decidir qué aspectos de su vida deben o no ser conocidos o reservados por el resto de los individuos que integran la sociedad, y que conlleva la obligación de dejarlos exentos e inmunes a invasiones agresivas o arbitrarias por parte de terceros o de la autoridad pública, debe potencializarse ante las nuevas herramientas tecnológicas²⁶.

Por ello pueden ser problemáticas futuras o correcciones oportunas a realizarse inmediatamente, solo el tiempo dirá cuál elección se tomó.

5. PANORAMA INTERNACIONAL RESPECTO A LA PROTECCIÓN DE DATOS Y LA PANDEMIA

Human Rights Watch, señala que el derecho internacional de los derechos humanos garantiza que todas las personas disfruten del derecho al más alto nivel posible de salud y obliga a los gobiernos a adoptar medidas para prevenir las amenazas a la salud pública y brindar atención médica a quienes la necesitan. Las normas de derechos humanos también reconocen que en el contexto de serias amenazas a la salud pública y emergencias públicas que pongan en peligro la vida de una nación, las restricciones a algunos derechos pueden justificarse siempre

25 El Convenio n. 108 del Consejo de Europa, fue el primer instrumento internacional jurídicamente vinculante adoptado en el ámbito de la protección de datos. Tiene como fin garantizar a cualquier persona física "el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona". Con el Protocolo que ha modificado el Convenio se pretende ampliar su ámbito de aplicación, aumentar el nivel de protección de los datos y mejorar su eficacia. Véase <https://www.europarl.europa.eu/factsheets/es/sheet/157/la-proteccion-de-los-datos-personales>.

26 Tesis: I.10o.A.6 CS (10a.). "PROTECCIÓN DE DATOS PERSONALES. EL DEBER DEL ESTADO DE SALVAGUARDAR EL DERECHO HUMANO RELATIVO DEBE POTENCIALIZARSE ANTE LAS NUEVAS HERRAMIENTAS TECNOLÓGICAS, DEBIDO A LOS RIESGOS QUE ÉSTAS REPRESENTAN POR SUS CARACTERÍSTICAS". *Gaceta del Semanario Judicial de la Federación*. Libro 70, septiembre de 2019, tomo III, página 2200, y número de registro digital en el Sistema de Compilación 2020564.

y cuando tengan una base legal, sean estrictamente necesarias según evidencias científicas y no sean arbitrarias ni discriminatorias en su aplicación, sean de duración limitada, respeten la dignidad humana, estén sujetas a revisión y sean proporcionales para lograr su objetivo²⁷.

Así, los DDHH no son absolutos sin que ello implique una flexibilidad tal que implique su renuncia o afectación de manera desproporcionada y sin ponderación de las medidas tomadas para la protección de la salud y el goce del derecho humano en juego, tal como se dijo anteriormente.

Maria Florencia Bossi, expone una serie de cuestiones que pudieran presentarse: las limitaciones para el tratamiento de datos relativos a la salud (catalogados - en general - como datos sensibles en los sistemas jurídicos); las facultades especiales que ciertas legislaciones - como la de Argentina - otorgan los Estados para tratar los datos de sus ciudadanos sin consentimiento en el marco del cumplimiento de funciones públicas; las disposiciones que eventualmente pueden contener las legislaciones sobre excepciones en materia de tratamiento de datos ante situaciones extraordinarias, como lo es la pandemia (en la ley de datos personales de Argentina también se contempla este tipo de supuestos); y, la polémica en torno a ciertos desarrollos tecnológicos implementados en algunos países para ayudar a frenar la crisis sanitaria, los cuales pueden aportar importantes beneficios, aunque al mismo tiempo, pueden representar riesgos para la privacidad de las personas.

Un breve panorama de las medidas sobre protección de datos tomadas en algunos de los países afectados por la pandemia. A nivel internacional, las autoridades vinculadas a la protección de datos ya se han expedido sobre la problemática que representa la pandemia, y han emitido distintos comunicados²⁸.

La protección de datos se encuentra en ese derecho humano, y trasciende a la protección de la familia, pues ante esta pandemia el perjuicio puede ir más allá del ámbito individual para, por temor o estigmas, trascender a la discriminación.

Las agresiones al personal médico son ejemplo de ello, pero también el aislamiento o expulsión de sus casas o comunidades ante la divulgación de datos como la enfermedad de un familiar, provoca dichas situaciones.

27 Véase <https://www.hrw.org/es/news/2020/03/31/dimensiones-de-derechos-humanos-en-la-respuesta-al-covid-19>.

28 Véase <http://www.sajj.gob.ar/maria-florencia-bossi-proteccion-datos-personales-privacidad-tiempos-pandemia-dacf200038-2020-03-24/123456789-0abc-defg8300-02fcanirtcod?&o=3&f=Total%7CFecha%7CEstado%20de%20Vigencia%5B5%2C1%5D%7CTema%5B5%2C1%5D%7COrganismo%5B5%2C1%5D%7CAutor%5B5%2C1%5D%7CJurisdicci%F3n%5B5%2C1%5D%7CTribunal%5B5%2C1%5D%7CPublicaci%F3n%5B5%2C1%5D%7CColecci%F3n%20tem%Etica%5B5%2C1%5D%7CTipo%20de%20Documento/Doctrina&t=5>.

ENSAYOS

Los retos de la protección de datos personales ante la pandemia del coronavirus COVID-19-(SARS-CoV2)

En “El economista” se citan varios casos²⁹:

“En la India, por ejemplo, hasta antes de declarar el aislamiento total, el gobierno había puesto estampas en las puertas de las personas que se encuentran en cuarentena por el coronavirus. Según medios locales, esto ha ocasionado que estas personas sean estigmatizadas en los complejos residenciales en donde viven, algo que también afecta a los médicos, a quienes incluso sus vecinos les prohíben entrar a sus casas.

En México, varios medios de comunicación difundieron la falsa noticia el pasado 14 de marzo acerca de que un importante empresario mexicano había fallecido a causa del coronavirus. Tanto la Secretaría de Salud, como la familia del empresario desmintieron esta información.

A este caso se suma el de una joven guerrerense que envió una carta al diario El Universal para denunciar que el gobierno del estado había hecho público su caso antes de informarle que estaba contagiada con coronavirus. A raíz de que se hizo pública su información, la joven comenzó a ser insultada por miembros de su comunidad en redes sociales”.

Esto nos muestra la importancia de la protección de datos más allá de lo personal-individual para alcanzar lo personal-social-familiar.

Y como tal, acontece en otras latitudes de nuestro planeta, después de todo, la pandemia es global³⁰.

En Guatemala, considerando la gran interacción de las redes sociales en esta pandemia, se ha establecido sugerencia para proteger el derecho a la intimidad y la protección de datos, como por ejemplo no dar consulta, diagnóstico o recetas por prensa, radio, televisión o cualquier medio de comunicación e informática, sin conocimiento y evaluación clínica del paciente; no revelar la confidencialidad o el secreto profesional al utilizar redes sociales; no utilizar las redes sociales para realizar consultas, opiniones diagnósticas, recetas o dar seguimiento a pacientes; o al hacer uso de redes sociales, no permitir que el paciente tratado sea reconocido o identificado, a través de cualquier imagen o dato³¹.

Las consecuencias a alguna vulneración de lo anterior o la comercialización de los datos de los pacientes, publicidad indebida, injuria o difamación derivada por el uso de estos datos, involucra penas de prisión.

29 Véase <https://www.economista.com.mx/politica/Los-nombres-de-pacientes-de-Covid-19-son-datos-personales-y-deben-protegerse-20200324-0101.html>.

30 Véase https://www.who.int/csr/disease/swineflu/frequently_asked_questions/pandemic/es/.

31 Véase Florencio A. Gramajo y Francisco Zuluaga. <https://lexlatin.com/opinion/covid-19-proteccion-datos-personales-uso-redes-sociales>.

Pero ello es relativo en diversas latitudes.

En Europa, se acordó con diversas empresas telefónicas dar acceso a datos de geolocalización para vigilar y rastrear la pandemia; y en China, los habitantes tienen que dar información sobre su salud a través de una aplicación de **tracking** que genera un código QR, el cual les permite autorizar o no el acceso a todo tipo de lugares públicos. En Taiwán o Singapur, se puede utilizar el móvil de una persona en cuarentena para comprobar si permanece en casa. Si no, se le impone una multa y se publica su nombre³².

Por ello, Philippe Prince Tritto pregunta si en esta época en que lo primordial es combatir la epidemia de coronavirus se puede ceder en la privacidad de los usuarios de telefonía celular. Una propuesta es el anonimato del titular, pero debe analizarse cada contexto.

De entrada, en nuestro país el criterio de geolocalización es para la investigación de delitos³³, no para conocer la movilidad de las personas, lo que implicaría la generación de un nuevo marco regulativo.

En España, la Agencia Española de Protección de Datos, indicó que la protección de datos, el interés general, la protección de la salud pública y la lucha contra la epidemia, son compatibles, pues la propia normativa prevé soluciones que permiten el uso lícito de datos personales con las medidas necesarias para garantizar el bien común.

En el caso de la geolocalización podrán facilitarse datos “anonimizados” y agregados que permitan determinar el movimiento de las personas, pudiéndose solicitar información específica de un ciudadano; para ello, en la solicitud a los operadores solo deberían facilitar el número de móvil, salvo que se determinara imprescindible facilitar datos adicionales³⁴.

De igual manera, se emitió la orden la Orden SND/297/2020, de 27 de marzo, por la que se encomienda a la Secretaría de Estado de Digitalización e Inteligencia Artificial del Ministerio de Asuntos Económicos y Transformación Digital, el desarrollo de diversas actuaciones para la gestión de la crisis sanitaria ocasionada por el COVID-19, en la cual se recabaran datos sobre un diagnóstico médico preliminar no vinculante y la geolocalización del individuo, lo cual generó suspicacia sobre la adecuada administración de los datos proporcionados al ente gubernamental correspondiente, la ausencia de la agencia de protección de datos en la implementación de la aplicación tecnológica, la falta de transparencia en la responsabilidad de la administración y el marco de actuación en el tratamiento de datos³⁵.

32 Véase <https://politica.expansion.mx/voces/2020/04/13/columna-invitada-datos-personales-en-epoca-de-coronavirus>.

33 Véase <https://www2.scjn.gob.mx/AsuntosRelevantes/pagina/SeguimientoAsuntosRelevantesPub.aspx?ID=139112&SeguimientoID=575&CAP=> ; y, https://www.scjn.gob.mx/sites/default/files/sinopsis_asuntos_destacados_documento/2017-02/1S-180516-AZLL-3886.pdf.

34 Véase <http://www.legaltoday.com/blogs/nuevas-tecnologias/blog-ecija-2-0/tratamiento-de-datos-personales-en-la-lucha-contra-el-covid-19>.

35 Véase <https://hayderecho.expansion.com/2020/04/10/el-interes-publico-de-los-datos-personales-en-tiempos-del-covid-19/>.

ENSAYOS

Los retos de la protección de datos personales ante la pandemia del coronavirus COVID-19-(SARS-CoV2)

La autoridad protectora de datos colombiana (RIPD) informó que Colombia inició investigación a *TikTok* para establecer si recolecta y trata correctamente los datos de los niños, niñas y adolescentes, tras evidencias que, la Comisión Federal de Comercio (FTC, por sus siglas en inglés) acordará con la aplicación *TikTok*, el pago de \$5.7 millones de dólares a la luz de varias acusaciones relacionadas con la recolección y tratamiento ilícito de datos personales de niños niñas y adolescentes³⁶.

El 9 de abril de 2020, la Corte Interamericana de Derechos Humanos emitió un comunicado en el cual indicó que el acceso a la información veraz y fiable, así como a internet, es esencial, debiéndose disponer que las medidas adecuadas para que el uso de tecnología de vigilancia para monitorear y rastrear la propagación del coronavirus COVID-19, sea limitado y proporcional a las necesidades sanitarias y no implique una injerencia desmedida y lesiva para la privacidad, la protección de datos personales, y a la observancia del principio general de no discriminación³⁷.

6. A MANERA DE CONCLUSIÓN.

Ante todo lo expuesto deberíamos revalorar cómo proteger y potencializar la autodeterminación informativa, como lo identifica Johana Caterina Faliero³⁸. Dicha figura consiste en el derecho que tiene el titular del dato de gobernar los datos que a él refiere (otorga), así como la posibilidad de controlar quien accede a esos datos, como tratarse y el modo de dar esa autorización.

Se plantea que haya un consentimiento informado para que, a través de los principios de la proporcionalidad, razonabilidad y constitucionalidad imperen una obtención y divulgación de los datos de carácter sensible, y así pueda conservarse la privacidad de los titulares de esos datos.

Johana Caterina Faliero, sugiere disociar o anonimizar ese dato para quitarle la capacidad de identificar al titular, pero los mecanismos para hacerlo deben tener como punto base la información y consentimiento pleno del titular del derecho.

Esto será importante por las medidas que recientemente se han estado implementado por esta contingencia, por ejemplo en Querétaro con la descentralización de datos para sancionar a aquellas personas contagiadas o diagnosticadas que incumplan la cuarentena, o ante la creación de una base de datos para compartir el plasma en el tratamiento de personas recuperadas de COVID-19 con las que se encuentran enfermas³⁹.

36 Véase <https://www.redipd.org/es/noticias/autoridad-colombiana-de-proteccion-de-datos-inicio-investigacion-tiktok-para-establecer-si>.

37 Véase http://www.corteidh.or.cr/tablas/alerta/comunicado/declaracion_1_20_ESP.pdf.

38 Video charla "La protección de datos personales en el escenario del COVID-19", disponible en YouTube, canal "DerechoUBA".

39 Javier Martínez Cruz en "Conversatorio de Acciones y Recomendaciones de Protección de Datos Personales ante el COVID-19", disponible en YouTube, canal "COTAINL".

¿O será necesario aplicar las medidas de China, Corea del Sur o Singapur en los cuales se proporcionan datos personales en “app” para proteger (restringir) a las personas sanas de las enfermas con el libre tránsito?⁴⁰

7. FUENTES DE INFORMACIÓN

“Conversatorio de Acciones y Recomendaciones de Protección de Datos Personales ante el COVID-19”, disponible en YouTube, canal “COTAINL”. Link <https://www.youtube.com/watch?v=UmaJTHAn930>.

Constitución Política de los Estados Unidos Mexicanos.

Diario Oficial de la Federación. Tomo DCCLXXVII. No. 13. Edición Vespertina. 12 de junio de 2018. Link <https://www.dof.gob.mx/index.php?year=2018&month=06&day=12>.

----- Edición del mes: 23. Edición Matutina. 22 de abril de 2020. Link <https://www.dof.gob.mx/index.php?year=2020&month=04&day=22&edicion=MAT>.

----- Edición del mes: 9. Edición Matutina. 15 de mayo de 2020. Link <https://www.dof.gob.mx/index.php?year=2020&month=05&day=15&edicion=MAT>.

Dirección de Internet <http://covid19.iacip.org.mx/>. Protección de datos personales. Instituto de Acceso a la Información Pública para el Estado de Guanajuato.

----- <http://www.legaltoday.com/blogs/nuevas-tecnologias/blog-ecija-2-0/tratamiento-de-datos-personales-en-la-lucha-contra-el-covid-19>. Tratamiento de datos personales en la lucha contra el Covid-19. María González Moreno.

----- <http://protecciondatos.mx/>. Cibercrimes y COVID-19 / Cybercrime and COVID-19. Cristos Velasco.

----- <http://www.saij.gov.ar/maria-florencia-bossi-proteccion-datos-personales-privacidad-tiempos-pandemia-dacf200038-2020-03-24/123456789-0abcdefg8300-02fcanirtcod?&o=3&f=Total%7CFecha%7CEstado%20de%20Vigencia%5B%2C1%5D%7CTema%5B%2C1%5D%7COrganismo%5B%2C1%5D%7CAutor%5B%2C1%5D%7CJurisdicci%F3n%5B%2C1%5D%7CTribunal%5B%2C1%5D%7CPublicaci%F3n%5B%2C1%5D%7CColecci%F3n%20tem%Etica%5B%2C1%5D%7CTipo%20de%20Documento/Doctrina&t=5>. Sistema Argentino de Información Jurídica (SAIJ). La protección de datos personales y de la privacidad en tiempos de pandemia. María Florencia Bossi.

----- <https://aristeguino.com/2504/mexico/el-gobierno-de-morelos-difunde-datos-personales-de-pacientes-recuperados-de-covid-19-video/>. El gobierno de Morelos difunde datos personales de pacientes recuperados de Covid-19 | Video. Estrella Pedroza.

----- <https://bloqueconstitucional.com/el-derecho-a-la-proteccion-de-los-datos-personales-frente-a-la-pandemia-del-covid-19/>. Bloque Constitucional. Reinstitutionalización del Sistema de Justicia de Venezuela. María Luisa Acuña López.

40 Bernardo Sierra Gómez en “Conversatorio de Acciones y Recomendaciones de Protección de Datos Personales ante el COVID-19”, disponible en YouTube, canal “COTAINL”.

ENSAYOS

Los retos de la protección de datos personales ante la pandemia del coronavirus COVID-19-(SARS-CoV2)

- <https://hayderecho.expansion.com/2020/04/10/el-interes-publico-de-los-datos-personales-en-tiempos-del-covid-19/>. El interés público de los datos personales en tiempos del COVID-19. Ana Marzo Portera.
- <https://itaipue.org.mx/portal/documentos/datosPersonales/Recomendaciones-DP-C-19.pdf>. Recomendaciones para responsables de tratamientos de datos personales, derivados de la lucha contra el COVID-19. Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de Puebla.
- <https://lexlatin.com/opinion/covid-19-proteccion-datos-personales-uso-redes-sociales>. COVID-19: protección de datos personales y uso de redes sociales. Las tecnologías de información y comunicación y especialmente las redes sociales, utilizadas adecuadamente, representan una herramienta muy valiosa para contrarrestar la crisis sanitaria. Florencio A. Gramajo y Francisco Zuluaga.
- <https://micrositios.inai.org.mx/covid-19/>. Datos personales seguros. Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI).
- <https://politica.expansion.mx/voces/2020/04/13/columna-invitada-datos-personales-en-epoca-de-coronavirus>. Philippe Prince Tritto pregunta si en esta época en que lo primordial es combatir la epidemia de coronavirus se puede ceder en la privacidad de los usuarios de telefonía celular. Philippe Prince Tritto.
- <https://updatemexico.com/destacadas/la-proteccion-de-datos-personales-frente-a-la-pandemia-covid-19/>. La protección de datos personales frente a la Pandemia COVID-19. Roberto Ramos Bonilla.
- <https://www.afmedios.com/blog/2020/05/20/recomiendan-cuidar-uso-de-datos-personales-durante-crisis-sanitaria-por-covid-19/>. Laura Sofía Gómez Madrigal, directora de Seguridad de Datos Personales del Instituto Nacional de Transparencia y Acceso a la Información, impartió videoconferencia a la comunidad académica de la Facultad de Derecho, en la que abordó el tema “Protección de datos personales en tiempos de COVID-19”. Redacción.
- <https://www.cinvestav.mx/Trasparencia-y-RC/Transparencia-Proactiva>. Centro de Investigación y de Estudios Avanzados del IPN.
- <https://www.eleconomista.com.mx/gestion/Panorama-de-la-proteccion-de-datos-personales-en-Mexico-20180905-0112.html>. Panorama de la protección de datos personales en México. Mario Gómez.
- <https://www.eleconomista.com.mx/politica/Los-nombres-de-pacientes-de-Covid-19-son-datos-personales-y-deben-protegerse-20200324-0101.html>. Datos sensibles. Rodrigo Riquelme.
- <https://www.europarl.europa.eu/factsheets/es/sheet/157/la-proteccion-de-los-datos-personales>. Fichas temáticas sobre la Unión Europea. Parlamento europeo.
- <https://www.hrw.org/es/news/2020/03/31/dimensiones-de-derechos-humanos-en-la-respuesta-al-covid-19>. Human Rights Watch.

- <https://www.infocdmx.org.mx/covid19/inicio/>. Datos personales y transparencia proactiva. Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México.
- <https://www.infocdmx.org.mx/covid19/proteccion/>. *Ibidem*.
- <https://www.infocdmx.org.mx/covid19/transparencia/>. *Ibidem*.
- https://www.scjn.gob.mx/sites/default/files/sinopsis_asuntos_destacados_documento/2017-02/15-180516-AZLL-3886.pdf. Suprema Corte de Justicia de la Nación. Mariel Albarrán Duarte.
- https://www.who.int/csr/disease/swineflu/frequently_asked_questions/pandemic/es/. Organización Mundial de la Salud. Alerta y Respuestas Mundiales (GAR).
- <https://www2.scjn.gob.mx/AsuntosRelevantes/pagina/SeguimientoAsuntosRelevantesPub.aspx?ID=139112&SeguimientoID=575&CAP=>. Suprema Corte de Justicia de la Nación. ACCIÓN DE INCONSTITUCIONALIDAD 32/2012. “Valida SCJN las normas que sustentan la geolocalización de los equipos de comunicación móvil vinculados a delitos considerados graves”.
- Gaceta del Semanario Judicial de la Federación*. Libro 5, abril de 2014, tomo II, página 1523, y número de registro digital en el Sistema de Compilación 2006298. Tesis: I.1o.A.60 A (10a.). “INFORMACIÓN PÚBLICA GUBERNAMENTAL. EL EXPEDIENTE CLÍNICO DE TODA PERSONA, INDEPENDIENTEMENTE DEL CARGO PÚBLICO QUE OCUPE, CONSTITUYE INFORMACIÓN PERSONAL DE CARÁCTER CONFIDENCIAL”.
- Gaceta del Semanario Judicial de la Federación*. Libro 39, febrero de 2017, tomo III, página 2364, y número de registro digital en el Sistema de Compilación 2013674. Tesis: I.2o.A.E.1 CS (10a.). “SISTEMAS DE PROTECCIÓN DE DATOS PERSONALES Y DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA. PRECEPTOS CONSTITUCIONALES QUE LOS REGULAN”.
- Gaceta del Semanario Judicial de la Federación*. Libro 70, septiembre de 2019, tomo III, página 2199, y número de registro digital en el Sistema de Compilación 2020563. Tesis: I.10o.A.5 CS (10a.). “PROTECCIÓN DE DATOS PERSONALES. CONSTITUYE UN DERECHO VINCULADO CON LA SALVAGUARDA DE OTROS DERECHOS FUNDAMENTALES INHERENTES AL SER HUMANO”.
- Gaceta del Semanario Judicial de la Federación*. Libro 70, septiembre de 2019, tomo III, página 2200, y número de registro digital en el Sistema de Compilación 2020564. Tesis: I.10o.A.6 CS (10a.). “PROTECCIÓN DE DATOS PERSONALES. EL DEBER DEL ESTADO DE SALVAGUARDAR EL DERECHO HUMANO RELATIVO DEBE POTENCIARSE ANTE LAS NUEVAS HERRAMIENTAS TECNOLÓGICAS, DEBIDO A LOS RIESGOS QUE ÉSTAS REPRESENTAN POR SUS CARACTERÍSTICAS”.
- Gaceta del Semanario Judicial de la Federación*. Libro 74, enero de 2020, tomo I, página 561, y número de registro digital en el Sistema de Compilación 2021411. Tesis: P. II/2019 (10a.). “DERECHO A LA INFORMACIÓN. LA RELACIÓN CON SUS LÍMITES CONSTITUCIONALES NO DEBE PLANTEARSE EN TÉRMINOS ABSOLUTOS”.

ENSAYOS

Los retos de la protección de datos personales ante la pandemia del coronavirus COVID-19-(SARS-CoV2)

“La protección de datos personales en el escenario del COVID-19”, disponible en YouTube, canal “DerechoUBA”. Link <https://www.youtube.com/watch?v=CXlczv94Ydl>.

Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México.

Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

NOM-004-SSA3-2012. Norma Oficial Mexicana. Del expediente clínico.

Semanario Judicial de la Federación y su Gaceta. Décima Época. Libro V, febrero de 2012, tomo 1, página 656, y número de registro digital en el Sistema de Compilación 2000234. Tesis: 1a. VIII/2012 (10a.). “INFORMACIÓN RESERVADA. LÍMITE AL DERECHO DE ACCESO A LA INFORMACIÓN (LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA GUBERNAMENTAL)”.