Protección de datos personales y COVID-19. Análisis de experiencias en México y Latinoamérica

Dra. Isabel Davara F. de Marcos
Socia Fundadora y Directora de Davara Abogados S.C.[1]

Resumen

En este artículo se analiza el marco jurídico vigente en materia de protección de datos personales y la naturaleza de distintos tratamientos de datos que han surgido en plena crisis sanitaria originada por la COVID-19 en México y algunos países de Latinoamérica, mismos que han dado lugar a una nueva serie de reflexiones sobre la relevancia de este derecho y la necesidad de encontrar un sano equilibrio entre las medidas de contención frente a la pandemia originada por el virus SARS-CoV-2 y la protección de los datos. Finalmente, se identifican los principales retos para la efectiva protección de los datos personales que supone la crisis sanitaria actual para México y la región.

PALABRAS CLAVE:

Protección de Datos, Dato Personal, Datos Sensibles, Tratamiento, Situación de Emergencia

[1] Agradezco su inestimable ayuda para la investigación de este artículo al Mtro. Gregorio Barco Vega.

I. Introducción

El derecho a la protección de datos personales tiene una indiscutible relevancia en la actualidad, pues, aunque a veces se visualiza como un concepto demasiado técnico y poco estudiado, cierto es que, cada vez más se escucha más y las personas están siendo más conscientes de su significado e implicaciones tanto jurídicas como prácticas. La pandemia originada por el Coronavirus SARS-CoV-2 ha puesto de manifiesto que la privacidad de las personas importa y está inexorablemente ligada con la dignidad y libertad humanas, pues, mientras mayor control tenemos sobre el uso y destino de nuestros datos, podemos tomar decisiones de trascendental importancia, decisiones que inciden de forma directa en la forma en la que vivimos y visualizamos el mundo.

Sin embargo, el uso de esta importante información en el entorno tecnológico actual también puede acarrear importantes riesgos y afectaciones a la garantía del derecho a la protección de datos personales, pues las tecnologías existentes que combinan el uso del internet con la satisfacción de múltiples requerimientos de la vida diaria, colocan a la persona en una situación de vulnerabilidad donde se vuelve más difícil que el titular pueda controlar el uso que se hace de su información personal, sobre todo en el entorno electrónico, máxime cuando la pandemia ocasionada por el COVID-19 ha acelerado significativamente el uso de la tecnología y el proceso de digitalización en el mundo.

Ante este panorama las personas han caído en la cuenta de que constantemente entregan información a diversos proveedores de servicios, que cada actividad que realizamos en internet deja una huella cuasi imborrable, que el mal uso de nuestros datos puede llevar a consecuencias funestas como la discriminación social o la segregación por ser sospechoso o declarado portador de la enfermedad COVID-19. Esta situación, aunado al incesante uso de la tecnología ha puesto de manifiesto una cosa, todos somos datos, y los datos importan en la medida en que se vinculan con nosotros, pues, si se hace mal uso de estos, la persona sufrirá negativamente las consecuencias.

En consecuencia, deviene imprescindible reflexionar sobre los tratamientos de datos personales que se han visto reforzados y renovados a causa de la pandemia originada por la COVID-19, pues tanto las empresas como los gobiernos han puesto en marcha planes, estrategias y acciones para abatir la pandemia que tienen como insumo principal el uso de datos personales. Ante ello, resulta crucial reflexionar sobre el equilibrio que debe guardarse entre estas medidas de contención y el respeto de los derechos humanos como la privacidad y la protección de datos.

II. Protección de datos en México y situación de emergencia

En México, el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos (“CPEUM”) consigna el derecho de protección de datos personales de todas las personas, en los términos siguientes:

> *“Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros”.*

La redacción anterior tiene profundas implicaciones legales, de un lado, se instaura el derecho humano a la protección de datos y los mecanismos para su ejercicio como son los denominados Derechos ARCO, se ordena el establecimiento de disposiciones reguladoras que serán aplicables tanto para el sector público como el privado, y se establecen las limitantes que podrá revestir este derecho. Concretamente, aquí ya se puede identificar una premisa relevante: el derecho a la protección de datos personales no es absoluto y admite supuestos de excepción por *razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.*

En este contexto, aunque este derecho como hemos dicho es relevante para proteger la dignidad y libertad de la persona, cierto es que encuentra límites concretos, tal y como lo prevén el artículo 4 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares ("LFPDPPP")[2] y el artículo 6 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados ("LGPDPPSO").[3] No obstante, dichas limitaciones deben ser vistas como una excepción, pues "ningún derecho fundamental es absoluto y puede ser restringido siempre que ello no se haga de manera abusiva, arbitraria o desproporcional".[4]

Así, la Corte Interamericana de Derechos Humanos ("CoIDH") ha sostenido que "el ámbito de la privacidad se caracteriza por quedar exento e inmune a las invasiones o agresiones abusivas o arbitrarias de terceros o de la autoridad pública, y prohíbe ese tipo de injerencias en la vida privada de las personas, enunciando diversos ámbitos de ésta, como la vida privada de sus familias".[5]

De este modo, cuando hablamos del derecho a la protección de datos personales y las limitaciones señaladas, entonces surge la pregunta ¿Cuándo se considera que la restricción a este derecho es lícita y no arbitraria? Al respecto, la Primera Sala de nuestro Máximo Tribunal ha precisado que, de la interpretación armónica y sistemática del contenido del artículo 1 constitucional y el artículo 30 de la Convención Americana sobre Derechos Humanos se concluye que los requisitos para considerar válidas las restricciones o la suspensión de derechos, son: *a) que se establezcan en una ley formal y material (principio de reserva de ley) dictada en razón del interés general o público, en aras de garantizar los diversos derechos de igualdad y seguridad jurídica (requisitos formales); y, b) que superen un test de proporcionalidad, esto es, que sean necesarias; que persigan un interés o una finalidad constitucionalmente legítima y que sean razonables y ponderables en una sociedad democrática (requisitos materiales)*.[6]

Es decir, para que el derecho de protección de datos pueda limitarse, incluso en situación de emergencia, como podría calificarse la emergencia[7] sanitaria derivada de la pandemia de la COVID-19, debe existir un ejercicio de debida ponderación y justificación legal en aras de no impedir el ejercicio de este derecho, dificultarlo más allá de lo razonable o bien, despojarlo de una necesaria protección con el propósito de preservar su núcleo esencial.[8]

De este modo, el 30 de marzo de 2020, el Consejo de Salubridad General emitió el Acuerdo por el que se declara como emergencia sanitaria por causa de fuerza mayor, a la epidemia de enfermedad generada por el virus SARS-CoV2 (COVID-19).[9] Este acto jurídico, como decimos no queda ajeno a la obligación de garantía de los derechos humanos, pues como señala VELAZQUEZ ARRROYO este acto "… no queda exento de la exigencia de racionalidad jurídica- constitucional mínima de fundar y motivar sus actos..."[10]

---

[2] Artículo 4.- Los principios y derechos previstos en esta Ley, tendrán como límite en cuanto a su observancia y ejercicio, la protección de la seguridad nacional, el orden, la seguridad y la salud públicos, así como los derechos de terceros.

[3] Artículo 6. El Estado garantizará la privacidad de los individuos y deberá velar porque terceras personas no incurran en conductas que puedan afectarla arbitrariamente.

El derecho a la protección de los datos personales solamente se limitará por razones de seguridad nacional, en términos de la ley en la materia, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.

[4] Tesis 1a. CCXIII/2009, Semanario Judicial de la Federación y su Gaceta, Novena Época, t. XXX, diciembre de 2009, p. 276.

[5] Tesis 1a. XLIX/2014 (10a.), Gaceta del Semanario Judicial de la Federación, Décima Época, t. I, febrero de 2014, p. 641.

[6] Tesis: 1a. CCXV/2013 (10a.), Semanario Judicial de la Federación y su Gaceta, Décima Época, t. I, julio de 2013, p. 557.

[7] Para un estudio de la expresión "situación de emergencia" y protección de datos recomendamos consultar la voz correspondiente a este término en Davara F. de Marcos, Isabel (Coord), Diccionario de Protección de Datos Personales, México, Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), 2019, Disponible en https://home.inai.org.mx/wp-content/documentos/Publicaciones/Documentos/DICCIONARIO_PDP_digital.pdf

[8] Tesis: 2a. XCII/2016 (10a.), Gaceta del Semanario Judicial de la Federación, Décima Época, t. I, Septiembre de 2016, p. 842.

[9] https://www.dof.gob.mx/nota_detalle.php?codigo=5590745&fecha=30/03/2020

[10] VELAZQUEZ ARRROYO Laura, "Análisis del acuerdo por el que se declara como emergencia sanitaria por causa de fuerza mayor", en GONZÁLEZ MARTÍN, Nuria (coord.), Emergencia sanitaria por COVID-19: Reflexiones desde el derecho (III), México, Universidad Nacional Autónoma de México/ Instituo de Investigaciones Jurídicas, 2020.

III. Tratamiento de datos personales en México y crisis sanitaria

El tratamiento de datos personales -de acuerdo con nuestra legislación aquellos que se refieren a una persona física identificada o identificable- se realiza en todas las organizaciones ya sean públicas o privadas, y en la crisis sanitaria antes referida han sido más notables, sobretodo porque estamos en presencia del tratamiento de categorías especiales de datos o "datos personales sensibles" entendidos como "aquellos datos personales que afecten a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste."[11] En particular, se consideran sensibles aquellos que puedan revelar aspectos como origen racial o étnico, estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual. Los datos tratados por las organizaciones para conocer si una persona es portadora o no del COVID-19, si se ha recuperado, si se ha vacunado o si ha estado en contacto con personas portadoras de la enfermedad entran en esta categoría.

Sin embargo, a diferencia de otros acontecimientos similares que han afectado significativamente a la humanidad como (peste negra, gripe española, gripe aviar, entre otras) el día de hoy contamos con el aliado cuasi omnipresente de la tecnología. El uso de grandes conjuntos de datos e información en combinación con sofisticados sistemas de procesamiento, algunos incluso basados en inteligencia artificial, está probando su eficacia y gran capacidad de respuesta en el corto tiempo.

No obstante, aunque podríamos pensar que la tecnología y las poderosas formas de procesar los datos hacen uso de información anónima, la realidad es que, en muchos casos, la información puede adscribirse directamente a un individuo.

Por ejemplo, muchos nos preguntamos ¿Cómo ha hecho China para combatir la crisis generada a partir del coronavirus COVID-19? La respuesta parece ser el reflejo de un futuro distópico, pero no lo es. El acelerado uso de la tecnología y de grandes conjuntos de datos (*Big Data*)[12] es una innegable realidad. China ha aprovechado la tecnología para combatir y controlar la crisis. En distintas ubicaciones del país asiático se han podido observar robots desinfectantes, cascos inteligentes y drones equipados con cámaras térmicas. Para hacer todo esto, China se ha valido, entre otras cosas, del *Big Data* y de un sofisticado software de reconocimiento facial. El gobierno puede saber cuando alguien sale de su casa, si tiene temperatura o no, y enviar un dron para disuadir a la persona de salir de casa y recordarle que la reclusión domiciliaria es obligatoria.

Asimismo, los ciudadanos chinos pueden saber con alta precisión donde se ubican las personas infectadas y evitar zonas infectadas. La aplicación "detector de contacto cercano" notifica al usuario si ha estado en contacto cercano con un portador de virus y muestra un mapa entero de los infectados. Todos los movimientos de una persona son rastreables y esa información es usada para fines lícitos y también para otros fines ampliamente debatibles. En México no hemos estado lejos de dicha realidad pues, el uso de aplicaciones de rastreo es una realidad, por ejemplo, el Gobierno de la Ciudad de México el 13 de noviembre de 2020 lanzó el controvertido "Sistema para identificación de contagios en espacios cerrados" en el marco de las acciones de Rastreo Epidemiológico implementadas por el Gobierno de la Ciudad de México"[13] con el propósito de identificar casos positivos de COVID-19 y notificar a las personas que coin-

[11] Para un estudio de la expresión "Datos personales sensibles" recomendamos consultar la voz correspondiente a este término en Davara F. de Marcos, Isabel (Coord), Diccionario de Protección de Datos Personales, México, Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), 2019, Disponible en https://home.inai.org.mx/wp-content/documentos/Publicaciones/Documentos/DICCIONARIO_PDP_digital.pdf

[12] Para un estudio de la expresión "Big Data" recomendamos consultar la voz correspondiente a este término en Davara F. de Marcos, Isabel (Coord), Diccionario de Protección de Datos Personales, México, Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), 2019, Disponible en https://home.inai.org.mx/wp-content/documentos/Publicaciones/Documentos/DICCIONARIO_PDP_digital.pdf

[13] Trigésimo Aviso por el que se da a conocer el color del Semáforo Epidemiológico de la Ciudad de México, se establecen diversas medidas de protección a la salud que deberán observarse derivado de la Emergencia Sanitaria por COVID-19 y se establecen modificaciones a los Lineamientos para la Ejecución del Plan Gradual hacia la Nueva Normalidad en la Ciudad de México, disponible en

https://data.consejeria.cdmx.gob.mx/portal_old/uploads/gacetas/2fb946e2848d72358ad2e36dbdda3327.pdf

cidieron en un mismo lugar, a efecto de cortar cadenas de contagio para minimizar, contener y controlar la propagación del virus.

El ejemplo anterior pone de manifiesto una cosa muy clara. La tecnología y el uso de datos pueden ser sumamente útiles, pero también pueden tener una incidencia clara en nuestro derecho humano a la privacidad, o técnicamente hablando, a la protección de datos personales.

Por ello, es preciso tomar en cuenta que, si bien, la contención del COVID-19 y la adopción de medidas para su mitigación es una finalidad legítima y congruente con las obligaciones que, en materia laboral, de salud y prevención de riesgos laborales establece la normatividad aplicable, contar con una base de legitimación del tratamiento de datos sensibles no basta. Según lo previsto por la LGPDPPSO, la LFPDPPP y las normativas locales de protección de datos personales será esencial y obligatorio que todo tratamiento garantice la observancia de los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, los deberes de seguridad y confidencialidad, y por supuesto, con las limitaciones concretas que existen permita el ejercicio de los derechos ARCO.

Esta tarea no es sencilla, pues una interrogante constante es la de ¿Cómo garantizar la adecuada protección de los datos en un contexto tan complejo e impredecible? Sin embargo, es importante precisar que las autoridades nacionales e internacionales de protección de datos personales han desempeñado un papel fundamental al emitir recomendaciones y guías de orientación concretas al respecto.

En este contexto, autoridades de protección de datos personales en países como Albania, Alemania, Andorra, Argentina, Australia, Austria, Bulgaria, Canadá, Colombia, República Checa, España, Estados Unidos, Filipinas, Finlandia, Francia, Georgia, Gibraltar, Hungría, Irlanda, Italia, Lituania, Luxemburgo, Nueva Zelanda, Países Bajos, Perú, Polonia, Reino Unido y Suiza han emitido recomendaciones específicas para legitimar el tratamiento de datos personales en relación con el COVID-19.[14] En el panorama internacional ha sido fundamental el papel del Comité Europeo de Protección de Datos[15] que ha emitido numerosas recomendaciones a este respecto y que sirven de orientación para las autoridades de control en el mundo, entre las que destacan por su importancia práctica las Directrices 04/2020 sobre el uso de datos de localización y herramientas de rastreo de contactos en el contexto de la pandemia de COVID 19[16] y las Directrices 03/2020 sobre el tratamiento de datos relativos a la salud con fines de científica en el contexto del brote de COVID 19.[17]

En México, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), que también forma parte de la GPA y será la autoridad encargada de presidirla a partir de este año, ha destacado por las acciones emprendidas para orientar el tratamiento de datos relacionados frente a la crisis originada por la COVID-19. El INAI creó el micrositio “Datos Personales Seguros COVID- 19”[18] con el propósito de brindar a las personas que son atendidas por Coronavirus, en instituciones públicas o privadas, información clara y precisa sobre su derecho a la protección de datos personales, y además, publicó la “Guía de protección de datos personales para las personas titulares en situaciones de emergencia”[19] para dar a conocer a las personas titulares de los datos personales qué información se deberá recabar, para qué fines, quién hará el tratamiento y, en su caso, cómo se debe hacer la transferencia o transmisión de ésta.

---

[14] En el enlace https://globalprivacyassembly.org/covid19/ de la Global Privacy Asseembly (GPA) se pueden consultar directamente los distintos materiales generados por las autoridades de los países citados

[15] https://edpb.europa.eu/edpb_es

[16] Comité Europeo de Protección de Datos, “Directrices 04/2020 sobre el uso de datos de localización y herramientas de rastreo de contactos en el contexto de la pandemia de COVID 19”, abril de 2020, disponibles en https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_es.pdf

[17] Comité Europeo de Protección de Datos, “Directrices 03/2020 sobre el tratamiento de datos relativos a la salud con fines de científica en el contexto del brote de COVID 19”, abril de 2020, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_es.pdf

[18] Disponible en https://micrositios.inai.org.mx/covid-19/

[19] INAI, Guía de protección de datos personales para las personas titulares en situaciones de emergencia, 2020, disponible en https://home.inai.org.mx/wp-content/uploads/GuiaTitularesPDP_Emergencia_VF.pdf

IV. Experiencia comparada: medidas aplicadas en Latinoamérica

En Latinoamérica la pandemia ha obligado a diversos países de la región a implementar medidas concretas para la contención de la pandemia, entre estas acciones destacan aquellas relacionadas con el uso de la tecnología, principalmente de aplicaciones de rastreo siendo uno de los países pioneros en su uso Uruguay. A continuación, señalamos algunos de los casos más relevantes en la región.

- **Uruguay.** El Ministerio de Salud Pública de Uruguay señala como parte de la Estrategia Digital frente al coronavirus COVID-19, el gobierno uruguayo junto a la colaboración de distintos actores puso a disposición de la población la aplicación Coronavirus UY. Coronavirus UY permite conectar a los ciudadanos con posibles síntomas del coronavirus COVID-19 con los prestadores de salud, a fin de reducir los tiempos de espera de consultas y atención ante la emergencia sanitaria.[20]

- **Argentina.** El gobierno de Argentina lanzó la aplicación denominada *CUIDAR*[21] que entre sus funcionalidades y propósitos incluye la posibilidad de geolocalizar a los individuos.

- **Chile.** La División de Gobierno Digital del Ministerio Secretaría General de la Presidencia desarrolló una aplicación de seguimiento y asistencia en materias relacionadas con el contagio de COVID-19, llamada CoronApp.[22]

- **Colombia.** El gobierno lanzó la aplicación denominada CoronApp que facilita el monitoreo en tiempo real de datos recopilados al Centro de Operaciones de Emergencias del Instituto Nacional de Salud (INS), para que puedan actuar rápidamente y dar apoyo en coordinación con las autoridades locales, departamentales y nacionales.[23]

- **Costa Rica.** La Caja Costarricense del Seguro Social, institución pública proveedora de servicios de salud, incorporó un nuevo apartado a la aplicación del Expediente Digital Único en Salud (EDUS), para uso exclusivo de lo referente al COVID-19.[24]

- **Panamá.** El gobierno de Panamá lanzó la aplicación “Protégete Panamá” desarrollada por la Autoridad Nacional para la Innovación Gubernamental (AIG) en conjunto con el Ministerio de Salud, utilizando un desarrollo realizado por las empresas Apple y Google, que permite comunicarle a los usuarios, de manera anónima, si han estado expuestos con algún positivo de COVID-19.[25]

- **Perú.** El gobierno peruano creó la aplicación *PERÚ EN TUS MANOS*[26] para advertir a los ciudadanos sobre las zonas con mayor probabilidad de contagio.

Los ejemplos anteriores son una muestra clara del uso intensivo de la tecnología para atender y mitigar los riesgos relacionados con la COVID-19, y aunque su uso puede ser lícito, es importante reiterar la importancia de que estos desarrollos incorporen desde la fase previa a su diseño y durante todo el ciclo de vida de la información las garantías necesarias para proteger los datos personales de las personas.

[20] https://www.gub.uy/ministerio-salud-publica/politicas-y-gestion/informacion-sobre-aplicacion-coronavirus

[21] https://www.argentina.gob.ar/aplicaciones/coronavirus

[22] https://coronapp.gob.cl

[23] https://coronaviruscolombia.gov.co/COVID19/aislamiento-saludable/coronapp.html

[24] https://www.ccss.sa.cr/appedus/

[25] https://protegete.panamasolidario.gob.pa/descargar.html

[26] https://apps.apple.com/mx/app/peru-en-tus-manos/id1506397362

V. Conclusiones

Tratar datos personales para enfrentar la pandemia originada por el COVID-19 es esencial, y la normatividad de protección de datos personales no inhibe su tratamiento ni lo prohíbe, pero sí obliga a los responsables de los sectores público y privado a cumplir con una serie de obligaciones concretas durante el ciclo de vida del tratamiento de esta información. Es absolutamente relevante tomar en cuenta esta premisa para realizar un uso legítimo de los datos y garantizar los derechos humanos de las personas, pues, como se señaló en el encuentro más importante de autoridades de protección de datos “GPA 2021) “la protección de datos debe estar enfocada en el ser humano” quien es el sujeto de los derechos y a quien la normatividad protege frente al uso ilícito de los datos personales.

Sin embargo, las organizaciones, tanto públicas como privadas, además deben tener en cuenta que, es evidente que la normatividad no puede brindar todas las respuestas plausibles ni hacer frente a los desafíos derivados del uso de la tecnología, por lo que, los responsables del tratamiento de los datos deben pensar además en la adopción de un marco ético frente al tratamiento de los datos personales que permee todas las decisiones de la organización e incluya esta máxima como un principio rector de todo tratamiento de datos, sea automatizado o no.

Dra. Isabel Davara F. de Marcos

Socia Fundadora y Directora de Davara Abogados S.C.

Doctora en Derecho y Licenciada en Derecho, y en Ciencias Económicas y Empresariales, por la Universidad Pontificia Comillas de Madrid. Vicepresidenta del Ilustre y Nacional Colegio de Abogados de México, Consejera del Consejo General de la Abogacía Mexicana, Secretaria del Consejo Directivo de la Asociación de Internet MX, líder de Privacidad de la American Chamber of Commerce of Mexico y Socia Fundadora de DAVARA ABOGADOS, Firma legal especializada en Derecho Digital, Tecnología e Innovación. Correo: Idavara@davara.com.mx

VI. Fuentes de Consulta

Documentos consultados

Comité Europeo de Protección de Datos (2020), “Directrices 03/2020 sobre el tratamiento de datos relativos a la salud con fines de científica en el contexto del brote de COVID 19”, Recuperado de https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_es.pdf

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

Davara F. de Marcos, I. (Coord). (2019). Diccionario de Protección de Datos Personales, México, Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. Recuperado de https://home.inai.org.mx/wp-content/documentos/Publicaciones/Documentos/DICCIONARIO_PDP_digital.pdf

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (2020), Guía de protección de datos personales para las personas titulares en situaciones de emergencia, Recuperado de https://home.inai.org.mx/wp-content/uploads/GuiaTitularesPDP_Emergencia_VF.pdf

Velázquez Arrroyo L. (2020) “Análisis del acuerdo por el que se declara como emergencia sanitaria por causa de fuerza mayor”, en González Martín, Nuria (Coord.) Emergencia sanitaria por COVID-19: Reflexiones desde el derecho (III). (pp. 86-91), México, IIJ-UNAM. Recuperado de https://covid19.humanidades.unam.mx/covid19/2020/05/24/emergencia-sanitaria-por-covid-19-reflexiones-desde-el-derecho-iii-158/

Criterios jurisprudenciales

Tesis 1a. CCXIII/2009, Semanario Judicial de la Federación y su Gaceta, Novena Época, t. XXX, diciembre de 2009, p. 276.

Tesis 1a. XLIX/2014 (10a.), Gaceta del Semanario Judicial de la Federación, Décima Época, t. I, febrero de 2014, p. 641.

Tesis: 1a. CCXV/2013 (10a.), Semanario Judicial de la Federación y su Gaceta, Décima Época, t. I, julio de 2013, p. 557.

Tesis: 2a. XCII/2016 (10a.), Gaceta del Semanario Judicial de la Federación, Décima Época, t. I, Septiembre de 2016, p. 842.