La protección de los datos personales y la geolocalización en el contexto de la pandemia

Autora:
Basterra, Marcela I.

Cita: RC D 3219/2020
Sumario:

1. Introducción. 2. Las aplicaciones oficiales y la protección de datos en el derecho comparado y los organismos internacionales. 3. La aplicación "Cuid.Ar" en Argentina y la protección de datos. 4. La geolocalización personal. 5. Conclusiones.

La protección de los datos personales y la geolocalización en el contexto de la pandemia

1. Introducción

La expansión del COVID-19 originó una situación de emergencia pública en virtud de la cual se implementaron instrumentos de contención, que en muchos casos suponen la suspensión y/o limitación de derechos fundamentales.

Las acciones estatales incluyeron el uso de tecnología de vigilancia para rastrear la propagación del virus y el almacenamiento de datos de forma masiva. En este sentido, los estados diseñaron aplicaciones para la prevención y autoevaluación del coronavirus, con la finalidad de evitar contagios y optimizar los recursos sanitarios. Estos instrumentos recolectan diversos datos personales de los usuarios, e incluso algunas permiten a las autoridades obtener datos sobre la geolocalización de los individuos, situación que motivó algunos interrogantes, ocasionando un fuerte debate en Argentina como en otros países del mundo, ante lo que *"prima facie"* implica una colisión de derechos fundamentales. Por un lado, el derecho a la salud pública y, por el otro, el derecho a la privacidad, más específicamente, a la protección de datos personales de los usuarios.

2. Las aplicaciones oficiales y la protección de datos en el derecho comparado y los organismos internacionales

Las agencias de protección de datos personales de los distintos países adoptaron diversas posiciones respecto al procesamiento de información de los posibles afectados por el virus COVID-19, pudiéndose distinguir tres (3) tipos de enfoques; restrictivo, neutral y permisivo[1]. El enfoque restrictivo se caracteriza por aplicar como variable rígida la ley local de protección de datos personales, exigiendo siempre el consentimiento del individuo. Es decir, se pondera el derecho a la privacidad y al control de los datos sobre el derecho a la salud pública. El segundo enfoque, es un criterio intermedio, se permite recolectar información personal del usuario, pero aplica limitaciones basadas en los principios vigentes en la materia. De esta forma, la potestad del Estado de obtener datos se encuentra condicionada, por ejemplo, debe destruirse la información obtenida una vez finalizada la emergencia sanitaria. Por último, el criterio permisivo prioriza el derecho a la salud frente a las normas de protección de datos personales, posibilitando compartir e incluso publicar la información cuando sea eficaz para la prevención del contagio.

En el marco de la emergencia sanitaria es importante tener presente los parámetros de los organismos internacionales. En efecto, el Comité Europeo de Protección de Datos señaló que las normas del Reglamento General de Protección de Datos[2] no obstaculizan las medidas adoptadas en la lucha contra la pandemia, e incluso en este tipo de situaciones excepcionales, el control y el procesamiento de la información deben proteger los datos personales de los interesados. Para garantizar la licitud en el tratamiento, cualquier medida tomada en este contexto debe respetar los principios generales del derecho y no debe ser irreversible[3].

3. La aplicación "Cuid.Ar" en Argentina y la protección de datos

En Argentina, el gobierno nacional implementó la aplicación denominada *"COVID 19-Ministerio de Salud",* herramienta tecnológica que ofrece información sobre los síntomas y/o prevención del COVID-19 con la finalidad de evitar la propagación del virus, como también para erigirse en una fuente de información fidedigna para los usuarios.

La implementación de esta medida motivó una fuerte polémica, básicamente porque la aplicación puede acceder a la geolocalización del usuario, lo que implica una injerencia en el derecho a la privacidad. En virtud de ello, la Agencia Nacional de Acceso a la Información Pública, indicó la forma en que debían tratarse los datos personales de los afectados señalando los principios fundamentales de la legislación vigente que deben tenerse en cuenta. Entre ellos, el requisito de recabar el consentimiento previo del titular de los datos (art. 5, LPDP), destacando que los datos referidos a la salud son considerados datos sensibles, conforme a los artículos 2 y 7 de la Ley 25326[4].

En esta línea, el consentimiento resulta ser un elemento esencial. Justamente, todos los bancos, archivos o bases de datos como regla general, deben requerir de modo previo el consentimiento de los titulares, salvo que los datos se encuentren en alguno de los supuestos legales que eximen del mismo[5]. La normativa nacional se diferencia de otros ordenamientos como el Reglamento de la Unión Europea, que prevé además, el interés legítimo para la licitud del tratamiento de datos personales, otorgando mejores posibilidades en el procesamiento de información ante la emergencia sanitaria. Es por ello, que la política de privacidad de la aplicación "Cuid.Ar" formula la necesidad de contar con el consentimiento del usuario para la licitud del tratamiento de datos personales, al no encontrarse comprendida en ninguna de las excepciones previstas en el artículo 5. En consecuencia, la herramienta exige el consentimiento para la recolección y procesamiento de determinada información personal del usuario.

La LDPD es aplicable aún en el contexto de pandemia. Sin embargo, la emergencia requiere que esa norma sea aplicada de manera que no impida que el Estado actúe en forma eficiente, toda vez que están en juego otros derechos fundamentales, como el derecho individual a la salud y el derecho colectivo a la salud pública.

4. La geolocalización personal

Sin lugar a dudas, la práctica estatal de conservar datos de localización de un individuo afecta su derecho a la privacidad, tal como lo ha reconocido la jurisprudencia del Tribunal Europeo de Derechos Humanos[6] y la Suprema Corte de los Estados Unidos, en el *leading case "Carpenter"*[7].

Sin embargo, algunos ordenamientos permiten el sistema de rastreo. En efecto, la Ley Orgánica española Nº 3/2018[8], establece en el ámbito laboral que los empleadores para el ejercicio de las funciones de control de los trabajadores podrán tratar los datos obtenidos a través de sistemas de geolocalización. Es preciso advertir que la Agencia Nacional de Acceso a la Información Pública, declaró que el monitoreo de la ubicación de las personas no se encuentra prohibido expresamente ni por la Ley 25326 ni tampoco por el Convenio 108[9], del cual Argentina es parte[10]. Además, señaló que la recopilación podrá realizarse cuando el titular haya prestado su consentimiento libre, expreso e informado, el que podrá ser obtenido a través de la aceptación de términos y condiciones en una aplicación o plataforma web.

Teniendo en consideración la política de privacidad que determina que los datos se preservarán únicamente mientras sean necesarios para cumplir con los fines para los que fueron recolectados y mientras dure la emergencia sanitaria, es decir, que cumplirán con el principio de finalidad y adecuación de los datos (art. 4.7 de la LPDP), podemos afirmar *"prima facie"* que la recolección de la información referida a la ubicación del usuario es consistente con los principios fundamentales de la regulación vigente en la materia, máxime, si se cumple con el requisito excluyente del consentimiento, en los términos establecidos en el art. 5 de la LPDP. No obstante ello, debemos estar muy atentos, dado que en caso de incumplimiento por parte del Estado de los principios referidos, se configuraría una lesión arbitraria e injustificada del derecho a la privacidad.

5. Conclusiones

La Corte Suprema de Justicia de la Nación, en el caso *"N. N. o U., V. s/ Protección y guarda de personas"*[11], expresó que si bien *"el resguardo de la privacidad de cada individuo es un ámbito de incuestionable tutela por parte de nuestra Constitución"*, debe ceder en los supuestos en los que se ponga en riesgo la salud de toda la comunidad. En este antecedente el Alto Tribunal pondera el derecho a la salud pública, sobre el derecho a la privacidad.

Sin lugar a dudas, la pandemia genera un dilema de compleja solución. La emergencia sanitaria no habilita la vulneración del derecho de protección de los datos personales, ni tampoco del derecho a la privacidad. Por el contrario, es indispensable que las medidas diseñadas para prevenir el contagio garanticen los parámetros consagrados en la normativa nacional y los criterios que la comunidad internacional ha esbozado en torno al tema.

Como lo señaló el Director Nacional de la Agencia de Acceso a la Información *"la emergencia sanitaria nos obliga a pensar soluciones inéditas para un problema que es, a la vez, inédito"*[12]. Por un lado, es indispensable garantizar el derecho fundamental a la protección de datos personales, pero al mismo tiempo, la normativa no puede limitar la efectividad de las medidas estatales. Indudablemente, este tipo de situaciones interpela a los gobiernos a diseñar instrumentos innovadores que no se encuentran previstos en la legislación.

El Comité Ejecutivo de la Asamblea Global de Privacidad ha reconocido que *"Los principios universales de protección de datos en todas nuestras leyes permitirán el uso de información en cuestiones que revistan interés público y aún proporcionarán las protecciones que el público espera"*[13]. Considero que es posible armonizar los derechos fundamentales en aparente colisión, si el tratamiento de la información cumple con los principios analizados, efectivizando el derecho a la privacidad, a la protección de los datos personales y, al mismo tiempo, generando significativos beneficios para un bien jurídico esencial como es la salud pública.

[1]

Ampliar de Palazzi, Pablo A., Elaskar, Mercedes, "Pandemia (COVID-19) y protección de datos personales. Primeras aproximaciones", L.L., 13/05/2020, Cita Online: AR/DOC/1068/2020., p. 2.

[2]

Reglamento de la Unión Europea (UE) 2016/679 del Parlamento europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento y a la libre circulación de datos personales, que deroga la Directiva 95/46/CE, aprobado el 27/04/2016 y vigente desde el 25/05/2018.

[3]

Comité Europeo de Protección de Datos, "Declaración sobre el procesamiento de datos personales en circunstancias de emergencia", publicado el 19/03/2020, disponible en https://blogs.upm.es/covid19upm/2020/03/30/declaracion-del-comite-europeo-de-proteccion-de-datos-sobre-el-procesamiento-de-datos-personales-en-circunstancias-de-emergencia/ (Consultado el 16/10/2020).

[4]

Agencia de Acceso a la Información Pública, "Protección de datos personales y geolocalización", 29/04/ 2020, disponible en https://www.argentina.gob.ar/noticias/proteccion-de-datos-personales-y-geolocalizacion (Consultado el 16/10/2020).

[5]

Puede ampliarse de Basterra Marcela I., "El consentimiento del afectado en el proceso de tratamiento de datos personales" JA -Lexis Nexis-. Número Especial, 28/04/2004, p. 6.

[6]

Tribunal Europeo de Derechos Humanos, Caso "Amann c. Suiza", 16/02/2000, párr. 65-67, "Rotaru c. Rumania", 04/05/2000, párr. 43-44; "Shimovolos c. Rusia", 21/06/2011, párr. 58-59.

[7]

Suprema Corte de los Estados Unidos, Caso "Carpenter v. United States", 22/06/2018.

[8]

Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales, publicada en el B.O el 06/12/2018.

[9]

Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal suscripto en 28/01/1981.

[10]

Agencia de Acceso a la Información Pública, "Protección de datos personales y geolocalización", op. cit.

[11]

CSJN, "N. N. o U., V. s/ Protección y guarda de personas", Fallos 335:888, 12/06/2012.

[12]

Agencia de Acceso a la Información Pública, "Protección de datos personales y geolocalización", op. cit.

[13]

Declaración del Comité Ejecutivo de la Asamblea de Privacidad Global sobre la pandemia de coronavirus (COVID-19), 17/03/2020, disponible en https://globalprivacyassembly.org/gpaexco-covid19/ (Consultado el 16/10/2020).