.

DIPUTADOS
ARGENTINA

2020 - Año del General Manuel Belgrano

PROYECTO DE RESOLUCIÓN

La Cámara de Diputados resuelve…

ARTÍCULO 1.- Solicitar al Poder Ejecutivo Nacional que, a través de la Secretaria de Innovación Pública dependiente de la Jefatura de Gabinete de Ministros de la Nación, brinde la siguiente información relacionada la aplicación móvil CuidAR - COVID 19-Ministerio de Salud -:

1.- Entidades estatales y/o establecimientos sanitarios nacionales, provinciales o municipales a los cuales la Subsecretaría de Gobierno Abierto cederá la información personal del usuario recolectada por la aplicación, luego de prestar el consentimiento requerido en el punto 5.5. de los “Términos y Condiciones” de la citada aplicación.

2.- Razones que justifican que la aplicación utilice la función de geolocalización de los todos sus usuarios.

3.- Organismos que actuarán como responsables del archivo y el tratamiento de los datos recolectados en la aplicación móvil.

4.- Plazo de registro y tratamiento de los datos recolectados en la aplicación móvil.

5.- Mecanismo para garantizar la supresión de los datos recolectados una vez cesada la emergencia sanitaria.

6.- Relación contractual con los sitios web de terceros en los que se encuentra publicada la aplicación móvil, en particular, Facebook, Google y Amazon.

7.- La APP permite la conexión a través de FACEBOOK, específicamente con el subsitio "server_side_reward", el cual es utilizado para monetizar el tráfico publicitario, o videos / imágenes en general:

- Indicar si la aplicación está permitiendo producir una ganancia económica a partir del tráfico de los usuarios y quién es el beneficiario de las mismas.
- Mencionar si se establece otra relación con Facebook para poder conectarse.
- Confirmar si se involucra el perfil del usuario de la APP instalada.

8.- La aplicación móvil utiliza "API" de GOOGLE (entre las que se destaca el uso de los métodos: fitness.blood_glucose.read/write, fitness.blood_pressure.read/write, entre otros):

- Indicar si existe alguna relación con GOOGLE para la para poder utilizar las API mencionadas.
- Confirmar si se está enviando la información médica (presión, glucosa) de los usuarios a través de la nube de Google.

9.- Del análisis de la conectividad de CuidAR, surge la utilización de la "nube" de Amazon, empresa que, a la fecha, no cuenta con infraestructura instalada en el país:

- Mencionar qué información se transmite por dicha nube
- Indicar si la información de usuarios argentinos se almacena fuera del país.

10.- Medidas técnicas y organizativas adoptadas para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado.

11.- Medidas técnicas y organizativas adoptadas que permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.

12.- Mecanismo adoptado para evitar la formación de archivos, bancos o registros con información sensible, recolectada por la aplicación móvil.

13.- Organismo encargado de enviar los avisos y mensajes *(“tipo push”)* insertos en la aplicación de conformidad con lo dispuesto en el punto 11 de sus “Términos y Condiciones”.

14.- Finalidad de los avisos y mensajes *(“tipo push”)* que la aplicación enviaría de conformidad con lo dispuesto en el punto 11 de sus “Términos y Condiciones”.

15.- Política de actualización de la aplicación, en particular, cuáles son los criterios para la actualización y si se requerirán nuevos permisos del usuario y de qué forma se comunicarán.

16.- Brindar el informe correspondiente al “pentest” - test de penetración- realizado a la aplicación.

Cristian Ritondo
Silvia Lospennato
Alvaro Gonzalez
Brenda Austin
Maximiliano Ferraro
Juan Manuel Lopez

FUNDAMENTOS

Señor presidente,

Los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, se encuentran protegidos por nuestra Constitución Nacional y los Tratados Internacionales sobre derechos humanos con jerarquía constitucional, a fin de garantizar el derecho al honor, a la privacidad y a la intimidad de las personas.

Mediante la Decisión Administrativa 432/2020 del Ministerio de Salud se implementó la utilización de la aplicación denominada COVID 19-Ministerio de Salud tanto en sus versiones para dispositivos móviles Android o IOS, como en su versión web, accesible a través de https://argentina.gob.ar/coronavirus/app. Y por disposición 3/2020 de la Jefatura de Gabinete de Ministros se dispuso crear la base de datos de igual nombre, con la finalidad de centralizar los datos recabados por dicha aplicación.

Que en el punto 5.3. del título 5 “Protección de Datos Personales. Política de privacidad” de los Términos y Condiciones de la Aplicación “COVID 19-Ministerio de Salud” se especifica que el usuario presta su “consentimiento expreso para que la Secretaría trate los datos personales que el usuario declare” e información “referida a su salud tal como síntomas, antecedentes médicos y diagnóstico”, como así también “información de geolocalización que la Aplicación recolecte en forma automatizada”.

Que en el punto 5.5. del título 5 “Protección de Datos Personales. Política de privacidad” de los Términos y Condiciones de la Aplicación “COVID 19-Ministerio de Salud”, se indica que el usuario “presta su consentimiento expreso para que la Subsecretaría de Gobierno Abierto ceda la información personal del Usuario recolectada por la Aplicación a otras entidades estatales y/o establecimientos sanitarios nacionales, provinciales o municipales, para que estos puedan contener y/o mitigar la propagación del virus COVID-19, ayudar a prevenir la sobreocupación del sistema sanitario argentino y para cualquier otra finalidad que se relacione con la emergencia provocada por la pandemia”.

La BASE DE DATOS "COVID-19 Ministerio de Salud" fue creada con la finalidad de receptar datos vinculados con el estado de salud de los usuarios a través de una autoevaluación propuesta por la herramienta informática, relacionada con los síntomas de COVID19, no obstante advertimos que: la información recabada no es anónima; se obtienen datos de georreferenciación en forma automática al ingresar desde los dispositivos móviles; se contempla la cesión de datos hacia jurisdicciones, entidades y organismos de la Administración Pública Nacional, sin identificación expresa del destinatario de los mismos

y el fin de dicha cesión y no se precisan las medidas técnicas y organizativas adoptadas para garantizar la seguridad y confidencialidad de los datos personales.

La Comisión Interamericana de Derechos Humanos (CIDH) publicó el documento "Pandemia y Derechos Humanos en las Américas" en el que recomienda a los Estados de la región que las medidas adoptadas para "la atención y contención del virus deben tener como centro el pleno respeto de los derechos humanos".

La CIDH recuerda que cualquier restricción o limitación a los derechos humanos para proteger la salud pública en el marco de la pandemia debe cumplir con los principios de legalidad, necesidad y proporcionalidad a dicha finalidad.

Particularmente, la CIDH también insta a los Estados a garantizar el derecho a la privacidad y tratamiento de datos personales de pacientes y personas que se realizan 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", indica la CIDH.

Respecto del uso de las herramientas de vigilancia digital para el seguimiento de la pandemia, la CIDH señala que "los Estados deben transparentar las herramientas de vigilancia que están utilizando y su finalidad, así como poner en marcha mecanismos de supervisión independientes del uso de estas tecnologías de vigilancia, y los canales y mecanismos seguros para recepción de denuncias y reclamaciones".

Se ha dicho, y con razón, que, *"[e]n el siglo XXI… los datos eclipsarán a la vez la tierra y la maquinaria como los bienes más importantes, y la política será una lucha para controlar el flujo de datos"* (HARARI, Yuval Noah, "21 lecciones para el siglo XXI", ed. Debate, 2019, p. 100).

Pues bien, entendemos imprescindible contar con la información técnica requerida para asegurar que el poder de turno - con independencia de su color político o ideológico - no entrará en la lógica del control de los datos personales. Máxime, de aquellos que revisten el carácter de sensible, relacionados de manera íntima - como adelantáramos - con el derecho a la intimidad, al honor, etc., protegidos tanto constitucional como convencionalmente.

Entre los aspectos consultados, se destaca la posibilidad de cesión de los datos recabados, de la cual, por cierto, no tenemos mayores precisiones. En este sentido, baste traer a colación el reciente escándalo de Facebook y Cambridge Analytica para ilustrar la preocupación que genera en la sociedad situaciones como ésta.

Por lo demás, la geolocalización de las personas plantea, asimismo, un poder en cabeza del Estado que, aun con las mejores intenciones, puede desembocar en una seria desviación que ponga en juego la intimidad de las personas, permitiendo que el Gobierno conozca los “pasos” de las personas, con las múltiples - y temibles - consecuencias que de ello pudiera derivarse.

Asimismo, es necesario dilucidar claramente cuál es la relación que tiene la aplicación con empresas tales como Facebook, Google, Amazon, etc.: más precisamente, si los datos recogidos por la “app” llegan a sus bases de datos.

En otro orden de ideas - pero siempre en la misma senda de la protección de los datos y de los derechos que sobre ellos se asientan - surgen múltiples cuestiones más técnicas, si se quiere, que precisan - a nuestro entender - una urgente aclaración (vg. "mensajes tipo push", el "copiado y pegado" del manual del usuario, el mecanismo de actualización de la aplicación, la existencia o no de un “pentest” y su detalle, entre otras).

Por último, no podemos dejar de lado el contexto en el cual nos encontramos, es decir, aquel en el que el Poder Ejecutivo Nacional ha venido gobernando mediante decretos de necesidad y urgencia de un tiempo a esta parte, lo que configura un fenómeno de centralización del poder que no es sino profundizado por la implementación de la aplicación de referencia.

Volviendo al terreno constitucional, nuestra ley fundamental nos conmina a garantizar los derechos humanos, es nuestro deber proteger el derecho a la intimidad, a la privacidad y al honor de las personas. Por ello resulta necesario contar con la información requerida a fin de garantizar el debido tratamiento de los datos personales de las personas que utilizan la Aplicación “COVID 19-Ministerio de Salud”.

Por las razones expuestas, solicito a los señores diputados el acompañamiento para la aprobación del presente proyecto de resolución.

Cristian Ritondo
Silvia Lospennato
Alvaro Gonzalez
Brenda Austin
Maximiliano Ferraro
Juan Manuel Lopez