PROYECTO DE RESOLUCIÓN

La Honorable Cámara de Diputados

RESUELVE

Solicitar al Poder Ejecutivo Nacional que, a través de los organismos que corresponda, brinde a esta Honorable Cámara de Diputados de la Nación la siguiente información:

1.- Indicar si la Agencia de Acceso a la Información Pública de la Nación emitió observaciones y/o recomendaciones respecto a la información requerida en el formulario de la aplicación Cuidar y en el Certificado Único Habilitante para Circulación (CUHC) según lo establecido en el artículo 4, inciso 1 de la Ley N° 25.326. En caso afirmativo, detalle las observaciones y/o recomendaciones por parte de la Agencia de Acceso a la Información Pública e identifique qué medidas adoptó la Secretaría de Innovación Pública ante dichos hallazgos.

2.- Informar si la Secretaría de Innovación Pública de la Nación suscribió acuerdos de confidencialidad con los Comités de Emergencia Operativa Provinciales (COEPS) y sus funcionarios dependientes, con el fin de resguardar el deber de secreto determinado en los artículos 8 y 10 de la Ley N° 25.326. En caso afirmativo, individualice con qué Provincias se firmaron acuerdos.

3.- Mencionar si la Secretaría de Innovación Pública de la Nación ha elaborado procedimientos para garantizar la seguridad y confidencialidad de los datos personales recolectados mediante la aplicación Cuidar y el Certificado Único Habilitante para Circulación (CUHC) en cumplimiento con lo dispuesto en los artículos 9 y 10 de la Ley N° 25.326 y en la Resolución AAIP N° 47/2018. En caso afirmativo, detalle dichos procedimientos y cuáles son los funcionarios responsables de ejecutar las medidas técnicas y organizativas para garantizar la seguridad y confidencialidad de los datos.

4.- Informar si la Secretaría de Innovación Pública de la Nación elaboró los correspondientes protocolos para la implementación de los procesos de eliminación de datos, asegurando que el contenido confidencial sea debidamente destruido, utilizando métodos de borrado seguro y aplicando un control eficaz del proceso, una vez que finalice la emergencia sanitaria determinada en el Decreto N° 260/2020. En caso afirmativo, detalle dichos procedimientos y cuáles son los funcionarios responsables de cada una de las acciones.

5.- Indicar si se han realizado auditorías y/o informes para verificar el estado en la seguridad y confidencialidad de las bases de datos de la aplicación Cuidar y del Certificado Único Habilitante para Circulación (CUHC). En caso afirmativo, informar qué organismo público o privado intervino; el detalle de las observaciones y/o recomendaciones y mejoras realizadas por la Secretaría de Innovación Pública.

6.- Informar si el Estado Nacional suscribió contrato de transferencia internacional con Amazon Web Services Inc. (AWS), que garantice el cumplimiento de las salvaguardas fundamentales en materia de protección de los datos personales de la aplicación Cuidar, de acuerdo a lo establecido en el artículo 12 de la Ley N° 25.326; el Decreto N° 1.558/2001; la Disposición DNPDP N° E-60/2016 y normas complementarias y modificatorias. En caso afirmativo, indicar quién es el funcionario público que suscribió el contrato por el Estado Nacional; cuáles son las obligaciones asumidas por Amazon Web Inc.; cuáles son los compromisos por parte del Estado Nacional e indique si la Agencia de Acceso a la Información Pública se expidió sobre el contrato y cuál fue su opinión.

7.- Mencionar si la Dirección Nacional de Ciberseguridad del Estado Nacional efectuó un análisis de las vulnerabilidades, estructuras de protección de centros de datos, y riesgos de ciber-amenazas en relación a las bases de datos de la aplicación Cuidar y del Certificado Único Habilitante para Circulación (CUHC). En caso afirmativo, informar los resultados de los monitoreos efectuados y el plan de acción desarrollado.

8.- Informar los avances respecto a la Estrategia de ciberseguridad desarrollada por el Estado Nacional determinada a través de la Resolución SGM N° 829/20 normas modificatorias y complementarias.

9.- Indicar las acciones instrumentadas por el Comité de Ciberseguridad creado a través del Decreto N° 577/2017 normas modificatorias y complementarias.

10.- Informar si el Estado Nacional ha efectuado una evaluación de la infraestructura provincial y/o municipal a efectos de proteger y detectar posibles amenazas que tuvieran origen o tránsito en el ciberespacio argentino. En caso afirmativo, detalle las acciones que se llevaron a cabo en cada uno de los estados subnacibronales.

Firmante: LOSPENNATO, Silvia
Co Firmantes: REY, María Luján
REVIZNOSKY, Dina
OCAÑA, Graciela
SOHER, El Sukaria
POLLEDO, Carmen
FREGONESE, Alicia
STEFANI, Hector
ENRIQUEZ, Jorge
JOURY, Mercedes
CRESCIMBENI, Camila
MORALES GORLERI, Victoria
CACERES, Adriana
PICCOLOMINI, Carla

FUNDAMENTOS

Señor Presidente,

Traemos a consideración de este cuerpo un pedido de informe en relación a las respuestas correspondientes a las preguntas N° 606 a N° 621 del Informe N° 126/2020 presentado por el Señor Jefe de Gabinete de Ministros ante la Honorable Cámara de Diputados de la Nación con fecha del 30 de julio del 2020 y en función al incremento del ciberdelito en la Argentina en el marco del "Aislamiento Social, Preventivo y Obligatorio (ASPO)".

El Poder Ejecutivo Nacional mediante el Decreto de Necesidad y Urgencia N° 260/2020 amplío la emergencia pública en materia sanitaria establecida por Ley N° 27.541, en virtud de la Pandemia declarada por la ORGANIZACIÓN MUNDIAL DE LA SALUD (OMS) en relación con el coronavirus Covid-19, por el plazo de UN (1) y el 19 de marzo del 2020, estableció a través del Decreto de Necesidad y Urgencia N° 297/2020 el *ASPO* para todo el territorio del país, con el objetivo de proteger la salud pública, desde el 20 de marzo de 2020 hasta *"el tiempo que se considere necesario en atención a la situación epidemiológica"*.

En dicho marco, el Estado Nacional implementó el sistema y aplicación Cuidar (en adelante Cuidar) a través de la Decisión Administrativa N° 432/2020 con el fin de detectar tempranamente los casos y garantizar la atención y seguimiento, así como para evitar la transmisión del virus Covid-19.

Asimismo, Cuidar se relaciona con un sistema más amplio que articula las bases de la mencionada herramienta informática y los datos recabados por las diferentes áreas sanitarias responsables del cuidado ante la emergencia a nivel provincial, y las ciudadanas y ciudadanos a su vez son puestos en contacto con el Comité de Emergencia Provincial (COEP) de la jurisdicción en la que se encuentren.

Por otra parte, Cuidar se vincula con el Certificado Único Habilitante para Circulación (CUHC) y posibilita emitirlo. La tramitación del CUHC tiene carácter obligatorio mientras dure el ASPO y se obtiene para que la ciudadanía pueda circular siempre y cuando estén exceptuados.

La OMS mediante un Informe publicado en mayo de 2020 sobre el uso de tecnologías de la información y la comunicación aplicada, indicó que: *"Los estados miembros están obligados, bajo las Leyes Internacionales de Salud a desarrollar sistemas de vigilancia de salud pública que capturen información crítica para la respuesta del Covid-19, asegurándose que dichos sistemas sean transparentes, respondan a las preocupaciones de la comunidad, y no impongan innecesarias cargas para la población, por ejemplo que no infrinjan la privacidad"*.

Mientras tanto, la Comisión Interamericana de Derechos Humanos (CIDH) en el punto Quinto del Comunicado de Prensa N° 58/2020 señala que: *"somos conscientes del creciente uso de herramientas de tecnología de vigilancia para rastrear la propagación del coronavirus. Si bien comprendemos y apoyamos la necesidad de realizar esfuerzos activos para hacer frente a la pandemia, también es crucial que el uso de dichas herramientas sea limitado, tanto en términos de propósito como de tiempo, y que se protejan rigurosamente los derechos individuales a la privacidad, la no discriminación, la protección de las fuentes periodísticas y otras libertades. Los Estados también deben proteger la información personal de los pacientes. cInstamos encarecidamente a que todo uso de esa tecnología se atenga a las más estrictas protecciones y que sólo esté disponible de acuerdo a la legislación nacional que sea compatible con las normas internacionales de derechos humanos"*.

A su vez, la CIDH en el apartado 20 de la Resolución N° 1/20: *"Pandemia y Derechos Humanos en las Américas"* sostuvo que: *"Asegurar que toda restricción o limitación que se imponga a los derechos humanos con la finalidad de protección de la salud en el marco de la pandemia Covid-19 cumpla con los requisitos establecidos por el derecho internacional de los derechos humanos. En particular, dichas restricciones deben cumplir con el principio de legalidad, ser necesarias en una sociedad democrática y, por ende, resultar estrictamente proporcionales para atender la finalidad legítima de proteger la salud".*

En ese mismo orden de ideas el apartado 35 establece que: *"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"*.

Nuestra Constitución en el artículo 43, sobre los registros personales, establece que: *"(...) Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquéllos"*.

La Ley N° 25.326 y el Decreto N° 1558/2001 tienen por objeto la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la

información que sobre las mismas se registre, de conformidad a lo establecido en el artículo 43 recientemente mencionado de nuestra Carta Magna.

La Corte Suprema de Justicia de la Nación (CSJN), en reiterados pronunciamientos, sostuvo que: *"(...) El derecho a la privacidad comprende no sólo a la esfera doméstica, el círculo familiar y de amistad, sino a otros aspectos de la personalidad espiritual o física de las personas tales como la integridad corporal o la imagen y nadie puede inmiscuirse en la vida privada de una persona ni violar áreas de su actividad no destinadas a ser difundidas, sin su consentimiento, o el de sus familiares autorizados para ello y sólo por ley podrá justificarse la intromisión, siempre que medie un interés superior en resguardo de la libertad de los otros, la defensa de la sociedad, las buenas costumbres o la persecución del crimen"* (fallos: 306:1892; 314:1531, voto del juez Boggiano, 316:479, disidencia de los jueces Cavagna Martínez y Boggiano; 316:703; CSJN, Autos: *"Ganora, Mario Fernando y otra s/ hábeas corpus"* (16/09/1999) - Fallos: 322: 2139).

Por su parte, la Asamblea General de Naciones Unidas sobre el derecho a la privacidad en la era digital expresó que: *"aunque la vigilancia no es en sí misma una violación de los Derechos Humanos"*, cualquier *"limitación del derecho a la privacidad debe respetar los principios generales de legalidad, necesidad y proporcionalidad"*.

Asimismo, manifestó que: *"Si bien los metadatos pueden aportar beneficios, algunos tipos de metadatos, tomados en conjunto, pueden revelar información personal y pueden dar indicación del comportamiento, las relaciones sociales, las preferencias privadas y la identidad de una persona",* pone de relieve que: *"La vigilancia y la interceptación ilegales o arbitrarias de las comunicaciones, así como la recopilación ilegal o arbitraria de datos personales, al constituir actos de intrusión grave, violan el derecho a la privacidad y pueden interferir con el derecho a la libertad de expresión y ser contrarios a los preceptos de una sociedad democrática, en particular cuando se llevan a cabo a gran escala"* y exhortó a los estados a que: *"Aseguren que las decisiones basadas en un tratamiento automatizado que afecte de manera significativa los derechos de una persona sean transparentes y no tengan efectos discriminatorios"*.

Lo parafraseado recientemente está en consonancia con lo establecido por el artículo 12 de la Declaración Universal de Derechos Humanos y el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos, ambos con jerarquía constitucional, de acuerdo a lo establecido por el artículo 75 inciso 22 de la Constitución Nacional.

Ahora bien, desde la Asociación Argentina de Lucha Contra el Cibercrimen (AALCC) indicaron que durante el ASPO se observó un incremento de delitos como la extorsión online (20,42 %), el *"phishing"* - robo de datos - (16,53 %) y el fraude (14,89 %). https://www.cibercrimen.org.ar/2020/05/03/importante-incremento-de-delitos-informaticos-en-cuarentena/.

Recientemente, una investigación de seguridad realizada por la empresa Comparitech, encontró que la información de CIENTO QUINCE MIL DOSCIENTOS OCHENTA Y UN (115.281) permisos de circulación del Gobierno Provincial de San Juan, incluyendo el nombre completo; número de Documento Nacional de Identidad (DNI); número de la Clave Única de Identificación Laboral (CUIL); género; fecha de nacimiento; foto; número de teléfono y correo electrónico estuvieron subidos a la red sin contraseña ni ningún otro tipo de autenticación de acceso. https://www.comparitech.com/es/blog/seguridad-de-informacion/en-argentina-el-ministerio-de-sanidad-hace-publica-la-informacion-personal/

Determinaron que la información pertenecía al Ministerio de Sanidad de San Juan por una cookie creada desde la misma dirección IP. El nombre de la cookie es: "certificados_covid_19_ministerio_de_salud_publica". La dirección de Protocolo de Internet (IP, por sus siglas en inglés) también incluía una página muy parecida a otras páginas oficiales del Gobierno de San Juan.

"Como se ha demostrado, el sistema empleado para la solicitud de los permisos de circulación es muy vulnerable. Los delincuentes podrían obtener los permisos a nombre de otras personas y usarlos para saltarse las restricciones de la cuarentena. Quienes hayan solicitado el permiso deberían estar pendientes, ya que podrían ser víctimas de un ataque de "phishing"e. Los delincuentes podrían usar la información de la base de datos para crear mensajes convincentes y engañar a las víctimas para que hagan click en enlaces de "phishing". Incluso podrían acosarlos con información personal o financiera más delicada".

Las estadísticas evidencian que los diversos organismos públicos que manejan bases de datos con información sensible de los argentinos deben diseñar estrictos procedimientos y protocolos de seguridad y privacidad, herramientas informáticas preventivas y coordinar acciones interjurisdiccionales con el fin de proteger derechos y libertades fundamentales de la ciudadanía.

Por las razones expuestas, solicito a mis pares el acompañamiento para la aprobación del presente proyecto de resolución.

Firmante: LOSPENNATO, Silvia
Co Firmantes: REY, María Luján
REVIZNOSKY, Dina
OCAÑA, Graciela
SOHER, El Sukaria
POLLEDO, Carmen
FREGONESE, Alicia
STEFANI, Hector
ENRIQUEZ, Jorge
JOURY, Mercedes
CRESCIMBENI, Camila
MORALES GORLERI, Victoria
CACERES, Adriana
PICCOLOMINI, Carla