República Argentina - Poder Ejecutivo Nacional
2021 - Año de Homenaje al Premio Nobel de Medicina Dr. César Milstein

Resolución

Número: RESOL-2021-64-APN-DNPDP#AAIP

CIUDAD DE BUENOS AIRES
Jueves 20 de Mayo de 2021

Referencia: EX-2020-51851773- -APN-DNPDP#AAIP. Resolución.

VISTO el EX-2020-51851773- -APN-DNPDP#AAIP, las Leyes Nros. 25.326 y 27.275, los Decretos Nros. 1558 del 29 de noviembre de 2001 y modificatorio, 746 del 25 de septiembre de 2017, 899 del 3 de noviembre de 2017 y 1012 del 16 de diciembre del 2020; las Resoluciones Nros. 30 del 14 de mayo del 2018, 47 del 23 de julio de 2018 y 83 del 23 de abril de 2020; y la Disposición DNPDP Nº 7 del 8 de noviembre del 2005 y sus modificatorias; y

CONSIDERANDO:

Que la AGENCIA DE ACCESO A LA INFORMACIÓN PÚBLICA (en adelante, "AGENCIA" o "AAIP"), a través de la DIRECCIÓN NACIONAL DE PROTECCIÓN DE DATOS PERSONALES (en adelante, "DIRECCIÓN" o "DNPDP") inició una investigación de oficio con motivo de una supuesta vulnerabilidad de la base de datos del portal de trámite de permisos de circulación de la PROVINCIA DE SAN JUAN, a partir de la cual se podría acceder a datos personales -incluyendo datos sensibles- de los ciudadanos que figuren en el registro único sobre historial médico del sistema sanitario público de la Provincia, "Andes Salud".

Que dieron motivo a la investigación los informes y noticias publicadas en la prensa durante el mes de agosto de 2020, que se incorporaron al expediente mediante IF-2020-51942791-APN-DNPDP#AAIP.

Que conforme al relato de los artículos periodísticos, una alerta sobre la vulnerabilidad del sistema habría sido enviada a la Dirección Nacional De Ciberseguridad el 28 de julio de 2020. Por ello, el 7 de agosto de 2020 esta AGENCIA remitió la nota identificada como NO-2020-51998899-APN-DNPDP#AAIP a la mencionada Dirección solicitando que, en caso de haber efectivamente tomado algún tipo de intervención, remitiera copias de lo actuado.

Que el 10 de agosto de 2020 la Dirección Nacional De Ciberseguridad brindó su respuesta confirmando que recibieron una notificación por parte del personal de la empresa consignada como Security Discovery sobre una posible exposición de información sobre datos de pacientes infectados con COVID-19 registrados en la base de datos del MINISTERIO DE SALUD de la PROVINCIA DE SAN JUAN (SJ). En este sentido, el organismo agrega que "*En un lapso breve de tiempo, personal de la Coordinación de Emergencias de Respuesta*

Teleinformáticas Nacional (CERT.ar) notifica por la misma vía al Subsecretario de Tecnologías de la Información y Comunicación de la Provincia de San Juan (...) Al día siguiente, 29 de julio, por la mañana, el personal del CERT.ar mantuvo contacto telefónico con las autoridades del área provincial de ciberseguridad quienes informaron que se encontraban trabajando en el caso. Alrededor del mediodía el servidor ya no se encontraba disponible."

Que la Dirección Nacional De Ciberseguridad especificó que pudieron corroborar que la referida era una base de datos de desarrollo del año 2019 de pacientes del Sistema Andes Salud, del registro único sobre historial médico del sistema de sanitario público de la PROVINCIA DE SAN JUAN y no contendría datos de pacientes infectados con COVID-19.

Que, asimismo, el organismo adjuntó un reporte de actuación del CERT.ar del cual surge que Security Discovery intentó contactarse primero con personal de San Juan y no obtuvo resultados. Por último, el CERT.ar informa que no tuvo registro de algún incidente informático vinculado a un uso malicioso de dichos datos por parte de terceros.

Que, a partir de la información proporcionada por la Dirección Nacional De Ciberseguridad, el 13 de agosto del 2020, la AAIP le requirió al MINISTERIO DE SALUD (SJ), por medio de la NO-2020-53311523-APN-AAIP, que indicara: si la base de datos correspondiente al Sistema Andes Salud fue la única base de datos en estado de vulnerabilidad durante el incidente de seguridad; quienes son los organismos responsables de la base del sistema y si la información que la integra corresponde únicamente al sistema de salud provincial; qué medidas de seguridad poseía la infraestructura antes del incidente y qué organismo realizaba su implementación; cuánto tiempo estuvo desprotegido; qué medidas adoptaron luego de tomar conocimiento del incidente aludido; y qué categorías de datos integran la base de datos del Sistema Andes Salud.

Que el 27 de agosto de 2020 el MINISTERIO DE SALUD (SJ) respondió las consultas por medio del correo electrónico oficial de la máxima autoridad de esa cartera. Dicha respuesta fue incorporada al expediente mediante el informe IF-2020-58563013-APN-DNPDP#AAIP.

Que, respecto de la primera consulta, el MINISTERIO DE SALUD (SJ) contestó que la referida base de datos se encontraba en ambiente de desarrollo y era la única con elasticsearch (ELK) v6.4.2. Además, el MINISTERIO DE SALUD (SJ) explicó que la misma prestaba un servicio de indexación para la gestión agilizada de la base de desarrollo Andes Salud.

Que en relación con el segundo punto solicitado por la AAIP, el MINISTERIO DE SALUD (SJ) sostuvo que es el responsable por la disponibilidad, confiabilidad e integridad de los datos de salud y que la Secretaría de la Gestión Pública, a través de la Dirección Provincial de Informática y la Subsecretaría de Infraestructura Tecnológica, es la responsable del código, arquitectura, componentes tecnológicos y seguridad de la aplicación.

Que sobre las medidas de seguridad que poseía la infraestructura, el MINISTERIO DE SALUD (SJ) detalló que antes del incidente el entorno de desarrollo era sólo accesible desde la red local. Sin embargo, a partir del mes de abril de 2020, la base se publicó en internet para facilitar el trabajo remoto y, por lo tanto, quedó desprotegida desde entonces.

Que luego de conocer la exposición, el MINISTERIO DE SALUD (SJ) indicó que apagó y retiró físicamente el único servidor con el servicio ELK y se hizo una solicitud de pentesting a la Dirección Nacional de Ciberseguridad de todas las URLs productivas de Andes.

Que, por último, el MINISTERIO DE SALUD (SJ) sostuvo que al momento del incidente la cantidad de registros de ciudadanos de la Provincia de San Juan que se encontraban en la base fue de CIENTO QUINCE MIL DOSCIENTOS OCHENTA Y DOS (115.282). Asimismo, detalló los datos personales que integran la base de datos del Sistema Andes Salud, indicando que son: nombre completo, número de DNI, número de CUIL, género, fecha de nacimiento, foto, número de teléfono y correo electrónico.

Que, en vista de la información proporcionada, se labró el Acta de Constatación identificada como ACTA-2020-60035662-APN-DNPDP#AAIP de conformidad con lo dispuesto por el artículo 31 del Anexo I del Decreto N° 1558 del 29 de noviembre de 2001 y modificatorios que establece el procedimiento a seguir en el caso de presuntas infracciones, y que expresamente dispone en el Punto 3 apartado g) que *"Cuando se considere "prima facie" que se han transgredido algunos preceptos de la Ley N° 25.326, sus normas reglamentarias y complementarias, se labrará un Acta de constatación…"*.

Que, en el Acta, se consideró que haber dejado expuesta la base de datos fue plena responsabilidad del MINISTERIO DE SALUD (SJ), pues no tomó las medidas de diligencia necesarias para asegurar la seguridad y la confidencialidad de los datos conforme a los artículos 9 y 10 de la Ley N° 25.326.

Que, en efecto, el artículo 9, inciso 1 de la Ley N° 25.326 establece que *"[e]l responsable o usuario del archivo de datos debe adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado, y que permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado"*.

Que, por su parte, el artículo 10, inciso 1 de la misma Ley sostiene que "*[e]l responsable y las personas que intervengan en cualquier fase del tratamiento de datos personales están obligados al secreto profesional respecto de los mismos"*.

Que, de esta manera, se concluyó que al *"[m]antener bases de datos locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se* determinen", el MINISTERIO DE SALUD (SJ) cometió UNA (1) infracción grave conforme el punto 2, inciso k) del Anexo I a la Disposición DNPDP Nº 7 del 8 de noviembre del 2005 y modificatorias.

Que, al mismo tiempo, al "*[i]ncumplir el deber de confidencialidad exigido por el artículo 10 de la Ley N° 25.326 sobre los datos de carácter personal incorporados a registros, archivos, bancos o bases de datos"*, el MINISTERIO DE SALUD (SJ) cometió, adicionalmente, UNA (1) infracción grave de conformidad con el punto 2, inciso j) del Anexo I a la Disposición DNPDP Nº 7/05 y modificatorias.

Que, sin perjuicio de las sanciones que resultan aplicables, resulta oportuno destacar que el organismo sancionado no ha tenido en cuenta la Resolución AAIP N° 47 del 23 de julio de 2018, por medio de la cual se establecieron un conjunto de medidas de seguridad recomendadas para el tratamiento y conservación de los datos personales en medios informatizados.

Que, en relación con lo anterior, corresponde destacar la Sección C del Anexo I de la Resolución AAIP N° 47/2018, en el que se recomienda, en materia de control de cambios, *"[d]isponer de un registro de las verificaciones y/o pruebas realizadas para asegurar la integridad, disponibilidad y confidencialidad de los datos"*.

Que, asimismo, ha de tenerse en cuenta la Sección E del mismo Anexo, referida a la gestión de vulnerabilidades,

en particular donde se recomienda "*[p]revenir incidentes de seguridad desde el diseño"*; "*[c]onsiderar y analizar los posibles amenazas a la que estarán expuestos los sistemas informatizados"*; y "*[e]stablecer controles de seguridad para las aplicaciones que procesen datos personales"*.

Que por otra parte, cabe señalar que la Disposición DNPDP 7/05 y modificatorias establece en el punto 2 de su Anexo II que en el caso de las INFRACCIONES GRAVES, la sanción a aplicar será de hasta CUATRO (4) APERCIBIMIENTOS, SUSPENSION DE UNO (1) a TREINTA (30) DIAS y/o MULTA de PESOS VEINTICINCO MIL UNO ($ 25.001,00) a PESOS OCHENTA MIL ($ 80.000,00).

Que, frente al Acta ACTA-2020-60035662-APN-DNPDP#AAIP ya aludida, la titular del MINISTERIO DE SALUD de la PROVINCIA DE SAN JUAN efectuó su descargo el día 23 de septiembre del 2020. Dicho descargo se incorporó al expediente bajo IF-2021-01499601-APN-DNAIP#AAIP.

Que, en particular, la señora Ministra expresó que *"...la Secretaría de la Gestión Pública, organismo encargado de la Dirección Informática y la Subsecretaría de Infraestructura Tecnológica desde el primer momento han abordado el tema ocupándose del mismo con la máxima celeridad y responsabilidad (...) concretando el descargo destaco que la vulnerabilidad imputada se produjo por el accionar incorrecto de un dependiente, que, sin autorización de su superior, en el marco de la pandemia y por el afán de proveer una solución de acceso remoto para teletrabajo, expuso el contenido con las consecuencias que se destacaron en la formulación del cargo oportunamente remitida (...) es dable destacar que se ha iniciado el expediente sumarial para determinar la responsabilidad que le cabe al agente en cuestión. Asimismo, entiendo conveniente poner en su conocimiento que a los efectos de la mejora de las acciones y seguridad de los datos estamos en proceso de contratación de una consultoría de diseño e implementación de un Plan Director de Ciberseguridad. Por otra parte, estamos abocados a la creación de un Equipo de Respuesta ante Incidentes de Seguridad, el "SJ-CSIRT" (Computer Security Incident Response Team), ello para reforzar la organización asociada a la gestión de ciberseguridad, con perfiles específicos y eso va a ser informado en forma progresiva a ese organismo. En razón de lo expuesto solicito a esa Dirección, tenga por formulado el descargo y reconsidere el cargo formulado, peticionando que, por ser el incidente imputado, el primero de su especie, sin más trámite se resuelva librarnos del cargo y el archivo de las actuaciones..."*.

Que más allá de los argumentos allí esgrimidos, se admitió una vez más que el MINISTERIO DE SALUD (SJ) es el responsable por la disponibilidad, confiabilidad e integridad de los datos de salud y, así también, es responsable por los actos de sus dependientes. En este mismo sentido, se admitió que la infraestructura de informática utilizada para exponer el contenido de la base de datos en estado de vulnerabilidad dependía del Ministerio, razón más que suficiente para atribuirle responsabilidad en tanto responsable de la base de datos y confirmar en todos sus términos las infracciones constatadas en autos.

Que, al momento de merituar la sanción, se tuvieron en cuenta distintas características del caso. En principio, se evaluaron rigurosamente los documentos que detallaron el obrar de la provincia y, como resultado, se comprobó que el MINISTERIO DE SALUD (SJ) activó prontamente los protocolos de sus áreas técnicas para dar una solución a la vulnerabilidad y mitigar sus efectos. Asimismo, se entendió que, dado el presente contexto de pandemia, resulta necesario contemplar la imperiosa necesidad que está atravesando la Provincia de San Juan -junto a toda la República Federal Argentina- de destinar la mayor cantidad de sus fondos públicos al manejo de la crisis económica y sanitaria, en pos del cuidado de la salud de los ciudadanos.

Que de esta manera, y acompañado por el hecho de que el aquí sumariado carece de infracciones previas, no se encuentra argumento para justificar la imposición de una sanción pecuniaria y, así pues, corresponde aplicar en

este caso DOS (2) APERCIBIMIENTOS de conformidad con lo dispuesto en la Disposición N° 7/2005 y modificatorias.

Que en orden a la competencia para dictar el presente acto administrativo cabe señalar que por el artículo 19 de la Ley N° 27.275 se creó la AGENCIA DE ACCESO A LA INFORMACIÓN PÚBLICA como ente autárquico con autonomía funcional en la órbita de JEFATURA DE GABINETE DE MINISTROS.

Que por Ley N° 27.275, modificada por Decreto N° 746 del 25 de septiembre de 2017 y el Decreto 899 del 3 de noviembre 2017 se atribuyó al citado ente, la facultad de actuar como Autoridad de Aplicación de la Ley Nº 25.326.

Que por ser la cesión de datos llevada adelante entre distintos organismos provinciales interconectados a la base de datos de Andes Salud, resulta pertinente aclarar que, sin perjuicio de ello, esta AGENCIA DE ACCESO A LA INFORMACIÓN PÚBLICA es el órgano competente para controlar el cumplimiento de la Ley Nº 25.326 en general, y la cesión de datos entre estos organismos en particular. La competencia de la AAIP al respecto surge de lo establecido en el artículo 44 de la mencionada ley, en cuanto dispone que *"[l]a jurisdicción federal regirá respecto de los registros, archivos, bases o bancos de datos interconectados en redes de alcance interjurisdiccional, nacional o internacional"*.

Que, de ello surge -tal como lo viene sosteniendo la AAIP- que toda cesión que exceda la sola jurisdicción de una provincia está sometida al contralor de los jueces federales y de la AAIP, que es la autoridad federal en materia de protección de datos.

Que el caso *sub-examine* prevé la configuración de una base de datos en ambiente de desarrollo, con servicio de indexación para la gestión agilizada de la base de desarrollo Andes Salud y, que si bien dichos servidores se localizan en la PROVINCIA DE SAN JUAN, estos se encuentran conectados a la Internet, ofreciendo un alcance transfronterizo inmensurable y, consecuentemente, de ningún modo limitado al alcance provincial.

Que, por ello, la AAIP es la autoridad competente para controlar que dichas cesiones se adecúen a las previsiones previstas por la Ley N° 25.326, e incluso llevar adelante las recomendaciones para el cumplimiento de la misma a las autoridades locales fuera de la órbita del Gobierno Federal.

Que ante ausencia del titular de la AAIP y a los efectos de garantizar el normal desenvolvimiento del organismo, de conformidad con lo dispuesto por la Resolución AAIP N° 30 del 14 de mayo de 2018, se ha encomendado la atención del despacho y la resolución de los asuntos concernientes a la competencia del titular de la AGENCIA DE ACCESO A LA INFORMACIÓN PÚBLICA, en el señor Director Nacional de Protección de Datos Personales, Dr. Eduardo Hernán CIMATO, delegándose la firma correspondiente.

Que ha tomado la intervención que le compete la Coordinación de Asuntos Jurídicos de la AGENCIA DE ACCESO A LA INFORMACIÓN PÚBLICA.

Que la presente medida se dicta en uso de las facultades conferidas por el artículo 19 de la Ley Nº 27.275; por el artículo 29, inciso 1, apartado f) de la Ley N° 25.326; y por la Resolución AAIP N° 30/18.

Por ello,

EL DIRECTOR NACIONAL DE PROTECCIÓN DE DATOS PERSONALES

DE LA AGENCIA DE ACCESO A LA INFORMACIÓN PÚBLICA

RESUELVE:

ARTÍCULO 1º.- Aplícase al MINISTERIO DE SALUD de la PROVINCIA DE SAN JUAN la sanción de DOS (2) APERCIBIMIENTOS por haber incurrido en DOS (2) infracciones graves consistentes en: *"[m]antener bases de datos locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen"*, e *"[i]ncumplir el deber de confidencialidad exigido por el artículo 10 de la Ley N° 25.326 sobre los datos de carácter personal incorporados a registros, archivos, bancos o bases de datos"*, de conformidad con los puntos 2, incisos k) y j), respectivamente, del Anexo I a la Disposición DNPDP Nº 7/05 y modificatorias.

ARTÍCULO 2º.- Notifíquese al MINISTERIO DE SALUD de la PROVINCIA DE SAN JUAN, haciéndole saber que la presente resolución agota la vía administrativa, quedando expedita la acción judicial, la que deberá interponerse dentro de los NOVENTA (90) días hábiles judiciales de notificado el acto. Asimismo, podrá deducir recurso de reconsideración dentro del plazo de DIEZ (10) días, de acuerdo con lo normado por el artículo 84 del Decreto N° 1759/72 (T.O. 2017).

ARTÍCULO 3º.- Hágase saber a la interesada que el 23 de abril de 2020 esta AGENCIA DE ACCESO A LA INFORMACIÓN PÚBLICA dictó la Resolución N° 83, mediante la cual estableció el criterio de declarar inadmisibles los recursos de alzada, en consonancia con la Ley N° 27.483 que en su artículo 1° aprobó el Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal, suscripto en la ciudad de Estrasburgo, República Francesa, el día 28 de enero de 1981, y el Protocolo Adicional al Convenio, suscripto en la ciudad de Estrasburgo, República Francesa, el día 8 de noviembre de 2001.

ARTÍCULO 4°.- Tómese nota en el REGISTRO DE INFRACTORES - LEY N° 25.326 y cumplido, oportunamente, archívese.

Digitally signed by CIMATO Eduardo Hernan
Date: 2021.05.20 11:13:17 ART
Location: Ciudad Autónoma de Buenos Aires

Eduardo Hernán Cimato
Director Nacional
Dirección Nacional de Protección de Datos Personales
Agencia de Acceso a la Información Pública

Digitally signed by Gestion Documental Electronica
Date: 2021.05.20 11:13:25 -03:00