

## AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS CONFIRMA SANCIÓN A ENTIDAD ESTATAL POR VULNERAR LAS NORMAS DE PROTECCIÓN DE DATOS MEDIANTE APLICACIÓN MÓVIL (APP) CONTRA LA COVID-19

En el marco del Procedimiento Sancionador N° PS/00222/2021 llevado en contra de la Secretaría de Estado de Digitalización e Inteligencia Artificial (en adelante, la “Secretaría de Digitalización”) del Ministerio de Asuntos Económicos y Transformación Digital (en adelante, el “MTD”) del Reino de España, el 10 de junio de 2022, mediante la Resolución N° RR/00189/2022, la Directora de la Agencia Española de Protección de Datos (en adelante, la “AEPD”) confirmó la sanción de apercibimiento impuesta por incumplir obligaciones previstas en el Reglamento (UE) 2016/679 - Reglamento General de Protección de Datos del 27 de abril de 2016 (en adelante, el “RGPD”).

En las siguientes líneas, presentamos los principales aspectos comprendidos en la Resolución y las implicancias de las sanciones contra entidades estatales.

### 1. CIRCUNSTANCIAS QUE PRODUJERON LA SANCIÓN

Conforme a lo establecido en el Acuerdo de fecha 23 de junio de 2020, respecto a las políticas del Consejo de Ministros del Gobierno Español para contrarrestar la crisis sanitaria por la pandemia de la COVID-19, en fecha 29 de junio de 2020 se puso a prueba el piloto de la aplicación para celulares (*app*) denominada “Radar COVID” en la isla canaria “La Gomera”, con el objetivo de conocer los contactos recientes de una persona con resultado positivo.

La aplicación fue desarrollada por la empresa INDRA en virtud del contrato suscrito con la Secretaría de Estado de

Digitalización, con la finalidad de rastrear los contactos que tuvo una persona contagiada en los últimos catorce (14) días, a través de la identificación que realizó la señal de *bluetooth* de su celular con los móviles de las personas que interactuaron con esta.

Para tal efecto, se recopilaban datos personales de terceros que serían conocidos con un código de uso único, brindado por el hospital luego del resultado positivo. Los datos servirían para las estrategias del Ministerio de Sanidad (o Ministerio de Salud en el Perú), quien con el MTD serían responsables del tratamiento de datos personales, mientras que la Secretaría de Digitalización tendría la condición de encargado.

En ese sentido, en fecha 03 de agosto de 2020, el MTD publicó que la *app* había superado la fase de pruebas y se lanzó a nivel nacional el 19 de agosto de 2020. Ello sin considerar que la Evaluación de Impacto de Protección de Datos (en adelante, la “EIPD”), realizada recién en fecha 12 de agosto de 2020, concluyó que la aplicación no presentaba un método de “anonimización” debido a que permitía que personas ajenas al ámbito sanitario puedan identificar y conocer la ubicación de quienes fueron registrados por la aplicación.

De esta manera, y a consecuencia de las constantes reclamaciones realizadas debido a las vulnerabilidades en el diseño en la aplicación, en fecha 21 de mayo de 2021, la AEPD apertura un Procedimiento Administrativo, que devino en la imposición de una sanción contra la entidad.

### 2. VULNERACIONES COMETIDAS CONTRA EL RGPD

En la Resolución del Procedimiento Sancionador N° PS/00222/2021 se impuso

a la Secretaría de Digitalización la sanción por infringir principalmente el artículo 35<sup>1</sup> del Reglamento General de Protección de Datos de la Unión Europea, que estipula la obligación del responsable del tratamiento de realizar previamente la EIPD, en el caso de nuevas tecnologías.

Al respecto, se debe puntualizar que, aunque la entidad estatal trató de justificar su actuar en la premura por la crisis sanitaria, la AEPD señaló que tales circunstancias no impedían la protección del derecho a la protección de datos que reconoce como derecho fundamental.

Por su parte, se atribuyó que, de lo previsto en el RGPD, la Secretaría de

Digitalización infringió: (i) el artículo 5<sup>2</sup> referente a los principios del tratamiento de la protección de datos; (ii) el artículo 18<sup>3</sup> respecto a la limitación del tratamiento de datos personales; (iii) el artículo 25<sup>4</sup> sobre a la protección de datos desde el diseño de un producto; y (iv) el artículo 28<sup>5</sup> que aborda las obligaciones del encargado del tratamiento de datos personales.

En consecuencia, al no encontrarse prevista una sanción específica para el caso de las entidades públicas, se resolvió efectuar un apercibimiento a la entidad, de conformidad a lo estipulado en el literal b<sup>6</sup> del numeral 2 del artículo 58 del RGPD.

<sup>1</sup> Reglamento (UE) 2016/679 - Reglamento General de Protección de Datos de 27 de abril de 2016:

Artículo 35. -Evaluación de impacto relativa a la protección de datos

*“1. Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, (...), el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales (...).”*

<sup>2</sup> Reglamento (UE) 2016/679 - Reglamento General de Protección de Datos de 27 de abril de 2016:

Artículo 5.- Principios relativos al tratamiento

*“Los datos personales serán:*

*a) tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»);*

*b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines (...).”*

<sup>3</sup> Reglamento (UE) 2016/679 - Reglamento General de Protección de Datos de 27 de abril de 2016:

Artículo 18.- Derecho a la limitación del tratamiento

*“1. El interesado tendrá derecho a obtener del responsable del tratamiento la limitación del tratamiento de los datos cuando se cumpla alguna de las condiciones siguientes: (...)*

*b) el tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso.”*

<sup>4</sup> Reglamento (UE) 2016/679 - Reglamento General de Protección de Datos de 27 de abril de 2016:

Artículo 25.- Protección de datos desde el diseño y por defecto

*“Teniendo en cuenta el estado de la técnica, (...), el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos (...).”*

<sup>5</sup> Reglamento (UE) 2016/679 - Reglamento General de Protección de Datos de 27 de abril de 2016:

Artículo 28.- Encargado del tratamiento

*“1. Cuando se vaya a realizar un tratamiento por cuenta de un responsable del tratamiento, este elegirá únicamente un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con los requisitos del presente Reglamento y garantice la protección de los derechos del interesado (...).”*

<sup>6</sup> Reglamento (UE) 2016/679 - Reglamento General de Protección de Datos de 27 de abril de 2016:

Artículo 58.- Poderes

*“2. Cada autoridad de control dispondrá de todos los siguientes poderes correctivos indicados a continuación: (...)*

*b. dirigir a todo responsable o encargado del tratamiento un apercibimiento cuando las*

### 3. MOTIVOS PARA DESESTIMAR LA REPOSICIÓN

Con la Resolución N° RR/00189/2022, se confirmó la sanción impuesta a la Secretaría de Digitalización y se descartó el recurso de reposición (o reconsideración en el Perú) interpuesto por la entidad.

Sobre el particular, conviene señalar que, la AEDP indicó que en el recurso no se presentó circunstancia nueva alguna que la lleven a cambiar de decisión, ya que la alegación de que el uso de la aplicación solo se realizó durante la fase piloto no desvirtuó el incumplimiento de su obligación.

En concordancia con ello, agregó que el hecho de llevar a cabo de manera posterior la EIPD no subsana su falta de realización oportuna, el cual ocasionó un daño intangible en los derechos de las personas.

### 4. COMENTARIO

La emisión de un pronunciamiento como este de la AEPD, en el que se confirma la sanción a una entidad estatal, no es una situación ajena al contexto nacional dada las noticias sobre filtración de datos personales por parte de la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros del Perú, que fue advertida por la Asociación de Bancos del Perú (ASBANC) durante el mes de mayo del presente año.

En tal sentido, llama la atención el hecho de que solo se haya sancionado a la Secretaría de Digitalización española con el “apercibimiento” en una situación de tratamiento de datos personales de salud que tienen

---

*operaciones de tratamiento hayan infringido lo dispuesto en el presente Reglamento”.*

categoría de sensibles, bajo el argumento de que no se tiene previsto normativamente sanciones específicas contra entidades públicas por infringir obligaciones de protección de datos, puesto que es una circunstancia similar a lo establecido en la Ley N° 29733 - Ley de Protección de Datos peruana.

En ese orden de ideas, se plantea un contexto de desigualdad ante la ley, en el que aparentemente ante infracciones se sanciona de manera estricta a los administrados, pero no así a la administración.

Al respecto debe señalarse que, en el Perú, la Autoridad Nacional de Protección de Datos Personales (ANPDP) sí tiene precedentes de sanción pecuniaria a entidades del Estado por vulnerar obligaciones legales referidas a la protección de datos personales, como el caso de la Superintendencia Nacional de Migraciones, a quien se le sancionó por la filtración de datos en el Aeropuerto Internacional Jorge Chávez con una multa ascendente a S/ 171,644.00.

Por tanto, resta esperar que, en la fiscalización aperturada por la ANPDP respecto a la denuncia de la ASBANC por la filtración de datos personales, se continúe con el criterio previamente empleado, puesto que de lo contrario se estaría ante un escenario de desigualdad ante la ley no justificado, que es contrario a lo establecido por el ordenamiento jurídico.