



Procedimiento Nº AP/00050/2017

RESOLUCIÓN: R/00432/2018

En el procedimiento de Declaración de Infracción de Administraciones Públicas **AP/00050/2017**, instruido por la Agencia Española de Protección de Datos a la entidad **INSTITUTO DE SALUD PÚBLICA Y LABORAL DE NAVARRA**, vista la denuncia presentada por el **SINDICATO AFAPNA**, y en virtud de los siguientes,

ANTECEDENTES

PRIMERO: Con fecha 22 de febrero de 2017, tiene entrada en esta Agencia un escrito de Don **B.B.B.**, actuando en nombre y representación del Sindicato AFAPNA, (en lo sucesivo el denunciante), en el que pone de manifiesto que el Instituto de Salud Pública y Laboral de Navarra ha creado con los datos facilitados por el Departamento de Educación del Gobierno de Navarra un grupo de “WhatsApp” sin el consentimiento de los afectados, en el que constan todos los números de teléfono de los D.D.D. en prácticas para comunicarles la realización de las revisiones médicas que ha de practicarles.

SEGUNDO: A la vista de los hechos denunciados, en fase de actuaciones previas, por los Servicios de Inspección de esta Agencia se solicita información al Instituto de Salud Pública y Laboral de Navarra, en adelante el Instituto denunciado o ISPLN, que ha puesto de manifiesto al respecto:

Que el grupo de “WhatsApp” se creó en los primeros días de febrero de 2017 y se eliminó a las 8 horas dado que sirvió a los efectos para los que fue creado.

La finalidad fue informar a los D.D.D. en prácticas que debían ponerse en contacto telefónico con la Sección de Valoración Clínico Laboral e Inspección Médica del Instituto para llevar a cabo el preceptivo reconocimiento médico establecido en la convocatoria para el acceso a la función pública.

Los D.D.D. en prácticas eran cerca de 200, aunque en el grupo de “WhatsApp” creado sólo se incluyeron los 30 D.D.D. con los que no se había conseguido contactar a través de otras vías.

Cualquier miembro del grupo puede acceder a la información propia que se recoge en la aplicación “WhatsApp” entre los que está el número de teléfono de todos los miembros incluidos, el nombre que hayan puesto al usuario y fotografía del perfil que hayan incluido. Por parte del Instituto no se remitió al grupo ningún dato carácter personal adicional.

No se estableció ningún procedimiento para garantizar la confidencialidad y privacidad de la información enviada a cada usuario.

No se creó ningún fichero de usuarios de WhatsApp. Se utilizaron los números de teléfono facilitados por los D.D.D. en prácticas para el proceso de selección para remitir información dada la dificultad de contacto con ellos. Una vez cumplida la necesidad de contactar, el grupo se eliminó a las 8 horas de su creación.

El Instituto denunciado remite copia del expediente que se ha tramitado por el Defensor del Pueblo de Navarra con motivo de una queja por el mismo asunto,

también presentada por el denunciante. Entre la documentación que integra dicho expediente se encuentra el informe remitido al Defensor del Pueblo por el Departamento de Educación del Gobierno de Navarra en el que consta:

*“Las personas que solicitaron ser admitidas al procedimiento selectivo de ingreso en el D.D.D. aprobado por Resolución ***RESOLUCION.1, de DD de MM, de la ***CARGO.1 del Departamento de Educación, facilitaron a la Administración convocante determinados datos personales con diversos fines relacionados con la gestión de la participación de estas personas en la convocatoria, entre ellos el número de teléfono con el objetivo de posibilitar la comunicación con la misma para cualquier cuestión relacionada con el procedimiento.*

La Base Duodécima de la convocatoria, que regula la fase de prácticas del procedimiento selectivo, establece en su apartado 5 que durante la misma al personal funcionario en prácticas se le efectuará un examen médico a fin de acreditar que reúne las condiciones físicas y psíquicas necesarias para el correcto desempeño de la correspondiente función docente, requisito exigido en la Base 2.1.c), disponiendo asimismo que quien no supere dicho examen médico, perderá todos los derechos a su nombramiento como personal funcionario de carrera.

Para dar cumplimiento a lo dispuesto por las Bases que rigen el procedimiento selectivo y que, por tanto, vinculan tanto a la Administración como a los participantes, desde el Departamento de Educación se facilitó al Instituto de Salud Pública y Laboral de Navarra, a mayor abundamiento también organismo de la Administración de la Comunidad Foral de Navarra y competente en la materia, los datos personales del personal funcionario en prácticas necesarios para que el personal del INSPN procediera a la comunicación con las personas funcionarias en prácticas, y pudiera efectuar las citaciones precisas para la realización del examen médico al que debía someterse.”

TERCERO: Con fecha 11 de octubre de 2017, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento de declaración de infracción de Administraciones Públicas al Instituto de Salud Pública y Laboral de Navarra por presunta infracción de los artículos 4.2 y 10 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD), tipificadas ambas como infracción grave en los artículos 44.3.c) y 44.d), respectivamente, de la citada Ley Orgánica.

CUARTO: Notificado el citado acuerdo de inicio de procedimiento de declaración de infracción de Administraciones Públicas, y con posterioridad a la recepción de la copia del expediente solicitada, en fecha 31 de octubre de 2017 se registra escrito de alegaciones del Departamento de Salud del Gobierno de Navarra, superior jerárquico del ISPLN, en el que, en síntesis, manifestaba lo siguiente:

-En cuanto a los hechos, el modelo de instancia facilitado a los posibles aspirantes a la convocatoria estudiada recababa, entre otra información, el dato de los teléfonos para que, de ser necesario a efectos de la realización de las pruebas, la Administración pudiera ponerse en contacto con los mismos.

De acuerdo con la normativa de ingreso y las bases reguladoras de la convocatoria que se citan, los aspirantes conocen la obligatoriedad de pasar un reconocimiento médico que se lleva a cabo por el ISPLN, y para cuya ejecución se precisan los datos de los opositores. Por lo que el Instituto, en el ejercicio de sus



funciones y con arreglo a la normativa de aplicación, comenzó a realizar los llamamientos para que los 200 funcionarios en prácticas pasasen los preceptivos reconocimientos médicos, acudiendo a las citaciones unos 170 que pasaron el reconocimiento. Dado que los 30 restantes no atendían a las citaciones, y ante las posibles consecuencias de no pasar el preceptivo reconocimiento médico, se decidió acudir a uno de los medios de comunicación más aceptados socialmente de tal modo que, a principios de febrero de 2017, se creó un grupo de WhatsApp con los teléfonos de contacto que en su día estos 30 opositores facilitaron para recibir información en el desarrollo de la oposición, canal a través del cual se les recordó la obligatoriedad del mismo y se les ofreció un cauce de comunicación para poder realizar las oportunas citaciones. El grupo fue cancelado a las 8 horas de su creación. Finalmente, todos los D.D.D. en prácticas han pasado el preceptivo reconocimiento médico y han accedido con todos los efectos a la función pública.

-Se invoca la Sentencia de la Audiencia Nacional, de 17 de septiembre de 2008 aduciendo que no es pacífica la interpretación doctrinal y jurisprudencial sobre si el uso del número de teléfono móvil, de forma aislada, supone un tratamiento de datos de carácter personal amparado por la normativa de protección de datos. De no estarlo, procedería el archivo del procedimiento.

- Para el caso de desestimarse alegato anterior, se entiende que el Acuerdo de inicio del procedimiento señalando que la conducta del Instituto puede suponer la comisión de dos infracciones graves es absolutamente desproporcionada por lo siguiente:

El ISPLN se ha comprometido con el Defensor del Pueblo de Navarra, en su comunicación en relación con la queja que por este tema presentó el Sindicato AFAPNA, a no volver a utilizar aplicaciones de mensajería instantánea para comunicarse de manera colectiva con opositores. Además, el Departamento de Salud, al que está adscrito el Instituto, aceptó el recordatorio de deberes del Defensor

El dato del teléfono de una persona es un dato de carácter básico.

Falta de reincidencia. Es la primera vez que se utiliza este canal de comunicación con los opositores para convocarles al examen médico.

Falta de afectación a los titulares de los datos, ya que la documentación obrante en el procedimiento muestra que los particulares presuntamente afectados por la revelación de su número de teléfono a terceros, manifiestan su gratitud por la información suministrada, en concreto los usuarios **A.A.A.**, siendo un sindicato no afectado por el tratamiento de estos datos, el denunciante.

La conducta analizada se ha producido en el marco de una práctica social que acepta o tolera el uso del servicio de mensajería instantánea "WhatsApp" sin mediar el consentimiento de los titulares de los datos personales tratados. Se añade que los usuarios de "WhatsApp" pueden configurar la aplicación a través de las opciones de privacidad para limitar la visibilidad de sus datos.

Los datos en un proceso selectivo de acceso a la función pública se rigen por los principios de publicidad y transparencia. No puede obviarse que el dato del teléfono se ha dado por parte de los opositores en el marco de un proceso selectivo de concurrencia competitiva, para el acceso a la función pública.

Las normativas de transparencia, en Navarra la Ley Foral 11/2012, de 21 de junio, de Transparencia y Gobierno Abierto, han ampliado los derechos de los ciudadanos al acceso a la información y a la documentación pública.

Se invocan las resoluciones de la AEPD números R/03187/2016,



R/00917/2015, R/00021/2015, R/01215/2011 y R/02302/2017 en las que, a su juicio, frente a conductas de mayor gravedad el posicionamiento de la AEPD ha sido más beneficioso para los inculpados, ello en tanto que se ha sancionado por la comisión de una única infracción, se ha optado por tramitar procedimientos de apercibimiento con arreglo a lo dispuesto en el artículo 45.6 de la LOPD en lugar de iniciar procedimientos sancionadores, se ha aplicado la figura del concurso medial mientras que en este supuesto no se ha tenido en cuenta o se ha resuelto archivar la denuncia. A la vista de dichas resoluciones, debería procederse al archivo del procedimiento sancionador o, en su caso, ser objeto de apercibimiento, añadiendo que en el caso de que se desestimase dichas alegaciones, a lo sumo, se podría imponer una única sanción en aplicación del concurso modal de sanciones.

- Subsidiariamente, se manifiesta:

En relación con la infracción del artículo 44.3.c) de la LOPD se indica que no procede sancionar porque no se ha cometido, puesto que el ISPLN ha actuado en marco de sus funciones y utilizando el dato del teléfono móvil para la finalidad que motivó su recogida (ponerse en contacto con los D.D.D. en prácticas por un asunto derivado del desarrollo del proceso selectivo).

En relación con la infracción del artículo 44.3.d) de la LOPD, se hace especial referencia a la discusión sobre si un número de teléfono aislado es un dato de carácter personal y si, en su caso, su cesión sin consentimiento supone un incumplimiento de la LOPD, sobre la publicidad de los datos de un proceso selectivo para las personas que participan en el mismo y, en cuanto a la proporcionalidad ligada a los datos, se reitera la aceptación social del uso del citado servicio y la ausencia de perjudicados.

QUINTO: Con fecha 3 de noviembre de 2017 la Instructora del procedimiento inició un período de práctica de pruebas en cuyo marco se ACUERDA practicar las siguientes pruebas:

- Incorporar al expediente del procedimiento arriba indicado, y por tanto dar por reproducida a efectos probatorios, la documentación recabada en las actuaciones previas de inspección que forman parte del expediente E/02345/2017. Asimismo, se dan por reproducidas a efectos probatorios, las alegaciones al acuerdo de inicio del procedimiento AP/00050/2017 presentadas por el Instituto de Salud Pública y Laboral de Navarra. Todo ello con su correspondiente documentación adjunta.

- Incorporar al expediente del procedimiento arriba indicado, y por tanto dar por reproducida a efectos probatorios, copia de las resoluciones de esta Agencia R/03187/2016, R/00917/2015, R/00021/2015, R/01215/2011 y R/02302/2017 citadas por el ISPLN en su escrito de alegaciones al acuerdo de inicio del procedimiento AP/00050/2017.

- Solicitar al ISPLN contestación a los siguientes extremos y remisión de la documentación que a continuación se cita: a) Acreditación del cierre del Grupo de WhatsApp en cuestión, con indicación de la fecha exacta en que se ejecutó esta acción; b) Especificación de las medidas concretas adoptadas a fin de evitar la creación de grupos colectivos cuando se utilicen este tipo de aplicaciones con finalidades de contacto; c) Remisión de copia de la Resolución ***RESOLUCION.1, de DD de MM, citada en el escrito de alegaciones.



SÉXTO: Con fecha 15 de noviembre de 2017 se registra de entrada escrito de contestación del Instituto de Salud Pública y Laboral de Navarra señalando lo siguiente:

-Que aunque se desconoce el día exacto de la creación del grupo de WhatsApp, su eliminación ocurrió a las ocho horas de su creación.

- En cuanto a las medidas concretas adoptadas indican que: *“Como ya se ha manifestado con anterioridad el Departamento de Salud en contestación a una petición de información del Defensor del Pueblo de Navarra, tras una queja presentada por este mismo asunto por el sindicato AFAPNA, ahora denunciante, señaló su compromiso de no volver a utilizar este tipo de aplicaciones para contactos colectivos. En cumplimiento de dicho compromiso la Directora Gerente del Instituto de Salud Pública y Laboral de Navarra se reunió con el Jefe del Servicio de Salud Laboral y con la Jefa de Sección de Valoración Clínico-Laboral e Inspección Médica, responsables de la actividad de revisión médica de “futuros funcionarios forales”, para transmitirles la incidencia y para solicitarles que no se volviese a repetir. La Jefa de Sección de Valoración Clínico-Laboral e Inspección Médica traslado al personal de su unidad esta Instrucción.”*

- Se aporta copia de la Resolución ***RESOLUCION.1, de DD de MM.

SÉPTIMO: Con fecha 20 de febrero de 2019, la Instructora del procedimiento emitió Propuesta de Resolución, en el sentido de que por la Directora de la Agencia Española de Protección de Datos se declare que el INSTITUTO DE SALUD PÚBLICA Y LABORAL DE NAVARRA ha infringido lo dispuesto en los artículos 4.2 y 10 de la LOPD, tipificadas, respectivamente, como graves en los artículos 44.3.c) y 44.3.d) de la citada norma, así como que se requiera a dicho Instituto la adopción de las medidas de orden interno que impidan que en el futuro pueda producirse una nueva infracción de los artículos 4.2 y 10 de la mencionada Ley.

OCTAVO: Notificada la propuesta de resolución con fecha 22 de febrero de 2018, no consta que por parte del INSTITUTO DE SALUD PÚBLICA Y LABORAL DE NAVARRA se haya ejercido su derecho a formular alegaciones frente a la misma en el plazo que le fue concedido a tales efectos.

HECHOS PROBADOS

PRIMERO: En el “Boletín Oficial de Navarra” de DD de MM de 2016 se publica Resolución ***RESOLUCION.1, de DD de MM, de la ***CARGO.1 del Departamento de Educación, por la que se aprueba el procedimiento selectivo de ingreso en el D.D.D., a plazas del ámbito de gestión de la Administración de la Comunidad Foral de Navarra y el procedimiento para que el personal funcionario de carrera del D.D.D. pueda adquirir nuevas especialidades en el citado cuerpo.

SEGUNDO: En la Base Duodécima del procedimiento selectivo de ingreso en el D.D.D., desarrollado en el Título I de la citada convocatoria, se establece que *“Durante la fase de prácticas al personal funcionario en prácticas se le efectuará un examen médico a fin de acreditar que reúne las condiciones físicas y psíquicas necesarias para el correcto desempeño de la correspondiente función docente. Quien no supere dicho examen médico, perderá todos los derechos a su nombramiento*



como personal funcionario de carrera, por Resolución de la Directora del Servicio de Recursos Humanos.”

TERCERO: Con fecha 22 de febrero de 2017, se registra de entrada en esta Agencia escrito de Don **B.B.B.** en el que, actuando en nombre y representación del Sindicato AFAPNA (en lo sucesivo el denunciante), manifiesta que el Instituto de Salud Pública y Laboral de Navarra (en adelante, ISPLN) ha creado, sin el consentimiento de los titulares de los datos y con la información cedida por el Departamento de Educación del Gobierno de Navarra, un grupo de “WhatsApp” en el que aparecen los números de teléfono móvil de los D.D.D. en prácticas al objeto de comunicarles las revisiones médicas obligatorias que deben realizar en fase de prácticas.

CUARTO: Consta que con fecha 13 de febrero de 2017 la institución del Defensor del Pueblo de la Comunidad Foral de Navarra recibió escrito del denunciante formulando una queja frente al Departamento de Salud y al Departamento de Educación del Gobierno de Navarra que traía causa en los mismos hechos denunciados ante la AEPD.

QUINTO: El ISPLN es un Organismo Autónomo adscrito a la Dirección General de Salud del Departamento de Salud del Gobierno de Navarra, que desde el 1 de enero de 2016 lleva a cabo los exámenes médicos de los aspirantes a empleados de la Administración de la Comunidad Foral de Navarra y de sus organismos autónomos previstos en los distintos procedimientos de selección de personal.

SEXTO: A principios de febrero de 2017 el ISPLN creó un grupo de “WhatsApp”, que denominó “Reconocimiento médico”, con los números de teléfono móvil de 30 funcionarios en prácticas usuarios de dicha aplicación de mensajería instantánea, y con los que dicho Instituto no había podido comunicarse individualmente por vía telefónica, para que contactasen con el Instituto a fin de realizar el examen médico establecido en la base Duodécima del Procedimiento Selectivo de Ingreso en el D.D.D., correspondiente a la convocatoria aprobada mediante Resolución ***RESOLUCION.1, de DD de MM, de la ***CARGO.1 del Departamento de Educación.

SÉPTIMO: Los integrantes del reseñado grupo de “WhatsApp” podían acceder a la información que se mostraba a través de la aplicación “WhatsApp” de miembros del grupo, en particular el número de teléfono de todos los miembros incluidos, el nombre que hayan puesto al usuario y fotografía del perfil que hayan incluido.

OCTAVO: El citado grupo de “WhatsApp” fue eliminado por el ISPLN ocho horas después de su creación.

NOVENO: Con fecha 15 de marzo de 2017, el Departamento de Educación del Gobierno de Navarra informó al Defensor del Pueblo de la Comunidad Foral de Navarra que *“Para dar cumplimiento a lo dispuesto por las Bases que rigen el procedimiento selectivo y que, por tanto, vinculan tanto a la Administración como a los participantes, desde el Departamento de Educación se facilitó al Instituto de Salud Pública y Laboral de Navarra, a mayor abundamiento también organismo de la Administración de la Comunidad Foral de Navarra y competente en la materia, los datos personales del personal funcionario en prácticas necesarios para que el personal del INSPLN procediera a la comunicación con las personas funcionarias en prácticas, y pudiera efectuar las citaciones precisas para la realización del examen médico al que debía someterse.”*



DÉCIMO: En el expediente tramitado a raíz de la reseñada queja, el Defensor del Pueblo de la Comunidad Foral de Navarra dictó con fecha 18 de abril de 2017 resolución en la que estimaba necesario *“Recordar al Departamento de Salud el deber legal de garantizar la protección de los datos de carácter personal de las personas, impidiendo que tales datos se traten sin el consentimiento inequívoco y específico de los interesados”*

FUNDAMENTOS DE DERECHO

I

Es competente para resolver este procedimiento la Directora de la Agencia Española de Protección de Datos, de conformidad con lo dispuesto en el artículo 37. g) en relación con el artículo 36 de la LOPD.

II

Con carácter previo al estudio del fondo del asunto debe dilucidarse la alegación referente a que en este caso procedería haber tramitado un procedimiento de apercibimiento conforme a lo dispuesto en el artículo 45.6 de la LOPD, precepto que establece lo siguiente:

“6. Excepcionalmente el órgano sancionador podrá, previa audiencia de los interesados y atendida la naturaleza de los hechos y la concurrencia significativa de los criterios establecidos en el apartado anterior, no acordar la apertura del procedimiento sancionador, y en su lugar, apercibir al sujeto responsable a fin de que, en el plazo que el órgano sancionador determine, acredite la adopción de las medidas correctoras que en cada caso resultasen pertinentes, siempre que concurren los siguientes presupuestos:

- a) *que los hechos fuesen constitutivos de infracción leve o grave conforme a lo dispuesto en esta Ley.*
- b) *Que el infractor no hubiese sido sancionado o apercibido con anterioridad.*

Si el apercibimiento no fuera atendido en el plazo que el órgano sancionador hubiera determinado procederá la apertura del correspondiente procedimiento sancionador por dicho incumplimiento”. (El subrayado es de la AEPD)

A la vista de lo dispuesto en dicho artículo, la citada pretensión debe ser rechazada, habida cuenta que el procedimiento de apercibimiento contemplado en el artículo 45.6 de la LOPD, que se declara expresamente como excepcional y cuya ponderación corresponde al órgano sancionador atendidas las circunstancias concurrentes y los presupuestos contenidos en el artículo mencionado, únicamente resulta de aplicación en sustitución de un procedimiento sancionador.

En el caso examinado, se ha tramitado un procedimiento de declaración de Infracción de Administraciones Públicas en atención a que, como resultado de las actuaciones previas de investigación practicadas, se constató que el responsable del tratamiento del que supuestamente deriva la comisión de las infracciones previstas en los artículos 44.3.c) y 44.3.d) de la LOPD era una Administración Pública, debiendo procederse con arreglo a lo establecido en el artículo 43. 2 de la LOPD que establece lo siguiente:



“2. Cuando se trate de ficheros de titularidad pública se estará, en cuanto al procedimiento y a las sanciones, a lo dispuesto en los artículos 46 y 48 de la presente Ley”.

A este respecto, el artículo 46 de la LOPD, dispone respecto de las *“Infracciones de las Administraciones Públicas”* que:

“1. Cuando las infracciones a que se refiere el artículo 44 fuesen cometidas en ficheros de titularidad pública o en relación con tratamientos cuyos responsables lo serían de ficheros de dicha naturaleza, el órgano sancionador dictará una resolución estableciendo las medidas que procede adoptar para que cesen o se corrijan los efectos de la infracción. Esta resolución se notificará al responsable del fichero, al órgano del que dependa jerárquicamente y a los afectados si los hubiera.

2. El órgano sancionador podrá proponer también la iniciación de actuaciones disciplinarias, si procedieran. El procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario de las Administraciones Públicas.

3. Se deberán comunicar al órgano sancionador las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores.

4. El Director de la Agencia comunicará al Defensor del Pueblo las actuaciones que efectúe y las resoluciones que dicte al amparo de los apartados anteriores”.

Por su parte, el artículo 48.1 de la LOPD, bajo la rúbrica *“Procedimiento sancionador”*, establece que: *“1. Por vía reglamentaria se establecerá el procedimiento a seguir para la determinación de las infracciones y la imposición de las sanciones a que hace referencia el presente Título. “*

A su vez, los artículos 126 y 129 del Reglamento de Desarrollo de la LOPD, aprobado por Real Decreto 1720/2007, de 21/12 (en adelante RLOPD), disponen:

“Artículo 126. Resultado de las actuaciones previas.

1. Finalizadas las actuaciones previas, éstas se someterán a la decisión del Director de la Agencia Española de Protección de Datos.

Si de las actuaciones no se derivasen hechos susceptibles de motivar la imputación de infracción alguna, el Director de la Agencia Española de Protección de Datos dictará resolución de archivo que se notificará al investigado y al denunciante, en su caso.

2. En caso de apreciarse la existencia de indicios susceptibles de motivar la imputación de una infracción, el Director de la Agencia Española de Protección de Datos dictará acuerdo de inicio de procedimiento sancionador o de infracción de las Administraciones públicas, que se tramitarán conforme a lo dispuesto, respectivamente, en las secciones tercera y cuarta del presente capítulo. “(El subrayado es de la AEPD)

“Artículo 129. Disposición general.

El procedimiento por el que se declare la existencia de una infracción de la Ley Orgánica 15/1999, de 13 de diciembre, cometida por las Administraciones públicas será el establecido en la sección tercera de este capítulo.”



En consecuencia, al no estar ante un procedimiento sancionador, sino ante un procedimiento de infracción de Administraciones Públicas, no procede tramitar el procedimiento de apercibimiento previsto en el artículo 45.6 de la LOPD.

Asimismo, debido a que el procedimiento tramitado no es sancionador ha de rechazarse el alegato relativo a la procedencia de aplicar lo previsto en el artículo 29.5 de la Ley 40/2015 de 1 de octubre, de Régimen Jurídico del sector Público, que establece que: *“Cuando de la comisión de una infracción derive necesariamente la comisión de otra u otras, se deberá imponer únicamente la sanción correspondiente a la infracción más grave cometida”*. Los procedimientos de infracción de Administraciones Públicas no llevan aparejada la imposición de ninguna sanción de multa de las previstas en los apartados 1 al 3 del artículo 45 de la LOPD, sino que se resuelven de acuerdo con lo dispuesto en el mencionado artículo 46 de la LPOD, y ello respecto de cada una de las infracciones administrativas de cuya comisión se estime responsable a la Administración Pública a la que se haya incoado el expediente.

En consecuencia, en este caso, resulta irrelevante a los efectos de la resolución a adoptar que de la infracción grave a lo dispuesto en el artículo 4.2 de la LOPD derive la infracción grave a lo previsto en el artículo 10 de la misma norma, ya que dada la naturaleza del procedimiento tramitado no puede imponerse sanción de multa alguna al ISPLN como responsable, conforme se justifica en los siguientes Fundamentos de Derecho, de las dos infracciones descrita.

Con arreglo a todo lo anterior, se ha justificado que el procedimiento de infracción de Administraciones Públicas es acorde a lo previsto en la normativa de protección de datos, no constituyendo por, tanto, ningún tratamiento desproporcionado con el seguido por esta Agencia en los procedimientos de apercibimiento que dieron lugar a las resoluciones citadas en el escrito de alegaciones, en las que, además, constan razonados los fundamentos fácticos y jurídicos que sustentan las mismas, dándose además la circunstancia que la resolución R/00021/2015 no se origina en una infracción a la LOPD, sino a una normativa distinta, en concreto la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y comercio electrónico.

III

El artículo 1 de la LOPD dispone: *“La presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar”*.

En cuanto al ámbito de aplicación de la citada norma el artículo 2.1 de la misma señala: *“La presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado”*; definiéndose el concepto de dato de carácter personal en el apartado a) del artículo 3 de la citada Ley Orgánica 15/1999, como *“Cualquier información concerniente a personas físicas identificadas o identificables”*, añadiendo el apartado 1.f) del artículo 5 del Reglamento de desarrollo de la LOPD, aprobado por Real Decreto 1720/2007, de 21 de diciembre (RLOPD), que dato de carácter personal es *“cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables”*.



La definición de persona identificable aparece en la letra o) del citado artículo 5.1 del RLOPD, que considera como tal *“toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social. Una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionados”*.

En este mismo sentido se pronuncia el artículo 2.a) de la Directiva 95/46/CE del Parlamento y del Consejo, de 24 de octubre de 1995, relativa a la Protección de las Personas Físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, según el cual, a efectos de dicha Directiva, se entiende por dato personal *“toda información sobre una persona física identificada o identificable; se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social”*. Asimismo, el Considerando 26 de esta Directiva se refiere a esta cuestión señalando que, para determinar si una persona es identificable, hay que considerar el conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona para identificar a aquélla.

Por lo que la imagen de una persona constituye también un dato de carácter personal, toda vez que la información captada concierne a personas que las hacen identificadas o identificables y suministra información sobre la imagen personal de ésta. En consecuencia, la imagen de la foto del perfil de los afectados que resulta accesible a través del grupo de “WhatsApp” se ajusta a este concepto siempre que identifique o permita la identificación de la persona que aparece en la misma.

Por otra parte, la aplicabilidad de la normativa de protección de datos de carácter personal, de acuerdo con lo indicado en el citado artículo 2.1 de la LOPD, requiere que dichos datos aparezcan registrados en un soporte físico que los haga susceptibles de tratamiento.

El artículo 3 de la LOPD define en su letra c) el tratamiento de datos como aquellas *“operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias”*.

Asimismo, dicho artículo 3 de la LOPD define en su apartado b) como *“Fichero: Todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.”*, mientras que en su apartado e) describe como *“Afectado o interesado”* a la *“Persona física titular de los datos que sean objeto del tratamiento a que se refiere el apartado c) del presente artículo.”*

Por tanto, la garantía del derecho a la protección de datos conferida por la normativa de referencia requiere que exista una actuación que constituya un tratamiento de datos personales en el sentido expresado. De acuerdo con la información facilitada por el Departamento de Salud del Gobierno de Navarra al Defensor del pueblo el ISPLN tiene *“acceso a los datos de identificación de las personas que tienen que pasar el reconocimiento médico previo a la adquisición de la condición de funcionario de la Administración de la Comunidad Foral de Navarra”*. En este caso, consta que dicho Instituto accedió a los datos identificativos y de



contacto de 200 D.D.D. en prácticas necesarios para poder citarles a los exámenes médicos, procediendo, posteriormente, a crear un grupo de “WhatsApp” con 30 de estos funcionarios en prácticas que no habían respondido a llamadas telefónicas iniciales, tratamientos que entran dentro el ámbito de aplicación de la LOPD.

Asimismo, el artículo 3 de la LOPD también recoge las siguientes definiciones:

d) Responsable del fichero o tratamiento: Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.

“h) “Consentimiento del interesado: Toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.”

“i) Cesión o comunicación de datos: toda revelación de datos realizada a la persona distinta del interesado.”

IV

El ISPLN es un organismo autónomo dotado de personalidad jurídica propia y plena capacidad de obrar para el cumplimiento de sus fines y que está adscrito a la Dirección General de Salud del Gobierno de Navarra, según consta en sus Estatutos.

El artículo 3 de dichos Estatutos, señala en cuanto al “Objeto” del citado Organismo que:

“El Instituto de Salud Pública y Laboral de Navarra se configura como un organismo:

a) Técnico-asistencial, especializado en materia de promoción de la salud y vigilancia, prevención e intervención sobre problemas colectivos de salud.

b) De impulso de las alianzas entre Servicios de Salud, otros sectores y ciudadanía y colaboración entre Departamentos del Gobierno en la línea de Salud en todas las Políticas.

c) De asesoramiento e intervención técnica en materia de salud laboral en el campo de la prevención de riesgos laborales y de protección de la salud en relación con las condiciones de trabajo de la población laboral navarra en las materias comprendidas en el artículo 14 de la Ley Foral de Salud.”

Mediante el Decreto Foral 242/2015, de 14 de octubre, se modificó el Decreto Foral 63/2012, de 18 de julio, por el que se crea y se aprueban los Estatutos del Organismo Autónomo Instituto de Salud Pública y Laboral de Navarra. En la Disposición Transitoria Cuarta de dicho Decreto, bajo la rúbrica “Examen médico de los aspirantes a empleados de la Administración de la Comunidad Foral de Navarra y de sus organismos autónomos”, se establece que “La Sección de Valoración Clínico-Laboral e Inspección Médica del Servicio de Salud Laboral se hará cargo de los exámenes médicos de los aspirantes a empleados de la Administración de la Comunidad Foral de Navarra y de sus organismos autónomos, previstos en el presente decreto foral, a partir del 1 de enero de 2016, asumiendo en dicha fecha la realización de aquellos reconocimientos o exámenes médicos previstos en los



distintos procedimientos de selección de personal, aprobados tanto con posterioridad a la entrada en vigor del presente decreto foral como con anterioridad a la misma y que se encuentren pendientes de su realización. Mientras tanto dichos exámenes médicos continuarán siendo realizados por los Servicios de Prevención de la Administración de la Comunidad Foral de Navarra y sus organismos autónomos.

En relación con la realización por parte del ISPLN de dichos reconocimientos o exámenes médicos previstos en los diferentes procedimientos de selección personal ha de tenerse en cuenta la siguiente normativa:

El artículo 5.4 del Decreto Foral Legislativo 251/1993, de 30 de agosto, por el que se aprueba el Texto Refundido del Estatuto del Personal al Servicio de las Administraciones Públicas de Navarra, establece que: *"Las pruebas selectivas deberán basarse, en todo caso, en los principios de mérito y capacidad ."*

A su vez el artículo 7.d) del mismo Decreto Foral Legislativo 251/1993 establece, entre otros requisitos, que *"Para ser admitido a las pruebas selectivas se requiere: "d) Poseer la capacidad física y psíquica necesaria para el ejercicio de las correspondientes funciones."*, condición que también se recoge en el artículo 6.c) del Decreto Foral 113/1985, de 5 de junio, por el que se aprueba el Reglamento de Ingreso en las Administraciones Públicas de Navarra, al disponer que *"Para ser admitido a las pruebas selectivas se requiere: c) Poseer la capacidad física necesaria para el ejercicio de las correspondientes funciones."*

El artículo 14 del mencionado Decreto Foral 113/1985, establece que: *"Las bases de las convocatorias vinculan a la Administración convocante, a los Tribunales que han de juzgar las pruebas selectivas y a quienes participen en las mismas."*

En el caso analizado, mediante la Resolución ***RESOLUCION.1, de DD de MM, de la ***CARGO.1 del Departamento de Educación, por la que se aprobó el procedimiento selectivo de ingreso en el D.D.D., a plazas del ámbito de gestión de la Administración de la Comunidad Foral de Navarra y el procedimiento para que el personal funcionario de carrera del D.D.D. pueda adquirir nuevos especialidades en el citado cuerpo.

La Base Segunda del Procedimiento Selectivo de ingreso en el D.D.D., relativa a los "Requisitos de los Candidatos", establecía en su apartado 1.c) como uno de los requisitos generales que debían reunir los aspirantes que participasen en dicho procedimiento selectivo *"c) No padecer enfermedad ni estar afectado por limitación física o psíquica que sea incompatible con el desempeño de las funciones correspondientes al Cuerpo y especialidad a que se opta."*

La Base Duodécima del mismo Procedimiento Selectivo, referida a la "Fase de Prácticas" establecía en su apartado 5 que: *"5 Durante la fase de prácticas al personal funcionario en prácticas se le efectuará un examen médico a fin de acreditar que reúne las condiciones físicas y psíquicas necesarias para el correcto desempeño de la correspondiente función docente. Quien no supere dicho examen médico, perderá todos los derechos a su nombramiento como personal funcionario de carrera, por Resolución de la ***CARGO.1."*

De la citada normativa, se colige que el ISPLN estaba habilitado para acceder y tratar los datos identificativos y de contacto (datos de carácter personal) de los funcionarios en prácticas del D.D.D. necesarios para realizar a los mismos, en el ejercicio de las competencias establecidas en los Estatutos del Organismo, el examen médico que permita acreditar que reunían las condiciones físicas y



psíquicas necesarias para el desempeño de la función docente, y cuya superación constituye un requisito previo a la adquisición de la condición de funcionario de la Administración de la Comunidad Foral Navarra. Por lo cual, el tratamiento de los datos de carácter personal de los D.D.D. en prácticas asociado a esa exclusiva finalidad no precisaba del consentimiento inequívoco de los titulares de los datos.

Téngase en cuenta que el artículo 6.1 de la LOPD, que consagra el principio del consentimiento, dispone como regla general en su apartado 1 que *“El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa”*, estableciendo en el apartado 2 del mencionado artículo como una de las excepciones a dicho consentimiento: *“Cuando se refieran a las partes de un contrato o precontrato de una relación comercial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento”*.

Tampoco la comunicación entre los Departamentos de Educación y de Salud del Gobierno de Navarra de los datos personales de los D.D.D. en prácticas que resultaban necesarios para que el ISPLN pudiera llevar a cabo los citados reconocimientos médicos vulneraba la normativa de protección de datos, ya que en este caso se produce el supuesto contemplado en el artículo 11.2.c) de la LOPD, que establece que no será preciso el consentimiento del interesado exigido en el artículo 11.1 de dicha norma:

“c) Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique. “

V

El artículo 4 de la LOPD, que consagra el principio de calidad de datos, establece en sus apartados 1 y 2 lo siguiente:

“1. Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

2. Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos”.

El principio de calidad que prohíbe utilizar datos para una finalidad incompatible o distinta de aquella para la que los mismos fueron recabados, se contiene en el Título II de la LOPD, como uno de los principios básicos de la protección de datos.

Las *“finalidades”* a las que alude este apartado 2 han de ligarse o conectarse siempre con el principio de pertinencia o limitación en la recogida de datos regulado en el artículo 4.1 de la misma Ley, precepto que establece que . Conforme a dicho precepto los datos sólo podrán tratarse cuando *“sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.”*

En consecuencia, si el tratamiento del dato ha de ser *“pertinente”* al fin



perseguido y la finalidad ha de estar “*determinada*”, difícilmente se puede encontrar un uso del dato para una finalidad “*distinta*” sin incurrir en la prohibición del artículo 4.2, aunque emplee el término “*incompatible*”. A este respecto, la Sentencia del Tribunal Constitucional, dictada el 30 de noviembre de 2000, en el Recurso número 1463/2000, señala, en su Fundamento de Derecho decimotercero: “*el derecho a consentir la recogida y tratamiento de los datos personales no implica en modo alguno consentir la cesión de tales datos a terceros (...). Y, por tanto, la cesión de los mismos a un tercero para proceder a un tratamiento con fines distintos de los que originaron su recogida, aun cuando puedan ser compatibles con éstos supone una nueva posesión y uso que requiere el consentimiento del interesado. Una facultad que sólo cabe limitar en atención a derechos y bienes de relevancia constitucional y, por tanto, esté justificada, sea proporcionada y, además, se establezca por Ley, pues el derecho fundamental a la protección de datos personales no admite otros límites*”.

En esta línea se ha pronunciado en diversas ocasiones la Audiencia Nacional. Así en Sentencia de 17 de marzo de 2004, la Audiencia señala que “*Aplicando de forma literalista el artículo 4.2 de la Ley Orgánica, quedaría privado de sentido y vaciado de contenido y para evitar este resultado indeseable esta Sala considera que lo que prohíbe el precepto es que los datos de carácter personal se utilicen para una finalidad distinta de aquella para la que han sido recogidos.*”

De este modo, tomando la expresión “*finalidades incompatibles*” que utiliza el legislador de la LOPD como sinónimo de “*finalidades distintas*”, se concluye que, entregados los datos para una finalidad concreta, el uso o tratamiento posterior que no esté en consonancia con la finalidad para la que fueron facilitados, constituiría un desvío de finalidad que vulneraría el artículo 4.2 de la LOPD, precepto cuya vulneración se inculpa al ISPLN.

La Audiencia Nacional, en su Sentencia de fecha 15/06/05, considera que el artículo 4 de la LOPD establece una sutil distinción entre finalidad de la recogida y finalidad del tratamiento, “*pues la recogida sólo puede hacerse con fines determinados, explícitos y legítimos, y el tratamiento posterior no puede hacerse de manera incompatible con dichos fines. Así pues, y de acuerdo con el artículo 1.b) de la Directiva 95/46/CE de 24 de octubre de 1995 (en cuya redacción se inspira el repetido artículo 4.2 de nuestra LOPD), si la recogida se hizo con fines determinados, cualquier uso o tratamiento posterior con finalidad distinta es incompatible con la primera finalidad que determinó la captura por lo que, en este contexto, diferente o incompatible significan lo mismo.*”

En definitiva, los datos no pueden ser tratados para fines distintos a los que motivaron su recogida, pues esto supondría un nuevo uso que requiere el consentimiento del interesado.

En el caso concreto que nos ocupa, no se discute la habilitación con la que el ISPLN cuenta para tratar los datos personales de los D.D.D. en prácticas para realizar los exámenes médicos de evaluación de las condiciones físicas y psíquicas que se les requerían a estos aspirantes a empleados de la Administración de la Comunidad Foral de Navarra para el desempeño de las funciones correspondientes al Cuerpo y especialidad a la que optaban. Lo que se cuestiona es que el ISPLN utilizase los datos de carácter personal correspondientes a 30 de los 200 funcionarios en prácticas (en concreto el número de teléfono móvil) para crear un grupo de “WhatsApp”, finalidad no prevista ni comunicada a los afectados



respecto del uso de los datos facilitados al cumplimentar las instancias de participación en el proceso selectivo en cuestión.

Tampoco debe obviarse que el tratamiento estudiado se vincula a un proceso selectivo de acceso a la función pública regido por los principios de transparencia y publicidad, y al que le resultan de plena aplicación los principios y garantías recogidos en la LOPD. En relación con esta cuestión, no hay que olvidar que en las bases de la Convocatoria aprobada por resolución ***RESOLUCION.1, de DD de MM, del proceso selectivo para el D.D.D. figura que la publicación de las listas de aspirantes seleccionados se realizaría en el Negociado de Información y Documentación del Departamento de Educación y en la página web del mismo: www.educacion.navarra.es, medios de publicación también utilizados en otras fases del proceso selectivo.

El ISPLN invoca la Sentencia de la Audiencia Nacional, de 17 de septiembre de 2008 para cuestionar que el uso aislado de los números de teléfono móvil de los afectados suponga la utilización de un dato de carácter personal protegido por la normativa de protección de datos, transcribiendo a tales efectos lo siguiente: *"Es claro que el número de teléfono asociado a un nombre y apellidos es un dato de carácter personal pues nos proporciona información sobre una persona identificada. Es más, el propio número del teléfono, sin aparecer directamente asociado a una persona, puede tener la consideración de dato de carácter personal si a través de él se puede identificar a su titular. En el presente caso, la Agencia Española de Protección de Datos no ha razonado, y menos ha acreditado, que a través del número de teléfono móvil se haya identificado al titular del mismo o que a partir del citado número fuese posible tal identificación, de forma que el citado número del teléfono ayuno de otras circunstancias que identifiquen o pudiesen identificar al titular del mismo impide que pueda encajarse en la definición legal de dato de carácter personal"*.

En relación con esta cuestión basta señalar que la mencionada sentencia se está refiriendo a ficheros utilizados por el responsable del fichero o del tratamiento que únicamente contienen números de teléfono móvil, es decir que no aparecen asociados a otra información concerniente a una persona identificada o fácilmente identificable. Sin embargo, en este supuesto, el Departamento de Salud del Gobierno de Navarra había facilitado al ISPLN los datos identificativos y de contacto de los D.D.D. en prácticas que resultaban necesarios para gestionar la realización de los exámenes médicos a que dichos funcionarios debían someterse durante la fase de prácticas, función cuyo desarrollo requiere conocer la identidad de estos D.D.D. en prácticas, es decir, nombre, apellidos y DNI de los afectados, amén de otros datos de carácter personal que permitían identificárseles individual o conjuntamente con otra información, como su dirección postal, número de teléfono móvil o número de teléfono fijo. Es decir, el ISPLN trató un fichero con información de carácter personal de los 200 D.D.D. en prácticas que habían aprobado la convocatoria en cuestión a fin de poder citarles para llevar a cabo los exámenes médicos previstos en las bases de la misma, y del que procedía la información de los números de teléfono móvil usados para crear un grupo de "WhatsApp" formado por los 30 funcionarios en prácticas cuya identidad completa el ISPLN también conocía. De lo que se colige que dicho Instituto no trató aisladamente el dato de los números de teléfono móvil de los integrantes del grupo, puesto que conocía la identidad de los 30 D.D.D. en prácticas que lo integraban, quienes al no haber respondido a los llamamientos iniciales estaban pendientes de realizar el examen médico al que se refería la base duodécima de la convocatoria.



A mayor abundamiento, el Defensor del Pueblo de Navarra en su resolución de fecha 18 de abril de 2017, referida a la queja presentada por el representante del Sindicato AFAPNA frente al Departamento de Salud y el Departamento de Educación del Gobierno de Navarra por los mismos hechos denunciados ante la AEPD, señalaba: *“Teniendo en cuenta que, en la aplicación de mensajería instantánea empleada, un número de teléfono puede ser vinculado fácilmente a su titular (a través de la foto del perfil, del nombre introducido como usuario...), no cabe duda de que, en este caso, el número de teléfono se configura como dato de carácter personal de los aspirantes incluidos en el grupo creado por el Instituto de Salud Pública y Laboral de Navarra”.*

VI

El artículo 44.3.c) de la LOPD, considera infracción grave: *“Tratar datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en el artículo 4 de la presente Ley y las disposiciones que lo desarrollan, salvo cuando sea constitutivo de infracción muy grave”*

En el presente expediente, la utilización por el organismo autónomo inculpado del número de teléfono móvil de 30 D.D.D. en prácticas para crear un grupo de “WhatsApp” no responde a la finalidad para la que dicho dato de carácter personal de los aspirantes se recogió en las instancias cumplimentadas por éstos. Así, en la convocatoria no consta que esa información pueda utilizarse para crear grupos colectivos de contacto por cuestiones derivadas del procedimiento selectivo de ingreso en el D.D.D.. Lo que no obsta para que el citado Instituto pueda usar dicho dato para comunicarse, en forma individualizada y no colectiva, mediante esa misma aplicación de mensajería instantánea con los aspirantes o funcionarios en prácticas por asuntos directamente relacionados con la realización de los exámenes médicos de los aspirantes a empleados de la Administración de la Comunidad Foral de Navarra y de sus organismos autónomos.

Por lo tanto, la conducta descrita supone una desviación de la finalidad en el tratamiento de los datos de los afectados (número de teléfono móvil de los D.D.D. en prácticas que no habían realizado el examen médico), establece la base de facto para fundamentar la comisión, a título de culpa, de la infracción del artículo 4.2 de la LOPD.

VII

El artículo 10 de la LOPD que se considera infringido dispone *“El responsable del fichero y quienes intervengan en cualquier fase de tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aún después de finalizar sus relaciones con el titular del fichero, o, en su caso, con el responsable del mismo”.*

Dado el contenido de este precepto, ha de entenderse que el mismo tiene como finalidad evitar que, por parte de quienes están en contacto con los datos personales almacenados en ficheros, se realicen filtraciones de los datos no consentidas por los titulares de los mismos a terceros. Este deber de secreto, que incumbe a los responsables de los ficheros y a todos aquellos que intervengan en cualquier fase del tratamiento de los datos de carácter personal, comporta que el responsable de los datos almacenados no pueda revelar ni dar a conocer su contenido teniendo el *“deber de guardarlos, obligaciones que subsistirán aún después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del*



mismo”, de modo que los datos tratados no puedan ser conocidos por ninguna persona o entidad ajena fuera de los casos autorizados por la Ley, pues en eso consiste precisamente el secreto.

Así el Tribunal Superior de Justicia de Madrid declaró que: *“El deber de guardar secreto del artículo 10 queda definido por el carácter personal del dato integrado en el fichero, de cuyo secreto sólo tiene facultad de disposición el sujeto afectado, pues no en vano el derecho a la intimidad es un derecho individual y no colectivo. Por ello es igualmente ilícita la comunicación a cualquier tercero, con independencia de la relación que mantenga con él la persona a que se refiera la información (...)”*.

Este deber de sigilo resulta esencial en las sociedades actuales cada vez más complejas, en las que las personas están situadas, cada vez más, en zonas de riesgo para la protección de derechos fundamentales, como la intimidad o el derecho a la protección de los datos que recoge el artículo 18.4 de la Constitución Española. En efecto, este precepto contiene un *“instituto de garantía de los derechos de los ciudadanos que, además, es en sí mismo un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos”* (Sentencia del Tribunal Constitucional 292/2000, de 30/11). Este derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino que impida que se produzcan situaciones atentatorias con la dignidad de la persona, es decir, el poder de resguardar su vida privada de una publicidad no querida.

En este sentido el deber de sigilo como se señala en las SSAN, Sec. 1^a, de 14 de septiembre de 2002 (Rec.196/00), 13 de abril de 2005 (Rec. 230/2003), 18 de julio de 2007 (Rec. 377/2005) *“es una exigencia elemental y anterior al propio reconocimiento del derecho fundamental a la libertad informática a que se refiere la STC 292/2000 (...) Este deber de sigilo resulta esencial en las sociedades actuales cada vez más complejas, en las que los avances de la técnica sitúan a la persona en zonas de riesgo para la protección de los derechos fundamentales, como la intimidad o el derecho a la protección de datos que recoge el artículo 18.4 de la CE (...)”*.

En este procedimiento ha quedado acreditado que el ISPLN creó, a principios de febrero de 2017, un grupo de WhatsApp con los números de teléfono móvil de 30 D.D.D. en prácticas para comunicar a los afectados las citaciones para las revisiones médicas que debían realizar en fase de prácticas.

En este caso, ese deber de secreto comporta que el mencionado Instituto, como responsable de la custodia de los datos de carácter personal de los D.D.D. en prácticas que obran en su poder, no puede revelarlos a terceros, salvo con consentimiento de los afectados o en los casos autorizados por la ley (artículos 11 y 12 de la LOPD).

Sin embargo, el uso por el ISPLN del teléfono móvil de los afectados para crear, sin consentimiento de los mismos para esa finalidad, un grupo de mensajería instantánea convierte a dicho Instituto en responsable de la difusión entre los miembros del grupo de la información personal concerniente a los números de teléfono móvil, fotos de perfil y nombres de usuario utilizados por éstos que resulta accesible desde el propio grupo. No hay que olvidar que ha sido dicho Instituto el que ha decidido utilizar esa aplicación de mensajería instantánea que permite acceder a esa información referida a los usuarios.



Cabe recordar también que en la resolución del Defensor del Pueblo de fecha 18 de abril de 2017 antes citada, se señala que *"La medida establecida por el Instituto de Salud Pública y Laboral de Navarra, aun cuando pueda calificarse de efectiva para el propósito perseguido de comunicar a los interesados las citaciones para las revisiones médicas, no puede adoptarse al margen de la normativa que protege los datos de las personas físicas, con mayor motivo si existen alternativas para conseguir los mismos resultados sin dar a conocer el número de teléfono del resto de los aspirantes sin su consentimiento."*

VIII

La conducta descrita en el anterior Fundamento de Derecho se incardina en el artículo 44.3.d) de dicha norma que considera como tal: *"La vulneración del deber de guardar secreto acerca del tratamiento de los datos de carácter personal al que se refiere el artículo 10 de la presente Ley"*.

De acuerdo con lo expuesto en el Fundamento de Derecho anterior, por parte del citado Instituto se producido una vulneración del deber de guardar secreto que le incumbe, toda vez que se ha producido una ausencia de confidencialidad derivada de la revelación de los datos personales concernientes a los 30 D.D.D. en prácticas que integraban el grupo de WhatsApp creado por dicho Instituto entre los propios miembros del grupo, ya que todos los integrantes podían acceder a la información de carácter personal de los restantes participantes del grupo, motivo por lo que se considera a dicho organismo autónomo responsable, a título de culpa, de la comisión de la infracción descrita.

El hecho constatado de la difusión de datos personales de los D.D.D. en prácticas, establece la base de hecho para fundamentar la imputación de la infracción del artículo 10 de la LOPD.

IX

El artículo 46 de la LOPD, *"Infracciones de las Administraciones Públicas"*, dispone:

"1. Cuando las infracciones a que se refiere el artículo 44 fuesen cometidas en ficheros de titularidad pública o en relación con tratamientos cuyos responsables lo serían de ficheros de dicha naturaleza, el órgano sancionador dictará una resolución estableciendo las medidas que procede adoptar para que cesen o se corrijan los efectos de la infracción. Esta resolución se notificará al responsable del fichero, al órgano del que dependa jerárquicamente y a los afectados si los hubiera.

2. El órgano sancionador podrá proponer también la iniciación de actuaciones disciplinarias, si procedieran. El procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario de las Administraciones Públicas.

3. Se deberán comunicar al órgano sancionador las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores.

4. El Director de la Agencia comunicará al Defensor del Pueblo las actuaciones que efectúe y las resoluciones que dicte al amparo de los apartados anteriores".

En el presente supuesto no se considera necesario requerir al ISPLN la adopción de medidas concretas para que se cesen o corrijan los efectos de las infracciones estudiadas, toda vez que los hechos analizados responden a una



conducta puntual frente a la cual el citado Instituto ha adoptado medidas tendentes a evitar su repetición. En concreto, se tiene en cuenta la concurrencia de las siguientes circunstancias:

- Ha sido la primera vez que se ha utilizado la creación de un grupo de "Whatsapp" para contactar con los D.D.D. en prácticas.

- El grupo se eliminó a las 8 horas de su creación, tan pronto como se contactó con los afectados por dicho canal.

- En la resolución del Defensor del Pueblo, de fecha 18 de abril de 2017 incorporada al procedimiento, se recoge parte del contenido del informe del Departamento de Salud donde se señalaba que "*... el Instituto de Salud Pública y Laboral de Navarra se compromete, a que, en el futuro, en el caso de utilizar las aplicaciones de mensajería instantánea para comunicarse con determinadas personas, esa comunicación se realizará individualmente, sin crear grupos colectivos, para que de esta forma quede asegurada la protección de datos de carácter personal (en este caso el número de teléfono particular del aspirante a empleado público).*".

Vistos los preceptos citados y demás de general aplicación,

La Directora de la Agencia Española de Protección de Datos **RESUELVE:**

PRIMERO: Declarar que el **INSTITUTO DE SALUD PÚBLICA Y LABORAL DE NAVARRA** ha infringido lo dispuesto en los artículos 4.2 y 10 de la LOPD, tipificadas como infracción grave en los artículos 44.3.c) y 44.3.d), respectivamente, de dicha norma.

SEGUNDO: **NOTIFICAR** la presente resolución al **INSTITUTO DE SALUD PÚBLICA Y LABORAL DE NAVARRA** y a su superior jerárquico, el **DEPARTAMENTO DE SALUD DEL GOBIERNO DE NAVARRA**.

TERCERO: **COMUNICAR** la presente resolución al Defensor del Pueblo, de conformidad con lo establecido en el artículo 46.4 de la LOPD.

De conformidad con lo establecido en el apartado 2 del artículo 37 de la LOPD, en la redacción dada por el artículo 82 de la Ley 62/2003, de 30 de diciembre, de medidas fiscales, administrativas y del orden social, la presente Resolución se hará pública, una vez haya sido notificada a los interesados. La publicación se realizará conforme a lo previsto en la Instrucción 1/2004, de 22 de diciembre, de la Agencia Española de Protección de Datos sobre publicación de sus Resoluciones y con arreglo a lo dispuesto en el artículo 116 del reglamento de desarrollo de la LOPD aprobado por el Real Decreto 1720/2007, de 21 diciembre.

Contra esta resolución, que pone fin a la vía administrativa (artículo 48.2 de la LOPD), y de conformidad con lo establecido en los artículos 112 y 123 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, se podrá interponer potestativamente recurso de reposición ante la Directora de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución, o, directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional con arreglo a lo dispuesto en el artículo 25 y



en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa (en lo sucesivo LJCA), en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 del referido texto legal.

Sin embargo, el responsable del fichero de titularidad pública, de acuerdo con el artículo 44.1 de la LJCA, sólo podrá interponer directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la LJCA, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 del referido texto legal.

Mar España Martí
Directora de la Agencia Española de Protección de Datos