



Roj: **STS 4902/2024 - ECLI:ES:TS:2024:4902**

Id Cendoj: **28079130032024100227**

Órgano: **Tribunal Supremo. Sala de lo Contencioso**

Sede: **Madrid**

Sección: **3**

Fecha: **07/10/2024**

Nº de Recurso: **6949/2022**

Nº de Resolución: **1565/2024**

Procedimiento: **Recurso de Casación Contencioso-Administrativo (L.O. 7/2015)**

Ponente: **EDUARDO CALVO ROJAS**

Tipo de Resolución: **Sentencia**

Resoluciones del caso: **SAN 3172/2022,**

**ATS 283/2023,**

**STS 4902/2024**

## **TRIBUNAL SUPREMO**

### **Sala de lo Contencioso-Administrativo**

#### **Sección Tercera**

##### ***Sentencia núm. 1.565/2024***

Fecha de sentencia: 07/10/2024

Tipo de procedimiento: R. CASACION

Número del procedimiento: 6949/2022

Fallo/Acuerdo:

Fecha de Votación y Fallo: 01/10/2024

Ponente: Excmo. Sr. D. Eduardo Calvo Rojas

Procedencia: AUD.NACIONAL SALA C/A. SECCION 1

Letrada de la Administración de Justicia: Sección 003

Transcrito por: MAB

Nota:

R. CASACION núm.: 6949/2022

Ponente: Excmo. Sr. D. Eduardo Calvo Rojas

Letrada de la Administración de Justicia: Sección 003

## **TRIBUNAL SUPREMO**

### **Sala de lo Contencioso-Administrativo**

#### **Sección Tercera**

##### ***Sentencia núm. 1565/2024***

Excmos. Sres.

D. José Manuel Bandrés Sánchez-Cruzat, presidente

D. Eduardo Calvo Rojas



D. José María del Riego Valledor

D. Diego Córdoba Castroverde

D. Isaac Merino Jara

En Madrid, a 7 de octubre de 2024.

Esta Sala ha visto el recurso de casación nº 6949/2022 interpuesto por el AYUNTAMIENTO DE ALGEMESÍ, representado por la procuradora Dª Mª del Mar Gómez Rodríguez y asistido por el abogado D. Guillermo Balaguer Pallás, contra la sentencia de la Sección 1ª de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional de 10 de junio de 2022 dictada en el recurso contencioso-administrativo nº 1684/2020. Se ha personado como parte recurrida la ADMINISTRACIÓN GENERAL DEL ESTADO, representada y asistida por la Abogacía del Estado.

Ha sido ponente el Excmo. Sr. D. Eduardo Calvo Rojas.

## ANTECEDENTES DE HECHO

**PRIMERO.-** La Sección 1ª de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional dictó sentencia con fecha de 10 de junio de 2022 (recurso contencioso-administrativo nº 1684/2020) en cuya parte dispositiva se acuerda:

<< FALLAMOS: Desestimar el recurso contencioso administrativo interpuesto por la Procuradora de los Tribunales Sra. Gómez Rodríguez, en nombre y representación del Ayuntamiento de Algemesí, frente a la Resolución de la Directora de la Agencia Española de Protección de Datos de fecha 27 de noviembre de 2020 (PS/00062/2019); con imposición de costas a la parte demandante>>.

**SEGUNDO.-** Según recoge el fundamento jurídico segundo de la sentencia de la Audiencia Nacional, la resolución de la Agencia Española de Protección de Datos impugnada en el proceso de instancia se basa en un relato de hechos probados del que cabe destacar lo siguiente:

<< La reclamante prestaba servicios en el Ayuntamiento de Algemesí como funcionaria con habilitación de carácter nacional, como interventor-tesorera.

El 27 de marzo de 2018 le es entregado un acuerdo de notificación de solicitud de incoación de expediente disciplinario adoptado por el Pleno el 22 de marzo de 2018, a propuesta de la Alcaldía de 20 de marzo de 2018. Entre las actuaciones efectuadas por la reclamante, junto a la justificación de asistencia aportada a una supuesta jornada de formación, a la que, recabada información, resultó no haber asistido, se indica en el punto segundo de dicho acuerdo que: " *al haber aparecido documentos en el escáner y la impresora que podrían suponer que la reclamante realiza actividades personales o profesionales dentro de la jornada de trabajo que nada tienen que ver con sus funciones de tesorera y que incluso podrían resultar incompatibles, mediante providencia de 26/02/2018, se ordenó al departamento de informática que investigue los documentos del ordenador personal de trabajo para aclarar esos hechos. De la inspección efectuada se obtuvieron varias carpetas de documentos personales sobre actividades privadas que se grabaron en un DVD*".

En el mismo acuerdo del Pleno se acuerda remitir la documentación al órgano competente para la instrucción del expediente disciplinario, la Dirección General de Administración Local de la Comunidad Valenciana, si bien la copia del DVD se presenta en registro por el Ayuntamiento de Algemesí el 18 de abril de 2018, manifestando que era la primera copia efectuada, que no iba encriptada, ni portaba elemento alguno que lo identificara como soporte de su contenido.

La providencia de la Alcaldía firmada el 26 de febrero de 2018, a que se refiere el citado Acuerdo del Pleno, indica " *Considerando que se han encontrado documentos, impresora y escáner de la funcionaria... sobre actividades que nada tienen que ver con las funciones públicas correspondientes a su puesto de trabajo como Tesorera del Ayuntamiento... y que pueden resultar incompatibles con su puesto de trabajo*". Dispone " *Que por el Departamento de informática se acceda al ordenador de trabajo de la funcionaria, a fin de comprobar la existencia de documentos que evidencien actividades diferentes a las funciones que como Tesorera de este Ayuntamiento tiene encomendadas*" ... " *destinando la información que se pueda obtener a los efectos de los expedientes que a la vista de los documentos obrantes puedan iniciarse*".

Ese mismo día 26 de febrero de 2018 se produjo el acceso al ordenador de la reclamante, titularidad del Ayuntamiento y con el que prestaba sus servicios, por el responsable informático que lo llevó a efecto con clave como administrador del sistema, sin necesidad de acudir físicamente al mismo, quien manifestó que no vio ni le fueron mostrados los documentos hallados en la impresora y escáner. " *Le dijo la alcaldesa que había que hacer una inspección de documentos. De la carpeta mis documentos que se encuentra en los servidores,*



*visible solo por cada usuario, cogió las carpetas que había en mis documentos y además, otros documentos del ordenador del escritorio, siendo dos o tres carpetas, los seleccionó y los copió en un DVD conforme a las instrucciones recibidas de la alcaldesa. El DVD no se encriptó y se lo dio personalmente a la alcaldesa en el momento en que lo grabó", "No llegó a abrir ningún documento, no entró en el correo electrónico ni en los datos de navegación" "Cuando se hizo la intervención del ordenador no se hacía ninguna advertencia a los funcionarios sobre el contenido de la información que se podía tener en los ordenadores".*

La reclamante se enteró del acceso a su ordenador cuando se le notifica el 26 de febrero de 2018 el acuerdo de solicitud de incoación de expediente disciplinario. Los representantes de los trabajadores tampoco fueron advertidos de dicho acceso ni de los documentos "aparecidos en el escáner y en la impresora".

Del contenido del DVD enviado por el reclamado en pruebas, que plasma los documentos copiados del ordenador usado por la reclamante, se destaca que contenía tres carpetas "mis documentos" y "download" con espacio de 1,7 GB. La vista de las tres carpetas revela que se contiene tanto información personal como profesional, copia de contrato de seguro de vehículo, declaración de hacienda, datos de contratos de préstamo hipotecario, o pago de bienes inmuebles, claves personales, datos bancarios, y de empresas como la franquicia Now You, cuenta de resultados Gestión Spa Hotel Myr, facturas de empresa de fotografía a nombre de otra persona, listado de cuentas anuales, pérdidas y ganancias del ejercicio 2017 de la empresa Aditivos Bio Energéticos, documentos sobre una sociedad que se dedica al negocio de la óptica denominada Ángel Visión.

Los documentos "aparecidos en el escáner y en la impresora", inicialmente no son especificados, ni figura diligencia que explique el modo en que se llega a saber de esos documentos, quien los encuentra o en qué fecha. El contenido del DVD, según el Ayuntamiento, sólo fue mostrado a un miembro de un grupo político que tenía que votar en el Pleno y por esta razón.

De la información obtenida en pruebas se verifica que la expresión "documentos aparecidos en el escáner impresora", se refiere al almacenamiento de documentos en la memoria interna del escáner que utilizaban los tres empleados del departamento de Tesorería y al modo de configuración de dicho medio, permitiendo su almacenamiento como fichero de este tipo de información. Entre los documentos hallados hay diversos de la Franquicia Now You SL y relacionados con las nóminas de sus empleados, pudiéndose deducir que la reclamante era administradora de dicha sociedad. También se aprecia que se escanea por la reclamante un documento relacionado con su salud, sobre Resolución de expediente de determinación de la contingencia causante de un proceso de IT en el que figura un informe del Evi contenido la patología diagnosticada.

Según el Ayuntamiento, a las carpetas que figuraban en el escáner del departamento de Tesorería podía acceder cualquiera de los tres empleados de la misma, circunstancia de la que no fueron advertidos dichos empleados, precisando que uno de ellos vio los documentos y advirtió a los responsables. Esta configuración del escáner de acceso múltiple a carpetas del escáner, según el reclamado, ha sido variada.

No consta que el Ayuntamiento tuviera al momento del acceso al ordenador usado por la reclamante, el 26/2/18, una política y protocolo de uso del equipo informático de los empleados, prohibiciones o tipos de acceso permitidos, con advertencia sobre medios de control y consecuencias del mismo>>.

Explica la propia resolución administrativa que, atendida la fecha en que suceden los hechos, febrero de 2018, resulta de aplicación la disposición transitoria tercera de la Ley Orgánica 3/2018, de protección de datos personales y garantía de los derechos digitales (LOPDGDD): *"1. Los procedimientos ya iniciados a la entrada en vigor de dicha Ley se regirán por la normativa anterior salvo que esta ley orgánica contenga disposiciones más favorables para el interesado"*, por lo que aplica la normativa anterior, considerada más beneficiosa.

En fin, la resolución de la Agencia Española de Protección de Datos termina acordando en su parte dispositiva:

<< PRIMERO: Declarar que el Ayuntamiento de Algemesí ha infringido:

- el artículo 6.1 de la LOPD, tipificada como grave en el artículo 44.3.b) de la LOPD, y
- el artículo 9 de la LOPD, en relación con los artículos del RLOPOD: 92, 97.1 y .2 y 101, tipificada como grave en el artículo 44.3.,h) de la LOPD (...)>>

**TERCERO.-** La sentencia ahora recurrida, tras acotar en su fundamento jurídico primero la cuestión abordada en el procedimiento administrativo -y luego también en el proceso -" (...) se trata de determinar, desde la perspectiva de los derechos fundamentales, si el acceso a los contenidos de los ordenadores u otros medios informáticos, en el presente caso, vulnera el artículo 18.4 de la Constitución ", expone en sus fundamentos jurídicos tercero y siguientes las razones en las que la Sala de instancia fundamenta la desestimación del recurso contencioso-administrativo.



En lo que se refiere a la infracción del artículo 6.1 de la LOPD, el F.J. 3 de la sentencia explica que el Ayuntamiento de Algemesí no comparte la interpretación de la AEPD, sustentada en la aplicación de la sentencia *Barbulescu*, señalando el Ayuntamiento que dicha doctrina se refiere a un conflicto laboral en el seno de una empresa privada y aquí nos encontramos ante una Administración Pública; y que, por la propia naturaleza de los bienes, tanto ordenador como escáneres o impresoras del Ayuntamiento, sobre los que se pretende situar la expectativa de privacidad, sometidos al régimen del artículo 132 de la Constitución, y sobre esta clase de bienes no existe ni puede existir esa potestad de tolerancia con ciertos usos personales. Frente a ello, el Abogado del Estado aduce que aunque en el presente caso el sujeto infractor sea una Administración pública, resulta de aplicación la doctrina contenida en la sentencia *Barbulescu* que interpreta el artículo 8 de la Carta Europea de Derechos Humanos, por cuanto el derecho fundamental del artículo 18 de la Constitución y el artículo 8 de la Carta Europea no desaparece por encontrarnos en el ámbito estatutario; y que el Ayuntamiento yerra al calificar la naturaleza del bien, pues los ordenadores e impresoras son bienes patrimoniales, que habrán de inscribirse en el inventario de Bienes de las Corporaciones Locales, según el artículo 27 del Real Decreto 1372/1986, de 13 de junio, y esa naturaleza patrimonial del bien no excluye que opere la expectativa de privacidad.

La posición de la Sala de la Audiencia Nacional sobre este apartado de la controversia queda recogida en el F.J. 4 de la sentencia, cuyo contenido es el que siguen:

<< (...) CUARTO.- Constituye un hecho incontrovertido que el 26 de febrero de 2018 se realizó el acceso al ordenador de trabajo de la reclamante, titularidad del Ayuntamiento y con el que prestaba sus servicios como interventor-tesorera, por el funcionario encargado del servicio de informática de dicho Ayuntamiento, que lo llevó a efecto sin necesidad de acudir físicamente al ordenador con clave como administrador del sistema, y copió en un DVD las carpetas halladas en dicho ordenador. Acceso a dicho ordenador acordado por providencia de la Alcaldía de esa misma fecha -página 30 del expediente- al haberse "encontrado documentos (impresora y escáner) de la funcionaria (...) sobre actividades que nada tienen que ver con las funciones públicas correspondientes a su puesto de trabajo como tesorera del Ayuntamiento d'Algemesí y que podrían resultar incompatibles con su puesto de trabajo".

Es decir, frente a lo alegado en la demanda y tal como resulta de la citada providencia, el hallazgo de dichos documentos en el escáner, calificado por el recurrente como "hallazgo casual", fue el único dato o indicio tomado en consideración para acordar el acceso al ordenador de la funcionaria.

"Hallazgo" que difícilmente puede calificarse como casual, cuando no se trata de documentos que aparecieron o fueron dejados en el escáner o la impresora, ni a los que cualquiera pudiera acceder, como en conclusiones señala el demandante, sino que se hallaban almacenados en carpetas en la memoria interna del escáner que utilizaban los tres empleados del departamento de Tesorería, ya que la documentación que era escaneada en el escáner impresora se almacenaba en su memoria interna, con acceso indiferenciado de todos los empleados del departamento a dichas carpetas. Configuración del escáner de acceso múltiple a las carpetas del escáner, de la que no habían sido informados los empleados y que, según el Ayuntamiento, ha sido variada.

Tampoco se indica en la citada providencia cual son esos documentos que motivaron acordar el acceso al ordenador de la reclamante, ni consta diligencia que documente el "hallazgo", ni su fecha, habiéndose constatado que entre los documentos almacenados en carpetas en el escáner figuraban diversos de la Franquicia Now You S.L y relacionados con las nóminas de sus empleados, así como un documento relacionado con la salud de la reclamante, otro sobre resolución de expediente de determinación de la contingencia causante de un proceso de IT en el que figura un informe de Evi contenido la patología diagnosticada, es decir, de datos de salud, que son especialmente protegidos.

Además, y pese a la existencia de esos documentos con datos de salud en las carpetas del escáner, el funcionario del departamento de informática del Ayuntamiento que ejecuta la providencia en la que se dice "que investigue los documentos del ordenador del trabajo", al no relacionarle documento alguno del escáner para saber que tiene buscar en esa investigación, copia todas las carpetas sin ver antes los archivos, de tal forma que, como subraya la resolución recurrida, la investigación no es tal, sino un volcado de carpetas y archivos, que se recogen en un DVD que entregó a la alcaldesa.

Las tres carpetas copiadas revelan que contienen tanto información profesional como personal, copia de contrato de seguro de vehículo, declaración de hacienda, datos de contratos de préstamo hipotecario, o pago de bienes inmuebles, claves personales, datos bancarios y de empresas como la franquiciada Now You S.L, Gestión Spa Hotel Myr, Aditivos Bio Energéticos, Angels Visión. DVD que estuvo a disposición de los portavoces de los grupos del Ayuntamiento en la reunión donde se decidió proponer la incoación del expediente disciplinario a la reclamante.



Sostiene el demandante, como hemos dicho, que no resulta de aplicación al caso la doctrina de la STDH *Barbulescu 2* al referirse a un conflicto laboral en el seno de una empresa privada y aquí se trata de una relación de sujeción especial entre un funcionario público y el Ayuntamiento que es una Administración pública.

Ahora bien, esa relación de sujeción especial que implica una situación de dependencia mayor que la que se produce en las relaciones de sujeción general, efectivamente, tiene manifestaciones propias, como puede ser la modulación del principio non bis in ídem, pero no llega a la exclusión de un derecho fundamental que no encuentra fundamento legal por la naturaleza jurídica pública del Ayuntamiento actuante, pues los principios generales del derecho de protección de datos son aplicables tanto a entidades públicas como privadas aunque en algunos supuestos la normativa pública pueda influir en el tratamiento llevado a cabo.

Las particularidades de ser una Administración Pública, que las hay, son fundamentalmente, en lo que aquí se refiere, las contenidas en el artículo 46 LOPD, que suponen la no imposición de sanción al Ayuntamiento por las vulneraciones de los artículos 6.1 y 9.1 de la LOPD, pero el hecho de que el sujeto infractor sea una Administración Pública no lleva, en lo que aquí atañe, a la desaparición del derecho fundamental del artículo 18 CE o del artículo 8 de la Carta Europea de Derechos Humanos. Al respecto y aunque no resulte aplicable por razones temporales, resulta ilustrativo el artículo 87 del RGPD transcrita por la resolución impugnada, por lo que parece razonable la proyección de la doctrina contenida en la STDH *Barbulescu 2*, de 5 de septiembre de 2017, al ámbito del empleo público.

En este sentido, el Real Decreto Legislativo 5/2015, por el que se aprueba el Estatuto Básico del Empleado Público (EBEP), establece dentro del Capítulo I del Título III "derechos de los empleados públicos" en el artículo 14, que los empleados públicos tienen los siguientes derechos de naturaleza individual en correspondencia con la naturaleza jurídica de su relación de servicio: "j bis) A la intimidad en el uso de dispositivos digitales puestos a su disposición y frente al uso de dispositivos de videovigilancia y geolocalización (...) en los términos establecidos en la legislación vigente en materia de protección de datos personales y garantía de los derechos digitales". Apartado añadido por la Disposición final 14 de la Ley Orgánica 3/2018, de 5 de diciembre y si bien no resulta aquí aplicable por razones temporales, se estima de interés citar al venir a reforzar el criterio sostenido.

El hecho de que el artículo 54 del EBEP sobre "Principios de conducta", establezca en el apartado 5, citado por la actora, que "Administrarán los recursos y bienes públicos con austeridad, y no utilizaran los mismos en provecho propio o de personas allegadas. Tendrán así mismo el deber de velar por su conservación", no tiene el alcance que pretende otorgarle la actora, por cuanto, además de lo ya expuesto, debe tenerse en cuenta que el artículo 20.2 del mismo EBEP dispone que "Los sistemas evaluación del desempeño (...) se aplicarán sin menoscabo de los derechos de los empleados públicos" y el artículo 14.h) contempla entre dichos derechos, a la fecha de los hechos, el derecho al respeto de su intimidad y dignidad en el trabajo.

Por ello, y en orden a establecer una ponderación o justo equilibrio de los intereses en juego, resultan esenciales, en este caso en que no resulta aplicable *ratione temporis* el artículo 87 del RGPD, las pautas o criterios establecidos en la STDH *Barlubescu 2*, de la Gran Sala, que anula la STDH de 12 de enero de 2016 (*Barlubescu 1*).

De otro lado, el Auto de la Audiencia Provincial de Valencia, Sec. 3<sup>a</sup>, de 23 de diciembre de 2019. obrante a las páginas 295 y siguiente del expediente, invocado por la actora, después de efectuar una serie de consideraciones por las que estima penalmente irrelevante la actuación de la alcaldesa "con relación a los archivos guardados por la querellante en el sistema informático del Ayuntamiento (ordenador y servidor)", añade en el Razonamiento Jurídico primero, in fine, -página 298- "aunque siempre sin perjuicio del valor probatorio que en otra jurisdicción pueda atribuirse a la información así obtenida o incluso de la responsabilidad administrativa en que haya podido incurrir en virtud de la legislación de protección de datos".

Asimismo, tampoco obsta a lo expuesto la Sentencia de 18 de enero de 2019, del Juzgado de lo Contencioso administrativo nº 7 de Valencia que desestima el recurso interpuesto por la reclamante contra el acuerdo del Ayuntamiento de solicitar la incoación de expediente disciplinario. Sentencia confirmada en apelación por la del Tribunal Superior de Justicia de la Comunidad Valenciana, Sec. 2<sup>a</sup>, de 9 de febrero 2022 (Rec. apelación. 83/21), como ha podido comprobar la Sala a través del CENDOJ y qué tras argumentar sobre la desestimación del recurso, señala "siendo cuestión distinta que el Ayuntamiento durante sus actuaciones de investigación haya vulnerado la legislación en materia de protección de datos cuestión ésta que ha sido enjuiciada y resuelta por parte del órgano competente".

La STS, Sala de lo Social, de 8 de febrero de 2018 (Rec. 1121/2015) invocada por el demandante, en la que nos vamos a detener al haber sido dictada, a diferencia de otras también citadas, con posterioridad a la Sentencia *Barbulescu 2*, entre otros parámetros, toma en consideración en su Fundamento de Derecho sexto, que los empleados del Grupo empresarial "cada vez que acceden con su ordenador a los sistemas informáticos de la compañía, y de forma previa a dicho acceso, deben de aceptar las directrices establecidas



en la Política de Seguridad de la Información del Grupo (...), en la que se señala que el acceso lo es para fines estrictamente profesionales, reservándose la empresa el derecho de adoptar las medidas de vigilancia y control necesarias para comprobar la correcta utilización de las herramientas que pone a disposición de su empleados, respetando en todo caso las legislación laboral y convencional sobre la materia y garantizando la dignidad e intimidad del empleado, por lo que el actor era conocedor de que no podía utilizar el correo para fines particulares y que la empresa podía controlar el cumplimiento de las directrices en el empleo de los medios informáticos por ella facilitados".

Es decir, se trata en ese caso de una empresa que tiene un completo manual de instrucciones y reglas que los trabajadores deben conocer y aceptar al usar los sistemas informáticos

En tanto que en el caso de autos no se informó a los empleados de la utilización de los equipos informáticos, con la advertencia de la existencia de medidas de control o supervisión del ordenador sobre las comunicaciones de los empleados, que es uno de los factores tomados en consideración por la sentencia *Barbulescu 2*.

El artículo 6 de la LOPD establece 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".

En tanto, que el apartado 2 contiene una serie de excepciones a dicha regla general y dispone "No será preciso el consentimiento cuando los datos de carácter personal se recojan en el ejercicio de las funciones públicas de las Administraciones públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento (...)"

El Tribunal Constitucional en la Sentencia 292/2000 ha considerado como parte esencial del derecho a la protección de datos el derecho a ser informados de las finalidades, usos y derechos que conlleva el tratamiento de datos de carácter personal.

La legitimación para el tratamiento consistente en el acceso al equipo informático asignado a la reclamante puede obedecer a la comprobación del cumplimiento de sus funciones dentro de la relación que mantiene con el Ayuntamiento, y se puede arbitrar este tipo de accesos cuando se haya informado previamente del uso de los datos para dichos fines y en supuestos en que resulten proporcionales dichos accesos. Sin embargo, en el caso de autos no existía información previa sobre dicho uso o fines y tampoco existió proporcionalidad de la medida adoptada, pues se accede a todas las carpetas y archivos sin discriminar su contenido, de una forma especialmente invasiva, de tal forma que se han visto afectados documentos privados de la reclamante, documentos de salud, etc. que se han recogido de forma innecesaria y sin relación con lo que se buscaba.

Por tanto, se considera acreditada la infracción por vulneración del principio del consentimiento del artículo 6 LOPD, sin que nos hallemos ante ninguno de los supuestos habilitantes previstos en los incisos c) y e) del RGPD, invocados por la actora, pues no concurren ninguno de los presupuestos establecidos en el artículo 8 de la LOPDGDD para entender que se pueda considerar fundado el tratamiento de datos personales en cumplimiento de obligación legal, interés público o ejercicio de poderes públicos>>.

Por último, en cuanto a la infracción del artículo 9.1 LOPD, en relación con los artículos 92, 97.1 y 2, y 101 del Reglamento de desarrollo de dicha Ley aprobado por Real Decreto 1720/2007, explica la sentencia (F.J. 5) que, según el Ayuntamiento demandante, la conducta no se encuentra tipificada en el marco de la LOPDGDD pues el artículo 73.f) de la misma, en relación con el artículo 32.1 del RGPD, no vincula el cumplimiento de las obligaciones de seguridad del responsable del tratamiento a unas medidas concretas, sino que se orienta a través de un enfoque de riesgo. Por ello, invocando el principio de retroactividad de las disposiciones sancionadoras más favorables, el Ayuntamiento considera que es de aplicación la nueva normativa al no haberse llevado a cabo actividad probatoria pertinente sobre la evaluación de las medidas de seguridad del Ayuntamiento de conformidad con las previsiones del artículo 32 del RGPD y no puede valorarse que no cumpla con los principios del citado artículo 32.

La Sala de la Audiencia Nacional no comparte el planteamiento del Ayuntamiento de Algemesí; y ello por las razones que expone el propio F.J. 5 de la sentencia:

<< (...) Alegaciones [del Ayuntamiento] que no desvirtúan las consideraciones efectuadas al efecto por la resolución recurrida, que da adecuada respuesta a dicha cuestión planteada en similares términos en vía administrativa.

Así establece el RGPD en su artículo 5.2 "El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo (responsabilidad proactiva)". Y el apartado 1 se refiere a los principios del tratamiento entre los que se encuentran. apartados a) y f), el modo en que han de ser tratados



los datos "de manera lícita, leal y transparente", y "de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección (...) contra su pérdida, destrucción o daño accidental mediante la aplicación de medidas técnicas u organizativas apropiadas adecuadas.

Ello implica, como subraya la AEPD, que la entidad es la que asume su propia responsabilidad dirigiendo y coordinando la materia en cuanto al personal que le presta servicios.

En este sentido el 32 del RGPD "Seguridad del tratamiento", establece:

"1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros: (...) b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios del tratamiento".

Precepto con el que se conecta el artículo 73.f) de la LOPDGDD, que tipifica como infracción grave "f) La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento, en los términos exigidos por el artículo 32.1 del Reglamento (UE) 2016/679".

Se necesita, por tanto, un desenvolvimiento proactivo sobre la protección de los datos y guardar las evidencias de los pasos que se dan para cumplir con el RGPD junto a la circulación y vida de los datos, incluyendo eventuales instrucciones no solo de seguridad de soportes, sino como las que ha dictado para adaptarse al manejo de datos en sistemas de información y acceso del personal a los datos. De tal forma, que el hecho de que no se establezca expresamente como han de tratarse los soportes de almacenamientos de datos, no significa que no esté tipificado en el RGPD, y que deba reunir unos requisitos, y en ambos casos la conducta infractora acarrearía una infracción de medidas de seguridad en el tratamiento de datos.

Además, ambas normativas establecen un periodo de prescripción de la infracción de dos años.

Por tanto, al no haberse acreditado que el RGPD resulte más favorables que la LOPD vigente al momento de comisión de los hechos, es aplicable la citada LOPD en virtud de lo dispuesto en la Disposición transitoria tercera de la LOPDCDD.

En definitiva, queda acreditada la comisión de la infracción tipificada en el artículo 44.3.h) de la LOPD), por no tener activadas las medidas de seguridad que le eran exigibles para evitar que el soporte DVD que contiene datos e información asociada a la extracción en disco de datos del ordenador de la reclamante, que sirve como prueba en el procedimiento disciplinario, que forma parte de un expediente, como soporte que contiene datos personales, no se haya cifrado, registrado, diligenciado y descrito su contenido. Extremos que no se cuestionan por el recurrente que se limita a propugnar la aplicación del RGPD y la LOPDGDD>>.

Por todo ello la Sala de la Audiencia Nacional termina desestimando el recurso contencioso-administrativo.

**CUARTO.-** Notificada la sentencia a las partes, preparó recurso de casación contra ella la representación del Ayuntamiento de Algemesí, siendo admitido a trámite el recurso por auto de la Sección Primera de esta Sala de 19 de enero de 2023 en el que asimismo se acuerda la remisión de las actuaciones a la Sección Tercera, con arreglo a las normas sobre reparto de asuntos.

En la parte dispositiva del auto de admisión del recurso se acuerda, en lo que ahora interesa, lo siguiente:

<< (...) 2.º) Declarar que la cuestión planteada en el recurso que presenta interés casacional objetivo para la formación de la jurisprudencia consiste en determinar si, en aplicación del artículo 6.1 de la Ley Orgánica de Protección de Datos 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal -actual artículo 6 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales- se vulnera la normativa de protección de datos por el hecho de que el sujeto infractor sea una Administración Pública o, por el contrario, se puede considerar fundado el tratamiento de datos personales en cumplimiento de obligación legal, interés público o ejercicio de poderes públicos, y si resulta razonable la proyección de la doctrina contenida en la STEDH Barbulescu 2, de 5 de septiembre de 2017, al ámbito del empleo público y las garantías del procedimiento sancionador en el régimen disciplinario de los empleados públicos.

3.º) Identificar como normas jurídicas que, en principio, serán objeto de interpretación: el artículo 6.1 de la Ley Orgánica de Protección de Datos 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, actual artículo 6 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, así como el artículo 8 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección



de Datos Personales y garantía de los derechos digitales. Así como el artículo 18 de la Constitución Española, sin perjuicio de que la sentencia haya de extenderse a otras cuestiones o normas si así lo exigiere el debate finalmente trabajado en el recurso>>.

**QUINTO.-** La representación del Ayuntamiento de Algemesí formalizó la interposición de su recurso de casación mediante escrito de fecha 6 de marzo de 2023 en el que, tras exponer los antecedentes y los datos que considera relevantes, la parte recurrente desarrolla los argumentos en los que basa su impugnación.

**A/** En lo que se refiere a la infracción del artículo 6.1 LOPD, el planteamiento el Ayuntamiento recurrente se sustenta, en los puntos que ahora pasamos a sintetizar.

- La regla establecida en el artículo 6.1 LOPD (*"El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa"*) tiene sus excepciones; entre ellas las enunciadas en el artículo 6.2: *"No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado"*. Sin embargo, la sentencia recurrida no toma en consideración este precepto.

- Tampoco se comparte la interpretación de la Audiencia Nacional y la AEPD, basada en la asimilación de administración pública y empresa privada. La doctrina *Barbulescu* se refiere a un conflicto laboral en el seno de una empresa privada y no resulta de aplicación a la presente litis al encontrarnos en otro supuesto de hecho, y ante otro tipo de relación (de índole pública), y que además no se reúne los requisitos para entender vulnerada la esfera de intimidad que alega la reclamante.

- Por la propia naturaleza de los bienes sobre los que se pretende situar la "expectativa de privacidad" en los hechos objeto de este procedimiento, tanto ordenador como escáneres e impresoras del Ayuntamiento, es evidente que se trata de bienes sometidos al régimen del artículo 132 de la Constitución y, por desarrollo del legislador, a la Ley 33/2003, de 3 de noviembre, del Patrimonio de las Administraciones Públicas, Real Decreto 1373/2009, de 28 de agosto, por el que se aprueba el Reglamento General de la Ley 33/2003, de 3 de noviembre, del Patrimonio de las Administraciones Públicas y, para el concreto caso de la Administración local, al Real Decreto 1372/1986, de 13 de junio, por el que se aprueba el Reglamento de Bienes de las Entidades Locales. Sobre dicho régimen de bienes, no existe ni puede existir esa potestad de tolerancia con ciertos usos personales, puesto que admitirla sería contrario a la legislación anteriormente citada que somete a un régimen concreto de obligaciones, finalidades y usos, los bienes sobre los que la Administración tiene titularidad o derechos de algún tipo.

- No discute este Ayuntamiento, la capacidad del empresario de gestionar como propietario de sus medios de producción, en consonancia con el artículo 33 y 38 de la Constitución. Sin embargo, el Ayuntamiento, en tanto que Administración Pública, no tiene esa posibilidad del empresario de "(...) autoorganización, dirección y control fijar las condiciones de uso de los medios informáticos asignados a cada trabajador (...)" . No obstante, el Ayuntamiento tiene la obligación de proteger el patrimonio público y velar para que su uso se destine a la finalidad pública fijada por el legislador, para el cual está destinado, y a ninguna otra, no pudiendo elegir el grado de mayor o menor severidad en la observancia de dicho requisito, puesto que de lo contrario, no solo iría en contra de las anteriores disposiciones legales anteriormente citadas, la propia naturaleza que fundamenta los bienes públicos, sino que

- Respecto al "código interno" o documento similar prohibiendo expresamente el uso privativo de los dispositivos puestos a disposición de los funcionarios facilitado por las Administraciones Públicas, el Ayuntamiento no puede asimilarse a una entidad empresarial en el sentido que el propio ingreso en la institución implica el conocimiento y aceptación de un régimen estatuario propio con rango de ley en condición de funcionario público, que no sólo debe cumplir su propio régimen estatutario, sino que también tiene deberes de cumplir y hacer cumplir la legislación dentro del ámbito de sus competencias. Por ello, no sólo el personal del Ayuntamiento está sometido en su conducta a una prohibición expresa de uso privativo de medios o bienes públicos, tal como establece el propio EBEP, sino que el legislador contempla una conducta sancionadora al respecto. Conducta típica que además no solo sanciona el empleo de dichos medios si no también la autorización de uso, lo que en efecto impone un deber de cuidado sobre otras autoridades o funcionarios públicos, por lo que la obligación de verificar y asegurar que no se utiliza para finalidades particulares es ineludible e inexcusable en el contexto de la Administración Pública.



- De admitir que existe una tolerancia en el uso para finalidades particulares de medios de la Administración, se dejaría sin efecto, no solo los principios del artículo 103 y 132 de la Constitución, sino también toda la normativa reguladora del uso de dichos bienes por la administración que ha sido oportunamente citada en estas alegaciones. E intentar modular dichas obligaciones, a través de protocolos, documentos de seguridad o códigos de conducta internos, por parte de entidades locales, sin capacidad legislativa, implicaría que se están vulnerando los principios más básicos de jerarquía normativa, ya que, en la práctica, un protocolo interno de un Ayuntamiento, que admitiera que se permite el uso del ordenador de trabajo, aunque fuera para muy puntuales y tasadas tareas de tipo personal, sería contrario al propio EBEP y a la normativa disciplinaria, normas con rango de ley y con un rango evidentemente superior a protocolos o documentos internos de un Ayuntamiento. Por tanto, la afirmación de la sentencia de que "no existía información previa ni expectativas del uso de los datos para dichos fines..." pierde su sentido cuando nos encontramos ante una Tesorera municipal, funcionaria de carrera, que sabe perfectamente que el uso de los equipos tecnológicos en horario de su jornada laboral para sus fines propios no está permitido.

- Ni la doctrina del TC ni del TS ha vinculado la enervación de la expectativa de privacidad a una fórmula documental o formal concreta si no que lo ha orientado en un sentido material basado en su contenido (cita STC 170/2013, de 7 de octubre, que fundamenta esta enervación en disposiciones de un convenio colectivo). De acuerdo con la doctrina constitucional, no podía existir una expectativa fundada y razonable de confidencialidad respecto al conocimiento de las comunicaciones mantenidas por el trabajador a través de la cuenta de correo proporcionada por la empresa y que habían quedado registradas en el ordenador de propiedad empresarial. La expresa prohibición convencional del uso extralaboral del correo electrónico y su consiguiente limitación a fines profesionales llevaba implícita la facultad de la empresa de controlar su utilización, al objeto de verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, incluida la adecuación de su prestación a las exigencias de la buena fe [arts. 5 a) y 20.2 y 3 LET].

- Este Ayuntamiento no puede admitir que, desde un enfoque meramente formalista, que además confunde empresa con administración pública, se vincule la expectativa de privacidad, en el presente caso, a la falta de un documento interno. Máxime cuando en sentencias del TC y del TS se han admitido instrumentos tales como convenios colectivos o documentos de seguridad internos y, por tanto, no se establece una exigencia concreta de forma sobre el documento que debe contribuir a la enervación de la expectativa de privacidad. Es más, aplicando precisamente dicha jurisprudencia, cabe limitar o anular la expectativa de privacidad por otras vías tales como la vía convencional (convenio colectivo), por lo que *a fortiori*, dicha limitación puede provenir y proviene de normas con rango de ley, que deben considerarse una modulación necesaria en la traslación de la jurisprudencia constitucional de los derechos fundamentales del ámbito privado, al ámbito de la relación entre funcionario y Administración pública, precisamente por los principios y normas que rigen el Derecho Administrativo.

- Las actuaciones del Ayuntamiento han seguido el protocolo y han sido adecuadas, valorándose el juicio de necesidad, idoneidad y proporcionalidad.

- El escáner es, al igual que la impresora y cualquier otro bien o recurso público puesto a disposición de los funcionarios para la ejecución de sus funciones laborales, un medio para la ejecución de dichas funciones. No es necesario que sea un medio específico para el control laboral, ya que el hallazgo casual puede producirse en cualquier dependencia de la entidad pública. No se entiende la afirmación de que "en él (escáner) no se ejecuta la relación mediante dicho medio", ya que es un medio puesto a disposición del funcionario para la ejecución de sus funciones.

- Sobre la proporcionalidad y adecuación de la intervención, el Ayuntamiento no puede prever el rango de categorías de datos y su afectación a la intimidad que puedan existir indebidamente dentro de dispositivos, tanto escáneres e impresoras de uso compartido como ordenadores de trabajo, que puedan existir al llevar a cabo una primera e inicial búsqueda de información. Tampoco puede este Ayuntamiento ver limitada su actuación, que es reconocida por ley, por razón del nombre de las carpetas o archivos que puedan existir en un dispositivo que, recordamos, es de titularidad pública y sometido a concretas disposiciones legales sobre su uso y destino. Permitir que pueda limitarse una previa tarea indagatoria, basándose en nombres de carpetas o tipos de archivos, sería equivalente a permitir que dentro de bienes, insistimos, de titularidad pública y destinados por ley a finalidades públicas, se crearan parcelas o espacios particulares o privados a voluntad exclusiva del presunto infractor, desnaturizando como es evidente tanto el destino como la naturaleza del bien y limitando la eventual actividad instructora de un procedimiento disciplinario. Todo ello, sin perjuicio de que posteriormente el órgano decisor o los organismos jurisdiccionales, puedan delimitar el alcance de la prueba pertinente o incluso instar su nulidad si así lo consideran oportuno.

- Juicio de necesidad: En el presente caso, ante el hallazgo casual de determinada documentación y otros hechos tales como el incumplimiento reiterado de la jornada laboral y la presentación de un certificado de



asistencia falso, adjunto a un email no remitido por el supuesto remitente, fue necesario acceder al ordenador de la denunciante, precisamente por ser el medio idóneo dentro del Ayuntamiento para que la reclamante pudiera ejecutar las acciones irregulares sobre las que se debía investigar.

- También en relación con las exigencia de idoneidad y proporcionalidad, la providencia de Alcaldía de fecha 26 de febrero de 2018 dispone que el Departamento de Informática accediera al ordenador de la denunciante "... advirtiendo que esta medida se realice desde el cumplimiento de la normativa de protección de datos de carácter personal y con máxima confidencialidad destinando la información que se pudiera obtener a los solos efectos de los expedientes que, a la vista de los documentos obrantes, pudieran iniciarse".

En conclusión, este Ayuntamiento afirma que no se ha infringido el artículo 6.1 de la LOPD, y, en consecuencia, no existe tal infracción, tipificada como grave, del artículo 44.3.b) del mismo texto legal.

**B/** Respecto a la vulneración que se le reprocha del artículo 9.1 de la LOPD (*<<Artículo 9. Seguridad de los datos. 1. El responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.>>*), la argumentación del Ayuntamiento recurrente, expuesta aquí en forma resumida, es la que sigue:

- No puede ser de aplicación con consecuencias sancionadoras el régimen de obligaciones de la legislación anterior al RGPD y la nueva LOPDGDD. Se invoca el principio de retroactividad de las disposiciones sancionadoras que favorecen al infractor o presunto infractor.

- La anterior LOPD de 1999 y especialmente su desarrollo a través del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (RLOPD), establecía una serie de obligaciones relativas a las medidas de seguridad, de nivel básico, medio o alto, en función del tipo tratamientos y ficheros. Y el incumplimiento de tales obligaciones implicaba la imposición de sanciones conforme la anterior legislación por razón de la tipificación del artículo 44.3.h) del RLOPD (*<<3. Son infracciones graves (...) h) Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen>>*). En cambio, dicha conducta no se encuentra actualmente tipificada del mismo modo como sanción en la LOPDGDD. Si comparamos la redacción del artículo 44.3 h) de la anterior LOPD con la actual redacción de la LOPDGDD y su tipificación relativa a la infracción de medidas de seguridad, resulta más favorable el actual régimen, al no estar vinculado a la adopción de una lista concreta de medidas, sino que tal como dispone el artículo 73: "f) La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento, en los términos exigidos por el artículo 32.1 del Reglamento (UE) 2016/679 ", sin establecer unas obligaciones concretas en el sentido del ya derogado RLOPD.

En consecuencia, es de aplicación el principio recogido en el artículo 26.2 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, que a efectos sancionadores, dispone: *"Las disposiciones sancionadoras producirán efecto retroactivo en cuanto favorezcan al presunto infractor o al infractor, tanto en lo referido a la tipificación de la infracción como a la sanción y a sus plazos de prescripción, incluso respecto de las sanciones pendientes de cumplimiento al entrar en vigor la nueva disposición"*.

- En relación con lo anterior, no cabe considerar que las omisiones o defectos que puedan apreciarse en la actuación del Ayuntamiento sean constitutivas de la infracción administrativa tipificada del artículo 44.3.h) de la anterior LOPD, puesto en relación con los artículos 92, 97.1 y. 2 y 101, por ser más beneficioso el régimen sancionador establecido en la nueva LOPDGDD que en su regulación -artículo 73.f puesto en relación con el artículo 32.1 del RGPD- no vincula el cumplimiento de las obligaciones de seguridad del responsable del tratamiento a unas medidas concretas, sino que se orienta a través de un enfoque al riesgo. Así, a lo largo del procedimiento administrativo no se llevó a cabo actividad probatoria pertinente para evaluar las medidas de seguridad del Ayuntamiento, de conformidad con las previsiones del artículo 32 del RGPD y la posible omisión de los requisitos exigidos en el anterior RLOPD. En consecuencia, no puede afirmarse que el Ayuntamiento no cumpla con los principios del artículo 32 del RGPD al no existir una lista tasada u obligatoria de normas de seguridad que deba adoptar por razón de dicho artículo.

Por consiguiente, no cabe imponer sanción alguna al Ayuntamiento por razón del artículo 44.3.h/ de la anterior LOPD, ni entenderse cometida la infracción a la que se refiere del artículo 9.1 LOPD.



Termina el escrito del Ayuntamiento recurrente solicitando que se dicte Sentencia, revocando la sentencia recurrida, anulando y dejando sin efecto la resolución nº 560/2020, de 27 de noviembre de 2020, de la directora de la Agencia Española de Protección de Datos; con imposición de costas procesales a la contraparte.

**SEXTO.-** La representación procesal de la Administración del Estado formalizó su oposición mediante escrito presentado el 27 de abril de 2023 en el que, en primer lugar, hace una razonada exposición del significado y alcance de la doctrina contenida en la sentencia *Barbulescu II* y la "expectativa de privacidad" - sentencia de la Gran Sala del TEDH de 5 de septiembre de 2017, caso *Barbulescu contra Rumanía*, demanda nº 61496/08-, reseñando asimismo la doctrina contenida en pronunciamientos de distintos tribunales, en particular, sentencia de la Sala 4<sup>a</sup> de este Tribunal Supremo de 8 de febrero de 2018 (recurso unificación de doctrina 1121/2015); sentencia del Tribunal Constitucional 170/2013, de 7 de octubre de 2013; y sentencia de esta Sala 3<sup>a</sup> del Tribunal Supremo de 26 de abril de 2021 (recurso de casación 4645/2019).

A partir de ahí, la Abogacía del Estado expone sus argumentos en contra de lo razonado por la parte recurrente.

**A/** En lo que se refiere a la exigencia de consentimiento ( artículo 6.1 LOPD) y a los supuestos en que no es necesario, el planteamiento de la parte recurrida puede sintetizarse del modo que sigue:

- La parte recurrente discrepa de la interpretación la AEPD y la Audiencia Nacional porque se fundamenta en la asimilación entre Administración pública y empresa privada, alegando que la sentencia *Barbulescu* se refiere a un conflicto laboral en el seno de una empresa privada. Sin embargo, no cabe esa interpretación restrictiva propuesta por la recurrente porque la sentencia *Barbulescu* examina la cuestión desde la perspectiva del derecho fundamental a la protección de datos personales y ese derecho fundamental también corresponde a los funcionarios, aunque pueda presentar matices propios.

A esos efectos, el Estatuto Básico del Empleado Público (EBEP) ya reconocía a los mismos, en su redacción inicial, el derecho al respeto a su intimidad, a la propia imagen y a la dignidad en el trabajo ( artículo 14.h) EBEP), precisando ahora el apartado j) del artículo 14 EBEP, redactado por la Ley Orgánica 3/2018, que ese derecho a la intimidad se proyecta también sobre el uso de los medios digitales puestos a su disposición. A lo que cabe añadir que la ya citada STS, Sala 3<sup>a</sup>, de 26 de abril de 2021 (casación 4645/2019), aplica a los funcionarios los parámetros establecidos en sentencias referidas a la relación laboral en empresas privadas. Por lo demás, esa equiparación es reconocida expresamente por el artículo 87.1 de la Ley Orgánica 3/2018 ("1. Los trabajadores y los empleados públicos tendrán derecho a la protección de su intimidad en el uso de los dispositivos digitales puestos a su disposición por su empleador"); y si bien es cierto que los hechos que aquí se enjuician acaecieron a principios de 2018, antes de la entrada en vigor del artículo 87.1 de la Ley Orgánica 3/2018, ello no impide admitir que el precepto tiene un elevado valor interpretativo, pues expresa la voluntad del legislador en cuanto al alcance que debe darse a la protección de un derecho fundamental.

- La parte recurrente niega que la expectativa de privacidad puede invocarse en este caso en consideración a la propia naturaleza de los bienes, ordenador y escáner del Ayuntamiento, que quedan sometidos al régimen derivado del artículo 132 de la Constitución y a la legislación de patrimonio de las Administraciones públicas, lo que excluye cualquier margen de tolerancia para su uso privado o personal, sin que el Ayuntamiento disponga de la posibilidad que tiene el empresario para la autoorganización y fijación de las condiciones de uso de los medios informáticos. Frente a ello, cabe decir que una cosa es el régimen de uso de los bienes públicos derivado de las normas que regulan el patrimonio de las Administraciones Públicas y otra distinta el uso de los medios informáticos que atañe al presente recurso.

- Por otra parte, aunque la relación estatutaria sitúa al funcionario en una posición de sujeción especial, definida por el ordenamiento jurídico, ello no constituye un obstáculo para que se otorgue, o se admita de hecho, un margen de tolerancia en la utilización de los medios informáticos, ni impide que se dicten instrucciones dirigidas a los empleados públicos en las que se concrete en qué consiste el uso adecuado de los medios informáticos, así como el alcance del control que puede efectuarse sobre ellos (una previsión en ese sentido se incorpora a los apartados 2 y siguientes del artículo 87 LO 3/2018).

- Además, aunque admitiéramos que respecto de los bienes puestos a disposición del funcionario queda totalmente excluido el uso privado en virtud del régimen estatutario, de manera que las instrucciones de uso devienen innecesarias, todavía quedaría por resolver la cuestión relativa al alcance del control que puede efectuarse, algo sobre lo que la Administración pública sí que podría informar o dictar instrucciones dirigidas a los funcionarios. Y siendo así, la interpretación propugnada por la recurrente resulta insuficiente para desvirtuar los razonamientos de la Sala de instancia porque ambas facetas -la de la prohibición de uso y la del derecho a la información-, afectan a la "expectativa razonable de privacidad", como hemos visto al exponer la doctrina de los tribunales.



- Lo que está en juego no es, o no solamente, la utilización adecuada de los medios informáticos, sino la posibilidad de ejercer un control de dichos medios y su compatibilidad con los derechos del funcionario.

En fin, puede aceptarse que en la relación estatutaria la "expectativa razonable de privacidad" se reduce efectivamente por la prohibición de uso privado de los medios informáticos puestos a disposición del funcionario; pero ese es solamente uno de los aspectos que delimitan ese concepto jurídico indeterminado. En concreto, como se desprende de todas las sentencias que se han citado, esa faceta del concepto debe completarse con el derecho a la información, concretados en el apartado 121 de la Sentencia *Barbulescu* (aplicados al caso en el fundamento III de la resolución de la AEPD).

Por eso, y también porque las normas jurídicas no son tan rígidas que impidan con carácter absoluto el uso puntual de los medios informáticos para fines personales, la existencia de protocolos, avisos u otros instrumentos similares no infringe necesariamente el principio de jerarquía normativa y completa el régimen de garantías.

- Es cierto que ni el Tribunal Constitucional ni el Tribunal Supremo vinculan la enervación de la expectativa de privacidad a una fórmula documental concreta; y si atendemos al primer factor que integra ese concepto, es relevante y suficiente que exista una prohibición del uso privado de los medios puestos a disposición de los trabajadores o de los empleados públicos. Sin embargo, ese factor no agota el alcance del concepto, y, aunque no se exija una fórmula documental concreta, deben cumplirse los requisitos o principios enunciados por la jurisprudencia en orden a informar de manera suficiente sobre el uso de los medios informáticos y el alcance del control o monitorización.

En este punto, la cita de la STC 170/2013 incorporada al escrito de interposición no es decisiva ya que, como hemos visto, el propio TC invoca, junto a la prohibición de uso privado, el principio de proporcionalidad y el TEDH, con posterioridad a la sentencia del TC, desgrana una serie de criterios o principios que sirven de pauta para enjuiciar la documentación elaborada por el empresario o por la Administración pública.

- El enfoque adoptado por la AEPD y por la Sala de la Audiencia Nacional no puede tacharse de formalista, pues atiende y examina, a la luz del principio de proporcionalidad, las circunstancias "materiales" que concurren en el caso. No se está exigiendo, ni imponiendo, un contenido concreto al documento que plasma la política de uso de los medios informáticos de la Corporación, incluso hablamos de documento por llamarlo de alguna forma, pues podría limitarse, por ejemplo, a un mensaje descriptivo que se genera cuando se abre el ordenador, habitualmente utilizado tanto en la empresa como en las Administraciones públicas.

- En cuanto a la suficiencia de los indicios para realizar las actuaciones previas a la solicitud de incoación del expediente disciplinario, la cuestión alude a la necesidad de que el empresario, o en este caso el Ayuntamiento, proporcione razones legítimas para justificar la monitorización (control) de los medios informáticos y el acceso a su contenido real. El Ayuntamiento justifica la intervención sobre la base de la existencia de un "hallazgo casual" relevante, similar al contemplado en la STS 594/2018; no obstante, en el presente caso, la doctrina del hallazgo casual no puede beneficiar a la parte recurrente porque lo impide la oscuridad que, en el plano de los hechos, rodea al descubrimiento de los documentos que motivan la actividad investigadora; lo que permite a la Sala de instancia afirmar (F.J. 4 de la sentencia) que el hallazgo difícilmente puede calificarse como casual "cuando no se trata de documentos que aparecieron o fueron dejados en el escáner o la impresora, ni a los que cualquiera pudiera acceder", ni se indica cuáles "son esos documentos que motivaron acordar el acceso al ordenador de la reclamante, ni consta diligencia que documente el hallazgo, ni su fecha, habiéndose constatado que entre los documentos almacenados en carpetas en el escáner figuraban diversos de la Franquicia Now You S.L y relacionados con las nóminas de sus empleados, así como un documento relacionado con la salud de la reclamante, otro sobre resolución de expediente de determinación de la contingencia causante de un proceso de IT en el que figura un informe de Evi contenido la patología diagnosticada, es decir, de datos de salud, que son especialmente protegidos".

- Por último, el escrito de interposición defiende la proporcionalidad del acceso al ordenador, poniendo de manifiesto que el Ayuntamiento no puede discriminar *a priori* las categorías de documentos que puedan existir en el dispositivo en el momento de llevar a cabo una primera búsqueda de información.

Podemos admitir que sea difícil discriminar entre los documentos incorporados al ordenador del funcionario público, pero esa circunstancia no elimina el deber de intentarlo en la medida de lo posible, así como de eliminar, una vez comprobado su contenido, aquellos documentos de índole estrictamente privada que de nada sirven a la investigación (no lo decimos nosotros sino que es un factor más mencionado por el TEDH en el apartado 121 de la sentencia *Barbulescu*). Pues bien, la actuación del Ayuntamiento no supera ese mínimo exigible, y así lo aprecia la Sala de instancia.



- A modo de conclusión: el acceso al ordenador de un empleado público puede obedecer a la necesidad de comprobar el cumplimiento de sus funciones en el seno de la relación estatutaria pero debe cumplirse con el derecho a la información, en los términos fijados por la jurisprudencia, y superar el juicio de proporcionalidad (idoneidad, necesidad y proporcionalidad en sentido estricto).

#### B/ Sobre la infracción del artículo 9 LOPD.

El artículo 9 LOPD regula las medidas de seguridad que se deben cumplir en el tratamiento de datos de carácter personal. La resolución de la AEPD, confirmada por la Sala de instancia, impuso a la recurrente una sanción por infracción de ese artículo 9 LOPD, tipificada como grave en el artículo 44.3.h) LOPD. El escrito de interposición denuncia la infracción del artículo 9.1 LOPD sobre la base de que se le deba aplicar la Ley Orgánica, por tratarse de norma más favorable.

El auto de admisión del recurso de casación se limita a declarar que presenta interés casacional objetivo la posible infracción del art. 6.1 LOPD cuando ha de aplicarse en el ámbito de la función pública, sin mencionar la infracción del artículo 9.1 LOPD.

Además, es claro que ambas infracciones son independientes, de manera que es posible sancionar por el artículo 6.1 LOPD y no por el artículo 9.1 LOPD, y viceversa. Siendo así, resulta que no es necesario pronunciarse sobre el artículo 9.1 LOPD para fijar doctrina sobre la cuestión de interés casacional admitida.

Tampoco el escrito de interposición incluye un razonamiento tendente a motivar que la cuestión del artículo 9.1 LOPD presenta, pese a todo, interés casacional objetivo.

Todas esas circunstancias determinan, a nuestro juicio, que deba inadmitirse la cuestión relativa a la posible infracción del artículo 9.1 LOPD. Esta petición es conforme con lo previsto en el apartado V del Acuerdo no jurisdiccional del Pleno de la Sala 3<sup>a</sup> del TS de 3-11-2021, en cuya virtud:

*"La sentencia de casación debe limitar su examen a las infracciones jurídicas planteadas en el escrito de interposición sobre las que previamente se ha apreciado el interés casacional en el auto de admisión, pero puede extenderse a otras infracciones jurídicas asimismo planteadas en el escrito de interposición (y antes anunciadas en el de preparación) siempre y cuando guarden relación de conexidad lógico-jurídica con las identificadas en el auto de admisión como dotadas de interés casacional."*

Subsidiariamente, para el caso de que la Sala decida pronunciarse sobre la cuestión, el escrito de oposición se remite a los fundamentos de la sentencia de instancia.

En relación con la cuestión planteada en el auto de admisión la Abogacía del Estado propugna la siguiente doctrina:

En aplicación del artículo 6.1 de la Ley Orgánica de Protección de Datos 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal -actual artículo 6 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales- se puede considerar fundado el tratamiento de datos personales en cumplimiento de obligación legal, interés público o ejercicio de poderes públicos en el ámbito del empleo público y de las garantías del procedimiento sancionador en el régimen sancionador, siempre que se observen los factores establecidos en la STEDH *Barbulescu 2*, de 5 de septiembre de 2017 y la medida adoptada supere el juicio de proporcionalidad.

Termina el escrito solicitando que se dicte sentencia que fije doctrina en los términos interesados y desestime el recurso de casación, confirmando la sentencia recurrida.

**SÉPTIMO.-** Mediante providencia de 7 de junio de 2024 se acordó no haber lugar a la celebración de vista y quedaron las actuaciones pendientes de señalamiento para votación y fallo; fijándose finalmente al efecto el día 1 de octubre de 2024, fecha en que tuvo lugar la deliberación y votación.

## FUNDAMENTOS DE DERECHO

**PRIMERO.-** Objeto del recurso de casación.

El presente recurso de casación nº 6949/2022 lo interpone la representación del Ayuntamiento de Algemesí contra la sentencia de la Sección 1<sup>a</sup> de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional de 10 de junio de 2022, dictada en el recurso nº 1684/2020, en la que se desestima el recurso contencioso-administrativo interpuesto por el citado Ayuntamiento contra la resolución de la Directora de la Agencia Española de Protección de Datos de fecha 27 de noviembre de 2020 (PS/00062/2019); con imposición de costas a la parte demandante.



En el antecedente segundo hemos dejado reseñados los hechos que la Agencia Española de Protección de Datos declara probados la resolución, así como las razones que se exponen en la sentencia recurrida -en lo que interesa al presente recurso de casación- para fundamentar la desestimación del recurso contencioso-administrativo.

Procede entonces que entremos a examinar las cuestiones suscitadas en casación, en particular la señalada en el auto de la Sección Primera de esta Sala de 19 de enero de 2023. Y, como hemos visto en el antecedente cuarto, en ese auto de admisión del recurso se declara que la cuestión que presenta interés casacional objetivo para la formación de la jurisprudencia consisten en determinar si, en aplicación del artículo 6.1 de la Ley Orgánica de Protección de Datos 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal -actual artículo 6 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales- se vulnera la normativa de protección de datos por el hecho de que el sujeto infractor sea una Administración Pública o, por el contrario, se puede considerar fundado el tratamiento de datos personales en cumplimiento de obligación legal, interés público o ejercicio de poderes públicos, y si resulta razonable la proyección de la doctrina contenida en la STEDH *Barbulescu* 2, de 5 de septiembre de 2017, al ámbito del empleo público y las garantías del procedimiento sancionador en el régimen disciplinario de los empleados públicos.

#### **SEGUNDO.- Ámbito de enjuiciamiento en casación.**

Tiene razón el Abogado del Estado cuando en su escrito de oposición al recurso viene a señalar (véase antecedente cuarto, apartado B/) que el auto de admisión del recurso de casación se limita a declarar que presenta interés casacional objetivo la posible infracción del artículo 6.1 LOPD cuando ha de aplicarse en el ámbito de la función pública, sin mencionar el auto la infracción del artículo 9.1 LOPD.

En efecto, el auto de admisión del recurso fundamenta la apreciación de interés casacional en la constatación de que << (...) no existen pronunciamientos de esta Sala Tercera sobre si se vulnera la normativa de protección de datos por el hecho de que el sujeto infractor sea una Administración Pública, y si resulta razonable la proyección de la doctrina contenida en la STEDH *Barbulescu* 2, de 5 de septiembre de 2017, al ámbito del empleo público y las garantías del procedimiento sancionador en el régimen disciplinario de los empleados públicos>> (F.J. 3 del auto). En cambio, nada dice el auto respecto de las cuestiones relacionadas con la infracción del artículo 9.1 LOPD.

Siendo ello así, es notorio que se trata de infracciones que son enteramente independientes, de manera que para fijar doctrina sobre la cuestión de interés casacional admitida (infracción del artículo 6.1 LOPD) es del todo innecesario abordar cuestiones referidas a la infracción del artículo 9.1 LOPD.

En fin, constatamos que, como también señala la Abogacía del Estado, el escrito de interposición no incluye ningún alegato tendente a motivar que las cuestiones que se pretenden suscitar con relación al artículo 9.1 LOPD presentan interés casacional, ni ofrece ninguna razón para justificar que entremos a examinarlas.

Por todo ello, consideramos que no procede que entremos a pronunciarnos sobre una cuestión que no guarda relación con aquella otra que determinó la admisión del recurso de casación.

**TERCERO.- Doctrina del Tribunal Europeo de Derecho Humanos y del Tribunal Constitucional sobre protección de datos de carácter personal en el ámbito de las relaciones laborales y los límites a la capacidad de control del empresario sobre las comunicaciones del trabajador ( STEDH de 5 de septiembre de 2017, *Barbulescu* 2).**

De la fundamentación jurídica de la citada STEDH de 5 de septiembre de 2017, ( *Barbulescu* 2) interesa reproducir aquí los siguientes apartados:

<< [...] 119. A la luz de las consideraciones anteriores, el Tribunal considera que debe concederse a los Estados contratantes un amplio margen de apreciación al evaluar la necesidad de establecer un marco jurídico que regule las condiciones en que un empresario puede regular las comunicaciones electrónicas o de otro tipo de carácter no profesional de sus empleados en el lugar de trabajo.

120. No obstante, la discreción de que gozan los Estados en este ámbito no puede ser ilimitada. Las autoridades nacionales deben velar por que la introducción por un empresario de medidas para supervisar la correspondencia y otras comunicaciones, independientemente del alcance y la duración de esas medidas, vaya acompañada de garantías adecuadas y suficientes contra los abusos (véase, mutatis mutandis, *Klass* y otros contra Alemania, 6 de septiembre de 1978, párrafo 50, Serie A nº 28, y *Roman Zakharov*, antes citado, párrs. 232-34).

121. El Tribunal es consciente de la rápida evolución en este ámbito. No obstante, considera que la proporcionalidad y las garantías procesales contra la arbitrariedad son esenciales. En este contexto, las autoridades nacionales deben considerar relevantes los siguientes factores:



- (i) Si se ha notificado al empleado la posibilidad de que el empresario adopte medidas para supervisar la correspondencia y otras comunicaciones, y la implementación de esas medidas. Si bien en la práctica los empleados pueden ser notificados de diversas maneras en función de las circunstancias fácticas particulares de cada caso, el Tribunal considera que para que las medidas se consideren compatibles con los requisitos del artículo 8 del Convenio, la notificación debería normalmente ser clara sobre la naturaleza de la supervisión y darse con antelación;
- (ii) El alcance de la supervisión por parte del empresario y el grado de intrusión en la intimidad del empleado. A este respecto, debe distinguirse entre la monitorización del flujo de comunicaciones y de su contenido. También debe tenerse en cuenta si se han monitorizado todas las comunicaciones o sólo parte de ellas, así como la cuestión de si la monitorización fue limitada en el tiempo y el número de personas que tuvieron acceso a los resultados (véase Köpke, citado anteriormente). Lo mismo se aplica a los límites espaciales de la monitorización;
- (iii) Si el empresario ha proporcionado razones legítimas para justificar la monitorización de las comunicaciones y el acceso a su contenido real (véanse los párrafos 38, 43 y 45 supra para una visión general del derecho internacional y europeo en este ámbito). Dado que la monitorización del contenido de las comunicaciones es, por naturaleza, un método claramente más invasivo, requiere una justificación más ponderada;
- (iv) Si hubiera sido posible establecer un sistema de supervisión basado en métodos y medidas menos intrusivos, que el acceso directo al contenido de las comunicaciones del empleado. A este respecto, debería evaluarse, a la luz de las circunstancias particulares de cada caso, si el objetivo perseguido por el empresario podría haberse logrado sin haber accedido directamente al contenido completo de las comunicaciones del empleado;
- (v) las consecuencias del control para el empleado sometido a él (véase, mutatis mutandis, el criterio similar aplicado en la evaluación de la proporcionalidad de una injerencia en el ejercicio de la libertad de expresión según lo protegido por el artículo 10 del Convenio en el asunto *Axel Springer AG contra Alemania* [GC], nº 39954/08, párrafo 95, 7 de febrero de 2012, con otras referencias); y la utilización por el empresario de los resultados de la operación de monitorización, en particular si los resultados se utilizaron para alcanzar el objetivo declarado de la medida (véase Köpke, citado anteriormente);
- (vi) Si se habían proporcionado al empleado las garantías adecuadas, especialmente cuando las operaciones de supervisión del empresario eran de carácter intrusivo. Esas garantías deben garantizar, en particular, que el empresario no pueda acceder al contenido real de las comunicaciones en cuestión a menos que el empleado haya sido notificado con antelación de esa eventualidad.

En este contexto, cabe reiterar que, para ser fructíferas, las relaciones laborales deben basarse en la confianza mutua (véase Palomo Sánchez y otros, citado anteriormente, párrafo 76).

122. Por último, las autoridades nacionales deben garantizar que un empleado cuyas comunicaciones hayan sido objeto de monitorización, tenga acceso a un recurso ante un órgano judicial competente para determinar, al menos en esencia, si se observaron los criterios antes mencionados y si las medidas impugnadas eran legales (véase *Obst*, citado anteriormente, párrafo 45, y *Köpke*, citado anteriormente) [...]>.

Vistas las condiciones que integran el denominado "test Barbulescu", recogidas en el apartado 121 de la sentencia que acabamos de transcribir, la cuestión que se suscita en el presente recurso de casación consiste en dilucidar si es posible su traslación a una relación estatutaria de la Administración con sus funcionarios; o si las singularidades de esta relación, la específica sujeción que la caracteriza u otras razones derivadas del régimen de funcionamiento de las administraciones públicas hacen inviable la traslación de aquella doctrina.

De ello nos ocuparemos a continuación, tomando también como referencia anteriores pronunciamientos del Tribunal Constitucional (STC 170/2013, de 7 de octubre) y de la Sala Cuarta de este Tribunal Supremo (SsTS, Sala Cuarta, 26 de septiembre de 2007 y 8 de febrero de 2018, recursos unificación de doctrina 966/2006 y 1121/2015).

#### **CUARTO.- Examen de las cuestiones que plantea el auto de admisión del recurso.**

Es momento ya de abordar las cuestiones que plantea el auto de admisión del recurso de casación: si resulta razonable la proyección de la doctrina contenida en la STEDH *Barbulescu* 2, de 5 de septiembre de 2017, al ámbito del empleo público; qué relevancia tiene, a efectos de la aplicación del artículo 6.1 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (actual artículo 6 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales) el hecho de que el sujeto infractor sea una Administración Pública; y, en fin, si se puede considerar fundado el tratamiento



de datos personales del empleado público, sin el consentimiento de este, en cumplimiento de una obligación legal o por razones de interés público o ejercicio de poderes públicos.

Pues bien, desde ahora queda anticipado que el planteamiento del Ayuntamiento recurrente no puede ser acogido y que el recurso de casación habrá de ser desestimado; y ello por razones sustancialmente coincidentes con las expuestas por la Abogacía del Estado en su escrito de oposición, que consideramos acertadas. Veamos.

**A/** En primer lugar, carecen de consistencia las razones que esgrime el Ayuntamiento de Algemesí cuando sostiene que la sentencia recurrida no toma en consideración las excepciones a la exigencia del consentimiento del titular de los datos de carácter personal que se enuncian en el artículo 6.2 LOPD; que la doctrina *Barbulescu* no resulta de aplicación pues la STEDH se refiere a un conflicto laboral entre una empresa y un trabajador mientras que aquí se trata de un supuesto de hecho distinto y de otro tipo de relación, de índole pública; y que, además, no concurren los requisitos para entender vulnerada la esfera de intimidad que alega la empleada reclamante.

En cuanto a las excepciones a la exigencia de consentimiento en el tratamiento de datos de carácter personal, es cierto que el artículo 6.1 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (RGPD), enumera diversos supuestos en los que el tratamiento de datos de carácter personal es lícito aun sin el consentimiento del interesado, como son, en lo que aquí interesa, los que se indican en los apartados c/ y e/ del citado artículo 6.1 (<<...c/ el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento; [...] e/ el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;...>>).

Y en relación con esos supuestos contemplados en el Reglamento (UE), la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales -norma que no es aplicable al caso *ratione temporis*-, establece en su artículo 8 :

<<Artículo 8. Tratamiento de datos por obligación legal, interés público o ejercicio de poderes públicos.

1. El tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una obligación legal exigible al responsable, en los términos previstos en el artículo 6.1.c) del Reglamento (UE) 2016/679, cuando así lo prevea una norma de Derecho de la Unión Europea o una norma con rango de ley, que podrá determinar las condiciones generales del tratamiento y los tipos de datos objeto del mismo así como las cesiones que procedan como consecuencia del cumplimiento de la obligación legal. Dicha norma podrá igualmente imponer condiciones especiales al tratamiento, tales como la adopción de medidas adicionales de seguridad u otras establecidas en el capítulo IV del Reglamento (UE) 2016/679.

2. El tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, en los términos previstos en el artículo 6.1 e) del Reglamento (UE) 2016/679, cuando derive de una competencia atribuida por una norma con rango de ley>>.

Según vimos, la sentencia recurrida deja señalando en su F.J. 4 que << (...) se considera acreditada la infracción por vulneración del principio del consentimiento del artículo 6 LOPD, sin que nos hallemos ante ninguno de los supuestos habilitantes previstos en los incisos c) y e) del RGPD, invocados por la actora, pues no concurren ninguno de los presupuestos establecidos en el artículo 8 de la LOPDGD para entender que se pueda considerar fundado el tratamiento de datos personales en cumplimiento de obligación legal, interés público o ejercicio de poderes públicos>>. Y es que, en efecto, no basta con alegar que nos encontramos en presencia de alguno de los supuestos de excepción de contempla la norma sino que quien lo alega debe justificar su efectiva concurrencia. Pues bien, el Ayuntamiento recurrente no ha acertado a explicar, tampoco ahora en casación, cuál de las excepciones a la exigencia del consentimiento sería aquí de aplicación y por qué razón.

**B/** En cuanto a la aplicación de la doctrina *Barbulescu* al caso que nos ocupa, tiene razón la Abogacía del Estado cuando señala que no cabe hacer de ella la interpretación restrictiva que propugna la parte recurrente porque la STEDH examina la cuestión desde la perspectiva del derecho fundamental a la protección de datos personales y ese derecho fundamental también corresponde a los funcionarios, aunque pueda presentar matices propios. A tal efecto se indica que el Estatuto Básico del Empleado Público (EBEP), en su redacción inicial, ya reconocía a los el derecho al respeto a su intimidad, a la propia imagen y a la dignidad en el trabajo (artículo 14.h/ EBEP), precisando ahora el apartado j/ del artículo 14 EBEP, redactado por la Ley Orgánica 3/2018, que ese derecho a la intimidad se proyecta también sobre el uso de los medios digitales puestos a su disposición. En cuanto a la utilización de sistemas de videovigilancia en el ámbito de la Administración Pública y las limitaciones a que está sujeta tal utilización (derecho a la información, principio de proporcionalidad,...), puede verse la STS,



Sala 3<sup>a</sup>, de 26 de abril de 2021 (casación 4645/2019). En fin, aunque no es aquí de aplicación, por ser norma posterior a las fechas en que ocurrieron los hechos a los que se refiere la presente controversia (principios de 2018), es oportuno señalar que esa equiparación a la que nos estamos refiriendo quedó plasmada con claridad en el artículo 87.1 de la Ley Orgánica 3/2018 ("1. Los trabajadores y los empleados públicos tendrán derecho a la protección de su intimidad en el uso de los dispositivos digitales puestos a su disposición por su empleador").

En definitiva, compartimos el parecer de la Sala de la Audiencia Nacional cuando, después de señalar la especificidad contenida en el artículo 46 LOPD, que supone la no imposición de sanción al Ayuntamiento por las vulneraciones de los artículos 6.1 y 9.1 de la LOPD que se le reprochan, viene a aclarar en su sentencia que << (...) el hecho de que el sujeto infractor sea una Administración Pública no lleva, en lo que aquí atañe, a la desaparición del derecho fundamental del artículo 18 CE o del artículo 8 de la Carta Europea de Derechos Humanos>> (véase F.J. 4 de la sentencia recurrida, que antes hemos reproducido).

**C/** Por otra parte, para negar o cuestionar la expectativa de privacidad del empleado público el Ayuntamiento de Algemesí invoca la naturaleza de los bienes -ordenador y escáner del Ayuntamiento-, alegando que tales elementos materiales están sometidos al régimen derivado del artículo 132 de la Constitución y a la legislación de patrimonio de las Administraciones pública y que ello excluye cualquier margen de tolerancia para su uso privado o personal, sin que el Ayuntamiento disponga de la posibilidad que tiene el empresario para la autoorganización y fijación de las condiciones de uso de los medios informáticos. Sin embargo, tal alegación no puede ser acogida pues una cosa es el régimen de uso de los bienes públicos derivado de las normas que regulan el patrimonio de las Administraciones Públicas y otra distinta es que, so pretexto de controlar o fiscalizar el uso del material informático, el Ayuntamiento pueda incurrir en vulneración de los derechos de sus empleados y su expectativa razonable de privacidad.

**D/** En relación con lo anterior, el hecho de que la relación estatutaria sitúe al funcionario en una posición de sujeción especial, delimitada y regida por su específica regulación, no excluye ni impide que se dicten instrucciones dirigidas a los empleados públicos en las que se concrete en qué consiste el uso adecuado de los medios informáticos, así como el alcance del control que puede efectuarse sobre ellos (véase ahora -aunque no es norma aplicable al caso *ratione temporis*- la previsión contenida en el artículo 87.3 de la Ley Orgánica 3/2018). Es cierto que la enervación de la expectativa de privacidad no está vinculada a una fórmula documental concreta; pero deben cumplirse los requisitos o principios enunciados por la jurisprudencia en orden a informar de manera suficiente sobre el uso de los medios informáticos y el alcance del control o monitorización. Pues bien, la sentencia recurrida pone de manifiesto que << (...) en el caso de autos no se informó a los empleados de la utilización de los equipos informáticos, con la advertencia de la existencia de medidas de control o supervisión del ordenador sobre las comunicaciones de los empleados, que es uno de los factores tomados en consideración por la sentencia *Barbulescu 2*>>. (F.J. 4 de la sentencia). Y más adelante, en el mismo F.J. 4, la sentencia insiste: << (...) para el tratamiento consistente en el acceso al equipo informático asignado a la reclamante puede obedecer a la comprobación del cumplimiento de sus funciones dentro de la relación que mantiene con el Ayuntamiento, y se puede arbitrar este tipo de accesos cuando se haya informado previamente del uso de los datos para dichos fines y en supuestos en que resulten proporcionales dichos accesos. Sin embargo, en el caso de autos no existía información previa sobre dicho uso o fines...>>.

A propósito de este último dato que destaca la sentencia relativo a la falta de advertencia de la existencia de medidas de control o supervisión sobre las comunicaciones, tiene razón la Abogacía del Estado cuando señala que lo que está en juego no es, o no solamente, la utilización adecuada de los medios informáticos, sino la posibilidad de ejercer un control de dichos medios y su compatibilidad con los derechos del funcionario y su expectativa razonable de privacidad, en los términos a los que antes nos hemos referido.

**E/** Por último, el Ayuntamiento recurrente afirma la proporcionalidad del acceso al ordenador alegando que no podía discriminarse *a priori* las categorías de documentos que puedan existir en el dispositivo en el momento de llevar a cabo una primera búsqueda de información. Sin embargo, esta escueta alegación del Ayuntamiento no logra desvirtuar la apreciación de la Sala de la Audiencia Nacional en este punto de la controversia. Como vimos, el mismo F.J. 4 de la sentencia al que nos venimos refiriendo deja señalado que << (...) tampoco existió proporcionalidad de la medida adoptada, pues se accede a todas las carpetas y archivos sin discriminar su contenido, de una forma especialmente invasiva, de tal forma que se han visto afectados documentos privados de la reclamante, documentos de salud, etc. que se han recogido de forma innecesaria y sin relación con lo que se buscaba>>.

**QUINTO.-** Respuesta de la Sala a las cuestiones de interés casacional señaladas en el auto de admisión del recurso de casación.



A fin de dar respuesta a las cuestiones delimitadas en el auto de admisión del recurso, debemos declarar lo que sigue:

1/ Resulta razonable la proyección de la doctrina contenida en la STEDH *Barbulescu 2*, de 5 de septiembre de 2017, al ámbito del empleo público, sin perjuicio de que deban ser tomadas en consideración las especificidades del régimen estatutario.

2/ Cuando se impute a una Administración Pública la infracción del artículo 6.1 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (actual artículo 6 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales), por haber realizado el tratamiento de datos de carácter personal sin el consentimiento del interesado, para apreciar que no ha existido infracción no basta con que la Administración actuante invoque alguno de los supuestos de excepción a la exigencia de consentimiento que contempla el artículo 6.1 del Reglamento (UE) 2016/679, de 27 de abril de 2016, sino que debe justificar la efectiva concurrencia del supuesto de excepción alegado.

**SEXTO.- Resolución del recurso de casación y costas procesales.**

En consonancia con esta doctrina que acabamos de exponer en el apartado anterior, y de acuerdo con las consideraciones que hemos dejado recogidas en el fundamento jurídico cuarto, procede que declaremos no haber lugar al recurso de casación interpuesto en representación del Ayuntamiento de Algemesí contra la sentencia de la Sección 1<sup>a</sup> de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional de 10 de junio de 2022 (recurso contencioso-administrativo nº 1684/2020).

De conformidad con lo dispuesto en los artículos 93.4, 139.1 y 139.4 de la Ley reguladora de esta Jurisdicción, entendemos que no procede la imposición de las costas derivadas del recurso de casación a ninguna de las partes. Y en cuanto a las costas del proceso de instancia, debe mantenerse el pronunciamiento que hizo al respecto la Sala de la Audiencia Nacional.

Vistos los preceptos citados, así como los artículos 86 a 95 de la Ley de esta Jurisdicción,

**FALLO**

Por todo lo expuesto, en nombre del Rey y por la autoridad que le confiere la Constitución, esta Sala ha decidido

1.- No ha lugar al recurso de casación nº 6949/2022 interpuesto en representación del AYUNTAMIENTO DE ALGEMESÍ contra la sentencia de la Sección 1<sup>a</sup> de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional de 10 de junio de 2022 (recurso contencioso-administrativo nº 1684/2020).

2.- No se imponen las costas derivadas del recurso de casación a ninguna de las partes, manteniendo, en cuanto a las costas del proceso de instancia, el pronunciamiento de la sentencia recurrida.

Notifíquese esta resolución a las partes e insértese en la colección legislativa.

Así se acuerda y firma.