CNS 49/2009

Dictamen en relación con la consulta planteada por la instructora de un expediente disciplinario incoado a una funcionaria de un Ayuntamiento relativo al uso privado del correo electrónico del puesto de trabajo

Se presenta ante la Agencia Catalana de Protección de Datos un escrito de consulta emitido por la instructora de un procedimiento disciplinario incoado a una funcionaria de la administración local con habilitación de carácter estatal que ocupa el puesto de trabajo de Secretaría e Intervención en un Ayuntamiento.

La instructora pone de manifiesto que la incoación del expediente disciplinario trae causa de un posible incumplimiento por parte de dicha funcionaria local del deber de reserva profesional en lo que respecta a los asuntos que conoce con motivo de sus funciones, así como también en atención al tratamiento de los datos de carácter personal. La instructora formula una consulta a esta Agencia "ante un posible caso de cesión o comunicación de datos de carácter personal" y solicita a la misma la emisión de un informe "respecto al expediente incoado en su día".

I

(...)

II

En vista de que la consulta tiene por objeto unos hechos que han desembocado en la incoación de un expediente disciplinario, es relevante exponer el relato de los hechos que se desprenden de la documentación aportada.

Mediante escrito de fecha 11 de noviembre de 2009, el alcalde del Ayuntamiento al que pertenece la funcionaria local señala que, en fecha 1 de octubre de 2009, "como consecuencia de un proceso de copia de seguridad en cumplimiento de las normas de seguridad, completamente rutinario como los realizados con anterioridad, se notifica una incidencia que conlleva la activación del protocolo de seguridad y el inicio de obtención de información reservada para establecer la certidumbre y el alcance de los hechos observados en la incidencia antes referenciada".

En fecha 1 de octubre de 2009, el administrador y responsable de seguridad del sistema implantado en el Ayuntamiento comunica la incidencia número 1/2009 al mencionado alcalde, quien ostenta la condición de responsable del fichero. En el apartado "Incidencia" del escrito de notificación, que es de tipo formulario, se indica que en fecha 1 de octubre de 2009 el operador de la aplicación ha constatado, en el momento de realizar las copias de seguridad, que la carpeta de elementos enviados desde Outlook de Secretaría presenta un volumen muy elevado en comparación con la carpeta de entrada, teniendo en cuenta el corto periodo de tiempo (de 9/09/09 a 1/10/09), y que concretamente tiene un volumen superior a los 10 MB; además, en el apartado "Efectos que puede producir" se indica "un peligro para la seguridad de datos de carácter personal".

En el informe emitido en fecha 1 de octubre de 2009 por el operador de la aplicación encargado de administrar y mantener la estructura de los ficheros automatizados de datos de carácter personal de este Ayuntamiento, se afirma lo siguiente:

> "Que en el día de hoy, siendo las dieciocho horas, en aplicación de la normativa de seguridad para ficheros automatizados de datos de carácter personal con nivel de seguridad alto, a petición del responsable de seguridad del Ayuntamiento de xxx, se efectúa un control periódico de verificación del cumplimiento de las normas de seguridad, completamente rutinario como los realizados con anterioridad.
>
> Como es habitual, el control de verificación consiste, en primer lugar, en la revisión del servidor de archivos y de las diez cintas de soporte realizadas por el responsable de las copias de seguridad. En segundo lugar, se procede a la realización de las copias de seguridad de los correos electrónicos genéricos que se encuentran

en funcionamiento en el Ayuntamiento de xxx, de conformidad con las prescripciones de la Agencia Catalana de Protección de Datos.

A raíz de dicho control de verificación de cumplimiento se detecta una incidencia que puede crear un peligro para la seguridad de los ficheros, entendida como confidencialidad, integridad y disponibilidad de los datos."

Como consecuencia de la comunicación de esta incidencia, en la misma fecha el alcalde acuerda la apertura de una información reservada para esclarecer si la funcionaria "ha podido incumplir el deber de reserva profesional en lo que respecta al tratamiento de datos protegidos y a los asuntos que conoce con motivo de las funciones que tiene encomendadas".

Mediante escrito de fecha 16 de octubre de 2009 firmado por la propia funcionaria local —a pesar de que la expresión "recibido en fecha 16-10-2009 a las 12.15 h" induce a pensar que el escrito fue redactado por el propio Ayuntamiento—, la funcionaria manifiesta lo siguiente:

"Yo....., declaro que tengo conocimiento de mi acceso a los ficheros de datos personales:

Nombre de los ficheros
Outlook
Contabilidad
Tributos y Tasas

Por eso he recibido copia de mis funciones y obligaciones respecto a los citados ficheros y declaro haber leído y entendido lo que me obliga, comprometiéndome a respetar, en la medida en la que me corresponde según mi puesto de trabajo, el correcto cumplimiento de esta normativa.

También adquiero el compromiso de utilizar el acceso a la red exterior (Internet) y al correo electrónico, proporcionado por el Ayuntamiento, con motivos estrictamente y exclusivamente profesionales, y de no hacer, en ningún caso, un uso privado o particular de dichos recursos. Asimismo, autorizo de forma expresa e informada al administrador del sistema a que revise e inspeccione los *logs* de mis accesos a Internet, así como las direcciones de los correos recibidos y enviados."

En lo que respecta al contenido de estos ficheros, en el acuerdo de creación de ficheros automatizados que contienen datos de carácter personal del Ayuntamiento se indica lo siguiente:

- El fichero Outlook tiene como finalidad la gestión del correo electrónico del Ayuntamiento, obtiene datos personales del propio personal del Ayuntamiento y de las personas que se dirigen de forma presencial o telemática al Ayuntamiento, y en él se recogen los datos siguientes: nombre, apellidos, dirección del correo electrónico y otros datos exigidos por la legislación vigente. No se prevé hacer cesiones, el órgano responsable del fichero es el alcalde y tiene asignado un nivel básico de medidas de seguridad.

- El fichero Contabilidad tiene como finalidad la gestión contable del presupuesto y el registro de facturas, obtiene datos personales de los proveedores, de las personas que son deudoras del Ayuntamiento y del personal del Ayuntamiento, y en él se recogen los datos siguientes: "DNI/NIF/pasaporte, nombre, apellidos, dirección, datos bancarios, teléfono y otros datos exigidos por la legislación vigente". No se prevé hacer cesiones, el órgano responsable del fichero es el alcalde y tiene asignado un nivel básico de medidas de seguridad.

- El fichero Tributos y Tasas tiene como finalidad la gestión y control de todos los tributos y tasas del consistorio, obtiene datos personales de las personas que solicitan los servicios recogidos en las ordenanzas municipales del Ayuntamiento y de los contribuyentes, y en él se recogen los datos siguientes: nombre, apellidos, dirección del correo electrónico y otros datos exigidos por la legislación vigente. No se prevé hacer cesiones, el órgano responsable del fichero es el alcalde y tiene asignado un nivel medio de medidas de seguridad.

Como parte de la información reservada constan tres solicitudes de información sobre datos de carácter personal, todas de fecha 20 de octubre de 2009 y con el subtítulo "Ejercicio del derecho de acceso (artículo 15 de la LOPD)", mediante las cuales el representante legal del

Ayuntamiento solicita —entendemos que al encargado del tratamiento, quien parece ser el depositario del contenido de los ficheros— "que se le faciliten sus datos de carácter personal contenidos en el fichero indicado, así como la información relacionada con el tratamiento de los mismos, de conformidad con el derecho de acceso regulado en el artículo 15 de la Ley Orgánica 15/1999". En el apartado "Nombre del fichero o ficheros" se indica, respectivamente: secretaria@xxx.cat, ajuntament@xxx.cat y alcaldia@xxx.cat.

Conviene hacer un pequeño inciso para aclarar que el Ayuntamiento sufre una confusión cuando utiliza los modelos de solicitud previstos para el ejercicio del derecho de acceso regulado en el artículo 15 de la LOPD, para acceder a la parte de la información contenida en el fichero Outlook correspondiente a las direcciones de correo mencionadas. El derecho de acceso previsto en el artículo 15 de la LOPD se reconoce al titular de los datos personales, que en este caso sería la funcionaria local referida, quien puede ejercer dicho derecho ante el responsable del fichero Outlook, es decir, el alcalde del Ayuntamiento en cuestión, y acceder a la información correspondiente a las direcciones secretaria@xxx.cat, ajuntament@xxx.cat y alcaldia@xxx.cat. Otra cosa es el derecho que ostenta el alcalde (como representante legal del Ayuntamiento), o bien la persona a quien éste haya autorizado, a acceder a la información que sea necesaria para cumplir sus funciones, entre otras, velar por la seguridad de los datos recogidos en el ejercicio de sus funciones, cuestión esta que analizaremos en el epígrafe siguiente.

Entre la documentación aportada consta un *report* de los *logs* o registros de las direcciones de correo indicadas, en concreto, de lo siguiente: la fecha de emisión de cada correo enviado desde una de estas direcciones dentro del intervalo comprendido entre el 1 o el 2 de septiembre y el 23 de octubre de 2009, el destinatario del correo y el código de identificación *Queue ID* correspondiente a cada correo enviado.

En fecha 26 de octubre de 2009, el alcalde del Ayuntamiento incoa un expediente disciplinario a la funcionaria local referida mediante el Decreto de Alcaldía n.º 238/2009, cuyo apartado "Antecedentes" hace referencia a un informe emitido en fecha 23 de octubre de 2009 por la empresa *xxx,* encargada de la implantación del sistema de seguridad de los ficheros automatizados de datos de carácter personal en este Ayuntamiento. En ese mismo apartado se señala lo siguiente:

> "De este informe se desprende que xxx ha podido llevar a cabo acciones que son constitutivas de infracción normativa y, por consiguiente, de falta disciplinaria.
>
> 1. El incumplimiento del deber de reserva profesional en lo que respecta a los asuntos que conoce con motivo de las funciones que tiene encomendadas.
> 2. El incumplimiento del deber de reserva profesional en lo que concierne al tratamiento de datos protegidos de carácter personal."

El informe de 23 de octubre de 2009 al que hace referencia el Decreto de Incoación del expediente disciplinario está emitido por el abogado y representante de la empresa antes mencionada, y en dicho informe se indica lo siguiente:

> "Que el pasado 16 de octubre se efectuó una sesión de auditoría de los puntos informáticos del Ayuntamiento de xxx; finalizada la revisión se consideró oportuno instar a la Alcaldía a que, por motivos de seguridad, solicitara un *report* de los correos electrónicos a la entidad que suministra el servicio.
>
> En el día de hoy y examinados los *reports*, se constata que el correo denominado secretaria@xxx.cat consta en ellos desde el 9 de septiembre y hasta el 16 de octubre de 2009, con un total de 675 envíos, la mayor parte de los cuales a dos direcciones (xxx@hotmail.com y xxx@xxx.com) que se pueden considerar no oficiales para trámites del Ayuntamiento de xxx, así como un gran número a "empty", que se podría considerar correo oculto.
>
> Ante estos hechos, concluimos que puede haber una presunta fuga de información reservada y confidencial del Ayuntamiento de xxx y recomendamos a la Alcaldía que adopte medidas cautelares al respecto."

Finalmente, constan dos informes emitidos también por la empresa antes mencionada, uno de fecha 11 de noviembre de 2009, sobre el derecho a la intimidad y el correo electrónico laboral, y otro de fecha incierta, que lleva por título *Informe de actuaciones realizadas en el Ayuntamiento de xxx*. En cuanto a este segundo informe, conviene aclarar que en el apartado "Seguimiento" se indica que "en fecha 11 de noviembre de 2009 se comunicó la

incidencia a la directora del APDCAT para que constara como detectada", y también que "se comunicaron las medidas de carácter legal adoptadas". A pesar de esta afirmación, conviene poner de manifiesto que en el registro de esta Agencia no consta la entrada de este escrito ni de ningún otro donde se haya comunicado dicha incidencia, aparte obviamente del conocimiento que de ella se ha tenido a través de esta consulta.

III

De acuerdo con el escrito de consulta, la instructora del expediente disciplinario considera que los hechos relatados que son objeto del expediente disciplinario pueden considerarse una cesión o comunicación de datos de carácter personal.

En relación a esta cuestión, es necesario manifestar que dicha afirmación presupone, en primer lugar, la existencia de datos *de carácter personal*, es decir, de información referente a personas físicas identificadas o identificables (artículo 3.a de la LOPD); en segundo lugar, presupone la existencia de uno o más *tratamientos* de datos personales, entendiendo como tales el conjunto de 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 (artículo 3.c de la LOPD). El tratamiento al que es refiere la instructora, la cesión de datos, consiste en cualquier revelación de datos efectuada a una persona diferente del interesado (artículo 3.i de la LOPD). Hay que partir de la base que todas estas operaciones —realizadas por los trabajadores al servicio de un Ayuntamiento en el ejercicio de las tareas que tienen asignadas—, así como la gestión de la información personal que resulta de las mismas, deben regirse por lo que dispone la normativa de protección de datos.

De los hechos relatados en el epígrafe anterior se desprende que la funcionaria local referida tiene acceso a tres ficheros que contienen datos de carácter personal; que la propia funcionaria considera que la información que trata en el desarrollo de sus tareas laborales requiere la máxima confidencialidad en lo que respecta a los datos personales tratados; que del 9 de septiembre y hasta el 16 de octubre de 2009 se han enviado 675 correos, con un volumen de información superior a los 10 MB, desde la dirección de correo secretaria@xxx.cat, y que se han enviado esencialmente a dos direcciones: xxx@hotmail.com y xxx@xxx.com, las cuales se pueden considerar direcciones no oficiales para trámites de este Ayuntamiento, así como también a una dirección de correo que la empresa antes mencionada identifica como "empty", y que se podría calificar de correo oculto.

Teniendo en cuenta esta información se puede concluir lo siguiente: aunque no se puede descartar que entre el volumen de información enviada consten datos personales, sobre todo teniendo en cuenta las funciones que realiza dicha funcionaria y el acceso que tiene a los tres ficheros mencionados, esta Agencia no puede concluir, a la vista de la información de la que dispone, que se haya producido una cesión de datos personales, y ello por distintos motivos: en primer lugar, porque esta Agencia no tiene constancia fehaciente de que la funcionaria local haya revelado datos personales a una persona distinta de la persona o personas interesadas, es decir: el personal del propio Ayuntamiento, los proveedores y deudores del Ayuntamiento y los contribuyentes de los tributos y tasas del Ayuntamiento, entre otros. Las declaraciones en que se afirma que los destinatarios de los correos electrónicos enviados por la funcionaria son direcciones "no oficiales", y el hecho de que la carpeta de elementos enviados desde el Outlook de Secretaría tenga un volumen muy elevado en comparación con la carpeta de entrada, teniendo en cuenta el corto período de tiempo (de 9/09/09 a 1/10/09), concretamente un volumen superior a los 10 MB, entre otros, son ambos hechos objetivos que, debidamente acreditados, pueden constituir indicios de la comisión de una cesión de datos, pero dichos indicios son insuficientes en el marco de un procedimiento sancionador o, como es el caso, disciplinario. Sería necesario tener constancia del envío efectivo de datos personales. Y aun cuando se tuviera constancia de ello, sería necesario acreditar la autoría de la cesión, es decir, se deberían aportar los elementos de juicio suficientes que permitieran acreditar —probablemente en este caso podría ser indiciariamente— que la funcionaria imputada es la persona que ha efectuado la cesión. Con todo, debe tenerse en cuenta además que no todas las cesiones de datos son ilegítimas y, por tanto, sancionables, sino únicamente aquellas que contravienen las previsiones de la LOPD, contenidas fundamentalmente en los artículos 11 y 21 de dicha ley.

Aparte del escrito propiamente de consulta, en la Provisión de fecha 30 de noviembre de 2009 la instructora manifiesta la voluntad de solicitar informe a la Agencia "para que se pronuncie sobre si los hechos descritos en el expediente aportado constituyen alguna infracción de las tipificadas en la Ley Orgánica de Protección de Datos de Carácter Personal, Ley 15/1999, de 13 de diciembre".
La respuesta en este caso es la misma. A pesar de que de la información aportada a esta Agencia se desprende la detección de una incidencia en el sistema de seguridad de la información que puede poner en peligro la seguridad de los datos personales, lo cierto es que no se constata ningún tratamiento de datos personales, como podría ser la recogida, grabación, envío, destrucción, etc., de datos personales, sino que únicamente se presume. Por eso, no es posible concluir que se haya cometido una de las infracciones previstas en la LOPD.

Lo mismo se podría afirmar sobre la imputación que se señala en el acuerdo de incoación del expediente disciplinario, realizado mediante un decreto de alcaldía y consistente en "el incumplimiento del deber de reserva profesional en lo que se refiere al tratamiento de datos protegidos de carácter personal". No es posible concluir que se haya vulnerado el deber de reserva profesional o el deber de secreto al que hace referencia el artículo 10 de la LOPD si no se tiene constancia del tratamiento de datos personales, esto es, de los datos que identifican a una persona o que permiten su identificación mediante un esfuerzo razonable.

En relación a la otra imputación que figura en el acuerdo de incoación, consistente en "el incumplimiento del deber de reserva profesional en lo que concierne a los asuntos que conoce con motivo de las funciones que tiene encomendadas", conviene dejar claro que esta Agencia no es competente para emitir una valoración sobre cuestiones jurídicas que ultrapasan la normativa sobre protección de datos, por lo cual no emitiremos ninguna observación. Así pues, las conclusiones expuestas hasta el momento se emiten sin perjuicio de que los hechos puedan constituir una o más infracciones de otra normativa.

Dicho esto, se considera relevante poner de manifiesto que los responsables de los ficheros y los encargados de los tratamientos son las personas que están sujetas al régimen sancionador que establece la LOPD (artículo 43 de la LOPD). Igualmente, los responsables de los ficheros o tratamientos son las personas obligadas a garantizar la seguridad de los datos de carácter personal evitando, entre otros, el tratamiento no autorizado (artículo 9 de la LOPD). Por consiguiente, en caso de cesión ilegítima, sería el responsable del fichero, y no el funcionario autor del tratamiento ilegítimo, quien incurriría en responsabilidad. Otra cosa es que posteriormente el responsable del fichero conviniera incoar un expediente disciplinario al funcionario presuntamente autor del tratamiento ilegítimo con el fin de depurar responsabilidades administrativas, tal como prevé el artículo 46 de la LOPD.

IV

Si bien los términos en los que se ha planteado la consulta no permiten emitir ninguna otra valoración, el contenido de la información aportada ha puesto de manifiesto que el Ayuntamiento referido, directamente o través del encargado del tratamiento, ha ejercido un control sobre el correo electrónico de una empleada municipal, cuestión que reviste relevancia y actualidad desde el punto de vista del derecho a la protección de los datos personales, y más en concreto, en lo que se refiere a los límites y a las condiciones de ejercicio de dicho control. Por ese motivo, a continuación se analizarán los criterios concretos que el Ayuntamiento debe tener en cuenta desde el punto de vista de la normativa de protección de datos a la hora de ejercer un control, en general, de los sistemas de información y, en particular, del correo electrónico de los trabajadores que directa o indirectamente prestan servicios públicos para dicho Ayuntamiento.

Pera que se considere legítimo el tratamiento de datos que pueda derivar del control ejercido por el Ayuntamiento de los sistemas de información, debe tenerse en cuenta en primer lugar cuál es la *finalidad* del control. En este sentido, está claro que el Ayuntamiento debe poder ejercer un control cuando éste tenga como finalidad el mantenimiento de la infraestructura informática y telemática de la que dispone (ordenadores, aplicaciones, software y hardware, etc.) para que sus trabajadores cumplan con las tareas que tienen encomendadas. Las tareas de mantenimiento y revisión, que pueden conllevar, entre otras actuaciones, intervenciones en los directorios de red y en los ordenadores de los usuarios, son necesarias para la detección y eliminación de los elementos que pudieran causar problemas de

funcionamiento en los sistemas de información. En definitiva, son necesarias para asegurar el correcto funcionamiento de los sistemas de información.

Por otra parte, la jurisprudencia constitucional ha manifestado que el poder de dirección del empresario incluye facultades de control de la actividad laboral. En lo que respecta al control del ordenador, conviene destacar la Sentencia de 29 de septiembre de 2007 dictada por el Tribunal Supremo en el recurso de casación para la unificación de doctrina n.º 966/2006, cuya doctrina hacemos extensible al control del correo electrónico**.** En el Fundamento de Derecho Tercero, el Alto Tribunal señala, en relación con un supuesto en el que es aplicable el Estatuto de los Trabajadores (ET), que el ordenador, a diferencia de la taquilla o de los efectos personales del trabajador, no forma parte de la esfera privada del trabajador, sino que es un instrumento de producción, ya que a través del mismo el trabajador ejecuta la prestación del trabajo. El empresario es el titular de dicho ordenador, ya sea como propietario o por otro título. Por ello, no es aplicable el artículo 18 del ET —que establece una serie de garantías con el fin de que el control sea legítimo—-, sino el artículo 20.3 del ET, lo cual significa que el empresario puede controlar el uso que hacen los trabajadores del ordenador para verificar el cumplimiento de la prestación del trabajo. En palabras del Alto Tribunal: "el empresario ha de comprobar si su uso se ajusta a las finalidades que lo justifican, ya que en otro caso estaría retribuyendo como tiempo de trabajo el dedicado a actividades extralaborales".

En este sentido, se puede afirmar que el Ayuntamiento, en su condición de "empresario", también puede ejercer un control cuando éste tenga como finalidad verificar el cumplimiento por parte de los trabajadores de sus obligaciones laborales. Así pues, por ejemplo, si tenemos en cuenta que el artículo 54 de la Ley 7/2007, de 12 de abril, del Estatuto Básico del Empleado Público (EBEP), que establece como principio de conducta de los empleados públicos, entre otros, el deber de no utilizar los recursos y bienes públicos en provecho propio, el Ayuntamiento podría realizar actuaciones de control del ordenador de sus trabajadores con el fin de verificar el cumplimiento de este deber.

Por otra parte, la STS mencionada también considera legítimo el control de los ordenadores de trabajo por parte del empresario cuando dicho control tenga como finalidad coordinar y garantizar la continuidad de la actividad laboral en los supuestos de ausencia de los trabajadores, y también (aunque ésta podría incluirse en alguna de las que ya hemos mencionado), cuando tenga como finalidad prevenir las responsabilidades que puede tener la empresa como consecuencia de alguna forma ilícita de uso del ordenador frente a terceros.

Ahora bien, hay que tener en cuenta que este derecho que habilita al empresario a realizar un control de las herramientas de trabajo no es absoluto sino que está limitado por otros derechos fundamentales, especialmente, por el derecho a la intimidad personal y familiar, el derecho al honor y el derecho a la propia imagen (artículo 18.1 de la Constitución), así como por el derecho a la protección de datos personales (artículo 18.4 de la Constitución) y por el derecho al secreto de las comunicaciones (artículo 18.3 de la Constitución).

Para que dicho control no suponga una intromisión ilegítima en el derecho a la intimidad, en el derecho a la protección de datos personales, o en otro de los derechos mencionados anteriormente, deberá someterse al denominado *juicio de proporcionalidad*, que el Tribunal Constitucional ha delimitado como el examen de la medida limitadora de derechos respecto al objetivo perseguido (juicio de idoneidad). Tendrá que valorarse, además si la medida es necesaria, en el sentido en el que no existe otra medida más moderada para la consecución del propósito buscado con igual eficacia (juicio de necesidad) y, finalmente, si la medida es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto). En lo que se refiere específicamente al derecho a la protección de datos personales, debe tenerse en cuenta el *principio de calidad*, según el cual los datos sólo se podrán recoger y tratar 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 (artículo 4 de la LOPD).

En relación con el respeto a los derechos fundamentales mencionados, conviene subrayar que en la STS mencionada el Alto Tribunal supedita o condiciona la legitimidad del control del ordenador de los trabajadores al cumplimiento por parte del empresario del deber de informar a sus trabajadores sobre cuáles son las medidas de control de los sistemas de información. El Tribunal parte de la presuposición que existe un hábito generalizado de

tolerancia a ciertos usos personales de los medios informáticos de la empresa y considera que ello crea una expectativa de confidencialidad del uso que se haga de dichos medios. Por ese motivo, continúa, si el empresario quiere ejercer un control de los medios informáticos deberá informar previamente a los trabajadores sobre el contenido y el alcance de dicho control (Fundamento Jurídico Tercero).

En relación con el caso concreto, conviene señalar que el informe emitido por la empresa mencionada, que lleva por título *Informe de actuaciones realizadas en el Ayuntamiento de xxx, afirma* en su apartado "Conclusiones" que el Ayuntamiento ha advertido a los usuarios de los ficheros desde el año 2004 acerca de cuáles son sus obligaciones y responsabilidades. Sobre esta afirmación, conviene subrayar que, partiendo de la documentación que se ha aportado a esta Agencia, no se puede constatar que el Ayuntamiento haya informado sobre estos extremos a sus trabajadores. En cualquier caso, conviene advertir que, entre la información que se proporcione, deberá explicarse claramente cuáles serán las medidas de control de las herramientas de trabajo, entre ellas el correo electrónico. Además, dicha información deberá proporcionarse antes de ejercer el control. Hacemos esta observación para aclarar que el curso sobre las funciones y obligaciones del personal del Ayuntamiento que, según consta en este mismo informe, al parecer realizó la empresa mencionada a los trabajadores del Ayuntamiento, es posterior a los hechos que han sido objeto del expediente disciplinario.

En relación con el deber de información, es necesario hacer una segunda observación. En el informe emitido en fecha 1 de octubre de 2009 por el operador de la aplicación encargado de administrar y mantener la estructura de los ficheros automatizados de datos de carácter personal del Ayuntamiento, se explicitan las actuaciones que llevó a cabo el técnico que detectó la incidencia, y es de destacar que se refiera a las medidas de seguridad que aplican a los ficheros que tienen asignado un nivel *alto* de medidas de seguridad, entre las cuales figura la realización de "copias de seguridad de los correos electrónicos genéricos que se encuentran en funcionamiento en el Ayuntamiento de xxx". Hacemos esta observación porque los ficheros a los que tiene acceso la funcionaria local referida tienen asignado un nivel de medidas de seguridad básico (*Outlook*) y medio (*Contabilidad y Tributos y Tasas*). De acuerdo con lo que prevé el artículo 81.7 del LROPD, es posible aplicar medidas de seguridad de nivel alto a ficheros que tienen asignado un nivel básico o medio. Ahora bien, en caso de hacerlo, el Ayuntamiento deberá informar previamente a sus trabajadores de la aplicación de las medidas de seguridad de nivel alto también a los ficheros de nivel básico y medio, esto es, de que el control previsto se ejercerá sobre todos los ficheros.

Por todo ello se emiten las siguientes

Conclusiones

Los datos de carácter personal que trata el Ayuntamiento están sometidos a la protección específica de la normativa de protección de datos, en concreto a la LOPD y al RLOPD, y, por tanto, su tratamiento deberá respetar los principios y garantías que establece dicha normativa.

La información de la que dispone esta Agencia sobre el expediente disciplinario incoado a la funcionaria local no permite concluir que se haya producido una cesión de datos y que ésta sea ilegítima, ni ningún otro tratamiento de datos que pudiera suponer una infracción de la normativa de protección de datos, sin perjuicio de las conclusiones a las que pueda llegar la instructora del expediente disciplinario si dispone de más información.

El control que ejerza el Ayuntamiento sobre las herramientas de trabajo deberá respetar el marco normativo aplicable y los límites establecidos por la doctrina jurisprudencial, especialmente los referidos al respeto a los derechos fundamentales de los trabajadores a la intimidad personal y familiar, al honor y a la propia imagen, la protección de datos personales y el secreto de las comunicaciones.

El Ayuntamiento puede ejercer un control de las herramientas de trabajo, entre las cuales se encuentra el correo electrónico, cuando dicho control tenga como finalidad el mantenimiento de la infraestructura informática y telemática de la que dispone el Ayuntamiento, verificar el cumplimiento por parte de los trabajadores de sus obligaciones laborales, o bien coordinar y garantizar la continuidad de la actividad laboral en los supuestos de ausencia de los trabajadores. En todo caso, en aplicación del principio de calidad (artículo 4 de la LOPD)

deberán determinarse las actuaciones de control en función de la finalidad que se persiga en cada caso y elegir el sistema menos intrusivo para los datos personales, con la condición de que no se pueden tratar datos no pertinentes o excesivos. Será necesario, además, informar clara y previamente a los trabajadores sobre sus obligaciones, sobre las medidas de seguridad implantadas, así como sobre el alcance del control de las herramientas de trabajo que ejercerá el Ayuntamiento.