CNS 17/2009

Dictamen en relación con la consulta planteada por un representante sindical a un Ayuntamiento, respecto al contenido de la instrucción «Sobre el uso de los sistemas y tecnologías de la información y comunicación por parte del personal al servicio del Ayuntamiento [...]»

Se presenta ante la Agencia Catalana de Protección de Datos un escrito de un ciudadano, en nombre y representación de un sindicato, dirigido al Ayuntamiento, en relación con la instrucción del dicho Ayuntamiento «Sobre el uso de los sistemas y tecnologías de la información y comunicación por parte del personal al servicio del Ayuntamiento [...]».

En el escrito presentado se considera que la instrucción pone en grave peligro la confidencialidad de los datos personales de los ciudadanos y de los propios empleados y empleadas municipales. Concretamente, se solicita la opinión de la Agencia en relación con las estipulaciones de varios apartados de la instrucción, y otras que, a criterio de la Agencia, merezcan especial atención.

Analizada la consulta, que se acompaña de fotocopia de la instrucción del Ayuntamiento sobre la que se consulta, teniendo en cuenta la normativa vigente aplicable y visto el informe de la Asesoría Jurídica, se emite el dictamen siguiente.

I

[...]

II

La consulta del representante sindical se refiere a varios apartados de la instrucción del Ayuntamiento «Sobre el uso de los sistemas y tecnologías de la información y comunicación por parte del personal al servicio del Ayuntamiento [...]» (en adelante, la Instrucción).

A fin de situar la Instrucción en su contexto, hay que decir que la Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local (en adelante, LRBRL), reconoce a los municipios, en calidad de Administraciones públicas de carácter territorial, y dentro de la esfera de sus competencias, la potestad de autoorganización, entre otras (artículo 4). Según dispone el artículo 124.4 g) de la LRBRL, a los alcaldes les corresponde la función, entre otras, de dictar bandos, decretos e instrucciones. Y el mismo artículo 124 dispone, en su apartado 5, que:

> «El Alcalde podrá delegar mediante decreto las competencias anteriores en la Junta de Gobierno Local, en sus miembros, en los demás concejales y, en su caso, en los coordinadores generales, directores generales u órganos similares, con excepción de las señaladas en los párrafos b), e), h) y j), así como la de convocar y presidir la Junta de Gobierno Local, decidir los empates con voto de calidad y la de dictar bandos. Las atribuciones previstas en los párrafos c) y k) sólo serán delegables en la Junta de Gobierno Local.»

En el caso que nos ocupa, la Instrucción la firma el Gerente de Recursos Humanos y Organización. También hay que tener en cuenta lo que dispone el artículo 6 del Decreto Legislativo 2/2003, de 28 de abril, por el que se aprueba el Texto refundido de la Ley Municipal y de Régimen Local de Cataluña. Concretamente, el artículo 6 de dicho Decreto Legislativo dispone que:

> «1. Los entes locales se rigen por lo que dispone la Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local, por esta Ley y todas las otras disposiciones específicas y complementarias, y por el reglamento orgánico y las ordenanzas propias de cada ente.
> 2. La legislación sobre régimen local de la Generalidad de Cataluña garantiza a los entes locales los ámbitos normativos necesarios para hacer efectivo el principio de autonomía organizativa.»

Por consiguiente, la Instrucción se enmarca en la potestad de autoorganización y, en concreto, en el principio de jerarquía, dirigida a los empleados y empleadas al servicio del Ayuntamiento. Así se desprende del artículo 1 de la propia Instrucción, en el que se delimita su objeto y ámbito de aplicación:

> «1. Esta instrucción tiene por objeto establecer los criterios generales para la adecuada utilización de los sistemas de información y comunicación, y en particular del correo electrónico y de Internet, que se ponen a disposición del personal al servicio de la Administración municipal para el ejercicio de sus funciones.
> 2. Esta instrucción se aplicará al personal al servicio del Ayuntamiento de [...], de sus organismos autónomos y entidades públicas empresariales, así como del personal de las sociedades mercantiles que tengan acceso a estos sistemas y medios de información.»

Por último, a fin de enmarcar la finalidad de este dictamen, hay que decir que, teniendo en cuenta las funciones de la Agencia, citadas a los efectos que nos ocupan en el artículo 5 e) de la Ley 5/2002, y en el artículo 15.1 g) del Decreto 48/2003, de 20 de febrero, ya citados, la Agencia tiene que dar respuesta a las consultas planteadas en su escrito por el representante sindical, desde la perspectiva de la normativa de protección de datos de carácter personal. No corresponde, por tanto, a la Agencia informar sobre la pertinencia, el alcance o el contenido en conjunto de la Instrucción del Ayuntamiento, sino sobre aquellas cuestiones que se han puesto de manifiesto en la consulta planteada, así como aquellas otras que puedan ser relevantes desde el punto de vista de la normativa de protección de datos.

Por consiguiente, a continuación se harán las consideraciones que esta Agencia considera pertinentes, dados los términos de la consulta planteada.

III

En la consulta se considera que algunas de las estipulaciones de la Instrucción ponen en grave peligro la confidencialidad de los datos personales de los ciudadanos y de los propios empleados y empleadas municipales. Se puede deducir que en la consulta se manifiesta la preocupación de que la protección de los datos personales de los ciudadanos y de los empleados municipales no se lleve a cabo correctamente, vistos los términos de la Instrucción.

A fin de centrar la cuestión objeto de estudio en este dictamen, conviene hacer una aproximación general al derecho a la protección de datos de carácter personal, configurado en el artículo 18.4 de la Constitución Española, y al marco normativo aplicable a este derecho fundamental.

Como punto de partida, toda aquella información que trate el Ayuntamiento y que tenga la naturaleza de información de carácter personal, estará sometida a la protección específica de la normativa de protección de datos, concretamente, de la Ley 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante, LOPD), así como del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD (en adelante, RLOPD).

El artículo 1 de la LOPD establece que esta ley tiene por objeto garantizar y proteger, en lo que se refiere al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente su honor y su intimidad personal y familiar.

Debemos definir los «datos personales» como cualquier información referente a personas físicas identificadas o identificables (artículo 3 a) de la LOPD). Es evidente que el conjunto de la información de carácter personal que se pueda tratar en un Ayuntamiento, tanto de los propios empleados y empleadas municipales, como de los ciudadanos, queda protegido por la normativa de protección de datos personales, concretamente, por la LOPD y el RLOPD citados. La información que pueda llegar a tratar un Ayuntamiento en relación con sus competencias y que no sea información relativa, directa o indirectamente a personas físicas, no se encontrará protegida por dicha normativa, aunque puede estar protegida por otra normativa sectorial aplicable (normativa tributaria, de contratación o de propiedad intelectual o industrial, por citar algunos ejemplos).

Supone un «tratamiento» de dicha información personal 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). Todas estas operaciones, y la gestión de información personal que se derive de ello, realizadas por los trabajadores al servicio del Ayuntamiento en el ejercicio de las tareas que les son asignadas, deben regirse por lo que dispone la normativa de protección de datos.

La LOPD protege a las personas físicas a través de la protección de sus datos personales, mediante la aplicación de una serie de principios y garantías que resultan exigibles en relación con cualquier tratamiento que se realice. Haciendo una aproximación general a estos principios, sin perjuicio de las concreciones que se harán más adelante en este dictamen, cabe decir que cualquier tratamiento de datos personales debe dar cumplimiento al 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).

Sin hacer una relación exhaustiva, hay que señalar que hay otros principios y obligaciones en la LOPD que se deben cumplir en cualquier tratamiento de datos personales, como, entre otros, el deber de dar información a los afectados sobre el tratamiento de sus datos (artículo 5 de la LOPD); el deber de secreto profesional que se impone tanto al responsable del fichero como a cualquier persona que intervenga en el tratamiento (artículo 10 de la LOPD); la obligación de crear, modificar o suprimir ficheros de titularidad pública, como serían los de un Ayuntamiento, a través de disposición general publicada en el diario o boletín oficial correspondiente (por aplicación del artículo 20 de la LOPD); o bien las exigencias que se derivan para el Ayuntamiento en caso de que éste prevea el acceso a los datos personales por parte de un encargado del tratamiento (artículo 12 de la LOPD). Además, la normativa de protección de datos impone la aplicación de determinadas medidas de seguridad a los tratamientos de datos, por parte de los responsables de los ficheros o tratamientos (artículo 9 de la LOPD). Estos y otros principios y obligaciones definidos en la normativa de protección de datos deben ser tenidos en cuenta, en tanto que la Instrucción puede afectar a datos de carácter personal. Por consiguiente, se puede afirmar que la interpretación que se haga de los artículos de la Instrucción cuestionados en la consulta tiene que ser coherente y respetuosa con dichos principios y obligaciones.

Por consiguiente, aunque en la Instrucción no hay referencias generales y expresas a la legislación de protección de datos (aparte de la mención a la «LOPD» hecha en el artículo 5.2, en relación con los rastros de uso derivados de la gestión de aplicativos; apartado que se comentará más adelante en este dictamen), hay que interpretar el conjunto del contenido de la Instrucción, en lo que afecte al tratamiento de datos de carácter personal, en conexión con los principios y obligaciones que impone la normativa de protección de datos. Los principios y obligaciones establecidos en la LOPD son de obligado cumplimiento para toda persona física o jurídica que trate los datos personales, y, por tanto, para el responsable del fichero o tratamiento, entendido como la persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, el contenido y el uso del tratamiento (artículo 3 d) de la LOPD), así como para cualquier persona que intervenga en cualquier fase de lo que hemos denominado «tratamiento de datos».

Dados los términos expuestos en la consulta, se deberá tener especialmente en cuenta que la LOPD, como se ha dicho, impone el deber de secreto profesional tanto al responsable del fichero o tratamiento como a cualquier persona que intervenga en el tratamiento (artículo 10), de modo que el tratamiento de datos personales derivado de la Instrucción del Ayuntamiento debe asegurar el respeto por la confidencialidad de los datos personales, tanto de los empleados municipales como de cualquier otra persona física.

IV

Como se ha señalado, la Instrucción dispone en su artículo 1 que su objeto es establecer los criterios generales para la adecuada utilización de los sistemas de información y comunicación, y en particular del correo electrónico y de Internet, los cuales se ponen a disposición del personal al servicio de la Administración municipal para el ejercicio de sus funciones. El Ayuntamiento, de este modo, establece, en base a las competencias que le otorga la normativa citada en el apartado II de este dictamen, unas pautas relativas a la utilización y la gestión de los sistemas de información por parte de sus empleados y empleadas municipales; sistemas que tienen que utilizar habitualmente para realizar su trabajo.

Hay que añadir que el artículo 2 de dicha Instrucción especifica que ésta «se complementará con las siguientes normas: "Norma respecto al Tratamiento de Datos de Carácter Personal en el Ayuntamiento [...]" (NPD) y "Norma Técnica de Seguridad para los Usuarios de los Sistemas de Información del Ayuntamiento [...]" (NTS).» Dado que no se dispone de estos documentos, el presente dictamen se realizará teniendo en cuenta, principalmente, el contenido de la Instrucción que es objeto de consulta. En cualquier caso, en todo aquello que los documentos citados afecten al tratamiento de datos personales, deberán interpretarse conforme la normativa de protección de datos personales.

Así pues, el objeto de esta Instrucción se refiere a la utilización de «sistemas de información» (en adelante, SI), que podríamos considerar como el conjunto organizado de elementos que se interrelacionan, y que pueden ser elementos físicos, lógicos y organizativos que comporten el tratamiento de información de todo tipo, sea de carácter personal o no.

Con carácter general, podemos decir que integran los SI de una entidad o empresa —en el caso que nos ocupa, el Ayuntamiento— el conjunto de personas o usuarios que integran la organización y utilizan o tratan la información, así como la propia información, sea o no información personal, y también el conjunto de actividades o

procesos realizados dentro de la organización en relación con la información tratada, los flujos informativos que se generan y los recursos materiales empleados en estos procesos. A efectos de la normativa de protección de datos, y según dispone el artículo 5.2 m) del RLOPD, constituye un SI el conjunto de ficheros, tratamientos, programas, soportes y, en su caso, equipos utilizados para el tratamiento de datos de carácter personal. También deberemos tener en cuenta que, según el mismo artículo 5.2, apartado n), constituye un sistema de tratamiento la manera en que se organiza o utiliza un SI. Es decir, según el sistema de tratamiento, los SI pueden ser automatizados, no automatizados o parcialmente automatizados.

V

Este comentario respecto a lo que podemos considerar como SI, tiene relevancia a efectos de concretar la primera cuestión que la consulta somete a la opinión de la Agencia, que analizamos a continuación. Nos referimos al contenido del artículo 4 de la Instrucción, relativo al «uso de los sistemas de información en general», apartado 1, que tiene la redacción siguiente:

«Todos los recursos de los sistemas de información municipales, así como la información contenida, son propiedad del Ayuntamiento, por lo que no está permitido su uso fuera de las tareas asignadas a su puesto de trabajo.»

En relación con la frase «la información contenida [en los sistemas de información] son propiedad del Ayuntamiento» de este apartado, en la consulta se considera que no se tiene en cuenta que la mayor parte de la información de los ciudadanos, de las empresas y de los propios empleados y empleadas municipales contenida en los sistemas de información municipales sigue siendo propiedad de sus titulares, que de acuerdo con la ley, conservan intactos todos sus derechos de protección de sus datos, con todas las consecuencias.

En la consulta no se cuestiona que algunos de los elementos que, como se ha comentado, forman parte de un SI, puedan ser considerados como propiedad del Ayuntamiento o, sería necesario añadir, de terceros. La consulta cuestiona la propiedad sobre uno de los elementos que forman parte de todo SI, como es la información, entendida en un sentido amplio. Concretamente, se cuestiona que se considere al Ayuntamiento como «propietario» de la información contenida en los SI, sin más distinción y con carácter general, vista la redacción del artículo 4 de la Instrucción.

La Instrucción se refiere a información, en general, que puede ser de varios tipos, como ya ha quedado dicho. La información que puede gestionar un Ayuntamiento puede referirse a información de la propia organización, o información procedente de terceros, sean personas físicas, empresas o instituciones, otras Administraciones públicas, etc. La información relativa a las diferentes competencias que ejerce un municipio, que se encuentran concretadas en la normativa correspondiente (artículos 25 y siguientes de la LRBRL; y artículos 8 y 9, en cuanto a las potestades y competencias de los entes locales, y 66, en cuanto a las competencias municipales y locales, del Decreto Legislativo 2/2003, entre otros), puede ser muy variada.

Las competencias municipales y, por tanto, la información que puede tratar un Ayuntamiento, pueden englobar materias tan variadas como la seguridad en lugares públicos, la ordenación del tránsito o la protección civil, la prestación de servicios sociales y la participación en la gestión de la atención primaria de salud, el patrimonio histórico-artístico o las actividades culturales, el ejercicio de competencias en materia

de tributos, o la gestión del padrón municipal de habitantes, entre otras, y ello simplemente a título de ejemplo.

Es evidente que el Ayuntamiento debe tener una capacidad de control y decisión sobre los SI que gestiona, y que pone a disposición de sus empleados a fin de cumplir con las competencias que la normativa otorga al Ayuntamiento. Más que en términos patrimoniales, la referencia hecha en la Instrucción al término «propietario» se puede entender en el sentido de que el Ayuntamiento tiene esta capacidad de control y decisión en relación con los SI, y más concretamente, en relación con información que —insistimos—, no es sólo información personal. Desde esta perspectiva general, el Ayuntamiento es «propietario» de la información.

Desde la perspectiva de la protección de datos, ciertamente la LOPD no se refiere a los propietarios de la información, sino a los responsables y a los titulares de los datos personales. En cuanto al responsable, entendido como la persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decide sobre la finalidad, el contenido y el uso del tratamiento (artículo 3 d) de la LOPD), la consideración del Ayuntamiento como «propietario» resulta coherente con la normativa de protección de datos, si se interpreta que el Ayuntamiento es depositario y responsable de la información personal que trata, en los términos de la LOPD.

No hay que confundir el concepto de «propietario» de una información con el concepto de «afectado o interesado», que según el artículo 3 e) de la LOPD es la persona física titular de los datos que sean objeto de lo que hemos definido como tratamiento de datos personales. Aparte de que, en base a lo establecido en la diferente normativa aplicable, se deba tratar la información que gestiona un Ayuntamiento teniendo en cuenta los derechos o intereses que sobre dicha información tengan terceras personas físicas o jurídicas (por ejemplo, en materia de contratación, o de gestión de servicios públicos, o de propiedad intelectual o industrial, etc.), en cuanto a los datos de carácter personal, hay que tener presente que el derecho fundamental a la protección de datos (artículo 18.4 de la Constitución Española) se configura como un derecho de autodeterminación informativa que se otorga a los titulares de los datos y, por tanto, a las personas físicas (en cuanto a la concreción del contenido esencial de este derecho, nos remitimos a la STC 292/2000).

Los titulares tienen un poder de control y disposición de su información personal, con la modulación que pueda establecerse en la normativa correspondiente. Esta modulación lleva, por ejemplo, a que la LOPD exceptúe en determinados supuestos la necesidad de contar con el consentimiento del titular de los datos para efectuar un tratamiento de los datos, o bien para cederlos a terceros (artículos 6, 11 y 21 de la LOPD). De este modo, la LOPD parte de la base de que, con carácter general, el tratamiento de los datos de carácter personal requiere el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa. Esta disposición resulta plenamente aplicable a cualquier tratamiento de datos personales que se haga en el SI sobre el que se consulta.

En la consulta se apunta que [los titulares], de acuerdo con la ley, conservan intactos todos sus derechos de protección de sus datos, con todas las consecuencias. Ciertamente, el derecho a la protección de datos personales, configurado como una autodeterminación informativa, otorga a los titulares de los datos una serie de derechos, denominados derechos ARCO o derechos de *habeas data* (derechos de acceso, rectificación, cancelación y oposición) que el titular puede ejercer en relación con sus datos, y ante cualquier responsable de un fichero o tratamiento de sus datos. Por lo tanto, un titular de datos personales tratados por el Ayuntamiento (un empleado municipal, un ciudadano, etc.), siempre deberá estar en disposición de ejercer sus

derechos ARCO y, en su caso, de solicitar la tutela de sus derechos a las Agencias de protección de datos competentes, así como de ser indemnizado, y todo ello en los términos y condiciones que establece el Título III de la LOPD.

Considerando el contenido y la configuración del derecho a la protección de datos de carácter personal, lo establecido en el artículo 4 de la Instrucción se tendría que interpretar teniendo en cuenta los conceptos de «afectado o interesado» y de «responsable» en los términos apuntados, así como los principios y obligaciones que para el Ayuntamiento se deriven de la normativa de protección de datos, y especialmente el ejercicio de los derechos ARCO por parte de los interesados. En estos términos, se puede considerar que lo establecido en el artículo 4 de la Instrucción resulta compatible con la normativa de protección de datos de carácter personal.

VI

La consulta se refiere también al contenido del artículo 5 de la Instrucción, relativo a las «Normas de mantenimiento y explotación de los sistemas de información», apartado 1, que tiene la redacción siguiente:

«5.1. Los técnicos informáticos responsables del mantenimiento y explotación de los sistemas de información velarán por el correcto uso de las herramientas de trabajo que el Ayuntamiento pone a disposición del personal y, en este sentido, éstos están facultados para efectuar las tareas de mantenimiento que sean necesarias en los directorios de red y en los ordenadores personales de los usuarios, para la detección y eliminación de todos aquellos elementos que, sin tener relación con las funciones a ejercer en el puesto de trabajo, puedan causar problemas en el normal funcionamiento de los diferentes elementos que configuran las infraestructuras informática y telemática del departamento (juegos, protectores de pantallas, archivos de audio y vídeo, etc. no relacionados con el puesto de trabajo, etc.).»

Concretamente, se cuestiona la frase «Los técnicos informáticos […] están facultados para efectuar las tareas de mantenimiento que sean necesarias en los directorios de red y en los ordenadores personales de los usuarios, para la detección y eliminación de todos aquellos elementos […]».

En la consulta se considera que, de hecho, se está autorizando a este personal técnico a inspeccionar el contenido de todos los repositorios de información que utilizan los usuarios de la Red Municipal sin establecer ninguna garantía, como, por ejemplo, la comunicación previa al interesado o la petición de una autorización a algún responsable. En el escrito enviado por el representante sindical se añade que esto se considera muy grave, dada la naturaleza de la información que se puede encontrar, que pasa a formar parte de una única y enorme base de datos documental, que incluye datos de la más alta sensibilidad (filiación política y sindical, datos de carácter fiscal y económico, datos relativos a los Servicios Sociales, etc.). Además, se añade que los técnicos informáticos aludidos podrían muy bien ser operadores de empresas externas contratados con fórmulas no siempre fiables.

A fin de situar esta cuestión, hay que partir de la base de que el Ayuntamiento, en tanto que responsable de los ficheros o tratamientos afectados por la Instrucción, tiene una serie de obligaciones destinadas a asegurar que el tratamiento que se haga de los datos personales incluidos en los ficheros sea correcto y ajustado a la normativa de protección de datos. Concretamente, el artículo 9 de la LOPD establece la obligación, para los responsables de los ficheros o tratamientos, de aplicar una serie de medidas de seguridad. El apartado 1 de dicho artículo dispone que:

> «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 estén expuestos, ya provengan de la acción humana o del medio físico o natural.»

Las medidas de seguridad que son exigibles a los ficheros y tratamientos de datos de carácter personal se clasifican en tres niveles: básico, medio y alto, y en el Título VIII del RLOPD se concretan las medidas técnicas y organizativas que corresponden a cada nivel. Concretamente, el artículo 81 precisa los niveles de seguridad que se deberán adoptar, en atención a las categorías de los datos personales tratados, la finalidad del fichero o tratamiento y que estos ficheros y tratamientos sean manuales o automatizados. El Título VIII del RLOPD también concreta que se deberán consignar las correspondientes medidas en el documento de seguridad (artículo 88). Así pues, el responsable debe articular unas medidas que se refieren, entre otras cosas, al control de accesos por parte de los usuarios a los recursos necesarios para ejercer sus funciones, a medidas que garanticen la correcta identificación y autenticación de los usuarios, o a varias medidas en relación con la gestión de soportes y documentos. Algunas de estas medidas implican, por ejemplo, que el responsable tenga que implementar sistemas que permitan la autenticación, es decir, la comprobación de la identidad de un usuario, a través de una contraseña o de otros sistemas, en su caso, o que tenga que comprobar cuáles son los accesos autorizados a determinada información, es decir, conocer y establecer cuáles son las autorizaciones que hay que conceder a cada usuario en relación con la utilización de diversos recursos o informaciones. También hay que habilitar un procedimiento de notificación y gestión de las incidencias que afecten a los datos de carácter personal, y hay que establecer un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido —o, en su caso, detectado—, la persona que hace la notificación, a quién se le comunica, los efectos que se deriven de ello y las medidas correctoras aplicadas.

Es más, debemos tener en cuenta lo que dispone el artículo 89 del RLOPD, en relación con las funciones y obligaciones del personal, según el cual:

> «1. Las funciones y obligaciones de cada uno de los usuarios o perfiles de usuarios con acceso a los datos de carácter personal y a los sistemas de información estarán claramente definidas y documentadas en el documento de seguridad.
> También se definirán las funciones de control o autorizaciones delegadas por el responsable del fichero o tratamiento.
> 2. El responsable del fichero o tratamiento adoptará las medidas necesarias para que el personal conozca de una forma comprensible las normas de seguridad que afecten al desarrollo de sus funciones, así como las consecuencias en que pudiera incurrir en caso de incumplimiento.»

También hay que tener presente que el RLOPD exige que el responsable elabore un documento de seguridad en el que hay que hacer constar las medidas de índole técnica y organizativa conformes a la normativa de seguridad vigente, que es de cumplimiento obligado para el personal con acceso a los SI (artículo 88). Específicamente, el apartado 3. c) de este artículo exige que consten en el documento de seguridad las:

> «Funciones y obligaciones del personal en relación con el tratamiento de los datos de carácter personal incluidos en los ficheros.»

Partiendo de esta base, es evidente que el Ayuntamiento tiene que explicar a todas aquellas personas que accederán y trataran datos, principalmente a los empleados municipales, cuáles son las medidas que deben tener en cuenta, y cuáles son los procedimientos o protocolos de actuación. Con carácter general, se puede considerar que el objetivo y el contenido de la Instrucción se enmarcan en esta finalidad. En definitiva, es evidente que cualquier usuario, en el contexto del concepto de SI que hemos utilizado, debe estar al corriente de cómo tiene que gestionar los diferentes elementos que conforman el SI al que tiene acceso para realizar su trabajo.

Más allá de hacer una relación completa de las medidas de seguridad previstas, o del contenido del documento de seguridad, en relación con la cual nos remitidos a lo establecido en el RLOPD, se quiere poner de manifiesto que el responsable —en el caso que nos ocupa, el Ayuntamiento— tiene la obligación de velar por el cumplimiento de las medidas de seguridad que impone la normativa, las cuales, en mayor o menor grado, requieren la implicación directa de los usuarios. Por lo tanto, es evidente que el personal que presta sus servicios por cuenta de un responsable, debe tener constancia de las medidas y de las implicaciones que su cumplimiento le genera. De ello se puede deducir que informar a los usuarios y concretar los usos correctos de los SI por parte de éstos, en relación con sus funciones, constituye el objetivo la Instrucción sobre la que se solicita la opinión de la Agencia; objetivo que es respetuoso, con carácter general, con la normativa de protección de datos, ya que da cumplimiento a las obligaciones del Ayuntamiento contempladas en la normativa de protección de datos en relación con la gestión de los SI.

Por otro lado, en relación con la consideración que se hace en la consulta de que los técnicos informáticos aludidos podrían muy bien ser operadores de empresas externas contratados con fórmulas no siempre fiables, desde la perspectiva de la protección de datos es pertinente recordar las exigencias que se derivan de la propia LOPD al establecer las condiciones de acceso a los datos por cuenta de terceros. Concretamente, el artículo 12 de la LOPD, en relación con el «encargado del tratamiento», dispone que no se considera comunicación de datos el acceso de un tercero a los datos cuando el acceso sea necesario para la prestación de un servicio al responsable del tratamiento. En cualquier caso, el tratamiento de datos de carácter personal que tenga que realizar un tercero por cuenta del responsable —en el caso que nos ocupa, por cuenta del Ayuntamiento— deberá estar regulado por un contrato, en el que hay que establecer de manera expresa que el encargado sólo debe tratar los datos de acuerdo con las instrucciones del responsable, que es quien decide sobre la finalidad, contenido y usos del tratamiento. Es especialmente relevante lo establecido en el artículo 12 citado, respecto a que el encargado del tratamiento no puede ceder o comunicar los datos a otras personas. Asimismo, el encargado del tratamiento, y las personas que trabajan para dicho encargado, están vinculados por el deber de secreto respecto a la información que tratan (artículo 10 de la LOPD).

El documento de seguridad citado es especialmente importante en caso de que el Ayuntamiento encargue a terceros el tratamiento de datos, ya que en dicho documento se tienen que concretar las características del tratamiento de datos personales que pueden hacer los encargados del tratamiento, y en el mismo deberá constar la identificación de los ficheros o tratamientos que tienen que tratar los encargados, con referencia expresa al contrato o documento que regula las condiciones del encargo (artículo 88.5 de la LOPD). Por consiguiente, la LOPD establece una serie de controles y especificaciones que debe cumplir cualquier encargado del tratamiento que se contrate por parte del Ayuntamiento.

Más allá de las valoraciones genéricas hechas en la consulta sobre la fiabilidad de determinadas contrataciones, sobre las que esta Agencia no tiene elementos para

pronunciarse, no se puede deducir de la Instrucción estudiada que el Ayuntamiento no prevea someterse a les estipulaciones de la LOPD y del RLOPD (artículos 20 a 22) relativas a la actuación de posibles encargados del tratamiento.

Habría que añadir que tanto si el encargado del tratamiento presta servicios en los locales del responsable, como si el servicio se presta externamente o se produce un acceso remoto a los datos, en cualquier caso, dicho encargado del tratamiento, y el personal a su servicio, deben cumplir con las medidas de seguridad que sean pertinentes en cada caso (artículo 82 del RLOPD).

Como hemos señalado, la normativa de protección de datos exige a los responsables de ficheros y tratamientos de datos una serie de obligaciones en relación con la aplicación de medidas de seguridad, las cuales imponen la supervisión de que dichas medidas se cumplan, y la necesidad de informar convenientemente a los usuarios; función que cumple la Instrucción comentada.

Es evidente que, con carácter general, para poder dar cumplimiento a las medidas de seguridad que impone la normativa de protección de datos según el nivel exigible, el responsable tiene que poder llevar a cabo, a través de personas designadas para esta función, como puede ser el personal técnico informático en el caso que nos ocupa, diferentes tareas de comprobación del correcto uso de las herramientas de trabajo que el Ayuntamiento pone a disposición del personal. Esta tarea debe llevarse a cabo bajo el control, dirección y supervisión de los responsables designados al efecto por el responsable del fichero o tratamiento.

Es más, el Título VIII del RLOPD citado establece varias estipulaciones relativas a la autorización que hay que dar para acceder a los datos personales y tratarlos. Con carácter general, el artículo 84 del RLOPD dispone que las autorizaciones se atribuyen al responsable, y que pueden ser delegadas en las personas designadas al efecto. Aunque la redacción del apartado 5.1 de la Instrucción, ciertamente, no especifica qué personas están designadas para dirigir y supervisar las tareas que llevarán a cabo los técnicos informáticos, hay que considerar plenamente aplicables las estipulaciones del Título VIII del RLOPD en esta cuestión.

Como se menciona en el apartado 5.1, cuestionado, la finalidad del mantenimiento es la detección de lo que podría causar problemas en el normal funcionamiento de los diferentes elementos que configuran las infraestructuras informática y telemática del departamento (juegos, protectores de pantallas, archivos de audio y vídeo, etc. no relacionados con el puesto de trabajo, etc.). Por lo tanto, es evidente que ésta es la finalidad de las tareas de control, en los términos planteados en la Instrucción.

La estipulación del apartado 5.1 de la Instrucción respecto a la intervención de los técnicos informáticos, tiene una finalidad determinada, como es que se puedan efectuar las tareas de mantenimiento que sean necesarias, en los directorios de red y en los ordenadores personales de los usuarios, para la detección y eliminación de los elementos que, sin tener relación con las funciones a ejercer en el puesto de trabajo, puedan causar problemas de funcionamiento de los SI. La infraestructura informática y telemática de que dispone el Ayuntamiento para que sus empleados cumplan con las tareas que les son encomendadas —en definitiva, los ordenadores, aplicaciones, software y hardware, etc. que forman parte de lo que hemos denominado SI—, lógicamente tiene que estar sometida a unas tareas de mantenimiento y revisión, para asegurar su correcto funcionamiento.

Visto que la aplicación y supervisión del correcto cumplimiento de las medidas de seguridad puede comportar la realización, por parte del responsable, de tareas de

supervisión de los diferentes elementos que conforman un SI, en caso de que dichas tareas puedan comportar un acceso a datos de carácter personal, ya sea de ciudadanos o de los propios empleados municipales, la propia LOPD exige que los datos de carácter personal, en cualquier caso, se traten de acuerdo con el principio de calidad (artículo 4), y de acuerdo con la finalidad concreta y legítima que justifica el tratamiento. Esta finalidad se deberá cumplir, para que resulte ajustada a la normativa de protección de datos, conforme a las exigencias del Título VIII de la LOPD, al que nos hemos referido.

En especial, por aplicación del principio de calidad, hay que tener en cuenta la exigencia de proporcionalidad en el tratamiento de los datos, y el principio de minimización en cuanto a dicho tratamiento, entendido como la exigencia de tratar sólo los datos personales que sean estrictamente necesarios para el cumplimiento de la finalidad legítima. En este caso, esto comporta que los técnicos informáticos sólo accedan y visualicen la información mínima necesaria para realizar las tareas de mantenimiento, y que no puedan tratar o utilizar la información para ninguna otra finalidad.

A título de ejemplo, citamos la sentencia del Tribunal Supremo, en unificación de doctrina, de 26 de septiembre de 2007 (Fundamento Jurídico quinto), relativa al control de medios puestos a disposición del trabajador, concretamente, el ordenador personal.

> «Es cierto que la entrada inicial en el ordenador puede justificarse por la existencia de un virus, pero la actuación empresarial no se detiene en las tareas de detección y reparación, sino que, como dice con acierto la sentencia recurrida, en lugar de limitarse al control y eliminación del virus, "se siguió con el examen del ordenador" para entrar y apoderarse de un archivo cuyo examen o control no puede considerarse que fuera necesario para realizar la reparación interesada.»

Es evidente que el principio de proporcionalidad, derivado del principio de calidad de los datos, comporta no tratar más información de la que sea necesaria para resolver una incidencia concreta que se haya producido en los SI, como puede ser la detección de un virus informático.

VII

La consulta cuestiona parte del contenido del apartado 5 de la Instrucción, apartado 2, que tiene la redacción siguiente:

«Asimismo, estos responsables para garantizar la continuidad del servicio y hacer el seguimiento de la adecuada utilización de los sistemas de información guardarán el rastro de uso de los diferentes aplicativos y sistemas. Concretamente, se mantendrán los rastros siguientes:

- Rastros de uso derivados de la gestión del aplicativo y los que imponga la LOPD.
- Registro de las acciones realizadas en los servidores de ficheros.
- Páginas de Internet visitadas.
- Tráfico del buzón de correo.
- Registro de acceso a los sistemas de aplicativos y recursos informáticos.
- Cualquier otro registro que se requiera para garantizar el buen uso de los sistemas.»

Como hemos visto, en lo que se refiere a los datos y la información tanto de los propios empleados municipales como de los ciudadanos en general, la consulta pone de manifiesto la preocupación por un uso indebido de esta información, que puede ser, además, información personal sensible, a efectos de la LOPD. Por consiguiente, hay

que analizar las implicaciones que pueden tener para los derechos de los usuarios, especialmente los empleados del Ayuntamiento, las medidas propuestas en el apartado 5.2 de la Instrucción.

Antes de entrar en otras consideraciones, hay que dejar claro que la normativa de protección de datos, efectivamente, establece una protección reforzada para los datos considerados sensibles (artículo 7). Aparte de otras consideraciones hechas en dicho artículo, al que nos remitimos, el apartado 4 dispone que quedan prohibidos los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología o la afiliación sindical, entre otros. Aunque el Ayuntamiento debe tener en cuenta las estipulaciones de la LOPD respecto a los datos sensibles, hay que concluir, respecto a esta cuestión, que de la lectura del apartado 5.1 de la Instrucción no se puede deducir que se tenga que producir ningún tratamiento de información personal que contravenga las estipulaciones citadas.

En lo que se refiere, en términos generales, a los datos de los ciudadanos, ya ha quedado sobradamente expuesto que el tratamiento que haga el Ayuntamiento, en tanto que responsable, así como cualquier usuario, de los datos personales de los ciudadanos, debe ceñirse a las exigencias de los principios y garantías de la LOPD.

En lo que respecta específicamente a los datos de los empleados municipales, y en conexión con las exigencias del principio de calidad citado, habría que recordar que los trabajadores son titulares de los derechos fundamentales que les corresponden en tanto que ciudadanos, y que estos derechos, como ha reiterado el Tribunal Constitucional, no dejan de tener plena vigencia en el ámbito laboral, aunque su ejercicio puede resultar modulado (STC 88/1985 y STC 126/2003, entre otras). En este sentido, es evidente que la vinculación contractual entre trabajador y empresa no implica la privación del trabajador de los derechos que la Constitución le reconoce como ciudadano, entre ellos, a los efectos relevantes para este dictamen, el derecho fundamental a la intimidad personal y familiar, el derecho al honor y el derecho a la propia imagen (artículo 18.1 de la Constitución) y obviamente, el derecho a la protección de datos personales (artículo 18.4 de la Constitución). También se deberá tener en cuenta lo que se desprende del derecho fundamental al secreto de las comunicaciones, configurado en el artículo 18.3 de la Constitución. Estos derechos, aparte de lo que ya se ha dicho en materia de protección de datos, reciben protección específica en el ámbito civil (Ley Orgánica 1/1982, de 5 de mayo, de Protección Civil de los Derechos al Honor, la Intimidad Personal y Familiar y la Propia Imagen), y penal (a través de la figura del delito de descubrimiento y revelación de secretos, regulada en los artículos 197 y siguientes del Código Penal).

Citamos a continuación las estipulaciones en la normativa sectorial aplicable al ámbito que nos ocupa, a fin de delimitar los controles o intromisiones legítimos que una organización o empresa, en este caso, un Ayuntamiento, puede realizar respecto a los derechos de sus empleados.

En el ámbito municipal, según el artículo 21.1 de la LRBRL citada, el alcalde ostenta la atribución de dirigir el gobierno y la administración municipales, así como, entre otras, la de «desempeñar la jefatura superior de todo el personal, y acordar su nombramiento y sanciones, incluida la separación del servicio de los funcionarios de la Corporación y el despido del personal laboral». En el mismo sentido, el artículo 53.1.b) del Decreto Legislativo 2/2003 citado establece que el alcalde dirige el gobierno y la administración municipales. Por lo tanto, el alcalde dirige la administración municipal, incluyendo el personal que presta servicios en el Ayuntamiento. Finalmente, el artículo 92.1 de la LRBRL añade, en lo que se refiere a los funcionarios al servicio de la Administración local, que se rigen, en lo que no contemple la Ley de Bases, por la legislación del

Estado y de las Comunidades Autónomas en los términos del artículo 149.1.18ª de la Constitución.

Según dispone el artículo 2.1 de la Ley 7/2007, de 12 de abril, del Estatuto Básico del Empleado Público (EBEP), éste se aplica al personal funcionario y, en lo que proceda, al personal laboral al servicio de las Administraciones públicas, entre otras, las Administraciones de las entidades locales. En el artículo 14 del EBEP se reconocen los derechos individuales de los empleados públicos, como, entre otros, el respeto a su intimidad, propia imagen y dignidad en el trabajo, y demás derechos reconocidos por el ordenamiento jurídico. El artículo 52 del EBEP concreta los deberes de los empleados públicos y los principios que inspiran el código de conducta que éstos deben cumplir. Además, este artículo especifica que los principios y reglas establecidos en el Capítulo VI del EBEP informan la interpretación y aplicación del régimen disciplinario de los empleados públicos, concretado en los artículos 93 y siguientes. El ejercicio de la potestad disciplinaria corresponde a cada Administración pública respecto al personal a su servicio; en el caso que nos ocupa, corresponde al Ayuntamiento (artículo 94 del EBEP). El artículo 54 del EBEP concreta los principios de conducta de los empleados públicos, como, entre otros, desarrollar las tareas correspondientes a su puesto de trabajo de forma diligente y obedecer las instrucciones y órdenes profesionales de sus superiores, así como administrar los recursos y bienes públicos con austeridad, y no utilizarlos en beneficio propio o de personas allegadas. Tienen, también, el deber de velar por la conservación de dichos recursos y bienes.

Respecto al personal laboral, el artículo 92 del EBEP dispone que el personal laboral se regirá por el Estatuto de los Trabajadores (ET), aprobado por el Real Decreto Legislativo 1/1995, de 24 de marzo, y por los convenios colectivos que sean de aplicación. El ET establece los derechos básicos de los trabajadores, entre los que, a los efectos que nos ocupan, se cita el respeto a su intimidad y la consideración debida a su dignidad (artículo 4). Como ha puesto de manifiesto la jurisprudencia constitucional, el poder de dirección del empresario incluye facultades de control de la actividad laboral. Así, el artículo 20.3 del ET atribuye al empresario, entre otras, la facultad de adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento, por parte del trabajador, de sus obligaciones laborales con el debido respeto por la dignidad del trabajador.

Aunque los derechos fundamentales de los trabajadores no pueden impedir con carácter general el ejercicio de estas facultades por parte del empresario, sí es cierto que modulan su posibilidad de control, en el sentido de que siempre hay que respetar estos derechos. El control del grado de cumplimiento laboral no puede, en cualquier caso, suponer una intromisión ilegítima en los derechos a la intimidad o a la protección de datos de los trabajadores, entre otros.

En definitiva, la limitación de derechos fundamentales de los trabajadores en el marco de las relaciones laborales debe cumplir con el denominado juicio de proporcionalidad, que el Tribunal Constitucional ha delimitado como el examen respecto al objetivo propuesto con la medida limitadora de derechos (juicio de idoneidad); si, además, la medida es necesaria, en el sentido de que no hay 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). Simplemente a título de ejemplo, y en relación con la limitación de los derechos fundamentales mencionados en el ámbito laboral, citamos las STC 186/2000 y 98/2000. En cualquier caso, toda limitación del ejercicio de derechos fundamentales de los trabajadores, por

parte del empresario, tiene que ser una medida contemplada en una norma con rango de ley, proporcionada y necesaria en una sociedad democrática, como se desprende de la jurisprudencia constitucional.

En relación con la utilización de datos personales de los trabajadores, el Tribunal Constitucional ha manifestado que el derecho de control del flujo informativo procura evitar que la información de los datos personales propicie comportamientos discriminatorios. En la STC 94/1998, se ha reconocido que un tratamiento inadecuado de datos personales de los trabajadores puede poner en riesgo el legítimo ejercicio de derechos fundamentales de los trabajadores, por ejemplo, la libertad sindical, en conexión con el derecho a la protección de datos personales. La STC citada examina un supuesto en el que se había utilizado un dato especialmente sensible, como es la afiliación sindical de un trabajador, que se facilita única y exclusivamente a efectos de descontar de la retribución la correspondiente cuota sindical. Pese a ello, el dato fue utilizado para retener la parte proporcional del salario relativa a un periodo de huelga. Como destaca el Tribunal:

> «[...] se utilizó un dato sensible, que había sido proporcionado con una determinada finalidad, para otra radicalmente distinta con menoscabo del legítimo ejercicio del derecho de libertad sindical.»

Más concretamente, cabe decir que la jurisprudencia ha examinado varios casos en los que se plantean los límites del registro, por parte del empresario, de las herramientas de trabajo que pone a disposición del trabajador, como los teléfonos, ordenadores, etc. También se ha dedicado especial atención a las posibilidades de control de la utilización que hacen los trabajadores de las nuevas tecnologías, como las conexiones a Internet, y al uso correcto que debe hacer el trabajador de estas herramientas, en especial de Internet y el correo electrónico (entre otras, la STSJ de Cataluña, de 11 de marzo de 2004, o la STSJ de la Comunidad de Madrid, de 16 de enero de 2008).

En algunos casos se ha admitido, por ejemplo, como respetuoso con el derecho a la intimidad de los trabajadores, la colocación en red de programas que permiten verificar, sin entrar en el ordenador del usuario, qué uso hace éste del mismo; concretamente, para controlar la práctica de juegos durante la jornada laboral, considerando que se trata de una medida idónea y proporcionada (STSJ de Cataluña, de 29 de enero de 2001).

A los efectos que nos ocupan, recordamos la STS de 26 de septiembre de 2007 citada, relativa al control de medios puestos a disposición del trabajador, concretamente, el ordenador personal, y el uso que puede hacer del mismo. Como se desprende de dicha sentencia, el control mencionado se enmarca en lo contemplado en el artículo 20.3 del Estatuto de los Trabajadores, según el cual:

> «El empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad humana [...].»

Se constata en esta sentencia que en el uso que haga el trabajador de los medios informáticos facilitados por la empresa pueden producirse conflictos que afecten a la intimidad de los trabajadores, tanto en el correo electrónico, en el que la implicación se extiende también al derecho fundamental al secreto de las comunicaciones, como en la denominada «navegación» por Internet, y en el acceso a determinados archivos personales del ordenador. El conflicto existe, como añade la sentencia, porque existe

una utilización personalizada y no meramente laboral o profesional de estos medios (Fundamento Jurídico segundo).

Dicho esto, el TS añade que el control de los ordenadores se justifica por la necesidad de coordinar y garantizar la continuidad de la actividad laboral en los supuestos de ausencias de los trabajadores, por la protección del sistema informático de la empresa, que puede resultar afectado negativamente por determinados usos, y por la prevención de las responsabilidades que para la empresa puedan derivarse de formas ilícitas de uso ante terceros (Fundamento Jurídico tercero):

> «[...] es necesario recordar [...] la existencia de un hábito social generalizado de tolerancia con ciertos usos personales moderados de los medios informáticos y de comunicación facilitados por la empresa a los trabajadores. Esa tolerancia crea una expectativa también general de confidencialidad en esos usos; expectativa que no puede ser desconocida, aunque tampoco convertirse en un impedimento permanente del control empresarial, porque, aunque el trabajador tiene derecho al respeto a su intimidad, no puede imponer ese respeto cuando utiliza un medio proporcionado por la empresa en contra de las instrucciones establecidas por ésta para su uso y al margen de los controles previstos para esa utilización y para garantizar la permanencia del servicio. Por ello, lo que debe hacer la empresa de acuerdo con las exigencias de buena fe es establecer previamente las reglas de uso de esos medios con aplicación de prohibiciones absolutas o parciales e informar a los trabajadores de que va existir control y de los medios que han de aplicarse en orden a comprobar la corrección de los usos, así como de las medidas que han de adoptarse en su caso para garantizar la efectiva utilización laboral del medio cuando sea preciso, sin perjuicio de la posible aplicación de otras medidas de carácter preventivo, como la exclusión de determinadas conexiones. De esta manera, si el medio se utiliza para usos privados en contra de estas prohibiciones y con conocimiento de los controles y medidas aplicables, no podrá entenderse que, al realizarse el control, se ha vulnerado "una expectativa razonable de intimidad" en los términos que establecen las sentencias del Tribunal Europeo de Derechos Humanos de 25 de junio de 1997 (TEDH 1997, 37) (caso Halford) y 3 de abril de 2007 (TEDH 2007, 23) (caso Copland) para valorar la existencia de una lesión del artículo 8 del Convenio Europeo par la protección de los derechos humanos.»

Por consiguiente, en lo que se refiere al artículo 5.2 de la Instrucción, se habilita un rastreo de información para garantizar la continuidad del servicio y hacer el seguimiento de la adecuada utilización de los SI por parte de los empleados. Partiendo de la base, que ya se ha mencionado, de que en la medida en que estas finalidades pueden afectar a datos sometidos a la normativa de protección de datos personales, hay que contar con el consentimiento del afectado, o bien con una norma con rango de ley que habilite el tratamiento sin disponer de este consentimiento. Por lo tanto, hay que tener en cuenta el marco normativo aplicable en cuanto a la capacidad de control del Ayuntamiento y la manera de articular dicho control, y también hay que tener presente la jurisprudencia relevante en esta materia, a fin de de asegurar el respeto de los derechos fundamentales de los trabajadores.

Especialmente, como se desprende de la jurisprudencia relevante en esta materia, hay que poner de manifiesto la importancia del cumplimiento del deber de información por parte de la empresa —en el caso que nos ocupa, el Ayuntamiento— respecto a sus empleados, en relación con el cumplimiento de las finalidades de la Instrucción, y en relación con las medidas concretas de control de los SI. Es necesario que se dé información suficiente y clara a los trabajadores, con carácter general, sobre las medidas de control que se apliquen, sobre la información que se trate debido a la aplicación de estos controles y sobre las repercusiones que pueda tener un uso inadecuado de los SI. Si el Ayuntamiento, en el caso que nos ocupa, establece unas reglas de uso de los SI a través de la Instrucción e informa de ello adecuadamente a los empleados, éstos pueden tener un conocimiento adecuado sobre la utilización

correcta de los SI. Esta información, por tanto, es necesaria para el ejercicio legítimo de control por parte del Ayuntamiento respecto a las herramientas mencionadas, y para efectuar determinadas actuaciones de control, en su caso, en relación con el uso de dichas herramientas, en aplicación del marco normativo al que nos hemos referido.

VIII

Finalmente, hay que mencionar lo que se establece, en el artículo 5.2 de la Instrucción, sobre el «mantenimiento» del rastro de uso de los diferentes aplicativos y sistemas. En la consulta se considera que cuando se habla de crear y explotar registros de las páginas de Internet visitadas o del tráfico del buzón de correo, o de otros elementos que se consideren necesarios, «se está de hecho creando bases de datos de carácter personal sin ningún tipo de control ni declaración».

La Instrucción informa de que se mantendrán rastros de páginas web visitadas y de tráfico del buzón de correo, entre otros. Respecto a las páginas web visitadas, la información recogida a la que se refiere el artículo 5.2 puede ser, por ejemplo, las direcciones de las páginas web visitadas, la hora y el tiempo de conexión a la página visitada, la dirección IP y los datos identificativos de la persona física o el usuario que visita dichas páginas, entre otros. En cuanto al tráfico del buzón de correo, la información recogida podría ser la dirección de correo y la dirección IP de origen —en relación con el ordenador desde el que se envía el mensaje—, y la dirección de correo y la dirección IP del destinatario del correo, así como el asunto o encabezamiento del mensaje y la fecha y la hora de los mensajes, principalmente. En uno y otro caso, en función de la configuración que se establezca de los SI, la información que se pueda llegar a tratar podrá ser más o menos amplia.

Concretamente, en relación con la dirección IP, esta Agencia ha tratado su posible configuración como dato personal en el Dictamen 1/2008, en los términos siguientes (Fundamento Jurídico II):

> «En concreto, hay que hacer una especial referencia al dato relativo a la dirección IP. Este dato, en principio, se asocia a un ordenador, que puede tener un número variable o indeterminado de usuarios, pero también puede llegar a asociarse a una o más personas físicas concretas. A partir de la normativa aplicable a la protección de datos, citada, hay que mencionar el Dictamen 4/2007, de 20 de junio, sobre el concepto de datos personales, elaborado por el Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE. En ese dictamen, el Grupo considera las direcciones IP como datos sobre una persona identificable. En concreto, y como ya se había considerado en el anterior Documento de trabajo del Grupo, "Privacidad en Internet: enfoque comunitario integrado de la protección de datos en línea", de 21 de noviembre de 2000, los proveedores de acceso a Internet y los administradores de redes locales pueden identificar por medios razonables a los usuarios de Internet a los que han asignado direcciones IP, ya que registran sistemáticamente la fecha, hora, duración y dirección IP dinámica asignada [...].»

Por consiguiente, aunque a la dirección IP no se le puede atribuir, considerada aisladamente, la consideración de dato personal, sí debería tener esta consideración en todos aquellos casos en los que pueda hacer identificable a una persona física determinada. Visto el contexto de la Instrucción, y su alcance en relación con los empleados de una organización concreta como es un Ayuntamiento, que serán identificables, se podría considerar la dirección IP como un dato de carácter personal.

En cualquier caso, aparte de las consideraciones hechas en relación con la dirección IP, teniendo en cuenta que cualquier información sobre personas físicas identificadas o identificables tiene que ser calificada como dato de carácter personal y, por tanto, sometida a la LOPD, es evidente que el mantenimiento de la información derivada de

estos rastros, previsto en el artículo 5.2 de la Instrucción, afecta a datos considerados de carácter personal. Si tenemos en cuenta que los diferentes supuestos de rastreo explicitados en el artículo 5.2 de la Instrucción pueden contener en conjunto datos de carácter personal, y que incluso se puede dar un perfil sobre comportamiento de personas concretas, es evidente que se está generando un tratamiento de datos personales, a efectos del artículo 3 c) de la LOPD.

También debemos tener en cuenta que, si bien es cierto que el funcionamiento de los SI comporta que se guarden de forma automática ciertos registros, no es éste el supuesto al que se refiere la Instrucción, sino que de la redacción del artículo 5.2 se deduce una decisión del Ayuntamiento de conservar la información referida, para dar cumplimiento a las finalidades de control de la Instrucción; decisión que comporta un tratamiento de datos personales, a efectos de la LOPD.

Visto que el artículo 5.2 de la Instrucción establece claramente que «se mantendrán» determinados rastros que, como ha quedado dicho, comportan el tratamiento de datos personales, para el cumplimiento de las finalidades de la Instrucción, será necesaria la creación del correspondiente fichero o ficheros de datos personales por parte del Ayuntamiento, en tanto que responsable del tratamiento. La estipulación del artículo 5.2 comporta la conservación y el tratamiento de datos personales, y, por consiguiente, dicho tratamiento debe ajustarse a lo que disponen la LOPD (artículo 20) y el RLOPD (artículo 54), en cuanto a la creación de ficheros, y a la Ley 5/2002, de la Agencia, en cuanto a la inscripción correspondiente en el Registro de Protección de Datos de Cataluña.

Se hace notar que el artículo 5.2 es inconcreto en su última referencia, relativa a «cualquier otro registro que se requiera para garantizar el buen uso de los sistemas». En este sentido, no se da información concreta a los usuarios sobre qué tipo de registro o información se puede rastrear. Como ya se ha dicho ampliamente, la información que se da a los usuarios por parte de los responsables —en este caso, el Ayuntamiento— en relación con el uso correcto de los SI y las consecuencias de dicho uso, tiene una importancia especialmente relevante, por lo que sería recomendable una mayor concreción en este punto.

Respecto a los usuarios que pueden resultar afectados por el rastreo establecido en el artículo 5.2 de la Instrucción, no se da información concreta, por lo que los usuarios podrían ser todos los empleados del Ayuntamiento, o bien se podría configurar un rastreo sólo en relación con determinados usuarios, en atención a varios criterios.

Finalmente, cabe señalar que no se dispone de información en relación con el tiempo de conservación o mantenimiento de los rastros de uso de aplicativos y sistemas. En este sentido, en relación con los datos personales tratados, se deberá tener en cuenta que la LOPD exige su cancelación cuando el tratamiento de datos ha dejado de ser necesario para la finalidad que lo justifica (artículo 4.5 de la LOPD). Además, la cancelación da lugar al bloqueo, y los datos sólo se tienen que conservar en los casos previstos en el artículo 16 de la LOPD. A efectos de concretar el tiempo de conservación adecuado, se debería tener en cuenta que, con carácter general, no parece justificado mantener o guardar rastros respecto al uso de SI, concretamente, los datos personales que se deriven de ello, de forma indefinida, a menos que la finalidad legítima lo justifique. Por lo tanto, el Ayuntamiento deberá tener en cuenta lo establecido en la LOPD en cuanto al tiempo de conservación de información asociada directa o directamente a personas físicas usuarias de sus SI, en relación con las estipulaciones del artículo 5.2 de la Instrucción.

Por todo ello, se formulan las siguientes

Conclusiones

Los datos de carácter personal que trata el Ayuntamiento en aplicación de la Instrucción objeto de consulta se encuentran sometidos a la protección específica de la normativa de protección de datos, concretamente, de la LOPD, y, por consiguiente, las estipulaciones de la Instrucción deben respetar dicha normativa e interpretarse de acuerdo con los principios y garantías que en ella se establecen.

El artículo 4 de la Instrucción —«[...] la información contenida [en los sistemas de información municipales] son propiedad del Ayuntamiento [...]»— se tiene que interpretar teniendo en cuenta el concepto de afectado o interesado (artículo 3 e) de la LOPD), y los principios y obligaciones que para el Ayuntamiento se derivan de la normativa de protección de datos, a fin de respetar la autodeterminación informativa del interesado; específicamente, la necesidad de requerir el consentimiento del titular, en su caso, y la posibilidad de ejercer los derechos ARCO.

En aplicación del principio de calidad (artículo 4 de la LOPD), las tareas de mantenimiento y comprobación del correcto uso de las herramientas de trabajo que el Ayuntamiento pone a disposición del personal, realizadas por el personal técnico informático, deben servir única y exclusivamente para garantizar el normal funcionamiento de los sistemas, para la detección de incidencias y para solucionarlas convenientemente.

El legítimo ejercicio de control de la empresa sobre las herramientas citadas, con las finalidades establecidas en el artículo 5.2 de la Instrucción, se tiene que mantener en los términos establecidos en el marco normativo aplicable y en la jurisprudencia, a fin de asegurar el respeto de los derechos fundamentales de los trabajadores.

El artículo 5.2 de la Instrucción establece el mantenimiento de determinados rastros que comportan el tratamiento de datos personales para el cumplimiento de las finalidades de control establecidas en la Instrucción, y, por consiguiente, será necesaria la creación del correspondiente fichero o ficheros de datos personales por parte del Ayuntamiento, en tanto que responsable del tratamiento, a efectos de lo que disponen la LOPD (artículo 20) y el RLOPD (artículo 54), y la inscripción correspondiente en Registro de Protección de Datos de Cataluña.