El derecho a la protección de datos en el ámbito laboral

PID_00248573

Ferran Camas Roda

Tiempo mínimo de dedicación recomendado: 2 horas

Universitat Oberta de Catalunya

Los textos e imágenes publicados en esta obra están sujetos –excepto que se indique lo contrario– a una licencia de Reconocimiento-NoComercial-SinObraDerivada (BY-NC-ND) v.3.0 España de Creative Commons. Podéis copiarlos, distribuirlos y transmitirlos públicamente siempre que citéis el autor y la fuente (FUOC. Fundación para la Universitat Oberta de Catalunya), no hagáis de ellos un uso comercial y ni obra derivada. La licencia completa se puede consultar en http://creativecommons.org/licenses/by-nc-nd/3.0/es/legalcode.es

Índice

Introducción

El derecho a la protección de datos es un derecho fundamental autónomo que tiene su anclaje jurídico en el artículo 18.4 de la Constitución española (en adelante, CE), cuyo objeto es otorgar un poder de control a todo sujeto sobre sus datos personales.

La autonomía del derecho a la protección de datos lo es con respecto al derecho fundamental de intimidad personal y familiar reconocido en el artículo 18.1 CE. Fue la Sentencia del Tribunal Constitucional (en adelante, STC) número 292/2000, de 30 de noviembre de 2000, la que consolidó dicha diferenciación sobre el objeto de ambos derechos fundamentales al decir que, mientras el de intimidad busca proteger frente a cualquier invasión que pueda realizarse en dicho ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad, el de protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado. Más aún, mientras el contenido del derecho a la intimidad confiere a la persona el poder jurídico de imponer a terceros el deber de abstenerse de toda intromisión a su esfera íntima, el de protección de datos concede a su titular un haz de facultades que trasladan a los demás unos deberes «de hacer», principalmente, el derecho a que se requiera previo consentimiento para la recogida y uso de datos personales, el derecho a saber y a ser informado sobre el destino y uso de esos datos y el derecho a acceder, rectificar y cancelar esos datos, en definitiva, el poder de disposición sobre los datos personales (que van más allá de los estrictamente íntimos).

El desarrollo de este derecho fundamental se encuentra recogido en la Ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, complementada por el Real decreto 1720/2007, de 21 de diciembre. La Ley orgánica 15/1999 supuso la transposición al ordenamiento español de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

En relación con el ámbito laboral, debe comentarse que esta normativa protectora no es aplicable a los tratamientos de datos referidos a personas jurídicas y, como añade el Real decreto 1720/2007, tampoco a «los ficheros que se limiten a incorporar los datos de las personas físicas que presten sus servicios en aquellas, consistentes únicamente en su nombre y apellidos, las funciones o puestos desempeñados, así como la dirección postal o electrónica, teléfono y número de fax profesionales». Es decir, la normativa española, en su fase actual, no afecta a determinados datos que vinculan un sujeto con la empre-

sa-persona jurídica en la que presta sus servicios (nombre y apellidos del empleado en atención al cargo desempeñado en la empresa, dirección empresarial en el que aquel resulta localizable, etc.), pero atención, al contrario que aquellos datos, sí que entran dentro del ámbito de aplicación de la legislación española el tratamiento que la empresa realice de los datos del personal que bajo su régimen de organización y dirección trabaje para ella.

En este marco laboral, a los empleadores les resulta de aplicación los parámetros en los que se asienta la normativa española de protección de datos, principalmente los siguientes:

1) La regla general de la exigencia de consentimiento del afectado para tratarlos, excepto cuando se recaben con ocasión de la celebración de un contrato o precontrato o de la existencia de una relación laboral de la que sea parte el afectado y sean necesarios para su mantenimiento o cumplimiento, como se verá posteriormente.

2) La posibilidad de no prestar el consentimiento ante aquellos datos que son especialmente sensibles como la ideología, la religión o las creencias.

3) La imposibilidad de recabar datos que hagan referencia al origen racial, a la salud y a la vida sexual a no ser que cuando, «por razones de interés general, así lo disponga una ley o el afectado consienta expresamente». Asimismo, y como referentes principales de este marco regulatorio, debe traerse a colación el deber de los responsables de informar a los afectados del tratamiento de sus datos de carácter personal a través de un medio que permita acreditar su cumplimiento, debiendo conservarse mientras persista el tratamiento de los datos del afectado.

Esta legislación deberá, no obstante, adaptarse en un futuro cercano a lo dispuesto por la normativa adoptada por la Unión Europea en materia de protección de datos, en especial en materia laboral, como va a verse posteriormente.

Para empezar, debe mencionarse la Carta de los Derechos Fundamentales de la Unión Europea, cuyo artículo 8 reconoce el derecho de toda persona a la protección de los datos de carácter personal que le conciernan. También establece los principios básicos que presiden este derecho, particularmente el de que los datos personales se traten de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Además, se incluye el derecho a acceder a los datos recogidos que conciernan a la persona y a obtener su rectificación. El precepto finaliza estableciendo que el respeto a dichas normas de protección de datos estará sujeto al control de una autoridad independiente.

Al amparo de aquel reconocimiento al máximo nivel europeo, la norma que regula directamente el derecho de protección de datos y que resulta plenamente vinculante en España, en concreto a partir de mayo de 2018, es el Regla-

mento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

Del régimen de protección de datos recogido en el Reglamento 2016/679 resultan de interés centrar este estudio en tres cuestiones: uno, lo que cabe considerar como datos personales; dos, el tratamiento que se les debe otorgar y, en tercer lugar, como uno de los elementos de más importancia en la norma: la obtención del consentimiento para que sean tratados.

En primer lugar, la norma reglamentaria europea entiende de manera ciertamente amplia lo que deben considerarse como datos personales, al definirlos como «toda información sobre una persona física identificada o identificable ("el interesado")», resultando que debe considerarse como persona física identificable toda aquella «cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona» (art. 4.1 del Reglamento 2016/679). La evolución judicial de esta cuestión ha sido la de ratificar un concepto amplio sobre lo que se considera como datos personales, como por ejemplo lo prueba la Sentencia del Tribunal de Justicia de la Unión Europea (en adelante, TJUE), de 19 de junio de 2014, C-683/13, que consideró que el registro del tiempo de trabajo, que incluye una indicación para cada trabajador del inicio y del final del trabajo y las interrupciones o descansos correspondientes, coincide con la definición de datos personales de la normativa europea.

En segundo lugar, en relación con el modelo de tratamiento de datos personales que regula el Reglamento, su objeto se centra en abarcar cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, «ya sea por procedimientos automatizados o no» (art. 4.2). En consecuencia, la protección dispensada lo es tanto con respecto a mecanismos basados en sistemas informáticos como los que no operen de esa forma. También el Tribunal de Justicia de la Unión Europea ha incluido como tratamiento de datos la recogida, organización, conservación, consulta y utilización de datos de tiempo de trabajo y descansos por el empleador, por un lado, o la conducta consistente en hacer referencia, en una página web, a diversas personas y en identificarlas por su nombre o por otros medios, como su número de teléfono o información relativa a sus condiciones de trabajo y a sus aficiones, por otro[1].

(1)Véase la Sentencia del TJUE de 30 de mayo de 2013, Asunto C-342/12, o de 6 de noviembre de 2003, Asunto C-101/01.

En tercer y último lugar, en relación con la cuestión del consentimiento para el tratamiento de datos personales, el Reglamento 2016/679 entiende por tal «toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción

afirmativa, el tratamiento de datos personales que le conciernen». Como se ha visto anteriormente, en el ámbito laboral el consentimiento del trabajador es un asunto espinoso ya que, en el marco de una relación laboral, ocupa una posición negociadora débil en relación con la parte empresarial y, por lo tanto, se propone equilibrar esa posición a través de las garantías necesarias para proteger que el trabajador preste su consentimiento libremente y no coartado por el contexto laboral o de empleo.

En este sentido, para enfatizar la importancia del valor de un consentimiento libre y no impuesto en materia de protección de datos en el ámbito laboral, la doctrina laboral se apoya, entre otras manifestaciones judiciales, en la Sentencia de la Corte Europea de Derechos Humanos de 12 de enero de 2016 (Caso Barbulescu contra Rumanía), en la que se recuerda que no por entrar en la instalación empresarial los trabajadores dejan apartado su derecho a la protección de datos personales en las puertas de la empresa. Para la sentencia, «las nuevas tecnologías hacen que entrometerse en la vida privada de los empleados sea tanto más fácil para el empleador y más difícil para el empleado detectarlo, riesgo este que se agrava por la desigualdad connatural de la relación laboral». Por esa razón, la Sentencia aboga por mantener un enfoque garantista del derecho de protección de datos centrado en el reconocimiento de los derechos humanos en el uso de internet en el puesto de trabajo, ya que ello puede garantizar un marco normativo interno transparente, una política de implementación consistente y una estrategia de ejecución proporcionada por los empresarios (véase un comentario sobre esta sentencia en Hugo Preciado, 2017).

Referencia bibliográfica

C. Hugo Preciado (2017). *El Derecho a la Protección de Datos en el Contrato de Trabajo*. Cizur Menor: Thomson Reuters.

Esta postura garantista para el trabajador se ha visto fortalecida por otra sentencia de la Corte Europea de Derechos Humanos en el mismo asunto (Barbulescu) de 5 de septiembre de 2017, en el que dicho tribunal ha atribuido al empresario diversos límites cuando pretenda vigilar la actividad del trabajador cuándo este utilice dispositivos electrónicos puestos a disposición por la empresa. En este sentido, la Corte Europea advierte, entre otros aspectos, que el trabajador deber estar informado de la posibilidad de control empresarial en el uso de los instrumentos de comunicación electrónicos, así como del alcance de dicho control; también se dice por dicho tribunal que el empresario debe disponer de razones legítimas que justifiquen el control y el acceso al contenido de las comunicaciones, partiendo de la base que si el objetivo perseguido por el empresario puede ser alcanzado utilizando medidas de control menos invasivas que el acceso al contenido de las comunicaciones, aquellas deberá usarlas con preferencia.

1. Principios de referencia derivados de la normativa europea para el tratamiento de datos en el ámbito laboral

Consciente de la importancia que tiene el tratamiento de datos en las relaciones de trabajo, el Reglamento 2016/679 dispone de una serie de reglas de interés que se convierten en marcos de referencia para la concreción posterior por los Estados miembros o por los propios interlocutores sociales, de los derechos y deberes que en materia de protección de datos se producen en el ámbito laboral.

1) Para empezar, y aunque no sea un imperativo dirigido específicamente a los empleadores, aunque sí los incluya, el artículo 25 regula la protección de datos «desde el diseño y por defecto». Como regula el precepto, «teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados». A ello, el precepto añade que el responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento.

Llevada esta regulación al ámbito de las relaciones laborales, particularmente la de protección de datos, «desde el diseño puede afirmarse que si un empleador atribuye dispositivos tecnológicos de trabajo a los empleados, las soluciones más *privacy-friendly* (respetuosas y con simpatía por la privacidad de las personas) deben ser seleccionadas si se trata de tecnologías de seguimiento. También debe ser tenida en cuenta en la adopción de estos instrumentos la minimización de los datos tratados (véase la opinión publicada por The Working Party, 2017).

Referencia bibliográfica

The Working Party [article 29 data protection working party], *Opinion 2/2017 on data processing at work*, Adopted on 8 June 2017.

2) También de un modo general, aunque con afectación al ámbito de las relaciones laborales, el artículo 35 del Reglamento europeo aborda el tema de la «evaluación del impacto relativo a la protección de datos». Como regula el precepto, cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe «un alto riesgo» para los derechos y libertades de las personas físicas, «el

responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales». Un ejemplo de ello puede ser el caso de la valoración sistemática y extensa de aspectos personales de personas físicas basados en procesamientos automatizados, incluyendo la elaboración de perfiles (como después se tratará), y en función de los cuales se tomen decisiones que afectan legalmente o de forma significativa a la persona física. En este sentido, si la evaluación del impacto relativo a la protección de datos que se realiza indica que los riesgos identificados no pueden ser abordados suficientemente por el controlador, es decir, que los riesgos residuales permanecen altos, el responsable del tratamiento debe consultar a la autoridad de control antes del comienzo del procesamiento (art. 36.1) (The Working Party, 2017).

3) Ya de forma específica en materia de relaciones de trabajo, el artículo 88 del Reglamento europeo, que lleva por título «Tratamiento en el ámbito laboral», tiene por objeto aumentar la protección de los derechos y libertades de los trabajadores ante el tratamiento de sus datos personales por los empleadores para los que prestan sus servicios. En este sentido, el precepto otorga a los Estados miembros la posibilidad (por tanto, no la obligación) de que, a través de disposiciones normativas o de convenios colectivos pactados entre los empleadores y la representación de los trabajadores, se establezcan normas más específicas en materia de protección de datos que las recogidas en el Reglamento 2016/679.

Esta posibilidad de mayor especificación de las normas se hace con el objeto de garantizar la protección de los derechos del trabajador, no para disminuir el alcance de las reglas que estén incluidas en el Reglamento. Por tanto, la normativa aprobada por el Estado español o los pactos colectivos que puedan alcanzar las partes sociales podrán regular aspectos no previstos en el Reglamento, o concretar aquellos que resulten incluidos, pero bajo la óptica de salvaguardar el derecho a la protección de datos del trabajador.

De hecho, el Reglamento dispone de una serie de aspectos en los cuales se podrán establecer normas internas más específicas, sin perjuicio de que en cualquiera otros en materia laboral pueda hacerse lo mismo. He aquí aspectos que, a modo ejemplificativo han merecido una atención especial por la norma europea:

a) La contratación de personal.

b) La ejecución del contrato laboral, incluido el cumplimiento de las obligaciones establecidas por la ley o por el convenio colectivo,

c) La gestión, planificación y organización del trabajo.

d) La igualdad y diversidad en el lugar de trabajo.

e) La salud y seguridad en el trabajo.

f) La protección de los bienes de empleados o clientes.

g) El ejercicio y disfrute, individual o colectivo, de los derechos y prestaciones relacionados con el empleo.

h) La extinción de la relación laboral.

La adopción de dichas normas deberá incluir, como al efecto advierte el apartado 2 del artículo 88 que se está comentando, «medidas adecuadas y específicas para preservar la dignidad humana de los interesados, así como sus intereses legítimos y sus derechos fundamentales». Las normas que se adopten deberán salvaguardar la dignidad del trabajador, imposibilitando que el mismo pueda ser considerado una mera mercancía o dato, así como respetar sus intereses legítimos derivados de su relación laboral y sus derechos fundamentales, los cuales obviamente siempre deben ser reconocibles en el puesto de trabajo.

El Reglamento considera que, para cumplir con dichos compromisos, se deberá prestar atención a tres mecanismos propios de la gestión de datos en el ámbito de las relaciones laborales: en primer lugar, la necesidad de prestar atención a la transparencia en el tratamiento de los datos personales; en segundo lugar, tomar en consideración los aspectos relativos a la transferencia de los datos personales dentro de un grupo empresarial o de una unión de empresas dedicadas a una actividad económica conjunta; y finalmente, tener en cuenta los sistemas de supervisión en el lugar de trabajo.

4) Uno de los deberes impuestos por el Reglamento 2016/679 a los responsables del tratamiento de datos es el de llevar un registro de las actividades que realicen con tal motivo, y respecto de los encargados, de llevar un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta del responsable. El artículo 30 de la norma reglamentaria prevé que estas obligaciones no se apliquen a ninguna empresa ni organización que emplee a menos de 250 personas, por lo tanto, sí resultarán aplicables a las que superen dicha cantidad. No obstante, aun teniendo empleados a menos de 250 trabajadores, sí se deberá llevar el registro de actividades y de categorías de actividades cuando el tratamiento pueda entrañar uno de los siguientes aspectos: que suponga un riesgo para los derechos y libertades de los interesados; o que el tratamiento no sea ocasional; o bien que incluya datos personales relativos a condenas e infracciones penales conforme a lo que establece el artículo 10 del propio Reglamento; o bien, y esto es muy importante en el ámbito empresarial, que el tratamiento «incluya categorías especiales de datos personales indicadas en el artículo 9, apartado 1».

Se ha de traer a colación que el artículo 9.1 del Reglamento 2016/679 establece una prohibición general sobre el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o

filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida u orientación de una persona física. Ahora bien, dicha prohibición no resulta aplicable cuando el tratamiento sea necesario «para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice el derecho de la Unión de los Estados miembros o un convenio colectivo con arreglo al derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado».

Por lo tanto, cualquier empresa con una plantilla menor de 250 trabajadores que disponga el tratamiento de solo una de las categorías mencionadas, por ejemplo la afiliación sindical, si se ha aceptado dicho tratamiento por la legislación europea o española o un convenio colectivo con la previsión de garantías adecuada, deberá llevar a cabo el registro de sus actividades de tratamiento de datos.

5) En último lugar, sin perjuicio del reconocimiento por el Reglamento 2016/679 de que todo interesado plantee las acciones administrativas o judiciales que considere adecuadas para el amparo de sus derechos, se le reconoce también el derecho a presentar una reclamación ante una autoridad de control en materia de protección de datos. La competencia para conocer de su derecho será la correspondiente al Estado miembro en el que el interesado tenga su residencia habitual, pero también el lugar de trabajo o lugar de la supuesta infracción. De esta forma, el lugar de trabajo del interesado se erige en uno de los criterios que aquel puede escoger para atribuir la competencia a la autoridad de control en el conocimiento de las reclamaciones que aquel interponga por la infracción a las disposiciones del Reglamento europeo[2].

[(2)]Véase su artículo 77.

2. El derecho a la protección de datos en las fases previas a la contratación laboral

Con anterioridad a la concertación de la relación laboral entre parte trabajadora y parte empresarial, una primera situación de tratamiento de datos puede producirse cuando el demandante de empleo lleva a cabo gestiones para obtenerlo, ya sea con la empresa en la que quiere prestar servicios, ya sea con otra entidad interpuesta especializada en intermediación, selección o colocación laboral.

En estos casos, debe empezar por afirmarse que respecto de los datos facilitados por el solicitante de empleo no es exigible su consentimiento para ser tratados por la entidad que corresponda a los efectos de su colocación laboral, si dicho tratamiento es necesario para la aplicación a petición del interesado de medidas precontractuales de carácter laboral[3].

(3)Interpretación que surge de los arts. 6.2 de la Ley 15/99 en relación con el art. 10.3b) del Reglamento 1720/2007.

Aunque no es preciso el consentimiento, sí que resulta fundamental en estos primeros estadios de carácter previo a la relación laboral el cumplimiento del deber de información del responsable en el tratamiento de datos.

En este sentido, si un solicitante de empleo acude a presentar su candidatura, previa convocatoria por una empresa de selección, por un servicio de colocación laboral o por la propia empresa que necesita cubrir puestos de trabajo, el primer deber a cumplir por todas ellas es el de informar del tratamiento que van a dar a los datos de carácter personal del candidato. En el caso de que el solicitante de empleo tome la iniciativa en la búsqueda de empleo, por ejemplo, la presentación de su currículum sin que se le haya previamente solicitado, se deben disponer de procedimientos de información al demandante de trabajo por los cuales se pueda confirmar que este conoce las condiciones en las que se desarrollará el tratamiento de los datos que figuran en su solicitud.

En este marco, la Agencia Española de Protección de Datos (en adelante, AEPD) ha dispuesto, en relación con la recepción de currículums por las empresas que, aunque no se incorporen a un fichero informático y solo se impriman y se guarden ordenados, esa práctica constituye tratamiento de datos (véase la Guía sobre protección de datos en las relaciones laborales de 2009 o la Recomendación sobre selección de personal a través de internet de 2005). La AEPD ha dispuesto, en relación con la gestión de currículums, que:

1) Cuando sea conveniente y se cuente con recursos para ello, se dispongan de los modelos de impresos tipo para la formalización del currículum y de un procedimiento de formalización y entrega de los mismos por los candidatos;

2) Si el currículum se remitió por correo postal o electrónico, y se cuenta con una dirección electrónica facilitada por el propio interesado, pueda remitírsele información por ese medio solicitando confirmación de la recepción y condicionando el tratamiento de los datos al acuse de recibo.

3) Si el currículum se presentó en un mostrador u oficina de atención, el solicitante de empleo debería ser informado allí mismo por cualquier medio que acredite el cumplimiento de este deber, como por ejemplo carteles, documentos de acuse de recibo y, en general, cualquier otro medio que garantice y permita probar el cumplimiento del deber de información.

Finalmente, se recuerda por la AEPD que, en casos de grupos de empresas o de cualquier otra fórmula de colaboración empresarial, debe tenerse en cuenta que la cesión de los datos contenidos en el currículum o del propio documento debe contar con el consentimiento del candidato; a modo de conclusión, cabe recordar también que si el currículum se solicita a través de cualquier oferta de empleo, conviene incorporar la información que regula la legislación en la misma oferta.

Así, el contenido de la información que deberá facilitarse a los demandantes de empleo-candidatos a cubrir una oferta incluirá de forma general la existencia de ficheros de datos de carácter personal, de la finalidad de la recogida de estos y de los destinatarios de la información; del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas; de las consecuencias de la obtención de los datos o de la negativa a suministrarlos; de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición; de la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

Finalmente, los currículums en soporte papel y las valoraciones de los mismos, una vez terminado el proceso selectivo, deberían ser destruidos. Muestra de ello es la Resolución R/00029/2003 de la AEPD, que sanciona a una empresa por el hallazgo por parte de una periodista de unas 250 solicitudes de empleo dirigidas a dicha empresa, que habían sido desechadas en un cubo de la basura y en las que se incluían comentarios despectivos sobre los solicitantes. Entre los fundamentos jurídicos que llevaron a imponer la correspondiente sanción a la empresa se encuentra el artículo 5 de la Ley orgánica 15/99, ya que ni en las solicitudes de empleo que debían cumplimentar los candidatos ni en los cuestionarios que se les hacía confeccionar en las entrevistas, no se informaba de modo expreso, preciso e inequívoco de ninguno de los extremos recogidos en aquel precepto legal; también cabe citar que en el caso se incumplió el artículo 9 de la Ley orgánica en relación con otras disposiciones del reglamento que la desarrolla, que impone 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; en el caso, la empresa no había implementado ningún inventario en el que se

detallasen todos y cada uno de los soportes informáticos que se reciban del exterior (por ejemplo, la recepción de currículums remitidos por los interesados en participar en el proceso de selección) o que saliesen de la propia empresa.

2.1. Sobre la elaboración de perfiles en procesos de selección

Un aspecto especialmente importante en los procesos de selección es la realización de pruebas selectivas y la evaluación por las empresas de una «elaboración de perfiles» a partir de los datos suministrados por los solicitantes de empleo.

Se considera que existe una elaboración de perfiles, en todo sistema de tratamiento automatizado de datos personales, consistente en utilizar dichos datos para evaluar determinados aspectos personales de una persona física, en particular, para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física.

De forma general, la normativa europea de protección de datos reconoce el derecho del interesado a no ser objeto de una decisión basada únicamente en el tratamiento automatizado que produzca efectos jurídicos en él o le afecte significativamente de modo similar. No obstante, este derecho no resulta aplicable cuando la elaboración de perfiles resulte necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento. En consecuencia, a los efectos de la selección o contratación laboral, la decisión final de la empresa puede hacerse depender exclusivamente de la elaboración automatizada de perfiles, es decir, de la disposición y el cruce automatizado de los datos del solicitante para conocer características propias de su personalidad[4].

(4)Véase lo que sobre elaboración de perfiles establece el artículo 22, apartados 1 y 2, del Reglamento europeo 2016/679.

El único condicionamiento que se impone es que el responsable del tratamiento adopte las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, como mínimo el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión. Por tanto, las empresas de selección de personal o el propio empresario pueden elaborar perfiles de forma únicamente automatizada a los efectos de contratación. En su ejecución, la norma reconoce la necesidad de que el responsable intervenga de forma mínima, así como la aceptación del derecho del solicitante de empleo a expresar su punto de vista y a impugnar la decisión que finalmente se tome[5].

(5)Véase el art. 22.3 del Reglamento europeo.

2.2. Cuestiones de interés de las pruebas selectivas de acceso al empleo

Por lo que hace referencia a las pruebas selectivas, se ha de partir de la base de que el derecho fundamental a la intimidad personal o familiar resulta un primer filtro para todo solicitante de empleo sobre la imposibilidad de manifestarse sobre cuestiones que entran en su ámbito privado sin relación alguna con la ocupación de un trabajo, como pueden ser el estado civil o el embarazo.

Respecto de la práctica consistente en pedir referencia a antiguos empleadores, se debe recordar la obligación de cancelar los datos objetos de tratamiento cuando los mismos no son precisos y la necesidad del consentimiento del interesado para que la petición de dichas referencias se lleve a cabo. En relación con la ideología, religión o creencias, nadie puede ser obligado a declarar sobre ello, y en caso de pedir el consentimiento para realizarlo, se impone la necesidad de advertir al interesado sobre su derecho a no hacerlo[6].

[6]Véase el artículo 7 de la Ley orgánica 15/1999.

Con respecto al tratamiento de datos especialmente sensibles como son el estado de salud en el proceso selectivo, puede exigirse al trabajador que se someta a reconocimientos médicos en aspectos que puedan guardar relación con el trabajo a realizar, con la correspondiente garantía de la obligación de secreto por el profesional sanitario correspondiente. Lo que no puede hacer el empresario es recabar directamente los datos que se deriven del reconocimiento médico del trabajador, sino que deberá acceder a los que le proporcione el profesional sanitario, limitados a la constatación de apto/no apto para los requerimientos del puesto de trabajo, o también la declaración de la necesidad de adaptación del mismo al trabajador.

Lectura recomendada

Véase lo que sobre estas cuestiones dice la Guía de la AEPD: *La protección de datos en las relaciones laborales*, de 2009.

Finalmente, en relación con la posible realización de las llamadas listas negras o bases de datos ocultas cuyo objeto es obtener información de trabajadores con fines perjudiciales para estos (por ejemplo, para obstaculizar que quienes puedan estar incluidos en dichos listados sean contratados laboralmente en otras empresas), además de estar prohibidas por la legislación de empleo, en materia estricta de protección de datos la AEPD ha recordado su ilicitud por cuanto en dichos casos no hay consentimiento libre de los trabajadores para incluir sus datos en dichas bases de datos.

En todo caso, los datos obtenidos en el marco de un proceso de selección de personal no pueden ser utilizados como base de datos de clientes, para hacer ofertas de productos o servicios de la empresa a los candidatos. Cualquier utilización de los datos obtenidos para una finalidad distinta de la obtenida precisa el consentimiento del interesado.

3. El derecho a la protección de datos en el inicio, desarrollo y extinción de la relación laboral. Control de la actividad laboral

La confección del contrato de trabajo por escrito es un instrumento adecuado para informar al trabajador sobre el tratamiento que se realizará respecto de sus datos personales a todos los efectos relacionados con su prestación laboral. Por lo tanto, resulta válida la práctica de la empresa que al contrato de trabajo le adjunta la firma de un anexo en el que se traslada información al trabajador sobre el uso que debe dar a internet y al correo electrónico en la empresa. Así, la firma del contrato y de su anexo es uno de los medios a través de los cuales el empresario puede probar dicha circunstancia informativa.

El debate se centra más bien en que, si además de ser instrumento de información, el contrato laboral puede ser oportuno para incluir también el consentimiento del trabajador para el tratamiento de sus datos, es decir, si en el mismo pacto laboral que da inicio a la relación laboral puede incluirse, además del conjunto de derechos y deberes de carácter estrictamente laboral al que se vinculan las partes, el consentimiento del trabajador para que la empresa trate sus datos personales para cuestiones que exceden del trabajo concertado por el trabajador (por ejemplo, que al trabajador se le remitan ofertas publicitarias, o se prevea la suscripción de seguros de vida no relacionados con la prestación laboral, para lo cual se le pida correo electrónico personal o el número de móvil). Incluir estos aspectos en el contrato de trabajo de forma que, con su firma, el trabajador diese su consentimiento a que sus datos fueran tratados para cuestiones no relacionadas directamente con su trabajo invalidaría este clausulado contractual (es decir, su consentimiento sobre el tratamiento de datos), pero no todo el contrato laboral en sí mismo considerado[7].

[(7)]Véase el artículo 9.1 del Real decreto legislativo 2/2015 Real decreto legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del estatuto de los trabajadores, en adelante, LET.

En todo caso, si durante el desarrollo de la relación laboral se produce cualquier cambio que afectase a los datos del trabajador del que no fue informado en el momento de su contratación, la empresa debe realizarlo sin dilación indebida. Así por ejemplo, si el trabajador notifica a la empresa que se ha afiliado a un sindicato y solicita que se le descuente de su nómina la correspondiente cuota sindical, la empresa deberá informarle del tratamiento que realizará por este motivo. Si, por el contrario, es la empresa quien decide la instalación de un nuevo sistema de control, también deberá comunicarlo a los trabajadores ya que, en caso contrario, aquel devendría nulo o sin efectos.

Por un lado, en el caso de que la empresa establezca un sistema interno de denuncias o *whistle-blowing*, es decir, la creación de buzones internos, digitales o no, a través de los cuales los empleados denuncian conductas ilícitas de otros empleados, dichos mecanismos de control serán conformes a la normativa de protección de datos si se han llevado a cabo por la compañía los deberes pre-

vios de información sobre la existencia de estos sistemas, el tratamiento de los datos que conlleva la formulación de una denuncia, de las consecuencias que para el denunciado puede comportar este hecho y, naturalmente, si la gestión de estos sistemas de denuncias se han externalizado. Respecto de estos mecanismos, la tendencia mayoritaria es a que las denuncias no sean anónimas, sino que el denunciante aparezca identificado, manteniendo las debidas garantías de confidencialidad respecto de aquel.

Respecto de los controles empresariales basados en el uso de las tecnologías audiovisuales o digitales de vigilancia, lo primero que debe confirmarse es el derecho de las empresas a utilizarlas respetando, en el margen que corresponda, los derechos fundamentales que al trabajador también le corresponden, como el de intimidad personal o el de protección de datos. Para implantar estos mecanismos no es obligado que el empleador deba contar con el consentimiento de los trabajadores, ya que la finalidad de su instalación y tratamiento estarían enfocados al control estricto de la actividad laboral de los trabajadores, pero en cambio sí es necesario que estos resulten previamente informados de su puesta en práctica. En este caso, derivado de la evolución judicial sobre esta temática, debe confirmarse que la información a los trabajadores ha de ser clara en lo que respecta a la política de la empresa en cuanto a utilización del correo electrónico e internet, describiendo de forma pormenorizada en qué medida los trabajadores pueden utilizar los sistemas de comunicación de la empresa con fines privados o personales (véase, sobre este particular, Camas Roda, 2004).

Referencia bibliográfica

F. Camas Roda (2004). «La intimidad y la esfera privada del trabajador ante las nuevas modalidades de control y vigilancia de la actividad laboral». En: M. R. Alarcón Caracuel; R. Esteban Legarreta (coords.). *Nuevas tecnologías de la Información y la Comunicación y Derecho del Trabajo* (págs. 161-186). Alicante: Editorial Bomarzo.

Por lo que respecta a los medios de control de la prestación laboral del trabajador mediante la utilización de cámaras de videovigilancia, aparecen dos preguntas que son necesarias responder: en primer lugar, si es posible implantarlas en la empresa y cómo hacerlo; en segundo lugar, en qué medida esa vigilancia puede afectar a la normativa de protección de datos.

Respecto de la primera pregunta, debe afirmarse que la tendencia judicial tiende a validar la instalación permanente de cámaras de vigilancia siempre que no se implanten en espacios íntimos o de privacidad del trabajador en la empresa y que aquellos hayan sido previamente informados de ello. Por tanto, las cámaras de vigilancia pueden implantarse tanto en el lugar en el que trabaja el empleado como aquellas restringidas a terceros de la empresa pero a las que acudan los trabajadores del establecimiento, aunque solo sea para tomar un refrigerio. La vigilancia en estos casos se admite si la empresa puede argüir argumentos para ello, como la protección del patrimonio empresarial, y siempre que los trabajadores lo sepan, por ejemplo, por existir carteles indicadores de ello[8].

[8]Véase, por ejemplo, la STS de 17 de julio de 2016. Núm. de recurso: 3233/2014.

Por lo que se refiere a la segunda cuestión, es decir, el cumplimiento del derecho a la protección de datos personales por la instalación de aparatos receptores de imágenes en el lugar de trabajo, el Tribunal Constitucional ha dictami-

nado, en su Sentencia 39/2016, de 3 de marzo de 2016, dos cuestiones que son de interés: la búsqueda de un consentimiento «expreso» del trabajador para realizarlo y la información a suministrarle.

Por lo que se refiere al consentimiento, el Tribunal ha manifestado que no se requiere de ningún consentimiento «expreso» o específico del trabajador para el tratamiento de las imágenes que han sido obtenidas a través de las cámaras instaladas en la empresa con la finalidad de seguridad o control laboral, ya que se trata de una medida dirigida a controlar el cumplimiento de la relación laboral y es conforme con el artículo 20.3 del texto refundido de la Ley del estatuto de los trabajadores, que establece que

> «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».

Para el TC, el consentimiento se entiende implícito en la propia aceptación del contrato que implica reconocimiento del poder de dirección del empresario. Por lo demás, el hecho de que no se exija consentimiento expreso o específico para tratar los datos necesarios para el cumplimiento de la relación laboral abarca también los datos personales obtenidos por el empresario al controlar el cumplimiento de las obligaciones laborales del trabajador.

En referencia a la información a suministrar al trabajador, el Tribunal Constitucional ha avalado, en su sentencia de 3 de marzo de 2016, que puede ser suficiente para respetar el derecho fundamental a la protección de datos previsto en el artículo 18.4 de la Constitución española el cumplimiento de dicha obligación informativa a través de la colocación de distintivos en lugares visibles para el trabajador, que puedan mostrar que estos sabían de la existencia de las cámaras y la finalidad para la que habían sido instaladas.

Finalmente, en relación con la fase de extinción de la relación laboral, los elementos clave a considerar son los mecanismos de conocimiento de datos por representantes de los trabajadores en las fases instructoras del despido, posteriormente su bloqueo y finalmente su cancelación. Ejemplo del primer asunto es la fase de consultas en el ámbito de los despidos colectivos, donde los representantes de trabajadores deben conocer la lista nominal de trabajadores en la empresa y los criterios de selección para ser despedidos. En estos supuestos, se entiende que es posible que se utilicen estos datos en la fase de consulta con los representantes de los trabajadores sin consentimiento de los interesados, pues los datos son necesarios para el mantenimiento o extinción de la relación laboral, así como para la negociación sobre la reducción del número de afectados por el despido.

De hecho, la AEPD considera que, cuando los negociadores en un despido colectivo obtienen los datos personales de los trabajadores a los fines de negociar este procedimiento empresarial, se da el supuesto establecido en el artículo 6

(9)Véase Resolución de archivo de actuaciones de la AEPD sobre el art. 51 de la LET.

de la LOPD referido a que no se requiere el consentimiento para el tratamiento de los datos cuando una ley habilita el mismo[9]. En función de esta actuación, la doctrina iuslaboralista manifiesta que también en una modificación sustancial de las condiciones de trabajo de carácter colectivo, en un procedimiento de reducción de jornada o de suspensión de contratos, o en un procedimiento de inaplicación de convenios colectivos, si los negociadores obtienen los datos personales de los trabajadores a los fines de tramitar la medida colectiva en cuestión, se hallan amparados legalmente a no requerir el consentimiento de los trabajadores a los fines de negociar la medida colectiva en cuestión, tanto en función de la propia Ley del estatuto de los trabajadores que regula estos procedimientos como del derecho fundamental a la negociación colectiva y a la libertad sindical (Preciado, 2017).

Por otra parte, cuando finaliza la relación laboral, debe procederse al bloqueo de datos y a su cancelación. Cuando un empleado finaliza su relación contractual, cualquiera que sea la causa de ello, por propia voluntad o por un despido a voluntad de la parte empresarial, cesa también la causa que legitimaba el tratamiento de datos personales del trabajador por la empresa. Por esa razón, la primera consecuencia de ello es el bloqueo de los datos del empleado, es decir, la imposibilidad de que los mismos permanezcan inaccesibles a cualquier otro usuario o, como dice la doctrina estudiosa de esta temática, la puesta a disposición de dichos datos a disposición de las autoridades competentes (Preciado, 2017).

Referencia bibliográfica

C. Hugo Preciado (2017). *El Derecho a la Protección de Datos en el Contrato de Trabajo*. Cizur Menor: Thomson Reuters.

4. El derecho a la protección de datos en materia de prevención de riesgos laborales

Al igual que sucede con el tratamiento de datos en relación con la concertación de un contrato de trabajo y el desarrollo del haz de derechos y deberes laborales que vinculan a las partes, tampoco en materia de seguridad y salud laboral se exige un consentimiento específico para abordar datos de interés para dicha cuestión.

Se ha de partir de la base de que la normativa de prevención de riesgos laborales en España, plasmada principalmente en la Ley 31/1995, de 8 de noviembre, regula el derecho del trabajador a ser protegido de forma eficaz en relación con su seguridad y salud en el trabajo, y de forma correlativa la obligación del empleador de prevenir los riesgos laborales de forma general, pero también a través del cumplimiento de deberes específicos como son los de evaluar y planificar la actividad preventiva, organizar la prevención a través de los correspondientes recursos y servicios de prevención, informar y formar al trabajador en materia de riesgos laborales, dotarle de equipos de protección individuales y colectivos, vigilar su salud o atender a colectivos especialmente sensibles ante riesgos laborales.

De los citados, el aspecto que mayor conflictividad plantea es el de la vigilancia de la salud del trabajador, que la normativa de prevención establece como obligatoria para el empleador para dotarla, pero voluntaria para el trabajador en aceptarla. Es decir, de forma general el trabajador debe consentir la vigilancia de la salud ofrecida por la empresa. Las excepciones a esta regla general se dan en los supuestos en los que la realización de reconocimientos sea imprescindible para evaluar los efectos de las condiciones de trabajo sobre la salud de los trabajadores o para verificar si el estado de salud del trabajador puede constituir un peligro para el mismo, para los demás trabajadores o para otras personas relacionadas con la empresa o cuando así esté establecido en una disposición legal en relación con la protección de riesgos específicos y actividades de especial peligrosidad.

Ahora bien, tanto cuando el trabajador da su consentimiento a ser sometido a una vigilancia de la salud ante el ofrecimiento del empleador como cuando aquel debe pasar por dichas pruebas por venir así exigido por la legislación, quien debe realizarla son órganos específicos (nunca el propio empleador, sino el personal especialmente capacitado para ello de los servicios de prevención que disponga), así como también la información que recibirá el empleador sobre los resultados de la vigilancia será necesariamente limitada. La información que recibirá el empleador se ceñirá únicamente a hacer constar la aptitud o ineptitud del trabajador en materia de salud a los exclusivos efectos laborales para los cuales se haya realizado la vigilancia. La superación de esta estricta

información se admite de forma muy limitada, estrictamente para el cumplimiento de aquellas de sus obligaciones que desborden el contenido apto/no apto, por ejemplo, si debe adaptarse una pantalla de ordenador si se constatan problemas visuales. En este sentido, la Guía de la AEPD sobre protección de datos en las relaciones laborales de 2009 constata el hecho de que el deber del empresario de planificar la prevención de riesgos laborales en la empresa exige tener una relación detallada de los puestos de trabajo y de las personas que los ocupan, y por esa razón, deberá disponer de información sobre un conjunto de preguntas sobre los riesgos específicos del puesto cuya respuesta en muchas ocasiones dependerá de características personales o de salud del propio trabajador: ¿es alérgico a determinados elementos químicos?, ¿necesita ciertas condiciones de luminosidad o de tamaño de letra en la pantalla de su ordenador?, ¿es capaz de identificar con claridad una alarma acústica?

Por lo demás, los delegados de prevención en la empresa, que son los representantes de los trabajadores en el ámbito de la seguridad y salud laboral, también tienen acceso a datos personales sobre daños en la salud de los trabajadores solo para la finalidad de control y limitada a los datos estrictamente necesarios, entendiendo por tales los relativos a la gravedad y naturaleza de los daños. En todo caso, deberá guardar en particular el deber de confidencialidad respecto de los datos que en función de sus competencias de control disponga.

Los servicios de prevención acogidos por la empresa para ejecutar los deberes específicos de prevención que se le imputan por la normativa, en particular la vigilancia de la salud, que si son de carácter ajeno a la parte empleadora tienen la consideración de responsables del tratamiento de datos personales de los trabajadores, deben tener en cuenta cuestiones como el nivel de seguridad de los datos que tramitan, que será alto en aquellos casos en los que se incluyan datos de salud con identificación precisa de las enfermedades, traumatismos etc., o se gestionen historias de salud laboral. También deberían definir de modo preciso los perfiles de acceso a dichos datos, y finalmente deberán cumplir con lo previsto por la normativa de protección de datos en materia de historia clínica de los trabajadores, que impone la llevanza de la misma de forma exclusiva a los centros sanitarios o profesionales que realicen las actuaciones sanitarias en relación con el paciente, en este caso el trabajador que se somete a las pruebas que implican la realización de acciones de vigilancia de la salud.

5. El derecho a la protección de datos en el ámbito de las relaciones colectivas de trabajo

En el ejercicio de sus funciones de participación en la empresa y representación de los trabajadores, los organismos unitarios, el comité de empresa o los delegados de personal, o sindicales (secciones sindicales o delegados sindicales), están en disposición de acceder a datos personales de los trabajadores.

En el ejercicio de esas funciones, los representantes de los trabajadores pueden gestionar los datos de trabajadores en los tablones de anuncios a los que tienen derecho. Al realizarlo, los responsables del tratamiento de datos en el tablón de anuncios, y por tanto de las informaciones publicadas en el mismo, serán aquellos órganos que decidan sobre su uso y finalidad y sitúen materialmente la información en él. Dicha información en los tablones solo debe estar visible para aquellos a los que se dirige, los trabajadores; por esa razón, en caso de que el tablón sea digital o en línea, es fundamental que se instalen en la intranet de la empresa, nunca en internet[10].

(10)Véase la Sentencia de lo Contencioso-Administrativo de la Audiencia Nacional de 8 de julio de 2009.

Desde la doctrina iuslaboralista se sostiene también la importancia del principio de proporcionalidad en los tratamientos de datos gestionados por los representantes de los trabajadores, de forma que la información publicitada sea la estrictamente necesaria para ejercer con eficacia sus funciones. Así, por ejemplo, en caso de publicarse una determinada resolución administrativa o una sentencia judicial de interés para los trabajadores, debería procederse a la anonimización de los datos cuando se pueda afectar a los derechos de las partes u otras personas que pudieran aparecer en ellos y la publicación de los datos carezca de relevancia desde el punto de vista de la libertad sindical (Hugo Preciado, 2017).

En segundo lugar, hay que referirse al envío de información sindical a través del correo electrónico. Esta actividad requiere el tratamiento de datos personales, puesto que se considera la dirección electrónica como un dato personal. De entrada, ha de recordarse que la AEPD ha elaborado unas recomendaciones sobre al tratamiento de datos personales de los trabajadores a cargo de la representación sindical en la empresa. En este sentido, la AEPD admite que, en función del artículo 28.1 de la CE, que reconoce como derecho fundamental la libertad sindical, y por lo tanto la acción sindical en la empresa, es adecuado a derecho que la empresa comunique las direcciones de correo electrónico de los trabajadores a las secciones sindicales más representativas que están presentes en aquella.

Ahora bien, sobre la posibilidad de que los trabajadores que reciben información digital de los sindicatos o representación social, aunque es cuestión debatida, se puede admitir la posibilidad de que aquellos soliciten su baja en la

recepción de información excepto cuando se esté llevando a cabo un proceso electoral donde los trabajadores no pueden oponerse al tratamiento de sus datos personales, justamente por la preponderancia que en este asunto puede tener también el artículo 28.1 de la CE, siempre que el uso que realice el sindicato se ajuste a la finalidad para la que se envían dichos correos que es la propia campaña electoral de carácter sindical.

La AEPD manifiesta, en este ámbito, que debe reconocerse el derecho de los trabajadores a mostrar su oposición a la recepción de mensajes con contenido sindical y, por consiguiente, la obligación de los sindicatos de cesar en el tratamiento de los datos de los solicitantes. No obstante, en lo referente a la información sindical remitida a los trabajadores en período electoral, debería considerarse la preponderancia del derecho a la actividad sindical sobre el derecho a la protección de datos. En consecuencia, los trabajadores, durante el proceso electoral sindical, no pueden oponerse al tratamiento de sus datos personales, siempre que el uso que realice el sindicato sea adecuado para los fines del propio proceso electoral (véanse las consideraciones de la AEPD que se vierten sobre este particular en *La protección de datos en las relaciones laborales*).

En todo caso, la AEPD recuerda que existen procedimientos automatizados que pueden permitir la satisfacción del derecho a la libertad sindical sin necesidad de realizar una cesión de datos y, por tanto, minimizando los riesgos y las obligaciones de cumplimiento normativo para el empresario y el sindicato (la utilización de listas de distribución permite que el sindicato remita la información a una dirección corporativa de la empresa, sin acceso a los datos). También prevé la AEPD que la comunicación se limite a los estrictamente necesarios y que los datos se usen para la finalidad por la que son cedidos. Una vez recibidos, el sindicato es el organismo que debe cumplir con las obligaciones de la legislación de protección de datos.

Una de las cesiones de datos más comunes es la relativa al cobro de la cuota sindical en el pago de la nómina por la empresa. La Ley orgánica 11/1985, de 2 de agosto, de libertad sindical impone la necesidad de la conformidad del trabajador para realizarla. Puesto que se trata de una iniciativa que tiene su origen en la voluntad del trabajador, el consentimiento que da a dicha gestión puede resultar acreditado en el propio documento de afiliación sindical, en el que puede constar el tratamiento de las cesiones de datos que hubieran de realizarse entre el empresario y el sindicato para garantizar la efectividad de la forma de pago que el propio trabajador ha elegido. Por ello, es válida la cesión por el sindicato al empresario de los datos identificativos del trabajador que solicita el descuento de su nómina de la cuota sindical y la cesión por el empresario al sindicato de la efectiva deducción producida en la nómina de cada uno de sus afiliados, no siendo necesaria la solicitud de un consentimiento adicional al trabajador.

Finalmente, cabe recordar que en materia de retribuciones, el tipo de informaciones a las que puede acceder la representación obrera es limitado. La AEPD tiene fijado que cualquier cesión de datos de los trabajadores al comité de empresa o delegados de personal que exceda de las legalmente previstas en el artículo 64.1 y 9 de la Ley del estatuto de los trabajadores deberá contar con el consentimiento del interesado, en este caso de los trabajadores afectados, a no ser que exista un convenio colectivo que autorice dicha cesión. En consecuencia, partiendo únicamente de aquellas competencias legales, no puede haber cesión de nóminas de los trabajadores al comité de empresa o a los delegados de personal. Únicamente existe obligación de entregar los TC-1, boletín de cotización para la Seguridad Social en el que se reflejan los datos relativos a la identificación de la empresa y a la determinación de la deuda, y el TC-2, en el que aparece reflejada la relación nominal de trabajadores y los datos relativos a la identificación de los trabajadores, a sus bases de cotización y a las prestaciones que les hayan sido satisfechas en régimen de pago delegado (véase la guía *La protección de datos en las relaciones laborales*, 2009).

Bibliografía

Agencia española de protección de datos: https://www.agpd.es. En dicha página web pueden encontrarse como documentos de interés utilizados en este material docente, los siguientes:

Como Recomendación, la relativa a la «Selección de Personal a través de Internet (2005)».

En la sección de Publicaciones: Guía *La protección de datos en las relaciones laborales*, 2009.

También en la sección de Publicaciones: «Guía de videovigilancia», 2014.

Resolución de archivos de actuaciones de la AEPD de 9 de diciembre de 2010 (Expediente E-01327-2010).

Resolución de procedimiento sancionador: R/00029/2003, de 24 de enero de 2003. Puede consultarse en: http://www.agpd.es/portalwebAGPD/resoluciones/procedimientos_sancionadores/ps_2003/common/pdfs/PS-00099-2002_Resolucion-de-fecha-24-01-2003.pdf.

Camas Roda, F. (2004). «La intimidad y la esfera privada del trabajador ante las nuevas modalidades de control y vigilancia de la actividad laboral». En: M. R. Alarcón Caracuel; R. Esteban Legarreta (coords.). *Nuevas tecnologías de la Información y la Comunicación y Derecho del Trabajo* (págs. 161-186). Alicante: Editorial Bomarzo.

Hugo Preciado, C. (2017). *El Derecho a la Protección de Datos en el Contrato de Trabajo*. Cizur Menor: Thomson Reuters.

The Working Party [article 29 data protection working party], *Opinion 2/2017 on data processing at work*. Adopted on 8 June 2017.