Nuevas señales y paradojas de la protección de datos en la reciente doctrina de los Tribunales y de la Agencia Española de Protección de Datos

Jesús R. Mercader Uguina

Trabajo y Derecho, Nº 85, Sección Práctica Jurídica y Despachos Profesionales / Estudios de práctica jurídica, Enero 2022, Wolters Kluwer

LA LEY 13609/2021

1. La protección de datos: un universo en expansión

El derecho fundamental a la protección de datos sigue su imparable proceso de crecimiento en el ámbito de las relaciones laborales (1) . Ello se observa a simple vista si tenemos en cuenta los numerosos pronunciamientos judiciales que vienen dictándose en los últimos tiempos en esta materia. Tribunal Constitucional, Tribunal Supremo y el resto de Jueces y Tribunales integrantes de rama social del Derecho vienen ocupándose de esta materia conformando una importante doctrina en una tan nueva como relevante materia. De igual modo, la actuación de la Agencia Española de Protección de Datos (en adelante, «AEPD») muestra un incremento de las Resoluciones que tienen como objeto aspectos diversos de lo laboral.

Todo ello recomienda acercarse de nuevo a esta materia para seguir confirmando ese lento pero imparable proceso en el que el derecho a la protección de datos gana, día a día, terrenos al derecho a la intimidad. Como se ha señalado, «la protección de datos, si bien nació tímidamente, se ha convertido en un agujero negro que lo absorbe todo y no deja escapar nada de su entorno». Y, se añade, «a la luz de los amplios conceptos de datos personales y tratamiento, cualquier acto de comunicación basado en medios automáticos, como las telecomunicaciones, el correo electrónico o las redes sociales, relativo a una persona física, constituye una interferencia putativa tal de este derecho fundamental que requiere de justificación» (2) .

2. ¿Hasta dónde llega la protección de datos en la LOPD? El control sobre el uso de los dispositivos digitales y sobre el derecho a la desconexión digital en la empresa no es competencia de la AEPD

Una primera paradoja viene de la mano de lo que es y de lo que no es protección de datos en la Ley Orgánica 3/2018 de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPD). Como es sobradamente conocido, su Título X («Garantía de los derechos digitales»), incorporaba varios preceptos dirigidos a dotar de tutela y regulación específica a una importante serie de cuestiones que habían venido generando importantes controversias en el terreno judicial. Se creaba, así, un grupo normativo de pleno contenido laboral que, integrado por los artículos 87 a91 LOPD, fue completado con la incorporación de un nuevo artículo 20 bis al Texto Refundido de la Ley del Estatuto de los Trabajadores, aprobado por Real Decreto Legislativo 2/2015, de 23 de octubre (en adelante, ET). Pero lo cierto es que no todos los preceptos contemplados en el citado Título X parecían proyectar su ámbito de actuación sobre el derecho fundamental a la protección de datos e incorporaban reglas específicas en relación con el derecho a la intimidad o, directamente, creaban nuevas instituciones como el caso del derecho a la desconexión digital ¿Eran dichas normas disposiciones en materia de protección de datos y, por tanto, sometidas al control de la AEPD?

La duda derivaba del hecho de que varios preceptos de la LOPD ofrecían significativos frentes de duda a la hora de concretar su campo de aplicación. Por un lado, el art. 2.1 LOPD señalaba que:

«Lo dispuesto en los Títulos I a IX y en los artículos 89 a 94 de la presente ley orgánica se aplica a cualquier tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero». El tenor de la norma dejaba fuera de su ámbito de cobertura dos preceptos: el art. 87 referido al derecho a la intimidad y al uso de dispositivos digitales en el ámbito laboral y el art. 88 relativo al derecho a la desconexión digital en el ámbito laboral. Por otro, el art. 47 LOPD precisaba que: «Corresponde a la Agencia Española de Protección de Datos supervisar la aplicación de esta ley orgánica y del Reglamento (UE) 2016/679 (en adelante, RGPD) y, en particular, ejercer las funciones establecidas en el artículo 57 y las potestades previstas en el artículo 58 del mismo reglamento, en la presente ley orgánica y en sus disposiciones de desarrollo». La aplicación de dicha norma llevaba al entendimiento de que la AEPD poseía competencias para supervisar la aplicación de la completa normativa establecida en la LOPD, incluidos los citados artículos 87 y 88 LOPD.

En diversas intervenciones públicas representantes de la AEPD habían venido afirmando verbalmente la exclusión de su ámbito de competencias de lo dispuesto en los artículos 87 y 88 LOPD. Por ello, la Resolución de archivo de actuaciones del Procedimiento N.º: E/10250/2019 (LA LEY 1741/2020), posee especial importancia al resolver de manera expresa sobre esta cuestión. En el referido procedimiento se planteaba una reclamación contra una empresa sobre la base de que la misma había accedido al correo electrónico de un trabajador sin que éste hubiera sido previamente informado de la política de uso de las herramientas informáticas de la empresa, lo que había permitido el acceso a sus correos personales lo que, a juicio del trabajador, vulneraba su derecho a la protección de datos personales.

Entiende la AEPD que de la documentación aportada al expediente se desprende que el trabajador había sido informado en relación con la normativa sobre protección de datos dado que, según consta en el informe de actuaciones, en el documento aportado por la entidad «Informe de funciones y obligaciones del personal» relativa a la cláusula sobre «Correo electrónico», se señala que: «El responsable se reserva el derecho a revisar, sin previo aviso, los mensajes de correo corporativo del usuario, con el fin de comprobar el cumplimiento de estas normas y prevenir actividades que puedan afectar a la organización como responsable del fichero. El usuario utilizará la herramienta de correo electrónico proporcionada por el responsable con la configuración predeterminada. Se limitará a usarlo para fines relacionados con las funciones encomendadas y en base a los tratamientos autorizados…».

Aunque la AEPD entiende cumplido el deber de advertencia a que se refiere el art. 87 LOPD, la Agencia utiliza esta resolución para hacer algunas precisiones importantes sobre las dudas existentes en esta materia. En primer lugar, precisa que «el preámbulo de la LOPD señala que la ley en su Título X acomete la tarea de reconocer una serie de derechos digitales de los ciudadanos conforme el mandato establecido en la Constitución y, entre ellos, el reconocimiento del derecho a la desconexión digital en el marco del derecho a la intimidad en el uso de dispositivos digitales en el ámbito laboral. Estos derechos no se encuentran regulados en el RGPD y han sido incorporados en la nueva LOPD». Añade a lo anterior que «el art. 1 de la citada Ley se señala que esta tiene por objeto, en primer lugar, adaptar el ordenamiento jurídico español al RGPD en lo relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos y completar sus disposiciones y, en segundo lugar, garantizar los derechos digitales de la ciudadanía conforme al mandato establecido en el artículo 18.4 de la Constitución». En cuanto a su ámbito de aplicación, viene regulado en su artículo 2, y en su apartado 1, dicho ámbito se encuentra vinculado en relación a cualquier tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero. Sin embargo, «en cuanto a los preceptos digitales se trata de declaraciones de derechos sobre los que no se regulan ni se establecen mecanismos que los garanticen, es decir, ni se señala, ni en ningún caso se establece, que la AEPD tenga competencias para garantizar estos derechos quedando fuera de sus atribuciones, como *a sensu contrario*, sí se establece tanto en el RGPD como en la LOPD en relación a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales. Por consiguiente, de

conformidad con el artículo 2.1 de la LOPD de los citados artículos tan solo del 89 a 94 sí son competencia de la propia AEPD a nivel de garantizar su cumplimiento y ejercicio».

3. Datos sensibles en las relaciones laborales: salud y condenas e infracciones

1. Datos de salud de los trabajadores, la COVID-19 al margen

La COVID-19 está dando lugar a un sinnúmero de problemas vinculados con el control de los datos de salud de los trabajadores. En el presente estudio dejaremos fuera este importante conjunto de problemas: información sobre el estado de inmunidad frente a la COVID-19 en los procesos de selección, controles de temperatura, pasaportes de inmunidad y seguimiento de empresarial de los procesos de vacunación. Cuestiones importantes y de interés que merecen, sin duda, de un estudio más detenido del que resulta posible en estas páginas (3) .

A) La cesión voluntaria de datos a empresas encargadas del control del absentismo es admisible

La STS de 15 de junio de 2021 (Rec. 57/2020), se ocupa de una importante cuestión: la cesión de datos voluntaria por parte de los trabajadores a una empresa dedicada al seguimiento de las situaciones de absentismo. Es preciso recordar que el art. 20.4 ET precisa que: «El empresario podrá verificar el estado de salud del trabajador que sea alegado por este para justificar sus faltas de asistencia al trabajo, mediante reconocimiento a cargo de personal médico. La negativa del trabajador a dichos reconocimientos podrá determinar la suspensión de los derechos económicos que pudieran existir a cargo del empresario por dichas situaciones».

El procedimiento que en este caso se sigue por dicha empresa de control del absentismo, es la llamada telefónica al trabajador de baja, con los datos de filiación que extrae de una aplicación que comparte con la empresa para la que presta los servicios del control de los trabajadores en situaciones de incapacidad temporal (en lo sucesivo, IT). Dicha empresa se presenta como el servicio médico y le indica al trabajador la necesidad de entrevistarse con personal médico de la empresa de control del absentismo en relación con los motivos de su baja, y en caso de que se niegue se le cursa cita por SMS o burofax.

La sentencia considera que, en este marco, la solicitud de que el trabajador citado para la verificación del estado de salud aporte los informes médicos y pruebas diagnósticas sobre el proceso de la baja o de bajas anteriores, aparte de que no se efectúa en términos obligatorios sino voluntarios, resulta ser instrumental a la legítima finalidad de verificar el estado de salud del trabajador. En efecto, sigue diciendo, la aportación de tales documentos y pruebas resulta beneficiosa para ambas partes en la medida que permite aligerar el proceso y evita la inútil repetición de pruebas diagnósticas. Del relato de hechos probados se desprende que el tratamiento de los datos del trabajador se efectuará siempre y de manera exclusiva por personal médico. Consta expresamente también una cláusula de protección de datos en la que se informa al trabajador de que se han encargado a (una empresa de control del absentismo) los servicios de verificación de estados de enfermedad o accidente alegados para justificar la ausencia al trabajo, constando expresamente que el trabajador cede voluntariamente tales datos para que la entidad receptora pueda realizar tal labor de verificación y que puede no hacerlo, advirtiéndole expresamente de su derecho de acceso, rectificación, cancelación oposición o limitación respecto de los datos y su tratamiento. Consta, también, el deber de confidencialidad por parte de la empresa de control del absentismo.

En tales condiciones, la Sala entiende que se cumplen perfectamente las exigencias legales en materia de protección de tales datos habida cuenta de que, por un lado, «se recaba el consentimiento del trabajador, mediante la información de sus derechos y la aportación voluntaria de los documentos solicitados; y, por otro, los datos podrían ser necesarios para la ejecución del contrato de trabajo, de conformidad con el artículo 6.1.b RGPD». Por otro lado, «el hecho de que se advierta al trabajador de que la no aportación de datos podría determinar la imposibilidad de llevar a cabo la verificación de su estado de salud y que, en tal caso, podría suceder que la empresa adoptara las medidas previstas en el art. 20.4 ET, aparte de que no consta en los hechos probados

que tal posibilidad se haya llevado a cabo nunca, no puede identificarse con la obtención de datos sin su consentimiento, únicamente poner en conocimiento del trabajador las consecuencias legales que prevé el mencionado precepto».

El referido pronunciamiento nos suscita varias dudas desde la perspectiva de la protección de datos. En primer lugar, como ha recordado la AEPD, entre otros, en su Informe 0017/2020 (LA LEY 64/2020), para el tratamiento de datos de salud no basta con que exista una base jurídica del art. 6 RGPD, sino que de acuerdo con el art. 9.1 y 9.2 RGPD debe existir una circunstancia que levante la prohibición de tratamiento de dicha categoría especial de datos. Y, en este caso, resulta dudoso que puedan recurrirse a las excepciones que incorpora el art. 9.2 en sus apartados b) y h). En segundo término, el consentimiento, como es sabido, constituye una base débil para el tratamiento de datos personales con carácter general. En materia laboral el papel del consentimiento ha venido siendo visto con enormes reservas. El GT29 dejó sentado que «el recurso al consentimiento deberá limitarse a los casos en los que el trabajador pueda expresarse de forma totalmente libre y tenga la posibilidad de rectificar posteriormente sin verse perjudicado por ello» y ha subrayado que en la práctica el consentimiento es una condición de legitimación «excepcional». La AEPD en su Resolución R/0041/2019, ha llegado incluso a afirmar que «los trabajadores no están nunca en condiciones de dar, denegar o revocar el consentimiento libremente, habida cuenta de la dependencia que resulta de la relación».

B) Circulación de pruebas médicas entre trabajadores de una empresa

Otra faceta de esta cuestión se plantea en el Procedimiento Sancionador (en adelante, PS) 00247/2019 de la AEPD (LA LEY 495/2020). En ella, la reclamante justifica su reclamación ante la AEPD en el hecho que otro trabajador de la empresa para la que presta servicios ha accedido a sus datos de salud y los ha comunicado, al menos, a otros dos empleados de esa entidad. Se precisa que el jefe de Prevención de Riesgos Laborales abrió, escaneó y envió por correo electrónico a su jefe inmediato, con copia a ella, los resultados de las pruebas médicas que le practicaron en un reconocimiento promovido por la empresa y no, como habría sido lo correcto, sólo el informe emitido por la Mutua con la conclusión de apto o no apto para el trabajo. Añade que la Mutua había enviado a la empresa reclamada el resultado de sus pruebas médicas en un sobre cerrado dirigido a su atención y que sus datos de salud también fueron comunicados a otras personas de la empresa.

Entiende la AEPD que la documentación que obra en el expediente pone de manifiesto que la empresa no tenía implementados entre su personal los criterios de actuación respecto a los documentos de carácter privado que contuvieran datos de salud de los empleados. El art. 32 RGPD obliga al responsable del tratamiento a adoptar las medidas que garanticen que cualquier persona que actúe bajo su autoridad y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones del responsable. Y a su vez, esas instrucciones tienen que apoyarse en una previa valoración del riesgo que implica cada uno de los tratamientos que se efectúan para la debida garantía de la seguridad de los datos. La infracción del citado art. 32 RGPD lleva consigo la sanción establecida en el art. 83.4.a) RGPD imponiéndose una multa de 5.000 euros.

C) Cesión interempresarial de datos de salud entre clínica privada y Mutua colaboradora

La cesión de datos de salud entre una clínica privada y una Mutua colaboradora con la Seguridad Social es fuertemente reprochada en el PS/00262/2021 (LA LEY 959/2021) de la AEPD. En el caso, el reclamante, víctima de un accidente laboral, denuncia que un centro de diagnóstico de la imagen al que fue dirigido por la Mutua, colaboradora con la Seguridad Social en la gestión de las contingencias de accidente de trabajo había revelado su informe radiológico a dicha Mutua, lo que provocó la denegación de la baja por IT. Señala la AEPD que la mención a datos de salud previos procedentes de la asistencia en régimen privado del reclamante en la prueba vulnera el art. 5.1 f) RGPD [«Los datos personales serán tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas ("integridad y confidencialidad")»]. Sobre esta base y como consecuencia

se impone una multa por la infracción imputada de 30.000 euros sin perjuicio de una posible reducción si se procede al pago voluntario.

2. Datos relativos a condenas e infracciones penales

Cuestión controvertida y que plantea numerosas dudas prácticas es la posibilidad de que la empresa solicite a sus candidatos declaraciones o certificados de antecedentes penales durante los procesos selectivos. Para un adecuado análisis de esta cuestión es preciso tener presente, tanto el art. 10 RGPD, como el precepto concordante de nuestra normativa interna. Así el art. 10 RGPD dispone que: «El tratamiento de datos personales relativos a condenas e infracciones penales o medidas de seguridad conexas sobre la base del artículo 6, apartado 1, sólo podrá llevarse a cabo bajo la supervisión de las autoridades públicas o cuando lo autorice el Derecho de la Unión o de los Estados miembros que establezca garantías adecuadas para los derechos y libertades de los interesados. Solo podrá llevarse un registro completo de condenas penales bajo el control de las autoridades públicas». Por su parte, el art. 10.1 LOPD establece que: «El tratamiento de datos personales relativos a condenas e infracciones penales, así como a procedimientos y medidas cautelares y de seguridad conexas, para fines distintos de los de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, sólo podrá llevarse a cabo cuando se encuentre amparado en una norma de Derecho de la Unión, en esta ley orgánica o en otras normas de rango legal».

Como he señalado en otro lugar (4) , el legislador comunitario y, por extensión, el nacional han querido sustraer por completo los ficheros que pudiesen contener los referidos datos a cualquier ámbito particular determinando que sólo los poderes públicos pueden ser titulares de los mismos. Por consiguiente, no es legalmente posible exigir a los candidatos a un puesto de trabajo un certificado de antecedentes penales, que no puede ser objeto de tratamiento por los particulares, salvo en aquellos supuestos excepcionales en que, autorizados por una Ley y con las debidas garantías, se contemple dicha medida.

A) Antecedentes Penales y Protección de datos: no cabe solicitar ni certificados ni declaraciones del trabajador

La Sentencia de la Audiencia Nacional (Sala de lo Social) de 10 de febrero de 2020 (Proc. 148/2019) viene a extender el alcance de esta limitación, al valorar la práctica de una empresa del sector de seguridad privada de acuerdo con la cuál cuando la misma contrata a un trabajador nuevo o se subroga en personal de otras empresas de seguridad no pide un certificado de antecedentes penales sino una declaración del trabajador de carecer de ese tipo de antecedentes. En el caso del personal subrogado, la empresa les presenta, para la firma, un formulario en el que se declara que en los países en los que se ha residido carecen en los últimos cinco años de antecedentes penales en vigor.

Con toda corrección, la sentencia procede a analizar la base de legitimación *ex*art. 6 RGPD para el tratamiento de dichos datos, afirmando que la práctica empresarial que se impugna únicamente podrá reputarse lícita si colma con un doble requisito: 1. Que exista una obligación legal que faculte a la empresa para recabar tal circunstancia. 2. Que sea necesaria para la ejecución del contrato de trabajo.

Para el examen de tales exigencias la sentencia acude a la normativa legal en materia de seguridad privada, en concreto a la Ley 5/2014 de 4 de abril y, aun cuando sea norma de rango infralegal, al Real Decreto 2364/1994, de 9 de diciembre, por el que se aprueba el Reglamento de Seguridad Privada en cuanto que la disposición derogatoria única apartado 2 de dicha Ley lo declara vigente. Entiende la Sentencia que de la normativa que se ha expuesto «no cabe inferir en modo alguno que las empresas de seguridad estén facultadas para recabar datos referentes a condenas penales de los vigilantes de seguridad. Si bien para obtener la correspondiente habilitación que da derecho a la obtención de la tarjeta de identificación profesional es necesario que el trabajador en cuestión carezca de antecedentes penales en vigor, lo cierto es que ninguna intervención en la gestión y expedición de las mismas encomienda la legislación vigente a las empresas de seguridad, pues se trata de una competencia atribuida al Ministerio del Interior que se ejercita por medio de la Dirección

general de la Policía, por lo que habrá de ser esta, a través de los órganos correspondientes, la que deberá recabar y verificar tales datos tanto para la inicial expedición de la misma, como para el mantenimiento durante su vigencia, siendo tal autoridad pública, la única a la que faculta para el tratamiento de los datos relativos a los antecedentes penales».

A lo anterior se añade que «el tratamiento de los datos que por parte de la empresa demandada se viene efectuando resulta contrario a derecho pues carece de habilitación legal para recabar los mismos, y en modo alguno ha justificado que resulte necesario para el cumplimiento del contrato de trabajo, pues es la Dirección General de la Policía quién tiene encomendada la concesión y gestión de las habilitaciones para prestar servicios como vigilante de seguridad. Por otro lado, tal y como ha reconocido la empresa, el tratamiento de datos que lleva a cabo, carece de relevancia alguna para la ejecución del contrato, puesto que el hecho de que un trabajador exprese su negativa a suscribir la declaración, ni impide que la subrogación se lleve a efecto —pues la empresa en prueba de interrogatorio ha declarado que se ve obligada a incorporarlo a la plantilla por *mor* de los dispuesto en el Convenio sectorial de aplicación—, ni acarrea sanción disciplinaria alguna».

El referido pronunciamiento, a expensas de lo que pueda concluir el Tribunal Supremo, limita severamente la posibilidad de que empresas privadas soliciten certificados o declaraciones a los trabajadores sobre sus antecedentes penales incluso en sectores en los que, por el tipo de actividad, tal situación puede estar normativamente contemplada.

B) ¿Cuándo pueden pedirse certificados negativos del Registro Central de Delincuentes Sexuales?

La Ley 26/2015, de modificación del sistema de protección a la infancia y a la adolescencia, configura como necesario que todas las personas que por la prestación de sus servicios tengan contacto con menores, remitan a sus empresas un certificado negativo del Registro Central de Delincuentes Sexuales. Dicho Registro se encuentra regulado por el RD 1110/2015, de 11 de diciembre, por el que se regula el Registro Central de Delincuentes Sexuales.

En relación con la necesidad de certificación en el caso de una empresa de transporte público por carretera entre cuyos clientes se encontraban menores, el Informe 0401/2015 de la AEPD interpretó que para considerar «trabajo habitual con menores», es necesario que el puesto de trabajo implique, por su propia naturaleza y esencia, un contacto habitual con menores, siendo los menores los destinatarios principales del servicio prestado. No siendo necesario presentar el certificado en aquellas profesiones que, teniendo un contacto habitual con el público en general, entre los que pueden encontrarse menores de edad, no estén por su naturaleza exclusivamente destinados a un público menor de edad.

Por ejemplo, añade la AEPD, no cabe duda alguna que en el ejercicio de funciones docentes para los menores de edad será aplicable la norma en cuestión. No así en aquellas profesiones que, aun teniendo un contacto habitual con el público en general, entre el que se encuentran los menores de edad, no están por su propia naturaleza destinadas exclusivamente a un público menor de edad, como sucede en la empresa consultante, que se dedica a la prestación de servicios de transporte público de viajeros por carretera, aunque cuenta con numerosos trabajadores que en el desarrollo de su actividad están en contacto habitual con menores (conductores, azafatas, agentes de ventas, personal de estaciones de servicios, etc.).

En cualquier caso, señala la AEPD que dicha documentación puede almacenarse mientras cumpla con los fines previstos, en concreto, para las personas que pretendan acceder al ejercicio de tales puestos de trabajo, mientras dure el proceso de selección y hasta que no haya concluido. Solo pueden conservarse: (i) los datos de los que superen el proceso de selección y hayan accedido ya a tales puestos de trabajo; y (ii) cuando la empresa justifique que los datos de tales procesos de selección serán conservados para su uso ulterior en otros procesos de selección a celebrar inmediatamente, y solo en la medida en que los certificados se encuentren en vigor (tienen una validez de tres meses) y no exista derecho de oposición de los interesados.

C) Infracciones de tráfico equivalen a «condenas e infracciones penales» a efectos de protección de datos: El carnet por puntos como ejemplo

En este mismo ámbito resulta de interés la STJUE (Gran Sala) de 22 de junio de 2021 (C-439/19). En la misma se planteaba la posibilidad del acceso libre (vía Internet) a los «puntos» que cada persona ha perdido como consecuencia de las infracciones de tráfico. El TJUE considera que el tratamiento de los datos personales relativos a los puntos constituye un «tratamiento de datos personales relativos a condenas e infracciones penales» contemplado en el artículo 10 del RGPD, para el que el RGPD prevé una mayor protección debido al carácter especialmente sensible de los datos en cuestión.

Tras recordar los tres criterios pertinentes para apreciar el carácter penal de una infracción: la calificación jurídica de la infracción en Derecho interno, la naturaleza de la infracción y el grado de severidad de la sanción impuesta, el Tribunal de Justicia declara que las infracciones de tráfico en cuestión están comprendidas en el concepto de «infracción» en el sentido del RGPD. Por lo que respecta a los dos primeros criterios, el Tribunal de Justicia constata que, aunque las infracciones no se califiquen de «penales» en Derecho nacional, dicho carácter puede derivarse de la naturaleza de la infracción y, especialmente, de la finalidad represiva que persiga la sanción que la propia infracción puede implicar. Pues bien, en este caso, la atribución de puntos por infracciones de tráfico, al igual que las demás sanciones que la comisión de aquellas puede implicar, persiguen, entre otras cosas, esa finalidad represiva. La conclusión alcanzada por el TJUE puede tener importantes consecuencias al extender el alcance de las reglas contenidas en el art. 10 RGPD y art. 10 LOPD a determinadas infracciones administrativas con impacto en el ámbito de las relaciones laborales como ocurre, significadamente, en el caso de los trabajadores transportistas o conductores (5) .

4. Algunas cuestiones sobre el uso de los datos personales en la dinámica de las relaciones laborales

A) Ausencia de base de legitimación para solicitar a los empleados copia de la declaración de IRPF o datos fiscales del trabajador

La STS de 21 de diciembre de 2020 (Rec. 63/2019), ha confirmado la nulidad de un párrafo del artículo 8.2 de la Ordenanza del Banco de España 9/2017 en virtud del cual el Banco de España podía exigir a sus empleados una copia de su declaración del IRPF o datos fiscales en el marco de procesos de verificación de operaciones financieras privadas, al considerar que no existe una habilitación legal que permita a esta institución solicitar a sus empleados dicha información.

En este sentido, el Tribunal Supremo señala que la declaración del IRPF permite conocer no únicamente los datos económicos del afectado, sino otra serie de datos que aparecen en la misma, tales como los referentes a su religión, pertenencia o no a un sindicato, ideas…, los cuales, a tenor de la normativa aplicable en materia de protección de datos, tienen el carácter de especialmente protegidos. Se añade a lo anterior que «en el supuesto examinado los datos a los que se refiere el artículo 8 de la Ordenanza 9/2017 no son necesarios para el mantenimiento o cumplimiento de la relación laboral, por lo que se requiere el consentimiento expreso de la persona trabajadora para poder tener acceso a los mismos». De igual modo, «tampoco es posible prescindir del consentimiento de la persona trabajadora basado en que se busca la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento, tal y como establece el art. 6.1 f) RGPD ya que sobre dichos intereses prevalecen los derechos fundamentales del interesado, que requieren la protección de datos personales». Por todo ello, entiende la sentencia que, «no existiendo habilitación legal para que el Banco de España pueda solicitar a sus empleados sus declaraciones de la renta, ni mediando consentimiento de los interesados, la disposición contenida en el artículo 8.2 de la Ordenanza 9/2017 vulnera el derecho a la protección de datos de carácter personal y debe declararse, por tanto, su nulidad».

B) Ausencia de información en el contacto a través de WhatsApp y otras posibles cuestiones

El PS/00237/2021 (LA LEY 827/2021) de la AEPD resuelve sobre la reclamación planteada en relación con los siguientes hechos. En la página web de una empresa se publicó una oferta de empleo. El afectado contactó a través del teléfono que constaba en el anuncio y remitió su currículum por WhatsApp. El reclamante manifiesta que la entidad reclamada no le ha facilitado información relativa al tratamiento que efectuarían con sus datos personales ni de la posibilidad de ejercitar los derechos ante el responsable del tratamiento. La AEPD impone una multa de 2.000 euros por una infracción del art. 13 RGPD. En la resolución se señala que ni en el propio anuncio ni en conversaciones posteriores mantenidas por WhatsApp con el candidato, procedió la empresa a informarle sobre el tratamiento que iba a efectuar de sus datos personales ni de sus derechos, lo cual supone una infracción del art. 13 RGPD.

Aunque no tiene contenido laboral, es de interés por lo que de aviso a navegantes tiene también en este ámbito lo resuelto en el PS/00260/2021 (LA LEY 999/2021). En él la AEPD impone una sanción por incluir a un antiguo cliente (pensemos en comunicaciones con extrabajadores) en un grupo de WhatsApp, sin su consentimiento. La AEPD «considera que el reclamado ha tratado datos personales de la reclamante (número de teléfono móvil) sin su consentimiento, contraviniendo con ello el art. 6 del RGPD, y que, pese a no ser cliente desde hace más de diez años, aún conserva sus datos personales, vulnerándose el art. 5.1 e) del RGPD, ya que en dicho precepto se establece que los datos no podrán conservarse más que el tiempo necesario para la finalidad para la que fueron tomados (…)». Además, «facilitar el número de teléfono móvil de la reclamante a terceros, al incluirle en un grupo de WhatsApp supone una vulneración de su confidencialidad, como consecuencia de unas medidas de seguridad del reclamado que no son adecuadas a la normativa de protección de datos, suponiendo tales hechos dos infracciones más al contravenir los artículos 32.1 b) y 32.1 d) del RGPD respectivamente».

C) Derecho de acceso a las grabaciones resultantes de una prueba de selección

Como ha recordado la AEPD, el derecho de acceso es un derecho personalísimo. Permite al ciudadano obtener información sobre el tratamiento que se está haciendo de sus datos, la posibilidad de obtener una copia de los datos personales que le conciernan y que estén siendo objeto de tratamiento, así como información, en particular, sobre los fines del tratamiento, las categorías de datos personales de que se trate, los destinatarios o categorías de destinatarios a los que podrán comunicarse los datos, el plazo previsto o criterios de conservación, la posibilidad de ejercitar otros derechos, el derecho a presentar una reclamación ante la autoridad de control, la información disponible sobre el origen de los datos (si estos no se han obtenido directamente de titular), la existencia de decisiones automatizadas, incluida la elaboración de perfiles, e información sobre transferencias de datos personales a un tercer país o a una organización internacional.

En el caso resuelto por la R/00634/2021 de la AEPD, un interesado presentó una solicitud de acceso a una empresa de transporte con respecto a los resultados de un proceso de selección para un trabajo. El interesado no estaba de acuerdo con el resultado del proceso y quería acceder a los vídeos de uno de los exámenes de conducción. Dado que el responsable del tratamiento no respondió, el interesado presentó una denuncia ante la AEPD. En respuesta a la AEPD la empresa afirmó que no revelaría videos ya que las cámaras estaban configuradas para grabar solo el exterior de los vehículos, grabando así a terceras personas como pasajeros. El interesado comparó el caso con el acceso a respuestas escritas de un examen ya decidido por juicios previos.

La AEPD consideró que «dado que la nueva tecnología permite por medio de técnicas que anonimicen las imágenes mostrar grabaciones de forma que no perjudiquen a terceros y, añadiendo además un interés legítimo por parte del reclamante ya que está solicitando muestras de imparcialidad en la prueba realizada», y concluyó que no encontraba motivo para que «el reclamante no pueda tener las grabaciones que pueden constituir una parte fundamental de su prueba selectiva para obtener un puesto de trabajo».

5. Los riesgos de las cesiones de datos entre empresas

El PS/00360/2020 (LA LEY 794/2021) de la AEPD resuelve sobre un supuesto singular, pero en el que se pone de manifiesto la especial sensibilidad que está detrás del derecho a la protección de datos. Un trabajador interpuso reclamación ante la AEPD contra su empresa dado que la misma comunicó a otra, mediante correo electrónico, que se incorporarían al proyecto dos nuevos empleados (uno de ellos el reclamante), para los que solicitaba se facilitara acceso a la VPN y demás aplicaciones; en dicho correo electrónico, enviado con copia a ambos empleados, se facilitaban sus nombres y apellidos, correos electrónicos profesionales y números de DNI. El reclamante señala al respecto que tal comunicación debería haberse realizado de manera independiente, de modo que no tuviera conocimiento de los datos de su compañero y viceversa. La AEPD impone a la empresa que cedió los datos indebidamente una multa de 3.000 euros por infringir el art. 5.1 (f) RGPD.

Señala la AEPD que «se trata de una difusión de datos personales para la que la reclamada no dispone de base jurídica que la legitime». En consecuencia, se acredita que la reclamada vulneró el artículo 5 «Principios relativos al tratamiento» del RGPD, apartado 1.f), en relación con el artículo 5 «Deber de confidencialidad» de la LOPD. Añade que «este deber de confidencialidad, con anterioridad deber de secreto, debe entenderse que tiene como finalidad evitar esas filtraciones de los datos no consentidas por los titulares de los mismos. Se trata de una obligación que incumbe al responsable y encargado del tratamiento, así como a todo aquel que intervenga en cualquier fase del tratamiento; y que es complementaria del deber de secreto profesional». Frente a este incumplimiento no puede oponerse simplemente, como hace la reclamada en sus alegaciones, la responsabilidad mostrada en el cumplimiento de la normativa de protección de datos personales. Se trata de unos hechos que han quedado debidamente acreditados. Se rechaza, finalmente, la alegación realizada por la reclamada, cuando señala que los hechos no constituyen una revelación de datos dado el entorno laboral en que se producen; y considerando como probable que ambos compañeros tuvieran conocimiento de los datos personales del otro. Concluye la AEPD que «no existe ninguna razón legal para que un trabajador pueda tener acceso a los datos personales de otro trabajador por el solo hecho de pertenecer a la misma organización empresarial; ni la organización puede darlos a conocer a los compañeros en base a la mera suposición de que ya son conocidos por éstos».

Otro supuesto de cesión indebida de datos entre empresas es el resuelto en el PS/00245/2021 (LA LEY 1003/2021) de la AEPD y en el que se multa con 5.000 euros por infringir el art. 6 RGPD a una empresa por utilizar los datos personales de un empleado sin su consentimiento. Los motivos en que basa la reclamación son que un trabajador al solicitar informe de vida laboral tuvo conocimiento de que, si bien su relación de trabajo fue inicialmente concertada con la empresa «X» en una determinada fecha, esta empresa cursó su baja en la Seguridad Social sin su conocimiento y fue dado de alta de nuevo en una fecha posterior en la empresa «Y», sin que hubiese dado consentimiento alguno el trabajador para el tratamiento de sus datos personales por dicha empresa.

6. Una avalancha de problemas: Control tecnológico y protección de datos personales

El control a través de sistemas de videovigilancia, microfónicos y telefónicos, el rastreo a través de sistemas de geolocalización; los controles biométricos; el control informático de los niveles de productividad de los trabajadores en tiempo real; el seguimiento de los correos electrónicos y de las navegaciones por internet; el impacto de las redes sociales; o, en fin, la enorme proyección que sobre lo laboral comienzan a tener las técnicas del Big Data, conforman una realidad en permanente transformación en la que la vigilancia empresarial se ha convertido en algo más impersonal, pero no por ello menos invasivo. En este contexto, el derecho fundamental a la protección de datos personales se transforma en un elemento básico de la también nueva «ciudadanía electrónica».

1. Licitud de la prueba obtenida a través de sistemas de videovigilancia: La protección de datos al margen ¿Por cuánto tiempo?

A) Conocimiento evidente y notorio de la videovigilancia por el trabajador, pero desconocimiento de su finalidad

La STS 817/2021, de 21 de julio (Rec. 4877/2018), abordó un pleito en que un vigilante de seguridad estaba encargado del acceso principal de vehículos a un recinto ferial. El actor entregó a la empresa los impresos de requisa, declarando haber efectuado las correspondientes a los vehículos reflejados en ellos. Las videograbaciones revelaron que el demandante no había realizado dichas requisas, por lo que fue despedido disciplinariamente. Este Tribunal aplicó la doctrina establecida en la STC 39/2016, conforme a la cual «cuando el trabajador conoce que se ha instalado un sistema de control por videovigilancia (a través del distintivo de la instrucción 1/2006 de la AEPD), no es obligado especificar "la finalidad exacta que se le ha asignado a ese control" [...], para concluir que la sentencia recurrida, exigiendo que se hubiera informado expresamente de que la finalidad de la videovigilancia era controlar la actividad laboral, no se adecua a la STC 39/2016, 3 de marzo, pues, por el contrario, esta sentencia entiende que, si el trabajador sabe de la existencia del sistema de videovigilancia, no es obligado especificar la finalidad exacta asignada a ese control».

Debe tenerse en cuenta, adicionalmente, que, en determinadas circunstancias, la STEDH (Gran Sala) 17 octubre 2019 (López Ribalda II), admite que la empresa no advierta al trabajador de la existencia ni del emplazamiento de determinadas cámaras de videovigilancia, sin que ello conduzca a la nulidad de la prueba de videovigilancia que sustenta y acredita la sanción al trabajador. Señala el referido pronunciamiento que: «la información proporcionada a la persona objeto de vigilancia y su alcance son sólo uno de los criterios a considerar a la hora de valorar la proporcionalidad de tal medida en un caso determinado. Sin embargo, si falta esa información, las garantías derivadas de los demás criterios serán aún más importantes», «sólo un imperativo importante relativo a la protección de los intereses públicos o privados importantes podría justificar la ausencia de información previa»; (…) «si bien no puede aceptar que la mínima sospecha de robos u otras irregularidades cometidas por los empleados, pueda justificar la instalación de un sistema de videovigilancia encubierta por parte del empleador, la existencia de sospechas razonables de que se habían cometido graves irregularidades, y el alcance de los robos constatados en el presente asunto, pueden parecer una justificación seria».

En todo caso, en el presente supuesto, la sentencia recurrida parte de que «el sistema de videovigilancia era conocido por el trabajador por evidente y notorio» [...] el deber de información del art. 5 Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal permite al trabajador ejercer los derechos de acceso, rectificación, cancelación y oposición. Sin entrar ahora en mayores detalles, la base jurídica del tratamiento de datos está más bien en la ejecución y cumplimiento del contrato de trabajo y en las consiguientes facultades legales de control del empleador (art. 20.3 ET) y no tanto en el consentimiento del trabajador. Y, en el presente supuesto, se trataba de unas cámaras de seguridad de acceso al recinto ferial, conocidas por el trabajador, que podían permitir acreditar el incumplimiento de las normas de seguridad del acceso al recinto por el vigilante de seguridad, cuyo cometido era, precisamente, cumplir con esas normas de seguridad. Securitas tenía un interés legítimo amparado en sus facultades empresariales de control y en la carga de la prueba que sobre ella recaía a la hora de probar la veracidad de los hechos reprochados al trabajador. Concurrían también intereses públicos de gran importancia derivados del incremento de la amenaza terrorista [...] Por lo demás, nuestro examen se ha de ceñir a si la prueba debió o no admitirse, sin que deba extenderse a si se cumplieron todos los requerimientos de la legislación de protección de datos, tanto desde la perspectiva de la relación de la empresa con el trabajador despedido, como de la relación entre Securitas e Ifema.

Concluye la sentencia que aunque «la prueba no fuera nula desde la perspectiva de la impugnación judicial de la sanción disciplinaria impuesta al trabajador, no impide que la empresa pueda ser responsable en el ámbito de la legislación de protección de datos, de manera que las allí demandantes tenían otras medidas a su disposición, como la denuncia ante la agencia o el órgano responsable de la protección de datos o el ejercicio de acciones judiciales, pues la protección de datos en el marco de la videovigilancia en el lugar de trabajo puede garantizarse por diversos medios, que pueden corresponder sin duda al derecho laboral, pero también al derecho administrativo, civil o penal, medios estos últimos que las allí demandantes optaron por no utilizar».

B) Conocimiento parcial de la videovigilancia por el trabajador y licitud de la prueba: La protección de datos nuevamente al margen

a) El caso del conductor de autobús y la doctrina del Tribunal Supremo

La STS 3789/2021, de 13 de octubre (Rec. 3715/2018), resuelve sobre la licitud de las grabaciones realizadas a un conductor de un autobús de una empresa de transporte urbano de viajeros. Todos los trabajadores conocían la existencia de tres cámaras que grababan imágenes del interior del autobús, excepto el asiento del conductor, existiendo distintivos informativos que advertían de su presencia. El trabajador, despedido al ser captado en varias ocasiones fumando, orinando desde el vehículo, y haciendo «tocamientos» a una pasajera a la que le permitía viajar sin pagar el billete. El Tribunal Superior de Justicia de Galicia declaró nulo el despido al haber inadmitido como prueba las grabaciones de las cámaras de videovigilancia, obligando a la empresa a la readmisión del conductor y al abono de los salarios de tramitación.

Considera ahora el Tribunal Supremo que habida cuenta de la naturaleza del trabajo realizado por el actor (transporte urbano de pasajeros en autobús), con el riesgo que supone para él y para terceros: tanto los pasajeros del vehículo como otros usuarios de las vías públicas, la instalación de esas cámaras de vigilancia en el autobús era una medida justificada por razones de seguridad en sentido amplio, que incluye el control de la actividad laboral; idónea para el logro de esos fines, al permitir descubrir a eventuales infractores y sancionar sus conductas, con un efecto disuasorio; necesaria, debido a la inexistencia de otro tipo de medios menos intrusivos para conseguir la citada finalidad; y proporcionada a los fines perseguidos, debiendo hacer hincapié en que la videovigilancia no incluía el asiento del conductor, habiéndose utilizado el dato obtenido para la finalidad de control de la relación laboral y no para una finalidad ajena al cumplimiento del contrato.

En definitiva, concluye, «la prueba de la reproducción de lo grabado por las cámaras de videovigilancia era una medida justificada, idónea, necesaria y proporcionada al fin perseguido, por lo que satisfacía las exigencias de proporcionalidad, sin perjuicio, en su caso, de una eventual responsabilidad empresarial por parte de la AEPD por las infracciones que se hubieran podido cometer desde la óptica de la mencionada normativa de protección de datos. A juicio de esta Sala, estaba justificada la limitación de los derechos fundamentales en juego».

b) Sus secuelas: Pesadillas de la anonimización de las sentencias

Resultado del anterior pronunciamiento, hace unos días aparecía una noticia de prensa que ponía de manifiesto los límites de la anonimización de los datos personales en la sentencias de nuestros Tribunales (6) . En ella se relata la pesadilla de un chófer de autobus de Vigo por un nombre inventado (Plácido) que fue utilizado por la sentencia del Tribunal Supremo y que fue confundido con otro trabajador con el mismo nombre (Plácido «real») de la misma empresa (7) . Aunque el nombre de Plácido no figura en la sentencia auténtica, sí lo hace en el documento que fue publicado por el Centro de Documentación Judicial (CENDOJ) que puede ver cualquier ciudadano. Al cambiar el nombre por el de Plácido, con la finalidad de garantizar el anonimato del trabajador realmente implicado en la sentencia, no se tuvo en cuenta que, en una plantilla de 300 conductores, pudiese haber un chófer que se llamase igual.

El art. 236 quinquies 2 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, establece que: «Los Jueces y Magistrados, los Fiscales y los Letrados de la Administración de Justicia, conforme a sus competencias, podrán adoptar las medidas que sean necesarias para la supresión de los datos personales de las resoluciones y de los documentos a los que puedan acceder las partes durante la tramitación del proceso siempre que no sean necesarios para garantizar el derecho a la tutela judicial efectiva, sin que, en ningún caso, pueda producirse indefensión». Por su parte, el RGPD vino a establecer que «a fin de preservar la independencia del poder judicial en el desempeño de sus funciones, incluida la toma de decisiones», esa tarea se realizase por «organismos específicos establecidos dentro del sistema judicial del Estado miembro», dedicados en particular, a «garantizar el cumplimiento de las normas del presente Reglamento» (Considerando 20). En nuestro ordenamiento, esta labor recae, precisamente, en el CENDOJ.

Pero este proceso, como ponen de manifiesto diversas sentencias, no es perfecto y puede conducir a resultados absurdos (8) , como ocultar el nombre de un periodista en una sentencia, en la que sin embargo se menciona el nombre del programa de radio que dirige y que lleva su nombre (STS 1.ª 202/2019, de 3 de abril), o el de un torero, en una sentencia en la que se menciona, sin embargo, a una peña taurina que lleva su nombre (STS 1.ª 462/2019, de 10 de septiembre). El TJUE acordó que, a partir del 2 de julio de 2018, los asuntos prejudiciales en que se hallen implicadas personas físicas serán anonimizados y que se suprimirá igualmente cualquier dato adicional que permita identificar a esas personas. Pero esta práctica, como vemos, no se encuentra ni mucho menos generalizada y sus riesgos son, tal y como vemos, más que evidentes.

C) Videovigilancia y la presencia de la protección de datos

Los anteriores pronunciamientos son hijos de su tiempo: Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y el conjunto de pronunciamientos, incluida la doctrina del Tribunal Constitucional, nacidas a su luz. Pero tras la entrada en vigor del RGPD y de la LOPD a dicha realidad debe necesariamente añadirse el art. 89 LOPD, «derecho a la intimidad frente al uso de dispositivos de video vigilancia y de grabación de sonidos en el lugar de trabajo», el que se establece que «los empleadores podrán tratar las imágenes obtenidas a través de sistemas de cámaras o videocámaras para el ejercicio de las funciones de control de los trabajadores (…) previstas, respectivamente, en el artículo 20.3 ET (…), siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo», agregando que «los empleadores habrán de informar con carácter previo, y de forma expresa, clara y concisa, a los trabajadores o los empleados públicos y, en su caso, a sus representantes, acerca de esta medida». Pero se añade que «en el supuesto de que se haya captado la comisión flagrante de un acto ilícito por los trabajadores o los empleados públicos se entenderá cumplido el deber de informar cuando existiese al menos el dispositivo al que se refiere el art. 22.4 de esta Ley Orgánica». En dicho artículo 22.4 se establece que «el deber de información previsto en el art. 12 RGPD se entenderá cumplido mediante la colocación de un dispositivo informativo en lugar suficientemente visible identificando, al menos, la existencia del tratamiento, la identidad del responsable y la posibilidad de ejercitar los derechos previstos en los artículos 15 a22 RGPD. También podrá incluirse en el dispositivo informativo un código de conexión o dirección de internet a esta información. En todo caso, el responsable del tratamiento deberá mantener a disposición de los afectados la información a la que se refiere el citado Reglamento».

La integración de esta nueva realidad normativa se comienza a poner de manifiesto en algunos pronunciamientos hijos ya de esta nueva era y excelente ejemplo de ello es la rigurosa y bien fundamentada Sentencia del Tribunal Superior de Justicia de Galicia de 15 de febrero de 2021 (Rec. 4586/2020). La misma efectúa una muy precisa clasificación de las posibles situaciones y de las exigencias asociadas a cada concreta situación. El referido pronunciamiento concluye que de las «normas actualmente vigentes se deducen dos marcos habilitantes de la video vigilancia en el trabajo, sometidos cada uno a diferentes exigencias».

Distingue, en primer lugar, lo que la sentencia denomina «videovigilancia laboral específica», que obliga al empleador al cumplimiento de las exigencias establecidas en la legislación laboral (art. 20.3 ET, art. 18 de la CE y artículo 8 del Convenio Europeo de Derechos Humanos, de ahí la exigencia de superar, para la legitimidad de la restricción de los derechos fundamentales de la persona trabajadora, un juicio de proporcionalidad basado en los tres subjuicios de idoneidad, necesidad y proporcionalidad en sentido estricto) y a que informe con carácter previo, y de forma expresa, clara y concisa, a los trabajadores y, en su caso, a sus representantes, acerca de esta medida. Lo que no exige la norma es comunicar la ubicación exacta de las cámaras, con lo cual se habilita para la colocación de cámaras ocultas siempre que se cumplan las exigencias de idoneidad, necesidad y proporcionalidad en sentido estricto.

Un segundo marco de referencia «presupone la existencia de una video vigilancia implementada por personas físicas o jurídicas, públicas o privadas, con la finalidad de preservar la seguridad de las personas y bienes, así como de sus instalaciones (art. 22 LOPD), esto es de carácter no laboral

y en cuya ejecución aparece un hallazgo casual relacionado con la actividad laboral del personal al servicio de la empleadora, esto es "en el supuesto de que se haya captado la comisión flagrante de un acto ilícito por los trabajadores", sin limitar el acto ilícito al delito penal, con lo cual entraría un ilícito solo laboral». Basta en este caso, dice la sentencia, «para cumplir con el deber de información, con la colocación de un dispositivo informativo en lugar suficientemente visible identificando, al menos, la existencia del tratamiento, la identidad del responsable y la posibilidad de ejercitar los derechos ARCO reforzados según aparecen regulados en los artículos 15 a22 del RGPD (acceso, rectificación, cancelación y oposición + derecho al olvido, la limitación del tratamiento y la portabilidad de los datos)». Tampoco aquí, concluye, «se exige informar de la ubicación de las cámaras pues, aunque sea muy habitual colocar el dispositivo informativo debajo de la cámara, es suficiente con colocarlo en un lugar visible en que las personas interesadas puedan leerlo antes de que se las grabe y, por tanto, puedan decidir si seguir adelante y ser grabadas, o por el contrario no entrar en la zona videovigilada».

Finalmente, la sentencia precisa que «lo que no contemplan estas normas es la video vigilancia sin una información, más o menos amplia, a las personas interesadas (lo que constituiría una cámara secreta), salvo (y esto abría la posibilidad de un tercer marco legal habilitante de la video vigilancia) si esa video vigilancia está permitida por una norma en ámbitos en que no resulta aplicable la normativa sobre tratamiento de protección de datos personales (el ejemplo más evidente: el tratamiento por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención *ex*art. 2 RGPD y art. 2 LOPD)».

2. Sistemas de grabación del sonido y obligación de información de acuerdo con lo establecido en el art. 89 LOPD y en el art. 13 RGPD

El PS/00067/2020 (LA LEY 1553/2020) de la AEPD resuelve sobre la denuncia interpuesta por un sindicato contra una empresa cuyos mandos intermedios están grabando mediante unas grabadoras colgadas al cuello las conversaciones personales con los trabajadores y trabajadoras en su entorno laboral sin que éstos hayan prestado su consentimiento ni autorización. Según se recoge en la reclamación, la razón para actuar así surge tras el despido de una empleada que había agredido físicamente a una supervisora. Como solo había imágenes de lo sucedido y no registros de voz, se recurre a las grabadoras para dejar constancia de lo que pudiera decirse, con lo que se solventarían estos problemas. La Empresa dispone de un sistema de videovigilancia, pero no capta las conversaciones, sistema que se les comunica a todos los trabajadores tanto al inicio de la relación laboral en la firma del contrato de trabajo, como en el Manual de Bienvenida de la Empresa, así como al personal más antiguo con la firma a la instauración del sistema de videovigilancia y el uso que del mismo se puede realizar. El procedimiento se abre por posible infracción del art. 13 RGPD.

La AEPD recuerda que «las grabaciones de las conversaciones entre las encargadas y los trabajadores/as, se realizan en el ámbito laboral, en jornada laboral y con equipos proporcionados por la empresa, no son grabadoras personales, adquiridas por las propias encargadas, sino proporcionadas por la dirección de la empresa para el ejercicio de sus funciones como encargadas de planta, y no usadas para grabar conversaciones personales o privadas, de las encargadas por lo que, la afirmación que hace la entidad reclamada de, "grabar una conversación en la que uno ha intervenido no es delito; sin embargo, sí puede ser delito el uso que posteriormente se haga de dicha conversación", no puede ser tenida en cuenta en este ámbito». Añade la AEPD que la empresa está en su total derecho de «tratar las imágenes obtenidas a través de sistemas de grabación para el ejercicio de las funciones de control de los trabajadores» y así lo indica el art. 89 LOPD.

No obstante, se precisa que la norma le obliga a informar con carácter previo, y de forma expresa, clara y concisa, a los trabajadores o a sus representantes, de las medidas implantadas en la empresa, como en este caso, la utilización, por parte de las encargadas, de grabadoras de voz para el correcto desarrollo del trabajo, al igual que hace, según sus declaraciones, cuando informa a los trabajadores de la utilización de grabaciones de imágenes. Respecto de la información que debe ser

facilitada a los trabajadores o a sus representante, el artículo 13 del RGPD, indica que, cuando se obtengan de un interesado (trabajador) datos personales relativos a él, como en este caso, su voz, el responsable del tratamiento, le facilitará información, entre otra cosas, sobre: la identidad y los datos de contacto del responsable del tratamiento; los fines del tratamiento y la base jurídica del mismo; el plazo durante el cual se conservarán los datos personales; los derechos existentes, etc.

En este sentido, en el documento presentado por la empresa en el que se procede a realizar la referida información, no se encuentra firmado, ni sellado por la empresa, ni se identifica a ninguna persona responsable del mismo, en el caso de que fuera un documento expuesto en el tablón de información a los trabajadores. Tampoco está firmado, como acuse de recibo, por ningún miembro del comité de empresa o representante sindical, si este documento hubiera sido enviado al Comité de Empresa o a los representantes de los trabajadores. Por lo tanto, «aunque la empresa, esté legitimada para la utilización de medios de control laboral, como en este caso, la utilización de grabadoras de voz también está obligada a informar de forma expresa, clara y concisa, de estos hechos a los trabajadores». La AEPD apercibe a la empresa por infracción del art. 13 RGPD y la requiere para que, en el plazo de un mes desde la notificación de la resolución, tome las medidas necesarias para informar a los representantes de los trabajadores de las medidas tomadas en la grabación de audios en el ámbito laboral ajustándose a lo estipulado en el art. 89 LOPD y en el art. 13 RGPD.

3. Sistemas de geolocalización

El art. 90 LOPD establece que: «Los empleadores podrán tratar los datos obtenidos a través de sistemas de geolocalización para el ejercicio de las funciones de control de los trabajadores o los empleados públicos previstas, respectivamente, en el art. 20.3 ET (…), siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo». Presupuesto fundamental para el lícito tratamiento de los datos resultantes es el cumplimiento del deber de información. Señala el art. 90.2 LOPD que: «Con carácter previo, los empleadores habrán de informar de forma expresa, clara e inequívoca a los trabajadores o los empleados públicos y, en su caso, a sus representantes, acerca de la existencia y características de estos dispositivos. Igualmente deberán informarles acerca del posible ejercicio de los derechos de acceso, rectificación, limitación del tratamiento y supresión». Por todo ello, se requiere que exista una: (i) Información previa al establecimiento a los trabajadores que deberá versar sobre la existencia y características de los sistemas de geolocalización; (ii) Dicha información deberá ser expresa, clara e inequívoca a los trabajadores; (iii) La información alcanza al posible ejercicio de los derechos de acceso, rectificación, limitación del tratamiento y supresión y, en fin (iv) Información previa al establecimiento a los representantes de los trabajadores en caso de que éstos existan en la empresa.

La STS 15 de septiembre de 2020 (Rec. 528/2018), ha considerado que el uso de los datos obtenidos por un GPS instalado en el vehículo de empresa es lícito en los casos en los que el trabajador esté informado de la instalación del dispositivo, tenga restringida la utilización del coche a la actividad laboral y sólo recojan información sobre el movimiento y localización del vehículo. Señala la sentencia que «la trabajadora conocía que el vehículo no podía ser utilizado fuera de la jornada laboral y, junto a ello, que el mismo estaba localizable a través del receptor GPS. De ahí que no apreciamos ninguna invasión en sus derechos fundamentales con la constatación de los datos de geolocalización que permiten ver que el indicado vehículo es utilizado desobedeciendo las instrucciones de la empresa en momentos en que no existía prestación de servicios».

4. Los controles biométricos a examen: Huellas digitales y sistemas de reconocimiento facial

Un espacio singularmente relevante en la realidad de nuestros días es el que tiene que ver con los datos biométricos. Estos datos permiten la identificación de una persona en cualquier momento sobre la base de una realidad biológica propia, permanente en el tiempo y de la que no pueden ser liberados. A la espera de una regulación propia como la existente en otros países, debemos acudir

en el nuestro a la referencia constitucional contenida en el art. 18.4 CE y al marco general que ofrece la normativa vigente en materia de protección de datos (9) .

A) Control biométrico de huella digital y evaluación de impacto

Las normas sobre registro de jornada (art. 34.9 ET) han traído al primer plano el tratamiento de las huellas dactilares. Es importante recordar que, si bien la huella dactilar completa identifica completamente a la persona, también es susceptible de identificarse a la misma persona con la toma de muestras o minucias recogidas de partes de la huella y transformadas en una plantilla, aunque sea a través de un algoritmo. Esas minucias, convertidas en algoritmos, mediante su registro en una base de datos, o incluso en una tarjeta o plantilla que porte el usuario permitirían, al ser tratados, la identificación de la persona cuando acceda a la instalación, a través del proceso de matchmaking (emparejamiento por comparación), entrando también en el ámbito del dato de carácter personal.

A esta situación se refiere la Resolución que puso fin al PS/00010/2021 de la AEPD. En el caso, la empresa tenía instalado un fichero en la puerta de acceso en la entrada de la nave industrial con lectura de huella digital y clave de operario. La empresa tenía instalados también cuatro ficheros más en las puertas de acceso al vestuario, a lavabos y comedor también con lectura de huella digital y clave de operario. La actividad de registro y gestión de la huella se lleva a cabo a través de un contrato de encargado de tratamiento por una empresa que lleva a cabo un «servicio integral de gestión de horarios», parametrización y soporte técnico, que realiza la identificación biométrica a través de la huella dactilar, consiste en el tratamiento única y exclusivamente de una serie de coordenadas relevantes obtenidas de las huellas dactilares de los usuarios que son procesadas y cifradas mediante un algoritmo, obteniéndose como resultado un código de hash que garantiza su irreversibilidad. Es relevante tener presente que la Inspección del Trabajo acordó levantar un acta de infracción por denuncia de los empleados.

La AEPD realiza varias reflexiones de interés comenzando por el hecho de que estamos en presencia datos sensibles cuyo principio general es la prohibición de su tratamiento *ex*art. 9 RGPD que solo puede ser levantada a través de la excepción contenida en el art. 9.2 b) RGPD: «el tratamiento es 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 (…)». De ese carácter «necesario», deriva que «para poder utilizar este sistema, de acuerdo con los parámetros establecidos en el RGPD, las empresas u organizaciones necesitan demostrar altos niveles de responsabilidad proactiva y diseño por defecto de Protección de Datos desde antes del tratamiento, incluyendo el hecho de ser capaces de justificar que el sistema utilizado es necesario, proporcionado en cada contexto específico en el que se va a implementar y acreditar que medidas técnicas menos intrusivas no existen o no funcionarían». Antes de implantar un sistema de reconocimiento de huella dactilar, el responsable debe de valorar si hay otro sistema menos intrusivo con el que se obtenga idéntica finalidad.

En el presente supuesto, se considera, además, que este sistema de acceso a vestuarios/aseos ha infringido el artículo 5.1 c) del RGPD, que indica: «1. Los datos personales serán: c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados ("minimización de datos")». Y ello dado que el referido sistema «a pesar de registrar en el informe de jornada el tiempo pasado por cada empleado en vestuarios/aseos, hora entrada, hora salida, no es necesario porque se considera tiempo trabajado, solo cuenta la entrada y salida, no interrumpe la jornada. Ello presupondría que no solo no se estimaría proporcional y necesario el uso del sistema de huella para este fin como se analiza en este caso, sino que la constancia de dichos datos no sería necesaria».

En segundo lugar, la AEPD considera que se ha de valorar que «el sistema utilizado sea idóneo para la finalidad, sea necesario, y proporcionado en su contexto específico, acreditándose que medidas técnicas menos intrusivas no existen o no funcionarían. Esta triple valoración requiere una exhaustividad, partiendo como ya se ha dicho, no solo de la prohibición de tratamiento de estos datos, pues nos encontramos ante categorías especiales de datos personales, sino los riesgos de

usar una tecnología intrusiva, los sesgos o la probabilidad de un error en la identificación, la suplantación de la identidad y el tipo de identidad única que contiene la huella, el impacto en la privacidad de las personas, las medidas de seguridad y la proporcionalidad o necesidad del citado tratamiento».

La AEPD considera que queda acreditada «la inidoneidad y desproporcionalidad y no pertinencia ni adecuación del sistema de toma de huellas para acceder a vestuarios/aseos con la finalidad implantada de seguridad de acceso de personas a dichos espacios, por su insuficiente motivación, y generalidad, existiendo sin lugar a dudas métodos para que terceros ajenos a la empresa no accedan a esos espacios menos intrusivos que la toma de la huella en todas y cada ocasión que el empleado o empleada acuda por necesidades a dichos espacios». Añade a lo anterior que «bajo el motivo de seguridad del acceso a un espacio interno, en realidad, se están limitando los derechos con la toma de huellas en cada ocasión, quedando registrados sus datos». Considerando los factores expuestos, por una infracción del art. 5.1.c) RGPD, de conformidad con el art. 83.5 a) RGPD, se impone una multa de 20.000 euros.

De igual interés son las conclusiones del PS/00050/2021 (LA LEY 939/2021) de la AEPD en el caso de una reclamación interpuesta por sección sindical «por su oposición a la implementación de un sistema de control presencial de los trabajadores a través de un sistema biométrico de huella digital en las dependencias de la empresa, mediante terminales que incorporan lectores para la captura de la huella dactilar de cada empleado» un sistema que además, se dice que «se conjuga con el lector de tarjeta». En el caso, se imputó a la empresa que, tratando datos de carácter personal de categoría especial, y existiendo la obligación de disponer de una Evaluación de Impacto en la Protección de los Datos Personales (EIPD) incumplió el art. 35 RGPD. La Resolución recuerda que la propia AEPD ha publicado una lista de actividades de tratamiento que requieren la realización de una EIPD: En el ámbito laboral la referida evaluación resultará imprescindible en la medida en que, por un lado, que se trate de «tratamientos que impliquen la observación, monitorización, supervisión, geolocalización o control del interesado de forma sistemática y exhaustiva» y, por otro, que los tratamientos «impliquen el uso de datos biométricos con el propósito de identificar de manera única a una persona física». El incumplimiento de la referida exigencia lleva a la imposición de una multa de 16.000 euros por incumplir el citado art. 35 RGPD al haber implementado un sistema de control para registrar las horas de sus trabajadores a través de un terminal biométrico de huellas dactilares, pero sin proporcionar EIPD.

B) Reconocimiento facial: El caso de Mercadona

«El tratamiento del rostro con *software* de reconocimiento facial se encuentra dentro de los datos biométricos» (Considerando 51 RGPD). La cara, al igual que las huellas dactilares, ha sido ampliamente utilizada como fuente de datos biométricos durante años. Como advierte el WP 193 del GT 29, «no solo la identidad puede determinarse a partir de una cara, sino también características fisiológicas y psicológicas tales como el origen étnico, emociones y bienestar. La capacidad para extraer este volumen de datos de una imagen y el hecho de que una fotografía puede tomarse a distancia sin conocimiento del interesado demuestra la cantidad de problemas de protección de datos que pueden derivarse de estas tecnologías».

El Dictamen 2/2017 sobre el tratamiento de datos en el trabajo, del GT 29 puso de manifiesto que son muchos los riesgos que plantea el uso de estos sistemas de reconocimiento unidos a los de video vigilancia como, por ejemplo, que el empleador pueda controlar las expresiones faciales de sus empleados o identificar desviaciones de patrones de movimientos predefinidos durante el desarrollo de su actividad laboral. Esto es lo que ha llevado al GT29 a llamar la atención sobre la necesidad de que «los empleadores se abstengan de utilizar estas tecnologías pues, aunque admite que podría haber algunas excepciones marginales, éstas no pueden ser utilizadas para invocar una legitimación general que dé cobertura, sin más, al uso de dicha tecnología». En la misma línea se mueve el Informe Jurídico 0036/2020 (LA LEY 3182/2020) de la AEPD que, aunque no se encuentra referido a lo laboral, ha reconocido que estamos en presencia de «una cuestión compleja, sometida a interpretación, respecto de la cual no se pueden extraer conclusiones generales, debiendo

atenderse al caso concreto según los datos tratados, las técnicas empleadas para su tratamiento y la consiguiente injerencia en el derecho a la protección de datos».

Particular interés tiene, por todo ello, la Resolución dictada por la AEPD en el PS/00120/2021 (LA LEY 782/2021). El referido procedimiento se inició por la Directora de la AEPD a la vista de las noticias publicadas en medios de comunicación acerca de la implantación que Mercadona, S.A. estaría realizando en sus establecimientos de un sistema de detección de aquellas personas con sentencias firmes y órdenes de alejamiento en vigor contra Mercadona o contra alguno de sus trabajadores. De las actuaciones previas de investigación, se concluye que Mercadona realiza un tratamiento de datos personales de datos biométricos (art. 4.14 RGPD) con la finalidad de identificar unívocamente a una persona concreta entre varias estando sujetos a las garantías de lo dispuesto en el art. 9 RGPD. El tratamiento no sólo se produce en relación con la identificación de condenados penales con imposición de medida de seguridad, consecuencia de la orden de alejamiento impuesta a aquellos en una sentencia penal, sino que afecta a cualquier persona que entre en uno de sus supermercados (incluidos menores) y a sus empleados. El tratamiento de datos implantado por Mercadona incluye la captación, el cotejo, conservación y la destrucción —en caso de identificación negativa— (tras 0,3 segundos de su recogida) de la imagen biométrica captada de cualquier persona que entre en el supermercado. En el tratamiento, dice la AEPD, se observa claramente un sistema de reconocimiento facial indiscriminado y masivo ya que dependiendo de los datos biométricos recogidos, pueden derivarse datos del sujeto como su raza o género (incluso de las huellas dactilares), su estado emocional, enfermedades, taras y características genéticas, consumos de sustancias, etc.

La extensa Resolución de la AEPD, en lo que a nosotros interesa, aporta criterios de interés al analizar el apartado correspondiente a la «Legitimación en cuanto a los datos de los trabajadores de Mercadona».

A tal efecto señala que «la base jurídica comprendida en el art. 6.1.e) RGPD en relación con el art. 22 LOPD sería suficiente para llevar a cabo un tratamiento de videovigilancia ordinario (no de carácter especial). Pero no sería bastante para un sistema de reconocimiento facial en los términos expuestos, esto es, un tratamiento radicalmente distinto al utilizar datos biométricos de forma masiva y remota del tipo "uno-a-varios", sin que quede levantada previamente la prohibición establecida en el art. 9.1 de RGPD». Y añade que «el art. 20.3 ET y las excepciones del art. 9.2.f) y 9.2.h) del RGPD no sostienen la legitimación del tratamiento para la finalidad pretendida». De todo lo anterior, concluye que el tratamiento en su conjunto no cuenta con legitimación para llevarlo a cabo, por lo que vulnera lo dispuesto en los arts. 9 y 6 RGPD, infracciones tipificadas en el art. 83.5.a) de dicha norma y consideradas muy graves a efectos de prescripción en el art. 72.1.e) y a), respectivamente, de la LOPD.

En el supuesto examinado no se ha realizado prueba de proporcionalidad alguna en relación a los riesgos y a la afectación de los derechos y libertades de los empleados. De modo que, «el tratamiento de datos biométricos de los empleados del supermercado supone un control indirecto de estos (en el sentido de que la finalidad del tratamiento se dirige a identificar unívocamente al condenando). Si hay que estar a la previsión del art. 89 LOPD a los efectos de respetar la intimidad de los trabajadores frente al uso de dispositivos de videovigilancia, mucho más si nos encontramos ante un tratamiento diferenciado de la videovigilancia, más invasivo, con riesgos más específicos y mayores, que conlleva la utilización de datos biométricos. Si tal precepto impone la medida de información previa a los empleados y a sus representantes, también deberá procederse en el supuesto examinado por *mor* de la transparencia. La información ha de ser suministrada, en todo caso, a los representantes de los trabajadores y a estos últimos en virtud del art. 13 del RGPD».

Igualmente precisa que, pese a considerarse por la empresa el colectivo de trabajadores como afectado por el tratamiento de reconocimiento facial, sin embargo, falta toda referencia a los riesgos sobre los derechos de los trabajadores en la EIPD (art 35 RGPD y lista de tipos de tratamientos de datos que requieren evaluación de impacto relativa a protección de datos). Ese control del sistema de reconocimiento facial en los términos expuestos produce también «una presión coercitiva sobre

los trabajadores y puede suponer un riesgo extremadamente elevado inasumible que coarte la libertad de los empleados, personal y profesionalmente. Es un riesgo de seguimiento de sus actividades sin que conste causa suficientemente justificada y, sobre todo, que no se ha tenido en cuenta en la elaboración del EIPD».

De lo expuesto por la AEPD cabe concluir lo siguiente: (i) Los sistemas de reconocimiento facial no son meros sistemas de videovigilancia y, por tanto, exigen bases de legitimación del tratamiento que van más allá de las establecidas en el art. 6 RGPD y, por tanto, requieren un tratamiento radicalmente distinto al utilizar datos biométricos de forma masiva y remota del tipo «uno-a-varios» debiendo tratarse en el marco del régimen excepcional que proporciona el art. 9 RGPD. (ii) Las características de estos sistemas imponen un estricto y reforzado cumplimiento de la obligación de información de acuerdo con lo establecido en el art. 13 RGPD cuando estamos en presencia de un tratamiento más invasivo, con riesgos más específicos y mayores, que conlleva la utilización de datos biométricos. (iii) Resulta imprescindible contemplar los riesgos sobre los derechos de los trabajadores en la elaboración del EIPD *ex*art. 35 RGPD.

7. Las dimensiones colectivas de la protección de datos

1. El Tribunal Constitucional desperdicia una buena oportunidad: Negociación colectiva y tratamiento de datos

El convenio colectivo posee un lugar importante en un terreno de la protección de datos personales. El RGPD subraya este protagonismo al establecer en su art. 88 RGPD que «los Estados miembros podrán, a través de disposiciones legislativas o de convenios colectivos, establecer normas más específicas para garantizar la protección de los derechos y libertades en relación con el tratamiento de datos personales de los trabajadores en el ámbito laboral (...)». La llamada a la negociación colectiva también se ha producido por la legislación española, en concreto, el art. 91 LOPD prescribe que «los convenios colectivos podrán establecer garantías adicionales de los derechos y libertades relacionados con el tratamiento de los datos personales de los trabajadores y la salvaguarda de derechos digitales en el ámbito laboral», lo que da entrada a la autonomía colectiva en la determinación del contenido de este derecho. El papel de los acuerdos colectivos en materia de protección de datos está llamada a tener un enorme protagonismo en el futuro. Por ello se ha perdido una buena oportunidad para fijar algunos criterios sobre su intervención en el diseño de este derecho fundamental en la reciente STC 160/2021, de 4 de octubre.

El recurrente, asesor comercial telefónico de una compañía de telefonía, fue despedido por la comisión de una falta muy grave con fundamento en que durante diferentes días y hasta en un total de ocho ocasiones se había constatado una deficiente atención y una dilación injustificada en la resolución de los problemas que le plateaban los clientes, sin seguir los procedimientos establecidos para encauzar las incidencias, incluso en algunos casos facilitándoles información errónea. Es importante tener presente que existía un acuerdo concluido por la empresa con la representación de los trabajadores en relación con la monitorización de las llamadas de los asesores, donde «la dirección de la empresa manifiesta que la finalidad del proyecto es la identificación de carencias formativas para la prestación de los servicios de atención y ventas, que permita la elaboración de planes individuales de formación y mejora de competencias capaces de superar las referidas carencias […] asumiendo la empresa el compromiso de que la monitorización no tendrá en ningún caso como objetivo su utilización como un mecanismo disciplinario». La cuestión es de gran relieve en la medida en que el pacto venía a determinar el alcance de la finalidad pretendida en el tratamiento de los datos y acordada por las partes. Esa primera cuestión hubiera merecido ser valorada: ¿un pacto colectivo puede fijar y con qué alcance la finalidad del tratamiento de los datos personales?

El demandante de amparo, con fundamento en el contenido de esas grabaciones, fue advertido en varias ocasiones de la incorrección de su proceder, dándose las indicaciones para una actuación adecuada, a pesar de la cual se mantuvo en su actitud. En vía judicial se consideró que no existió nulidad del despedido por vulneración del art. 18.4 CE, aunque sí improcedencia ante la falta de

constatación de un incumplimiento muy grave, con el argumento de que (i) la monitorización de las llamadas era una medida proporcionada dentro de las facultades de control empresarial de la que tienen perfecto conocimiento los asesores comerciales y (ii) lo acordado entre la empresa y los representantes de los trabajadores no excluye la utilización de las grabaciones como forma de comprobación del cumplimiento de la prestación de trabajo por parte de los asesores y, por tanto, el incumplimiento grave de sus deberes laborales que puedan llevar al ejercicio del poder disciplinario de la empresa.

Considera el Tribunal Constitucional que no se ha vulnerado al recurrente su derecho a la protección de datos de carácter personal (art. 18.4 CE). Precisa que el objeto de controversia no es ni la posibilidad legal de que el empleador adopte estas medidas de vigilancia laboral ni que en virtud de estas pudiera llegar a ejercerse el poder disciplinario empresarial. Y centra el problema constitucional que se plantea desde la perspectiva del derecho a la protección de datos de carácter personal (art. 18.4 CE), que «queda limitado a determinar la afectación que sobre este derecho tiene el supuesto incumplimiento del empleador de su compromiso con los representantes de los trabajadores de que la medida de observación y grabación del desarrollo laboral de esta categoría profesional no tendrá en ningún caso como objetivo su utilización como un mecanismo disciplinario».

El hecho de remitir a los órganos judiciales ordinarios la solución de casos como este por considerarlo ajeno al contenido del art. 18.4 CE resulta, cuando menos, cuestionable. El cambio unilateral de la empresa en el ejercicio de la finalidad pactada posee indudables efectos en materia de protección de datos al ser un principio esencial el que los datos deben ser recogidos con fines determinados, explícitos y legítimos, y no ser tratados posteriormente de manera incompatible con dichos fines (art. 5.1 b) RGPD). Los fines para los que son recabados u obtenidos los datos son la pauta de la proporcionalidad en su tratamiento, pues la idoneidad, necesidad y proporcionalidad se miden en función del fin para el que se han obtenido, como ha entendido el Tribunal de Justicia de la Unión Europea reiteradamente, entre otras en el STJUE 24 de noviembre de 2011, C-468/10 y C-469/10, ASNEF. No era pues, a nuestro juicio, una mera cuestión de legalidad ordinaria la que estaba en juego sino, antes bien, un elemento directamente conectado con el contenido esencial del derecho a la protección de datos personales que hubiera requerido de una respuesta más fundada por nuestro Tribunal Constitucional.

2. Límites a la solicitud sindical de información masiva

Una de las cuestiones que generan más controversia en la dinámica de las relaciones laborales es el acceso a la información de la empresa por los representantes de los trabajadores. El Estatuto de los Trabajadores atribuye un amplio haz de facultades a los mismos y el ejercicio de estas facultades puede comportar el acceso a datos personales de los trabajadores. Así, en el Estatuto de los Trabajadores se recogen amplísimas facultades de solicitud de información para el Comité de Empresa (copia básica de los contratos, notificación de prórrogas y denuncias de contratos, sanciones por faltas muy graves, decisiones en la empresa que pudieran generar cambios en la organización del trabajo, etc.), estando esta información vinculada al cumplimiento de las competencias de los órganos de representación de los trabajadores, entre las que se encuentra la «vigilancia en el cumplimiento de las normas vigentes en materia laboral, de seguridad social y de empleo, así como del resto de los pactos, condiciones y usos de empresa en vigor, formulando, en su caso, las acciones legales oportunas ante el empresario y los organismos o tribunales competentes».

La STS 9 de enero de 2020 (Rec. 100/2018), afirma que el derecho de los sindicatos, a través de las secciones sindicales y delegados sindicales en la empresa, a acceder a la misma información y documentación que la empresa ponga a disposición del comité de empresa, debe ir referido al ámbito de representación que tiene la sección sindical, en este caso toda la empresa, y no limitarse a los centros de trabajo con representación unitaria, sin que con ello se vulnere el derecho a la protección de datos personales ni el art. 18.4 CE. Todo ello dado que, de conformidad con el art. 10.3 LOLS, el contenido u objeto de información y documentación será el mismo que la empresa

ponga a disposición del comité de empresa (...). Entiende la sentencia que el propio preámbulo de la LOPD indica que los datos de afiliación sindical podrán ser tratados por el empresario para hacer posible el ejercicio de los derechos de los trabajadores al amparo del art. 9.2.b) RGPD o por los propios sindicatos en los términos del art. 9.2.d) RGPD a lo que anuda el deber de sigilo igualmente regulado en aquel art. 10 LOLS.

La STS (Contencioso-Administrativo) de 9 de febrero de 2021 (Rec. 1229/2020), establece, por su parte, más severas cautelas a la transmisión de información. Considera la sentencia que el reconocimiento del contenido, esencial y adicional del derecho de libertad sindical «no está exento de límites, pues sabido es que los derechos fundamentales no son derechos absolutos ni ilimitados. No obstante, conviene añadir que desde luego deben extremarse las cautelas para que la determinación de los límites no vacíe de contenido del derecho fundamental. En el caso examinado, el límite al derecho fundamental de la libertad sindical, respecto del acceso a documentación e información, se produce por el reconocimiento constitucional de otro derecho fundamental, el de la protección de datos de carácter personal». Precisa la sentencia que cuando se solicita la documentación e información por la organización sindical, «no se expresa ninguna explicación, ni se hace ninguna referencia o mención, sobre la utilidad de la misma para el cumplimiento de sus tareas sindicales. Tampoco se intenta vincular su solicitud de datos con las tareas legalmente atribuidas a los representantes sindicales. Dicho de otro modo, no se justificaron las razones por las que para el ejercicio de su función sindical resultaba necesario, relevante, o simplemente conveniente, que se procediera a ese volcado masivo e indiscriminado de datos personales». La sentencia concluye, por ello, que «la mera invocación, ayuna de justificación, de la representación sindical no puede servir de excusa para acceder a todo tipo de documentación, si no se quiere por esta vía vaciar el contenido del derecho fundamental a la protección de datos, cuando el titular de los mismos ignore el uso que se hace de sus datos, perdiendo su poder de disposición, en supuestos en los que no se justifica la concurrencia de alguna de las excepciones legalmente establecidas».

8. La eterna duda: ¿Cómo y hasta cuándo deben conservarse los datos personales?

Relevante en esta materia es el Informe Jurídico 00148/2019 de la AEPD que ayuda a clarificar distintos aspectos. Comienza señalando el referido Informe que la conservación de los datos de carácter personal y la eventual supresión de su tratamiento —bien por imperativo del principio de «limitación del plazo de conservación», o bien como consecuencia del ejercicio del derecho de supresión por los afectados—, se encuentra directamente vinculada con la finalidad para la que los datos fueron recogidos y tratados. Los datos de carácter personal serán suprimidos cuando hayan dejado de ser exactos y completos (art. 5.1 d. RGPD). A pesar de que se mantenga viva la finalidad para la cual se realiza el tratamiento, si el responsable no es capaz de mantener los datos actualizados de forma que respondan con veracidad a la situación real de las personas afectadas, estará obligado a suprimir esta información personal. Como es natural, también procede la supresión cuando se esté produciendo un tratamiento contrario a la normativa sobre protección de datos.

La normativa prevé limitaciones al derecho de supresión por medio de las cuales se habilita la conservación de los datos en los siguientes supuestos, que incluyen entre otras: (i) Cumplimiento de una obligación legal: El tratamiento (conservación) es necesario para el cumplimiento de una obligación legal, conforme a lo previsto en el artículo 17.3.b) del RGPD. (ii) Fines de archivo en interés público, investigación científica e histórica, fines estadísticos: Cuando los datos se traten para estos fines podrán ser conservados en virtud de los artículos 17.3.c) y 89 RGPD. (iii) Ejercicio o defensa de reclamaciones: Tal y como se establece en el artículo 17.3.e) del RGPD en relación con el art. 24 CE (derecho a la tutela judicial efectiva), se podrán conservar los datos cuando resulten necesarios para el ejercicio de derechos o la defensa frente a reclamaciones.

Sin perjuicio de las excepciones anteriormente mencionadas (y, por tanto, la posibilidad de conservación con base en estas excepciones), la AEPD considera que el sujeto obligado a conservar los datos debe cumplir con el resto de principios en materia de protección de datos durante dicho plazo de conservación. Entre ellos, es necesario asegurar el cumplimiento del principio de limitación

de la finalidad, y el principio de integridad y confidencialidad, con el objetivo de garantizar una seguridad adecuada en el tratamiento de los datos personales. En este sentido, el Informe Jurídico menciona algunos plazos de conservación a modo ejemplificativo. Así, el plazo de un mes en relación con los tratamientos de datos en materia de videovigilancia —al que se refiere su art. 22 LOPD—, o el de tres meses para las denuncias internas reguladas en su art. 24 LOPD.

El art. 22 de la Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales, dispone que: «En los supuestos en que la naturaleza de los riesgos inherentes al trabajo lo haga necesario, el derecho de los trabajadores a la vigilancia periódica de su estado de salud deber ser prolongado más allá de la finalización de la relación laboral, en los términos que reglamentariamente se determinen». La transcrita habilitación legal en orden al desarrollo reglamentario del plazo de obligatoriedad de la vigilancia periódica de la salud de los trabajadores se ha concretado en diversas normas jurídicas, algunas de las cuales elevan el plazo de conservación de determinados datos concernientes a la salud de los trabajadores, hasta los cuarenta (40) años.

Así, el artículo 9 del Real Decreto 664/1997, de 12 de mayo, sobre la protección de los trabajadores contra los riesgos relacionados con la exposición a agentes biológicos durante el trabajo. En similares términos, el artículo 9 del Real Decreto 665/1997, de 12 de mayo, sobre la protección de los trabajadores contra los riesgos relacionados con la exposición a agentes cancerígenos. Por su parte, el artículo 18 del Real Decreto 396/2006, de 31 de marzo, por el que se establecen las disposiciones mínimas de seguridad y salud aplicables a los trabajos con riesgo de exposición al amianto, prevé también en este caso la conservación de los datos de exposición de los trabajadores y los datos referidos a la vigilancia sanitaria específica de los trabajadores por un plazo mínimo de cuarenta (40) años después de finalizada la exposición. En otros casos, como el previsto el artículo 38 del Real Decreto 783/2001, de 6 de julio, por el que se aprueba el Reglamento sobre protección sanitaria contra radiaciones ionizantes, se fija en un mínimo de treinta (30) años el plazo de conservación de los datos de los afectados, debiendo archivarse y conservarse hasta que el trabajador alcance la edad de setenta y cinco años, y nunca por un período inferior a treinta años, contados a partir de la fecha de cese del trabajador en aquellas actividades que supusieran su clasificación como trabajador expuesto

Una particularidad de la normativa española (art. 32 LOPD) es que prevé que el proceso de supresión del dato personal, en determinadas circunstancias, pueda estar precedido por el bloqueo del dato de manera previa al borrado definitivo y físico del dato. Se establece así que el responsable del tratamiento estará obligado a bloquear los datos cuando proceda a su rectificación o supresión. En consecuencia, la supresión da lugar al bloqueo de los datos, lo que impide el tratamiento para la finalidad que justificó su recogida, conservándose únicamente (i) para la puesta a disposición de los datos a los jueces y tribunales, el Ministerio Fiscal o las Administraciones Públicas competentes, en particular de las autoridades de protección de datos, y (ii) para la exigencia de posibles responsabilidades derivadas del tratamiento y solo por el plazo de prescripción de estas (art. 32.2 LOPD).

En relación con lo anterior, la AEPD menciona en el informe al que nos venimos refiriendo que resulta imposible establecer una enumeración taxativa de la determinación de los periodos en los que el dato debe permanecer bloqueado. Sin embargo, la AEPD establece el siguiente listado ejemplificativo de plazos de bloqueo algunos de los cuales tienen plena proyección en nuestro ámbito de interés. En concreto:

(i) En materia de Seguridad Social, el art. 21.1 del Real Decreto Legislativo 5/2000, de 4 de agosto, por el que se aprueba el Texto Refundido de la Ley sobre Infracciones y Sanciones en el Orden Social (en lo sucesivo, LISOS), se refiere a la obligación —que incumbe al empresario y a las entidades de formación— en orden a la conservación durante cuatro años, de la documentación o los registros o soportes informáticos en que se hayan transmitido los correspondientes datos que acrediten el cumplimiento de las obligaciones en materia de afiliación, altas, bajas o variaciones que, en su caso, se produjeran en relación con dichas materias, así como los documentos de cotización y los recibos justificativos del pago de salarios y del pago

delegado de prestaciones. Dicho plazo se encuentra en consonancia con el fijado por el art. 24 del Real Decreto Legislativo 8/2015, de 30 de octubre, por el que se aprueba el Texto Refundido de la Ley General de la Seguridad Social.

También en relación con la Seguridad Social, se impone en este punto una referencia a los plazos de prescripción de los delitos establecidos en el art. 131 del Código Penal, aprobado por Ley Orgánica 10/1995, de 23 de noviembre, cuando dispone que «prescriben (…) a los diez (10) años aquellos cuya pena máxima señalada por la ley sea prisión o inhabilitación por más de cinco años y que no exceda de diez (…)» y «a los cinco (años), los demás delitos, excepto los delitos leves y los delitos de injurias y calumnias, que prescriben al año».

(ii) En relación con las infracciones en el orden social, el art. 4 LISOS se refiere a la prescripción de estas infracciones, disponiendo con carácter general —en su apartado 1— su prescripción en el plazo de tres años. A su vez, según se establece en los apartados 2, 3 y 4 de dicho precepto, prescribirán a los cuatro años, las infracciones cometidas en materia de Seguridad Social; al año, a los tres años o a los cinco años, dependiendo de su gravedad, las infracciones cometidas en materia de prevención de riesgos laborales, y a los tres meses, los seis meses, y al año —también en función de su gravedad—, las infracciones a la legislación de sociedades cooperativas. Dichos plazos han de computarse en todos los casos desde la fecha de la infracción.
(iii) Finalmente, en lo relativo a prescripción de acciones en el ámbito laboral, debe recordarse que, según dispone el art. 59 ET, las acciones derivadas del contrato de trabajo que no tengan previsto plazo de prescripción específico están sometidas al plazo de prescripción de un año.

Concluido el período de bloqueo procederá el borrado físico de los datos. Sin embargo, en aquellos casos en los que no exista obligación de bloquear los datos personales, por ejemplo, porque no se establezca en ninguna norma la necesidad de mantener el dato bloqueado, deberá procederse directamente a su borrado definitivo o físico.

(1)

Sigo en este trabajo la tradición iniciada en otros anteriores publicados en esta misma revista: «Protección de datos y relaciones laborales: apuntes prácticos sobre la entrada en vigor del Reglamento (UE) 2016/679», *Trabajo y Derecho*, 2018, n.º 41, pp. 113-126; «Aspectos laborales de la Ley Orgánica 3/2018, de 5 de diciembre: una aproximación desde la protección de datos», *Trabajo y Derecho*, 2019, n.º 52, p. 110 a 118; «Datos biométricos en los centros de trabajo», *Trabajo y Derecho*, 2020, monográfico n.º 11 (versión electrónica) y, este último, también en J. Baz Rodríguez (Dir.), *Los nuevos derechos digitales laborales de las personas trabajadoras en España*, Madrid, Wolters Kluwer, 2021, pp. 169 a 198.

(2)

D. CORDOVA y L. M. DIEZ PICAZO*, Reflexiones sobre los retos de la protección de la privacidad en un entorno tecnológico*, Asociación de Letrados del Tribunal Constitucional, *La privacidad en un nuevo entorno tecnológico*, Madrid, CEPC, 2016. También trasladaba esta idea en *La protección de datos se come a la intimidad: La doctrina de la Sentencia del Tribunal Europeo de Derechos Humanos de 5 de septiembre de 2017*, *Revista de Información Laboral*, 2017, n.º 10, pp. 7 a 12 en colaboración con I. GARCIA-PERROTE ESCARTIN.

(3)

Del tema me vengo ocupando en diversos trabajos, entre otros: «El Big data laboral: nuevos retos para la protección de datos en la era del cambio digital y el coronavirus», *El Cronista del Estado Social y Democrático de Derecho*, 2020, n.º 88-89, pp. 126 a 135 y *Tutela de la protección de datos personales y COVID-19: control de temperatura e información sobre anticuerpos en los procesos de selección de los trabajadores*,

Nueva Revista Española de Derecho del Trabajo, 2020, n.º 234, pp. 13 a 18 en colaboración con I. GARCIA-PERROTE ESCARTIN. Y, también, en varias entradas en el Foro de Labos.

(4)

J.R. MERCADER UGUINA, *Protección de datos y garantía de los derechos digitales en las relaciones laborales*, Madrid, Francis Lefebvre, 2019, 3ª edición, p. 94.

(5)

Tema del que me ocupe junto a C. ARAGON GOMEZ en «Las repercusiones laborales del permiso de conducir por puntos», *Tráfico y Seguridad Vial. Revista de Derecho de la Circulación,* 2006, n.º 91-92, pp. 5 a 20 y en «Efectos laborales del permiso de conducir por puntos», *Relaciones Laborales,* 2006, n.º 13, pp. 13 a 43.

(6)

Sobre el tema ampliamente, Y. CANO GALAN, *La seudonimización y la anonimización de datos personales en las sentencias del orden jurisdiccional social,* Documentación Laboral, 2020, n.º 119, pp. 31 a 56.

(7)

www.lavozdegalicia.es/noticia/vigo/vigo/2021/11/14/.

(8)

Como recuerda C.B. FERNANDEZ, *¿Qué problemas plantea la anonimización de los datos personales de las sentencias?*, diariolaley.laleynext.es/dll/2019/10/08/.

(9)

Un primer acercamiento a esta materia tras el RGPD, J.L. GOÑI SEIN. *La nueva regulación europea y española de protección de datos y su aplicación al ámbito de la empresa*, Albacete, Bomarzo, 2018, pp. 43-47. También, M. RODRÍGUEZ-PIÑERO ROYO, *Las facultades de control de datos biométricos del trabajador*, Temas Laborales, 2019, n.º 150, pp. 91-109 y J.R. MERCADER UGUINA, «Datos biométricos en los centros de trabajo», *Trabajo y Derecho*, 2020, monográfico n.º 11 (versión electrónica) y, este último, también en J. BAZ RODRÍGUEZ (Dir.), *Los nuevos derechos digitales laborales de las personas trabajadoras en España*, Madrid, Wolters Kluwer, 2021, pp. 169 a 198.