Foro, Nueva época, vol. 19, núm. 1 (2016): 395-411 ISSN:1698-5583
http://dx.doi.org/10.5209/FORO.53399

EL NUEVO REGLAMENTO EUROPEO DE PROTECCIÓN DE DATOS

Luis Antonio Fernández Villazón
Área de Derecho del Trabajo y de la Seguridad Social
Departamento de Derecho Privado y de la Empresa
Facultad de Derecho de la Universidad de Oviedo
villazon@uniovi.es

I. EL DERECHO A LA PROTECCIÓN DE DATOS COMO ESTANDARTE DEL PROCESO EUROPEO

Veintiún años después de que se aprobase la Directiva 95/46/CE, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos, la Unión Europea ha aprobado el Reglamento (UE) 2016/679, de 27 de abril de 2016, con el mismo título y conocido también como Reglamento General de Protección de Datos. En estas dos décadas, el derecho a la libertad informática ha experimentado una importante evolución, tanto en el ámbito de la Unión Europea como en el del Derecho interno de cada uno de los Estados miembros. Uno de los elementos claves de esa evolución lo constituye el paso de considerar el *habeas data* como un instituto de protección de otros derechos, principalmente la intimidad, a entenderlo como un derecho autónomo e independiente con su propia configuración y lógica internas.

Este dato salta a la vista en una comparativa de los primeros artículos de la Directiva de 1995 y del Reglamento de 2016. Así, el artículo primero de la Directiva señala que su objetivo es garantizar «la protección de las libertades y de los derechos fundamentales de las personas físicas y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales». Por su parte, el Reglamento señala en el mismo ordinal: «El presente Reglamento protege los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales». En otras palabras, durante este largo periodo el derecho a la libertad informática se ha independizado del derecho a la intimidad, constituyendo ahora un derecho fundamental autónomo, aunque su papel de garantía de otros derechos sigue teniendo importancia en la

lógica del legislador comunitario y en la de los tribunales constitucionales de los Estados miembros[1]. A esta evolución no ha sido ajeno el reconocimiento del derecho a la protección de datos en el art. 8.1 de la Carta de los Derechos Fundamentales de la Unión Europea y en el art. 16.1 del Tratado de Funcionamiento de la Unión Europea (TFUE).

Por lo demás, los objetivos iniciales de la regulación a nivel europeo del derecho no han cambiado sustancialmente. Se sigue insistiendo, por un lado, en la necesaria protección de un derecho humano y, por otro, en la importancia económica que tiene el garantizar el flujo de datos personales. La diferencia hoy está en la intensidad con que se insiste en tales fines. Si el flujo de datos tenía relevancia económica en 1995, no ha hecho más que multiplicar esa relevancia en los últimos años. La economía digital parece haberse convertido en un objetivo prioritario de la Unión Europea y los propios considerandos del Reglamento declaran sin ambages la importancia «de generar confianza que permita a la economía digital desarrollarse en todo el mercado interior» (7). Desde el punto de vista de la protección de las personas, los retos y los riesgos también se han vuelto mayores, pues el uso de datos personales por parte de las organizaciones públicas y privadas se realiza ahora «en una escala sin precedentes» (6).

Por otro lado, en el periodo transcurrido el derecho a la libertad informática se ha convertido en un elemento muy destacado y visible del proyecto europeo. Las sucesivas sentencias del Tribunal de Justicia de la Unión sobre la materia han ido aquilatando su contenido y lo han hecho llegar a lugares antes insospechados[2]. Además, en esa labor se han emitido resoluciones muy mediáticas contra importantes corporaciones multinacionales[3]. De tal modo, la normativa sobre protección de datos se ha convertido en un símbolo de los altos estándares de calidad del Derecho europeo y de su capacidad para imponerlos en el ámbito internacional, especialmente en las complejas relaciones Europa-Estados Unidos. De hecho, esta normativa no es sólo aplicable cuando el responsable del tratamiento tenga su establecimiento en territorio de la Unión, sino también cuando se traten datos personales de residentes en ella en relación con la oferta de bienes o servicios (de pago o no) o el control de su comportamiento (art. 3).

---

[1] *Vid.*, por ejemplo, dentro de nuestro ordenamiento, la STC 292/2000, de 30 de noviembre.

[2] Por ejemplo, a la utilización de información tal cual fue publicada en los medios de comunicación, STJUE, de 18 diciembre de 2008, caso C-73/07, *Tietosuojavaltuutettu y Satakunnan Markkinapörssi Oy, Satamedia Oy.*

[3] Es el caso de Google, STJUE de 13 de mayo de 2014, caso C-131/12, *Google Spain S.L., Google Inc. y Agencia Española de Protección de Datos.*

Es decir, tratar datos de ciudadanos europeos para ofrecerles bienes o servicios o controlar su comportamiento dentro del territorio de la Unión obliga a cumplir con las exigencias del Reglamento, aunque el responsable o encargado del aquél no esté establecido en la Unión Europea. Por todo ello, puede afirmarse que las instituciones comunitarias, al reforzar y modernizar su legislación en la materia, refuerzan el carácter de ésta como estandarte del proyecto europeo en su conjunto. Y lo han hecho, precisamente, en un momento en que tal proyecto afronta alguno de los mayores retos de su historia.

II. UN MARCO NORMATIVO MÁS SÓLIDO Y COHERENTE

Pasar de una directiva a un reglamento, instrumento que podemos considerar como auténtica ley europea, implica el paso de una regulación más flexible y abierta para los Estados miembros a otra de aplicación más uniforme y sólida en el conjunto de la Unión. No se ha querido sólo mejorar una regulación en parte superada por los nuevos retos planteados por la globalización y el desarrollo tecnológico, sino que se pretende asegurar «una ejecución estricta» que garantice una mayor seguridad jurídica. Esta preocupación se advierte claramente en el Documento de Trabajo de la Comisión que sirvió de base para la elaboración del Reglamento y otras disposiciones que conforman el llamado «paquete de protección de datos». En dicho documento se ponen de relieve las barreras que para los negocios y la actividad de las autoridades públicas derivan de la fragmentación de la normativa de protección de datos, la inseguridad jurídica y la falta de consistencia en la vigilancia de su cumplimiento.

Al incluir la Directiva conceptos abiertos y dejar un amplio margen a la acción de los Estados, se han detectado numerosas situaciones en las que un tratamiento de datos puede ser legal en unos Estados miembros y no en otros. La Comisión detectó faltas de coherencia de este tipo en la definición del consentimiento, en la regulación de las categorías de datos sensibles, en las reglas sobre notificación previa de los tratamientos o en las transferencias de datos a terceros países[4]. Una regulación más uniforme y sólida para toda Europa permitiría superar tales inconvenientes. La Comisión insiste también en que las diferencias de criterio de las distintas

[4] Documento de Trabajo de la Comisión de 25 de enero de 2012 [SEC (2012) 72 final], pp. 12-15.

autoridades nacionales de protección de datos a la hora de exigir el cumplimiento de la Directiva y las grandes diferencias existentes entre los distintos sistemas sancionadores en caso de incumplimiento de unos Estados a otros constituyen otras tantas «incoherencias» del sistema que pretenden salvarse con la nueva regulación. A estos últimos dos extremos aludiremos con más detalle en otro apartado.

Una regulación más sólida parece haber implicado también una normativa más prolija. Al querer dejar menos espacios a la aplicación e interpretación de los Estados, el Reglamento se ve obligado a abordar con mucho más detalle y exhaustividad los diferentes aspectos del tratamiento de datos de carácter personal. El resultado es una norma extensa y compleja que no va a contribuir, desde luego, a simplificar una materia ya de por sí tecnificada y burocrática. Ello puede llevar aparejadas, en nuestra opinión, dos consecuencias indirectas. Por un lado, se amplia y hace más prometedor un nicho de empleo, el de los consultores y expertos en materia de protección de datos. Por otro, esta complejísima regulación no ayuda a concienciar a los ciudadanos de a pie sobre el problema y los riegos que para sus derechos puede suponer la manipulación indebida de datos. Se corre el riesgo de que la materia se considere aún más una exigencia burocrática y gris cuyo sentido último acaba perdiéndose en un mar de especificaciones técnicas. De ahí que uno de los conceptos en los que insiste el Reglamento sea el de la transparencia y claridad con la que la información sobre los tratamientos debe llegar a los afectados. Pero sobre esto volveremos también un poco más adelante.

III. NUEVOS Y MEJORES DERECHOS

El Reglamento General de Protección de Datos ha introducido importantes novedades en el apartado de derechos del afectado, el conjunto de facultades que siempre se han entendido como parte del contenido esencial de la autodeterminación informativa. Por un lado, el Reglamento se hace eco de la doctrina del Tribunal de Justicia, que durante estas décadas ha realizado una nada desdeñable labor de precisión y concreción de conceptos a veces regulados con excesiva ambigüedad en la Directiva. Por otra parte, algunas modificaciones responden a la necesidad de adaptarse a los cambios tecnológicos y sociales que han tenido lugar en los últimos años, siempre con la premisa de conseguir una normativa de protección «tecnológicamente neutra».

Uno de los aspectos reformados es la prestación del consentimiento allí donde éste es necesario para la licitud del tratamiento. El Reglamento desarrolla ahora en su art. 7 las condiciones que ha de reunir este consentimiento para ser válido y exige «que el responsable deberá ser capaz de demostrar que aquél (el interesado) consintió el tratamiento de sus datos personales». Nótese que el consentimiento puede seguir siendo tácito (salvo cuando incumbe a categorías especiales de datos, donde se exige que sea explícito), pero la necesidad de probar su existencia hace que algunas prácticas frecuentes hasta ahora, basadas en la simple inactividad del interesado, resulten más difíciles de aceptar bajo la nueva regulación. Una adecuada demostración va a requerir una conducta más activa del afectado, aunque sea tácita. Por otra parte, el acceso cada vez mayor de los niños a los servicios de la sociedad de la información ha obligado a dedicar el art. 8 del Reglamento a regular su consentimiento. Básicamente, la nueva normativa fija una especie de «mayoría de edad» informática que da validez al consentimiento dado por las personas mayores de dieciséis años (aunque los Estados miembros pueden rebajarla hasta los trece). Por debajo de esa edad, será necesaria siempre la autorización del titular de la patria potestad o de la tutela, estando obligados los responsables del tratamiento a hacer «esfuerzos razonables» (teniendo en cuenta la tecnología disponible) para verificar que se han producido tanto el consentimiento como la autorización mencionada.

Otro de los derechos que se han reforzado con una regulación más detallada y amplia es el derecho de información del interesado cuando se recogen datos personales suyos con fines de tratamiento. Se trata de uno de los elementos clásicos del derecho de libertad informática, considerado parte de su contenido esencial. La nueva regulación no ha hecho sino insistir y profundizar en esa relevancia. Así, la transparencia es declarada como uno de los principios relativos al tratamiento en el art. 5. Mientras, el art. 12 del Reglamento insiste en que toda información al interesado ha de realizarse «en forma concisa, transparente, inteligible y de fácil acceso», preveyéndose incluso la utilización de «iconos normalizados». En otras palabras, el legislador comunitario es consciente de que en estas materias la información facilitada puede ser tan técnica que no resulte comprensible para un ciudadano medio. Ello puede convertirla en inútil y sembrar serias dudas sobre la validez del consentimiento dado en función de la misma. De ahí esa preocupación en simplificarla y hacerla más asequible. Los extremos sobre los que ha de informarse se regulan también con más detalle y amplitud en los arts. 13 y 14, así como las posibles excepciones.

En definitiva, podemos afirmar que el derecho a la información no sólo no ha perdido un ápice de importancia en la nueva regulación europea, sino que cobra un papel aún más protagonista. Ello podría obligar a replantearse en un futuro próximo algunas restricciones a que ha sido sometido en resoluciones recientes de nuestro Tribunal Constitucional[5].

Otro derecho reforzado es el de no ser sometidos a decisiones automatizadas del art. 22. Cuando este derecho fue introducido en la Directiva de 1995 seguramente era difícil prever la importancia que iba a alcanzar la elaboración de perfiles sobre la base del tratamiento masivo de datos personales a través de técnicas como la del *big data.* Ya sabemos que esas nuevas técnicas han revolucionado el *marketing* y la publicidad, pero su utilidad puede extenderse a la predicción del rendimiento en el trabajo, la situación económica, la salud, la fiabilidad, el comportamiento, etc. El número de datos que pueden manejarse y el número de personas afectadas han aumentado, además, en una escala impensable en 1995. De ahí que ahora se señale expresamente en el encabezamiento del artículo que se incluye en él «la elaboración de perfiles». No se trata en absoluto de impedir o limitar estas prácticas (éstas han abierto unas expectativas económicas que la UE no parece dispuesta a desaprovechar), sino de garantizar como mínimo el derecho del afectado a «tener intervención humana», a «expresar su punto de vista» y a «impugnar la decisión».

No sólo se ha mejorado la regulación de los derechos ya existentes, también se han introducido algunos nuevos. El primero de ellos es el «derecho al olvido» o derecho a exigir la supresión de los datos personales que le conciernan. Se trata de un derecho cuya existencia bajo la anterior regulación ya reconoció el Tribunal de Justicia en la conocida sentencia sobre el caso Google. La supresión procede cuando los datos han dejado de ser necesarios para los fines para los que fueron recogidos, cuando se haya retirado el consentimiento para su tratamiento o cuando lo exija alguna obligación legal. La supresión es también lo que procede cuando se ha ejercido con éxito otra facultad clásica de la libertad informática: el derecho de oposición. El Reglamento incluye una muy razonable mención a que los datos obtenidos con el consentimiento de niños que acceden a los servicios de la sociedad de la información están especialmente sujetos al ejercicio de este derecho.

[5] Como ha sucedido en relación con el uso de videocámaras ocultas para la comprobación de la existencia de incumplimientos laborales en la STC 39/2016, de 3 de marzo de 2016.

Otra nueva facultad del afectado es el derecho a la limitación del tratamiento (art. 18). Se trata de una especie de garantía preprocesal que puede funcionar en interés del interesado, pero también del responsable del tratamiento o, incluso, de otras personas implicadas. Cuando se ejercita este derecho, los datos no se suprimen, pero dejan de ser tratados y se conservan para facilitar la formulación, la defensa o el ejercicio de reclamaciones. De esta manera, se ataja el perjuicio que el proceso de la información pudiera estar provocando, a la vez que se permite su posterior revisión en caso de conflicto. La limitación está prevista en cuatro supuestos. En primer lugar, cuando el interesado haya impugnado la exactitud de los datos personales. Se limita entonces el tratamiento de éstos como garantía provisional «en un plazo que permita al responsable verificar la exactitud de los mismos». En segundo lugar, cuando el interesado se haya opuesto al tratamiento y el responsable haya alegado motivos legítimos imperiosos para continuarlo. También procede entonces la limitación provisional, en tanto se evalúa si esos motivos legítimos prevalecen sobre los intereses o las libertades del interesado. En tercer lugar, procede la limitación cuando el tratamiento de datos es ilícito y el interesado opta porque aquéllos no sean suprimidos. Finalmente, cuando los datos no son ya necesarios para el tratamiento, la regla general es que deben ser cancelados. No obstante, el interesado que los necesite para la formulación, el ejercicio o la defensa de reclamaciones puede obtener en su lugar la limitación. En definitiva, una medida práctica que trata de paliar los efectos indeseados que podrían derivarse de la drástica eliminación de la información tratada.

Finalmente, el Reglamento ha introducido en su art. 20 un nuevo derecho a «la portabilidad de los datos». Más que la libertad informática, lo que está en juego aquí es la libre competencia. Piense el lector en la gran cantidad de información personal que ponemos hoy en día en manos de las empresas que operan en la sociedad de la información (teléfonos, direcciones, fotografías, vídeos, etc.). Cuando ese volumen llega a cierto nivel, el miedo a perder esa información o a tener que volver a introducirla manualmente puede actuar como fuerte elemento disuasorio, si nos estamos planteando cambiar de servicio o de compañía. Pues bien, el reglamento reconoce nuestro derecho a recibir los datos personales que nos incumban «en un formato estructurado de uso común y lectura mecánica» y transmitirlos a otro responsable del tratamiento, sin que el primero pueda oponerse. Es más, la norma europea reconoce el derecho a que los datos «se transmitan directamente de responsable a responsable» cuando sea técnicamente posible.

IV. LAS OBLIGACIONES DEL RESPONSABLE DEL TRATAMIENTO: RACIONALIZACIÓN DE LOS TRÁMITES ADMINISTRATIVOS Y MAYORES RESPONSABILIDADES

Una de las preocupaciones de la nueva regulación europea ha sido la de racionalizar, y en lo posible simplificar, los trámites administrativos que para las empresas supone la implementación del sistema de protección de datos, especialmente para las pequeñas y medianas. Esa simplificación se ha centrado en la desaparición de la notificación previa a la autoridad de control que la Directiva exigía como regla general para la realización de un tratamiento de datos personales. Pero, cuidado, menos intervención previa de la autoridad no implica menos obligaciones. El nuevo Reglamento regula esta materia bajo el principio de «responsabilidad proactiva». Según este principio, los responsables del tratamiento deben cumplir las exigencias de la normativa europea de protección de datos y, además, ser capaces de demostrarlo. De esta manera, se reducen las trabas administrativas previas para el tratamiento de datos, pero sí habrá un control *a posteriori*, en el que el investigado debe asumir un papel activo, no sólo de colaboración con las autoridades de control, sino de acreditación de que efectivamente ha cumplido con la normativa.

En otras palabras, los encargados y responsables del tratamiento asumen un mayor control y capacidad de decisión sobre la protección de los datos personales que tratan, pero esa libertad se compensa con la obligación de acreditar todas las medidas de protección y control que adopten (para probar que se han hecho) y con una fuerte responsabilidad. Téngase en cuenta, en relación con este último aspecto, que el Reglamento prevé sanciones administrativas de hasta 20.000 euros o una cuantía equivalente al 4 por 100 del volumen de negocio total anual de la empresa, optándose por la de mayor cuantía (art. 83.5). En cualquier caso, la racionalización de los trámites no parece que vaya a suponer una reducción de la burocracia en sentido amplio. Más bien al contrario: todo ha de estar documentado. La relevancia del responsable es tal, que en los casos de tratamientos efectuados por entidades no establecidas en la Unión Europea, pero que han de someterse al Reglamento según el art. 3.2, éstas tienen la obligación de nombrar un «representante en la Unión» para que atienda las consultas de las autoridades de control y de los interesados sobre el tratamiento (art. 27).

Para que los encargados y responsables puedan actuar con una mínima seguridad jurídica, sin tener encima constantemente la espada de Damocles de una posible inspección de la autoridad de control de resultados imprevisibles, el Reglamento diseña un sistema basado, por un lado, en la elaboración de códigos de conducta debidamente supervisados y, por otro, en un sistema de certificación, sellos o marcas. Las autoridades nacionales de control tendrán la última palabra, tanto en la supervisión de los códigos de conducta, como en la emisión de certificaciones y sellos de protección de datos. No obstante, el Reglamento permite la realización de ambas actividades por organismos «que tengan un nivel adecuado de pericia» y estén debidamente acreditados. Se trata de un sistema claramente inspirado en los mecanismos de certificación de calidad industrial y que, sin duda, potenciará el próspero negocio de las auditorías privadas de protección de datos. Se abre también, como ya apuntamos, un interesante nicho de empleo para los graduados en Derecho que sepan especializarse en la materia.

Finalmente, el Reglamento General de Protección de Datos incluye una regulación mucho más detallada de las obligaciones que han de cumplir los responsables del tratamiento. En ella se ha procurado, por una parte, unificar estas exigencias en todo el territorio de la Unión para evitar duplicaciones y contradicciones. Por otra, la nueva normativa trata de limitar tales exigencias a los supuestos en que sean necesarias, con el fin de ahondar en su objetivo de racionalización. El nivel de necesidad se determina, en unos casos, en función del riesgo que implique el tratamiento para los derechos de las personas; en otros, en relación con el tamaño de la empresa. Por supuesto, también hay obligaciones, que son exigidas en todo caso.

Las obligaciones de carácter general tienen que ver principalmente con la seguridad del tratamiento y con el respeto a los principios de protección de datos. Respecto a este último, el Reglamento ha introducido el principio de «protección de datos desde el diseño y por defecto», que obliga a los responsables a tener presentes los principios de protección ya en el momento de diseñar los tratamientos que necesitan para su actividad económica. Con ello se pretende que la protección de datos no se considere en las empresas algo postizo, un requisito burocrático más que ha de cumplimentarse, sino que se integre y esté presente en todas las decisiones relacionadas con el tratamiento. Se recomiendan, además, mecanismos como la «pseudonomización» (tratamiento en el que la identificación de las personas afectadas requiere de una información adicional que figura por separado y está asegurada por suficientes medidas técnicas). En relación con la

seguridad, la normativa insiste en la necesidad de que exista un «proceso de verificación y valoración regulares de la eficacia de las medidas técnicas y organizativas para asegurar la seguridad del tratamiento» [art. 32.1 *d)*] y obliga, en caso de violación de seguridad, a informar a la autoridad de control competente y a los propios afectados (arts. 33 y 34).

Limitada en función del tamaño de la empresa es la obligación de registro de las actividades de tratamiento. Registro que debe incluir una información muy concreta y detallada descrita en el art. 30. La obligación pesa sobre los responsables y también sobre los encargados del tratamiento que efectúen éste por cuenta de un responsable. Sustituye claramente a la notificación previa a la autoridad de control de la normativa anterior y sólo se exige a las empresas que superen los 250 empleados, por lo que deja libres de tal carga a las pequeñas y medianas empresas.

Determinados tratamientos requieren medidas especiales. En concreto, aquellos que por su naturaleza, especialmente si utilizan nuevas tecnologías, suponen un alto riesgo para los derechos y libertades de las personas físicas requieren una evaluación de impacto del tratamiento. Ésta ha de incluir una evaluación de la necesidad y proporcionalidad del tratamiento, de los riesgos que implica para los derechos y libertades, y de las medidas previstas para paliarlos. Vuelven a introducirse aquí mecanismos ya ensayados en otros ámbitos del Derecho, pues estas autoevaluaciones recuerdan a las que se exigen en materias como la prevención de riesgos laborales o la igualdad. Las autoridades de control elaborarán una lista de los tratamientos que requieren una evaluación de impacto, aunque el propio Reglamento ya señala algunos supuestos. En concreto, la requerirán los tratamientos que supongan una evaluación sistemática y exhaustiva de aspectos personales, como la elaboración de perfiles, que sirvan de base para la toma de decisiones con efectos jurídicos sobre las personas. También la requerirán los tratamientos a gran escala de categorías especiales de datos y la observación sistemática a gran escala de una zona de acceso público. Si el resultado de la evaluación es que el tratamiento supone un alto riesgo para los derechos y las libertades de las personas, el responsable debe entonces, con carácter previo, consultar a la autoridad de control competente sobre la suficiencia de las medidas tomadas para evitarlo. La autoridad podrá entonces asesorar por escrito al responsable y tomar todas las medidas que estime necesarias para defender tales derechos y libertades. Los Estados miembros pueden, además, ampliar los supuestos en que es necesaria esa consulta previa.

Por último, el Reglamento introduce una nueva obligación para determinado tipo de tratamientos que consiste en la designación de un «Dele-

gado de protección de datos». Esta designación será necesaria siempre que el tratamiento lo efectúe una autoridad pública (salvo los tribunales), cuando las actividades del responsable o del encargado impliquen «una observación habitual y sistemática de interesados a gran escala» o cuando se traten a gran escala categorías especiales de datos. (art. 37.1). Los Estados miembros pueden ampliar los supuestos en que es obligatoria la designación, que puede ser también decidida voluntariamente en casos distintos de los previstos. El delegado de protección debe tener los conocimientos suficientes sobre la regulación de la materia y tiene garantizado por la normativa un estatus de independencia. De tal modo, no debe recibir instrucciones del responsable o del encargado del tratamiento, ni ser destituido o sancionado por el ejercicio de sus funciones. Puede ser un empleado del responsable o del encargado o realizar sus funciones desde fuera en el marco de un contrato de servicios. Sus funciones son básicamente tres: la primera, asesorar al responsable o al encargado del tratamiento sobre el cumplimiento de la normativa de protección de datos; la segunda, supervisar el cumplimiento en la entidad de esa normativa, y la tercera, actuar como punto de contacto de la autoridad de control, con la que debe colaborar y a la que puede dirigir consultas. No se prevé expresamente que el delegado pueda atender quejas o solicitudes de los afectados por el tratamiento, ya sean clientes o empleados de la empresa, por lo que no se le concibe como un «defensor del cliente» o del empleado en materia de protección de datos. Su figura se aproxima más bien a la de un auditor interno en materia de protección.

V. UN SISTEMA DE CONTROL MÁS COORDINADO, EFICIENTE Y EXPEDITIVO

Es ésta probablemente una de las dimensiones del Derecho europeo de protección de datos donde el Reglamento General ha tratado de poner más énfasis. No en vano la falta de cooperación entre las autoridades de control de los Estados miembros y las divergencias en la interpretación del Derecho comunitario fueron identificados por la Comisión como uno de los puntos débiles más importantes de la normativa anterior. Obviamente, el mayor problema viene del flujo transfronterizo de datos entre países de la Unión, pues en su control se ven efectivamente implicadas varias autoridades de control, cuyas actuaciones pueden estar muy descoordinadas e, incluso, ser contradictorias. Para evitar este problema la nueva normativa establece una diferenciación entre la autoridad principal, aquella que

corresponde al Estado donde el responsable del tratamiento o el encargado tienen su establecimiento principal (art. 56), y las autoridades interesadas, que se ven involucradas por el tratamiento al afectar éste sustancialmente a personas residentes en su territorio, tener un establecimiento del responsable en él o haber recibido una reclamación en relación con dicho tratamiento (art. 4.22).

Las autoridades de control tienen la obligación de cooperar entre sí (art. 60), de proporcionarse asistencia mutua (art. 61) y pueden realizar incluso «operaciones conjuntas» (art. 63). En el caso de tratamientos que afecten a uno o varios Estados, la competencia para resolver corresponde a la que hemos llamado autoridad principal, si bien debe presentar un proyecto de decisión a las autoridades interesadas para que éstas emitan un dictamen. El Reglamento insiste en que las autoridades deben esforzarse por llegar a un acuerdo. En el caso de que alguna de las autoridades interesadas plantee «una objeción pertinente y motivada», que la autoridad principal no estime conveniente seguir, se activa el «mecanismo de coherencia» del art. 63. El mecanismo de coherencia supone la intervención del Comité Europeo de Protección de Datos, que emitirá un dictamen, cuyo contenido la autoridad principal «tendrá en cuenta en la mayor medida posible». Se trata, pues, de un dictamen no vinculante. No obstante, si la autoridad principal desoye el dictamen del Comité, o directamente no lo solicita cuando procede, se activa el sistema de solución de conflictos previsto en el art. 65. Aquí el Comité vuelve a emitir una resolución, pero no en forma de dictamen, sino de «decisión vinculante». El mecanismo de coherencia está previsto también para unificar los criterios a la hora de elaborar las listas de tratamientos que requieren una evaluación de impacto, la supervisión de códigos de conducta, la acreditación de organismos certificadores, y las medidas suficientes de protección que ha de garantizar (a través de cláusulas tipo, cláusulas contractuales y normas corporativas vinculantes) el responsable de un tratamiento transfronterizo de datos con destino a un Estado cuya legislación no ofrezca unos estándares de protección equivalentes a los europeos.

El propio Comité Europeo de Protección de datos mencionado supone una importante novedad introducida por el Reglamento. La Directiva de Protección de Datos ya preveía la existencia de un «Grupo de protección de personas en lo que respecta al tratamiento de datos personales», en el que participaban todas las autoridades de control de los Estados miembros (art. 29), pero sus funciones eran estrictamente consultivas, de estudio y asesoramiento, sin que tuviera competencia para dictar decisiones

vinculantes. El nuevo Comité, formado también por representantes de las distintas autoridades de control nacionales, mantiene esas competencias asesoras, pero detenta además las importantes funciones que le confiere el mecanismo de coherencia.

Estamos ante su sistema de control más unificado y eficiente, pero también más expeditivo. El Reglamento prevé la imposición de sanciones administrativas en toda la Unión Europea por los incumplimientos de sus reglas y dedica una buena extensión de su articulado a establecer las normas comunes que han de inspirar tales sanciones (arts. 83 y 84). Se garantizan, además, el derecho a presentar reclamaciones y a la tutela judicial efectiva, tanto frente a decisiones de las autoridades de control, como frente a conductas de los responsables o encargados del tratamiento. Se ha abierto, además, la posibilidad de que las entidades sin ánimo de lucro puedan intervenir en tales reclamaciones. Ya sea por mandato expreso del interesado; ya sea, si lo autorizan los Estados, en forma de «acusación popular» (art. 80). Con ello se facilitará sin duda la interposición de reclamaciones administrativas y judiciales en una materia de indudable interés general, pero en la que los particulares pueden verse sobrepasados, dado su elevado carácter técnico y su extrema complejidad.

VI. ALGUNAS CONSIDERACIONES SOBRE EL ÁMBITO LABORAL Y DE SEGURIDAD SOCIAL

Que las relaciones laborales caen dentro del ámbito de aplicación de la normativa de protección de datos es hoy cuestión felizmente fuera de toda duda. Baste para ilustrarlo la opinión que sobre el particular emitió en su día el Grupo de Trabajo del art. 29 de la Directiva: «Empleadores y empleados deben ser conscientes de que muchas actividades realizadas rutinariamente en el contexto del empleo implican el proceso de datos de los trabajadores, a veces de información muy sensible». Más adelante el Grupo señala que «la normativa de protección de datos no opera aisladamente del Derecho del trabajo»; al igual que el Derecho del trabajo «no opera aisladamente de la normativa de protección de datos». Esa interacción «es necesaria y valiosa y debería ayudar al desarrollo de soluciones que protejan adecuadamente los intereses de los trabajadores»[6]. Si habla-

[6] Opinión 8/2001, de 13 de septiembre de 2001, *On the processing of personal data in the employment context* (5062/EN/Final WP 48).

mos de los sistemas de seguridad y protección social, es evidente que el tratamiento a gran escala de datos de las personas protegidas es constante e imprescindible.

Por esta razón muchos países europeos han aprobado normas específicas de protección de datos en el ámbito de las relaciones de trabajo, con especial atención a la vigilancia de la actividad laboral. El Derecho comunitario anterior al Reglamento que comentamos no había dado, sin embargo, ese paso, más allá de algunas previsiones puntuales. Las consecuencias de su aplicación en dicho ámbito debían de extraerse de las reglas y principios establecidos con carácter general. La misma situación puede observarse en otros Estados miembros de la Unión, como es el caso de la propia España, donde sus leyes específicas mencionan el tratamiento de datos en el contexto laboral sólo de forma aislada y sin demasiados detalles. No quiere decir ello que el tratamiento de datos personales de los trabajadores quede sin regulación, simplemente que le serán aplicables los preceptos generales, sin adaptaciones particulares.

El nuevo Reglamento no ha alterado sustancialmente la situación, si bien cabe advertir en él ciertos cambios, tímidos pero interesantes. La primera referencia al tema la encontramos en su art. 9.2, al hablar de los supuestos en que es lícito el tratamiento de categorías especiales de datos (los también llamados datos sensibles). La letra *b)* de dicho artículo señala que podrá efectuarse el tratamiento de tales categorías de datos cuando éste sea necesario «para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social». Todo ello en la medida en que lo autorice el Derecho de la Unión o el de los Estados miembros y siempre que se establezcan «garantías adecuadas». Se menciona además expresamente al convenio colectivo como instrumento que, «con arreglo al derecho de los Estados miembros», puede autorizar este tipo de tratamientos. Resulta muy sugerente el reconocimiento explícito de una fuente reguladora tan característica de las relaciones laborales en este contexto. Por su parte, la letra *h)* autoriza esos tratamientos también cuando son necesarios para fines de «medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los servicios de asistencia sanitaria y social».

Pero la previsión más específica y de mayor alcance la encontramos en el art. 88, específicamente titulado «tratamiento en el ámbito laboral». En él, la Unión Europea autoriza a los Estados miembros a «establecer nor-

mas 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». Labor que podrá realizarse a través de medidas legislativas o de «convenios colectivos». Lo primero que salta a la vista es que no se ha querido establecer una regulación mínima común en la materia para toda la UE. Es evidente que el Derecho del trabajo presenta un alto grado de sensibilidad política y económica que ha impedido adoptar una posición común sobre el particular a nivel europeo, al menos con carácter vinculante. La UE se ha limitado a permitir y salvaguardar las opciones de los países que han buscado una protección más específica, en coherencia con el principio de subsidiariedad que rige en la materia.

Por otra parte, como ya apuntamos, es interesante la mención expresa al convenio colectivo, pero deben tenerse en cuenta las dificultades con las que se encontrarán las partes negociadoras a la hora ejercer esta facultad que se les concede. La negociación colectiva no pasa en Europa por su mejor momento, y pedirle que se interne en terreno tan complejo y delicado puede suponer pedir más de lo razonable. En primer lugar, porque cabe dudar de que sindicatos y asociaciones empresariales dispongan de los expertos especializados en la materia que son necesarios para abordarla con rigor; en segundo lugar, porque incluir un nuevo campo para la negociación tiene consecuencias en el proceso negociador y, normalmente, un coste en la dinámica de cesiones/concesiones que lo caracteriza. En este contexto, la llamada al convenio, aunque tiene sentido, puede quedarse en un brindis al sol. Personalmente, considero que, si de verdad se quería impulsar la existencia de regulaciones laborales específicas sobre protección de datos, debió establecerse una regulación de mínimos a nivel europeo que les sirviese de plataforma de apoyo. No obstante, cabe recordar que el Derecho comunitario avanza despacio, pero avanza. Es posible que en el futuro podamos asistir a desarrollos normativos más ambiciosos.

Conviene hacer una última aclaración antes de terminar este apartado. Debe evitarse la confusión que puede producir en los especialistas del Derecho del trabajo el nombre de la institución «delegado de protección de datos». La similitud que presenta con figuras de la representación de los trabajadores en la empresa (como «delegado de personal» o «delegado de prevención») constituye un auténtico «falso amigo». El delegado de protección no es un representante de los trabajadores, ni siquiera parece que vaya actuar como un «defensor del empleado». Ya hemos tenido ocasión de poner de relieve que se trata, más bien, de un auditor interno que actúa de enlace con las autoridades nacionales de control.

VII. ¿ES NECESARIA UNA NUEVA LEY ORGÁNICA DE PROTECCIÓN DE DATOS?

Debemos recordar para responder a esta pregunta que nos encontramos ante un reglamento europeo, norma que goza de aplicabilidad y efecto directo plenos. Así pues, no es necesaria *a priori* ninguna norma de desarrollo o trasposición por parte de los Estados miembros. Además, la nueva regulación, aunque introduce importantes novedades, mantiene en esencia los fundamentos básicos de la regulación anterior, por lo que no es previsible que se produzcan incompatibilidades o contradicciones relevantes con las normas aprobadas en desarrollo de ésta. Aun en el caso de que se produzcan, no hay duda de que entonces el nuevo Reglamento desplazará sin más a las normas internas que no se ajusten a su contenido.

No obstante lo dicho, debemos destacar que el Reglamento General de Protección de Datos parte siempre del hecho de que va a existir una regulación interna. Regulación que expresamente autoriza en muchos de sus apartados y a la que encomienda tareas específicas en otros. El art. 88, que acabamos de comentar en al apartado anterior, es ejemplo de lo primero. Como muestra de lo segundo, podemos señalar el art. 83, donde se establecen las «condiciones generales para la imposición de sanciones administrativas». Es evidente que este precepto requiere para su cumplimiento del desarrollo de una norma en cada Estado que implemente sus principios y condiciones. Lo mismo sucede, por poner otro ejemplo, en el art. 54, donde se establece que cada Estado ha de regular por ley su propia autoridad de control. Una solución posible, y coherente con la lógica del Derecho de la Unión, sería derogar la Ley Orgánica de Protección de Datos hoy vigente, dejando que el Reglamento Europeo se erija en la norma principal de referencia en la materia, y aprobar una o varias leyes especiales dedicadas exclusivamente a la implementación de aquellos aspectos particulares en los que se permite o se exige la elaboración de una normativa nacional específica.

Con todo, hay razones de peso que aconsejan la elaboración de una nueva ley orgánica. Y uno no pequeño es la necesidad de hacer la normativa de protección de datos lo más sencilla y asequible posible a los operadores jurídicos y económicos. Si ya hemos dicho que la complejidad y tecnicismo de la materia están alcanzando niveles demasiado elevados, dispersar la regulación en diversos instrumentos comunitarios e internos no va a contribuir en absoluto a la comprensión y entendimiento de sus

normas. Por ello, la opción de una nueva ley que haga suyas las previsiones del Reglamento y las integre sistematizadamente con las introducidas en el legítimo desarrollo de las competencias estatales aparece como la más razonable. El propio Reglamento es consciente de ello y en sus considerandos señala que, «en los casos en que el presente Reglamento establece que sus normas sean especificadas o restringidas por el Derecho de los Estados miembros, éstos, en la medida en que sea necesario por razones de coherencia y para que las disposiciones nacionales sean comprensibles para sus destinatarios, pueden incorporar a su Derecho nacional elementos del presente Reglamento» (8). En conclusión, tendremos previsiblemente nueva Ley Orgánica de Protección de Datos, si bien para ello se dispone hasta el 25 de mayo de 2018, fecha a partir de la cual será aplicable la norma europea.