El cumplimiento de la normativa de protección de datos personales y su impacto en la Universidad

Compliance with personal data protection regulation and its impact on the University

Pilar Conde Colmenero
Facultad de Ciencias Jurídicas y Económicas
Universidad Isabel I
pilar.conde@ui1.es

Víctor Cazurro Barahona
Facultad de Ciencias Jurídicas y Económicas
Universidad Isabel I
victor.cazurro@ui1.es

Índice

Resumen:

La legislación define las Universidades Públicas como Administraciones, de modo que tienen todas las prerrogativas y potestades de éstas. Los Estatutos de las Universidades Públicas reconocen esta naturaleza jurídico-pública. Por otro lado, a las Universidades privadas les serán de aplicación las normas correspondientes a la clase de personalidad jurídica que estas hubieran adoptado. Las universidades son entidades que tienen como rasgo constitucional su autonomía. Y sean públicas o privadas, están sujetas a las obligaciones que la legislación estatal y comunitaria recoge en materia de protección de datos personales.

El progresivo reconocimiento del derecho fundamental a la protección de datos ha discurrido de forma similar a la implantación masiva de las tecnologías de la información y la comunicación en cualquier empresa, o institución y, en consecuencia, también en las

universidades. Éstas tratan datos personales para cumplir con su actividad de gestión, docencia e investigación. Las relaciones de la universidad con la administración pública, con su personal y con sus alumnos, se canalizan en su mayor parte a través de Internet y de campus virtuales.

El almacenamiento y el tratamiento de datos personales deben tener en cuenta la regulación vigente y todo lo que ello conlleva.

Para las instituciones académicas (públicas o privadas) esto ha supuesto adaptarse, cambiar su manera de trabajar y de comunicarse, y desarrollar protocolos que hagan compatible su actividad y la prestación de sus servicios con el cumplimiento de la legislación vigente en materia de protección de datos y, en consecuencia, con el amparo del derecho a la privacidad de los afectados por dichos tratamientos.

El cumplimiento normativo en esta materia complica la burocracia en la universidades viven inmersas. Además, la complejidad de su implantación y mantenimiento no es gratuita. Conlleva múltiples obligaciones, entre otras, una puesta al día en la materia; es posible que sean necesarios los servicios de una consultora externa que asesore en todo el proceso; aumentan las competencias y responsabilidades de algunas personas de la organización que deberán encargarse de este asunto; implica el diseño de protocolos específicos de almacenamiento, tratamiento y destrucción de datos; en función del nivel de las medidas de seguridad, precisará de auditorías; y requerirá de algunas acciones de formación e información de los agentes implicados en el tratamiento. Todo ello se traduce en un coste extra en personal, tiempo y dinero que requiere un estudio detenido.

Palabras clave

Universidad, universidad pública, universidad privada, protección de datos personales, gasto, gasto público, impacto económico

1. La universidad y la protección de datos personales

La universidad es probablemente uno de los agentes sociales que más datos personales maneja. Y, de entrada, y sin hacer distingos entre públicas o privadas, nos encontramos con que la labor

diaria de sus trabajadores (personal de administración y servicios, personal docente e investigador y órganos de gobierno) implica un tratamiento de datos ineludible que requiere de una mínima formación.

El personal de administración y servicios (en adelante PAS) maneja datos de todo tipo: datos de pre-alumnos, de alumnos, de docentes, de investigadores… Hacen un tratamiento diario de notas, datos económico financieros, contractuales, afiliación sindical y, excepcionalmente de datos relacionados con la salud (partes médicos, bajas laborales, certificados médicos necesarios para cursar alguna titulación –Ciencias de la Actividad Física y del Deporte, por ejemplo-, etc.).

El personal docente e investigador (en adelante PDI) trabaja inmerso en datos sobre calificaciones, listados de nombres y apellidos, DNI, etc. Ambos colectivos desconocen en profundidad la regulación de la protección de datos personales.

Si bien, es cierto que la mayor parte son datos que, sin llegar necesariamente a encajar en el tipo que la LOPD o el Reglamento considera acreedores de un nivel de seguridad alto, no dejan de ser especialmente sensibles que es lo que son, por ejemplo, los datos bancarios o las calificaciones.

Como se verá más adelante, a todo ello hay que sumar que el trabajo digital e internet han complicado las labores de seguridad y confidencialidad y eso, obviamente, afecta a la protección de los datos personales en las universidades. Máxime si estas tienen un tamaño grande, con diversos campus físicos, un campus virtual y una continua entrada y salida de soportes que contengan información sensible. Pero el tamaño o la diversidad de ubicaciones físicas son solo algunos de los factores que condicionan la llevanza diaria de los deberes a que obliga la normativa en la materia que ocupa esta reflexión. Es razonable pensar que algunas de las debilidades más importantes de cara a cumplir con una normativa tan compleja, se encuentran en la escasa formación especializada de las personas que efectúan el tratamiento de la información y la ignorancia de las graves consecuencias de no hacerlo conforme a derecho.

Por este motivo, las instituciones académicas deben ser conscientes de la inversión que es preciso realizar para contar con el necesario asesoramiento técnico que les ayude y les guíe, no solo a ejecutar una correcta puesta al día en materia de protección de datos, sino que les preste un servicio que permita a la Universidad mantener al día la documentación correspondiente, actualizados los protocolos de seguridad y funcionamiento, y que sea capaz de formar a la plantilla implicada. Solo de este modo, es posible cumplir escrupulosamente con las exigencias de la legislación nacional y europea vigente.

La necesidad de esta asistencia de consultoría lo es desde el momento en que cumplir con la ley y el reglamento implica realizar una serie de gestiones ante la Agencia Española de Protección de

Datos (en adelante AEPD), un aumento de las competencias y responsabilidades de determinadas personas de la organización que deben atender este asunto; supone el estudio y diseño de nuevos protocolos de seguridad, almacenamiento, tratamiento y destrucción de datos; y requiere de algunas acciones de formación e información de los agentes implicados en el tratamiento (PAS, PDI, etc.). Además, será preciso realizar las obligadas auditorías bienales a las que se deberá someter cualquier universidad. Como se verá en futuros epígrafes, todo esto se traduce en un coste extra en personal y otros recursos, o lo que es lo mismo: tiempo y dinero.

Por último, conviene señalar que la aprobación del nuevo Reglamento europeo (en adelante Reglamento UE) el 25 de mayo de 2016 trajo consigo algunas novedades que afectan de manera desigual (aquí sí) a universidades públicas y privadas. Por ejemplo, la figura del Delegado de protección de datos (que analizaremos luego) será una obligación de las públicas (como administración pública que son) y no de las privadas. La naturaleza pública o privada implica algunas diferencias tanto en las obligaciones como en la aplicación de asuntos tan relevantes como las sanciones por incumplimiento de la normativa, ya que, al contrario que las universidades públicas, las privadas podrán ser sancionadas económicamente.

2. La Universidad Pública: una administración frente al derecho a la protección de datos

La legislación española ha definido a las Universidades Públicas como Administraciones (personas jurídico-públicas del tipo Corporaciones y, por tanto, nacidas por Ley) de modo que tienen todas las prerrogativas y potestades de éstas. Sus actos son susceptibles de recurso en la propia vía administrativa y en la contencioso-administrativa también, desde la fuerza de la tutela judicial efectiva. En efecto, precisamente el que no sean sus actos *negociales* sino reglados, y normados, hace que cualquier debate sobre su razón, o revisión y evitación de todo exceso del *imperium* pueda ser recurrible, para que siempre se ajuste su actuación a Derecho.

En cuanto al derecho fundamental a la protección de datos personales, la actividad de las administraciones no es opcional sino obligada; por ello están sometidas a todos los deberes referentes a la protección de este Derecho fundamental. La consolidación de este derecho ha discurrido de forma paralela al uso masivo de las TIC en las Administraciones Públicas y, en consecuencia, también en las Universidades Públicas. Esto aporta un poco más de complejidad al asunto, ya que la implantación, coordinación, fomento y preservación de garantías en la transformación digital de toda la tramitación administrativa se ha de normalizar. Porque se ha de tener en cuenta que la política legislativa tiene fijado el reto de alcanzar esta normalización en la tramitación electrónica, asistiendo a una transformación digital con actuaciones en TIC para

implantar las previsiones contenidas en las Leyes 29 y 40/2015 (Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas y Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público).

Las universidades son administraciones que recaban, tratan y almacenan datos personales de sus alumnos (actuales e históricos), de su PDI y de su PAS. Esa información debe quedar organizada y almacenada en ficheros cuyo titular es la universidad. Tratamiento que las universidades deben hacer bajo la regulación vigente y todo lo que ello implica desde el punto de vista técnico y organizativo.

Esa regulación tiene un marco muy bien definido tanto en España como en Europa; en España, con la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD) y el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento que la desarrolla (RLOPD); y en la Unión Europea, con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en adelante Reglamento UE), que deroga la obsoleta Directiva 95/46/CE.

Ya desde el año 1999 con la LOPD, la legislación imponía una serie de obligaciones para las que las universidades (públicas y privadas) no estaban preparadas. Cumplir de manera escrupulosa con todos los deberes que la Ley requería era una labor complicada en unas instituciones que funcionaban (y algunas todavía funcionan) de manera anquilosada. Y es que el cumplimiento normativo (el hoy llamado *compliance*) en este ámbito contribuye aún más al síndrome de "*burocracia digital*" en la que se ven inmersas las universidades públicas que, sin embargo, no pueden dejar de ser efectivas y eficaces, y de ese modo responder al mandato del artículo 103.1 de la CE. Pero hay otro aspecto importante a tener en cuenta: la complejidad de su planificación e implantación conlleva más gasto público y una toma de conciencia y una apuesta decidida por parte de los órganos de gobierno de la universidad y de toda su comunidad.

Implica realizar una serie de gestiones ante la AEPD, designar a las personas responsables del asunto que tendrán un considerable aumento de sus responsabilidades; supone el diseño e implantación de nuevas reglas y protocolos de seguridad, modos diferentes de almacenamiento, tratamiento y destrucción de datos, etc.

Por todo ello, es recomendable, acudir al asesoramiento de los especialistas a través de la contratación de juristas o consultoras especializadas que guíen a la universidad en su puesta al día. Estos profesionales tendrán que asistir a la institución académica en las obligadas auditorías bienales a las que se deberá someter. Aunque esta es la obligación legal, la experiencia recomienda que dichas auditorías sean, al menos, cada año, pues el desfase que se puede producir

entre la documentación (Documento de seguridad, esencialmente) y los aspectos de índole organizativa es considerable. Conviene que el seguimiento, mantenimiento y actualización sea continuo. El título VIII del RLOPD regula un aspecto clave para la tutela del derecho fundamental a la protección de datos, la seguridad, que repercute los citados aspectos organizativos aspectos organizativos, de gestión y aún de inversión, en todas las organizaciones que traten datos personales.

Tener todo esto conforme a Derecho, se traduce en mayor coste de personal, más tiempo de dedicación y mayor inversión económica. Sobre todo porque esta carga de gestión de datos, tal y como se apuntaba previamente, se ha de sobrellevar sin perder celeridad y eficacia en la dinámica ordinaria, se ha de conciliar con las reglas de transparencia a las que el servicio público obliga; y todo ello, con el reto de alcanzar y mantener un equilibrio presupuestario.

3. La puesta al día en materia de protección de datos personales en la Universidad

Para llevar a cabo una debida puesta al día, es conveniente que los órganos de gobierno de la universidad decidan asesorarse a través de los servicios de una consultora externa o despacho especialista en protección de datos. Se trata de un primer coste que el presupuesto anual debe prever. Una consultora puede realizar la evaluación del estado de la cuestión, emitir un informe de adecuación y proponer y luego ejecutar las acciones necesarias para que la universidad disponga de un **Plan de Actuación** que recoja todo lo necesario para cumplir con la normativa.

Se trata de realizar la **adecuación del cliente a la LOPD, su RLOPD y, ahora al Reglamento UE**, a partir de la recogida, tratamiento y almacenamiento de la información en la universidad. Es preciso, por tanto, realizar la adaptación que dará lugar al informe de adecuación que el responsable o asesor técnico al responsable del fichero (la universidad), y en el que se identificarán las deficiencias encontradas con el fin de que se implanten determinados protocolos, o bien se adopten las medidas correctoras oportunas.

En consecuencia, es razonable afirmar que la universidad debe asesorarse para realizar una adecuación jurídica en virtud de la información que proporciona y así cumplir con lo contemplado en la LOPD y en su Reglamento y los procedimientos e instrucciones vigentes en materia de protección de datos.

Previamente a la adecuación, con el objeto de desarrollar el plan de actuación, serán necesarias algunas reuniones con las diferentes áreas de trabajo y departamentos de la universidad; esto facilitará la recogida de información que permita tener una imagen fiel de la situación de la institución en materia de protección de datos. En esta tarea es clave la figura del Responsable de

protección de datos en la entidad. Es preciso que haya una persona encargada (o un departamento si la institución tiene un tamaño importante) dentro de la plantilla de la universidad que sea capaz de facilitar y trasmitir a la consultora cómo funciona la institución, qué personas se ven implicadas en el tratamiento de datos y qué carencias pueden existir en ese momento concreto. En este punto, el Reglamento UE ha incluido la nueva figura del "**Delegado de Protección de datos**" o "*Data Protection Officer*" que queda regulada en los artículos 37 a 39. Se trata de un especialista en derecho de protección de datos, una figura obligada en las Universidades públicas (pues el tratamiento se lleva a cabo en un organismo público –art. 37.1.a) Reglamento UE), que se crea al lado de las figuras del responsable y del encargado del tratamiento de los datos, y que toda administración pública debe tener. Esta figura es una de las novedades de la regulación comunitaria. Aquí se evidencia un **nuevo coste para la universidad** que debe nombrar a una persona para que asuma, como mínimo, las funciones de informar y asesorar a los responsables y encargados del tratamiento de datos personales de las obligaciones que tienen; supervisar el cumplimiento de dicha legislación y de la política de protección de datos en la universidad, ofrecer el asesoramiento necesario para hacer la evaluación de impacto de un tratamiento de datos personales cuando entrañe un alto riesgo para los derechos de los afectados y supervisar su aplicación. En suma, la gestión universitaria se complica con la necesaria profesionalización de la tarea que se ha de desplegar, sabiendo que tal profesionalización, además de gestora ha de ser formadora (como se señalará en el punto 3).

4. Obligaciones legales básicas para las universidades

Entre otras obligaciones, las elementales para las Universidades son las de **inscribir los ficheros**, tanto informatizados como en soporte papel, que utilicen para el ejercicio de sus competencias, y comunicarlos al Registro de la AEPD. La universidad, con la ayuda de la consultora, identificará esos ficheros, el contenido de los mismos, el nivel de seguridad requerido, y los inscribirá en el Registro. Pero el trabajo en este punto no consiste solo en esta acción puntual, sino que debe ser continuo. Periódicamente, la universidad, a través de su Delegado en las públicas o de la persona o departamento responsable en las privadas y, en todo caso, asesorada, deberá analizar a lo largo del tiempo, la idoneidad de los ficheros inscritos, su adecuación a los niveles de seguridad y la conveniencia de inscribir nuevos ficheros, modificar o suprimir los existentes en el Registro de la AEPD.

Una vez definidos e inscritos los ficheros, es obligatorio elaborar el **Documento de Seguridad** de la universidad (artículo 88 RLOPD). Este ha de recoger los protocolos de actuación en cuanto protección de datos se refiere, la política y medidas de seguridad, los procedimientos internos implementados, los procedimientos usados para la recogida de los datos, el tratamiento y, en su caso cesión o utilización de los resultados del tratamiento. Huelga decir que otro de los nuevos

trabajos que debe asumir la institución es tener este documento permanentemente actualizado y a disposición de la posible inspección de la AEPD.

Pero, teniendo en cuenta la dimensión de algunas universidades, con diferentes campus que en ocasiones están ubicados en diferentes ciudades, con distintos centros o Facultades que disponen de sus propios negociados y equipo de administración, y casi seguro con un sistema de *cloud computing* que permite compartir la información de todos esos campus e implicar a muchas personas accediendo a la misma información, será preciso que la universidad articule **un departamento de juristas especialistas dedicado a la protección de datos** en torno al Delegado que ayude a organizar todo el sistema. Ese departamento debe ser capaz de resolver las incidencias que se presenten a diario y que, en circunstancias normales, no debiera depender solo de una consultora externa. Otra vez una necesidad: un departamento formado por juristas conocedores de la materia que, liderados por el Delegado, sean capaces de hacer este trabajo. Un coste más para incluir en el capítulo de gastos del presupuesto de la universidad.

Estas incidencias, consultas o cuestiones relacionadas con protección de datos pueden ser consultas del propio PAS o del PDI acerca del tratamiento de datos personales de los alumnos o del profesorado, quejas y reclamaciones, solicitudes de ejercicio de los derechos ARCO (acceso, rectificación, cancelación y oposición), por ejemplo, peticiones de cancelación de datos por parte de antiguos alumnos, ex docentes, etc.

Al Documento de seguridad deberán acompañarle diversos anexos: en primer lugar, un **anexo por cada fichero** que detalle aquello que recoge el mismo, su número de registro, personas con acceso a los datos de ese fichero, nivel de seguridad del mismo, fecha de su última actualización, etc.

En segundo lugar, será preciso redactar y tener actualizados todos aquellos **contratos de acceso a datos por cuenta de terceros** que el artículo 12.2 LOPD exige para la realización de tratamientos por parte de empresas o profesionales que presten, de manera externa, algún servicio a la universidad y por ese motivo tengan acceso a información sensible. Ese contrato "*deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento"*.

Esa área o departamento (o el Delegado de protección de datos) deberá elaborar un número elevado de contratos que la universidad como responsable del tratamiento deberá firmar con aquellos terceros que, en un momento dado y por diversas circunstancias, deban acceder a los datos que custodia la universidad. La elaboración, y sobre todo la actualización y resolución de estos contratos es una costosa tarea que también debe asumir la universidad.

En tercer lugar: será necesario estudiar y redactar todas las **cláusulas o leyendas** que la universidad debe incluir sobre recogida de datos, obtención del consentimiento y cesión de datos a terceros. Estas cláusulas responden al deber de información del artículo 5 de la LOPD, y son un elemento clave para cumplir con el precepto y, a su vez, satisfacer el derecho a estar informado del titular de los datos.

En este punto, se debe atender no solo a los datos recogidos en soporte papel, sino a los múltiples formularios digitales y apartados web que en una universidad (y, en ocasiones, todas sus facultades por separado) permiten una preinscripción, una matrícula o una solicitud de información por parte del interesado. Es preciso que las cláusulas y leyendas aparezcan de manera clara y la recogida del consentimiento del afectado también lo sea. En este sentido, el Reglamento UE, en su Considerando 32 hace referencia a que "*el consentimiento debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen, como una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal. Esto podría incluir marcar una casilla de un sitio web en Internet".* El soporte digital y operar en internet extiende los deberes y la responsabilidad del departamento de protección de datos al departamento informático de la universidad que también verá incrementado su volumen de trabajo así como su responsabilidad, pues no solo deberá implementar las casillas, cláusulas y leyendas oportunas que aseguren todas las garantías para el derecho a la protección de datos del interesado, sino que también deberán implicarse en el diseño e implementación de la política recogida en el Documento de seguridad. En este punto, cobra especial importancia la ciberseguridad y todo lo que referente a la salvaguarda de la información almacenada por la universidad, sea en servidores o equipos físicos locales o en la nube (*cloud computing*). Esto requiere de la implementación de sistemas de garantía (copias de seguridad, réplicas de las mismas en diversos espacios) que supone un nuevo gasto periódico que la universidad deberá sumar a todos los deberes ya expuestos.

En cuarto lugar, existe otro aspecto que se debe considerar: la **videovigilancia y el tratamiento que se da a las imágenes** grabadas (que son datos personales de alumnos, PDI, PAS, etc.), ya que prácticamente las instalaciones de cualquier universidad incorporan ya este tipo de sistemas de seguridad en sus campus.

La Guía sobre videovigilancia de la AEPD (Madrid, 2009) recoge que «*la videovigilancia generalmente persigue garantizar la seguridad de los bienes y las personas o se utiliza en entornos empresariales con la finalidad de verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales. Ambas finalidades constituyen bienes valiosos dignos de protección jurídica, pero sometidos al cumplimiento de ciertas condiciones. La utilización de*

medios técnicos para la vigilancia repercute sobre los derechos de las personas, lo que obliga a fijar garantías». Por tanto, la fijación de esas garantías también es una obligación de la universidad si quiere cumplir con las exigencias de la regulación vigente en esta materia. Esto implica que el departamento (o el Delegado de protección de datos en la universidad pública) se encarguen de este asunto y, en su caso, de controlar la actividad de quien preste este servicio (sea interno o externo), supervisando que se hace cumpliendo con lo exigido en la Instrucción 1/2006, de 8 de noviembre, de la AEPD, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras.

Por último, es preciso un análisis de la existencia de Transferencias Internacionales de Datos (TID), así como de las necesidades detectadas y las cláusulas necesarias que sea preciso incluir.

Pero el cumplimiento (el ahora llamado *compliance*) de todos los requerimientos descritos a que obliga la normativa no es suficiente. Garantizar los derechos de los afectados y tener a disposición de la AEPD la documentación necesaria debe acompañarse de una estrategia o de un plan de acción **coordinado entre los órganos de gobierno de la universidad, el departamento de protección de datos (o área jurídica encargada) y el departamento informático y de seguridad.** Si esto no se produjera, el trabajo estaría hecho solo a medias y la universidad dispondría de una documentación llena de buenas intenciones pero poco operativa de cara a la protección real y efectiva de los derechos de los afectados. Y, es evidente, que esta acción coordinada supone más horas de trabajo y medios (humanos y materiales) para las áreas implicadas, una estrategia, un cronograma de acciones y seguimiento de los trabajos ejecutados.

Además, no se trata de acciones puntuales; la ley obliga a la realización de auditorías bienales para determinados niveles de seguridad (medio y alto) con lo que constriñe a la universidad a llevar al día y actualizar la documentación oportuna, las modificaciones de los ficheros o creación de otros nuevos, etc.

5. La necesaria implicación de la comunidad universitaria en la gestión de la protección de datos personales

Al comienzo de este trabajo se hace referencia al compromiso de los órganos de gobierno en la puesta al día de la universidad en materia de protección de datos. Junto a este compromiso, es necesario que toda la comunidad universitaria se implique y tome conciencia de la relevancia del asunto. Es preciso que todos los colectivos afectados tengan las nociones básicas de qué es el derecho a la protección de datos personales, conozcan sus derechos y obligaciones (así como los de los demás) y manejen los protocolos de seguridad y las cautelas básicas cuando efectúa un

tratamiento de datos personales (PDI y PAS). Por ello, es importante no solo la labor jurídica y de gestión, sino también la labor pedagógica y de concienciación para toda la comunidad universitaria.

Es la propia universidad la que mejor conoce su funcionamiento y, por este motivo, es importante que sea la propia universidad la que, en estrecha colaboración con una consultora especializada, y en el caso de la universidad pública el Delegado de protección de datos, asuma una labor de formación e información del colectivo implicado. Obviamente, también la organización de este tipo de acciones conlleva una inversión de tiempo y recursos. De tiempo de aquellas personas y departamentos que han de formarse; de recursos de la universidad que han de destinarse a la programación, organización y ejecución de un plan de formación de su plantilla.

A la vista de lo expuesto, es razonable incluir la protección de datos en el calendario de acciones de formación continua que, ya de por sí, son habituales entre las plantillas de personal, junto a otras materias como la prevención de riesgos laborales, la implantación de sistemas de calidad, las nociones de primeros auxilios y la formación en nuevas aplicaciones y herramientas de trabajo.

Algunas universidades públicas, conscientes de la importancia del tema tratado tienen suscritos **convenios con la AEPD para la colaboración y desarrollo de programas de cooperación educativa**. Estos convenios incluyen en su objeto, la puesta en marcha de acciones de estudio, publicaciones, jornadas formativas, seminarios, conferencias o congresos, con el fin de contribuir a la divulgación del derecho a la protección de datos personales. Entre estas universidades se encuentran la Universidad de Alcalá, la Universidad Carlos III, la Autónoma de Madrid, la Complutense y la UNED (puede accederse al texto de estos convenios en el siguiente apartado de la web de la AEPD: https://www.agpd.es/portalwebAGPD/LaAgencia/gestion_economica/convenios/otros_convenios-ides-idphp.php).

La consideración de las universidades públicas como administraciones, la naturaleza y cuantía de los datos personales tratados, y el elevado número de afectados o interesados por estos tratamientos es de tal calibre que la extinta Agencia de Protección de Datos de la Comunidad de Madrid (APDCM), entonces dirigida por el Catedrático de Derecho Constitucional Dr. D. Antonio Troncoso Reigada, ya vio necesaria la edición de una valiosa publicación en abril de 2008: "*Protección de datos personales para Universidades*". La obra recoge las principales obligaciones de las universidades en materia de protección de datos, los servicios que la propia agencia prestaba a las universidades, las consultas frecuentes, una breve guía de las mejores prácticas, y numerosos modelos, formularios y documentos tipo. El hecho de que la agencia

autonómica decidiera dedicar un manual extenso al sector, da la medida de la importancia de todo lo que implica la puesta al día y mantenimiento de estas instituciones académicas en protección de datos.

Aunque lo habitual ha sido una progresiva y tardía adecuación a la norma, existe alguna excepción digna de mención en cuanto al compromiso con el asunto en cuestión. Es el caso de la Universidad de Castilla – La Mancha que, a día de hoy, es la única universidad española (sea pública o privada) que elaboró e inscribió un Código tipo en el Registro General de Protección de datos en el año 2004[1].

6. Conclusiones

Primera.- La puesta al día de una universidad (sea pública o privada) en materia de protección de datos personales conlleva un esfuerzo extra a las instituciones académicas, tanto en el apartado de recursos humanos y materiales como en de contratación de algunos servicios externos.

Segunda.- Estos esfuerzos se traducen en un mayor coste económico para la institución académica.

Tercera.- En este estudio se contribuye y se suscribe la doctrina que apuesta por la elaboración y actualización de un *manual de buenas prácticas* o código tipo (artículo 32 LOPD) que sirva como herramienta o instrumento normalizado para que en las universidades se garantice y preserve el debido tratamiento de los datos personales.

Cuarta.- La protección de datos como reto de la universidad. Hoy por hoy, la debida garantía del derecho a la protección de datos personales es una realidad. Y también, una oportunidad para organizar, sistematizar y asegurar el modo de tratar y almacenar la información sensible de millones de afectados por la actividad que diariamente se desarrolla en las universidades. Con la llegada de internet, las universidades han tenido que adaptarse, cambiar su manera de trabajar y desarrollar modos de hacer y protocolos que hagan compatible el despliegue de sus actividades con el cumplimiento de la normativa en materia de protección de datos.

Como se ha visto en los párrafos precedentes, esto exige un esfuerzo humano y de recursos económicos que hasta hace bien poco no era necesario contemplar. La implicación de los Órganos

[1] Un código tipo es un instrumento de autorregulación de la propia universidad en materia de protección de datos. En él se adoptan reglas o estándares específicos que permiten armonizar los tratamientos de datos efectuados por quienes se adhieren al código tipo, a facilitar el ejercicio de los derechos de los afectados y a favorecer el cumplimiento de la normativa. La fecha inscripción del código tipo de la Universidad de Castilla-La Mancha 14/07/2004. Se adecuó al RLOPD el 16/11/2009.

de Gobierno, la formación de la comunidad universitaria, la acción coordinada de los departamentos jurídico y técnico-informático, la creación de la figura del Delegado de Protección de Datos, y la posible creación de un departamento dedicado en exclusiva a este asunto son elementos imprescindibles que, de un modo u otro, incidirán en la partida de gastos del presupuesto de las universidades.