© ***RIDHyC***, Nº 2.:9-34 (Diciembre, 2015) · ISSN (2386-7795)
www.didacticahumanidadesyciencias.com

PROTECCIÓN DE DATOS Y DOCENCIA UNIVERSITARIA. APUNTES DESDE UNA VISIÓN PRÁCTICA

Data protection and university teaching. Notes from a practical view

JOSÉ JULIO FERNÁNDEZ RODRÍGUEZ
Profesor Titular de Derecho Constitucional
Universidade de Santiago de Compostela
Josejul.fernandez@usc.es

Resumen
En el presente trabajo se analiza la normativa española de protección de datos en lo que puede interesar a la docencia universitaria. Así se revisan distintas cuestiones situacionales relativas al derecho fundamental a la protección de datos (definición, ámbito de aplicación, conceptos básicos) y referidas a los principios y derechos subjetivos que rigen en este ámbito, y a los ficheros de datos, medidas de seguridad y sanciones. Tras ello se resumen las obligaciones de las universidades en la protección de datos y se examina la dinámica práctica que debe seguir el profesorado universitario en esta materia. También se muestran ejemplos de casos prácticos reales que dieron lugar a consultas.
Palabras clave: Protección de datos personales, docencia universitaria, principios y derechos de la protección de datos, actividad del profesorado universitario en la protección de datos

Abstract
This paper analyses the Spanish regulations of data protection which may be of interest to university teaching. So are reviewed different situational questions relating to the fundamental right to the protection of data (definition, scope of application, basics) and concerning principles and subjective rights that govern in this area, and to data files, security measures and sanctions. After that summarizes the obligations of universities in the protection of data and examined the practical dynamics that must follow the University teaching staff in this matter. Also shows examples of real practical cases that gave rise to queries.
Keywords: Personal data protection, university teaching, principles and rights of data protection, activity of university professors in data protection

1. INTRODUCCIÓN

La temática de la protección de datos es un área jurídica compleja, incluso abigarrada, que muestra múltiples aristas que dificultan su análisis. La regulación aparece como diversa, a veces detallada, que combina reglas y principios que podríamos denominar generales con distintas excepciones de relevancia. La situación es similar en nuestro

Recibido: 01/08/2015
Aceptado:29/12/2015

entorno, pues ha sido la Unión Europea la que promovió las actuales previsiones de este sector del derecho. Puede decirse que en nuestro continente hay una verdadera homogeneización en este ámbito.

Un rasgo de la protección de datos es su afectación a prácticamente cualquier actividad social cotidiana. Y entre ellas también se encuentra la docencia universitaria. El tema no solo tiene una importancia cuantitativa, al afectar de manera intensa a la vida ordinaria, sino también cualitativa, en la medida que la protección de datos se ha configurado como un derecho fundamental.

En este trabajo nos proponemos mostrar las claves de la protección de datos en la docencia universitaria, sin agotar la problemática para no extendernos en demasía. Asimismo, creemos oportuno contextualizar la cuestión mostrando una serie de elementos de carácter general en esta temática, que también debería tener en cuenta el docente universitario en su labor. Citaremos en varias ocasiones la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (en adelante LOPD), y solo en algún caso el Reglamento de desarrollo de dicha ley, aprobado por el Real Decreto 1720/2007, de 21 de diciembre (en adelante RELOPD).

Vivimos en la sociedad de la información, una sociedad que al lado de sus evidentes ventajas para el progreso y el desarrollo, también se visualizan aspectos negativos como los nuevos riesgos provocados a la privacidad, que se maximizan por la capacidad de procesamiento de la información masivo, eficaz y barato (Fernández Rodríguez, 2004, 85 y ss.). Frente a ese riesgo se alzan garantías como las que dimanan de la protección de datos. Ya en 1983 el Tribunal Constitucional alemán alertaba de que los avances tecnológicos podían convertir a la persona en transparente, en un "hombre de cristal", que no podría proteger su intimidad. Más de treinta años después esa premonición ha adquirido una fuerza impensable en aquel entonces.

2. EL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS

1.1 Definición

Un derecho fundamental es un derecho subjetivo que se conecta con la dignidad de la persona, y que, como tal, está previsto en un ordenamiento constitucional determinado. Como derecho que es, otorga al titular del mismo ciertas facultades (para hacer o para evitar algo). Esta terminología, de derecho fundamental, es la que se suele usar en el ámbito del derecho constitucional. En el derecho internacional podemos decir que la noción equivalente es la de derecho humano (los derechos humanos se prevén en tratados internacionales).

En sentido jurídico, en España existe un derecho fundamental a la protección de datos, derivado del art. 18 de la Constitución española, y que posee autonomía propia. Este derecho consiste en la facultad que tiene toda persona de tener control sobre sus datos personales y decidir el uso que se le da a los mismos. O sea, todos y todas somos titulares de

una potestad de control sobre nuestros datos personales, que nos permite disponer y decidir sobre ellos.

El antecedente de esta previsión hay que buscarlo en el derecho a la intimidad, que originalmente se configura como un derecho de reacción, de índole liberal, que protegía al ciudadano frente a las intromisiones del poder público. En este sentido, los norteamericanos Warren y Brandeis, en 1890, defendían el derecho a ser dejado a solas (Warren/Brandeis, 1890).

El ámbito de protección y contenido de este derecho a la intimidad evoluciona y va ampliándose. Aparecen, así, el derecho al secreto de las comunicaciones y la inviolabilidad del domicilio. A día de hoy se trata de derechos fundamentales diferentes, pues el objeto protegido cambia de uno a otro. En esta línea de ampliación progresiva, surge también el derecho a la autodeterminación informativa, que es donde se sitúa la protección de datos.

En nuestro país semeja que se ha producido una equivalencia entre el derecho a la autodeterminación informativa y el derecho a la protección de datos, lo cual no deja de ser un reduccionismo dado que la problemática de la protección de datos es una de las varias que nacen de la interacción entre intimidad e informática y, por lo tanto, no agota, ni mucho menos, la misma.

A nivel europeo hay previsiones normativas de singular relieve en lo que ahora nos ocupa. Sirvan de ejemplo, en el Consejo de Europa, el Convenio Europeo para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (el denominado Convenio 108 del Consejo de Europa, de 1981); y en el marco de la Unión Europea, la Directiva 95/46/CE, 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. Además, el artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea recoge este derecho a la protección de datos de carácter personal.

En España, como dijimos, se hace derivar el derecho a la protección de datos del art. 18.4 de la vigente Constitución, que fue en primer lugar desarrollado por la Ley Orgánica 5/1992, de regulación del tratamiento automatizado de datos de carácter personal, ya derogada, y luego por la actual LOPD, de 1999. En ejecución de ella se dictó el también citado RELOPD, en 2007. También tienen previsiones que afectan a este ámbito, entre otras, la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información; la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a la redes públicas de comunicaciones; la Ley 9/2014, de 9 de mayo, de telecomunicaciones; o la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.

La jurisprudencia de nuestro Tribunal Constitucional ha sido determinante para consolidar este derecho. La sentencia más importante en este sentido es la 292/2000[1].

[1] En dicha sentencia se afirma literalmente lo siguiente, en el fundamento jurídico 5: "Este derecho a la protección de datos, a diferencia del derecho a la intimidad del art.

1.2. Ámbito de aplicación

La normativa española delimita el ámbito de aplicación de la protección de datos en nuestro país. Se aplicará tanto a los datos albergados en soportes digitales como analógicos, o sea, a los datos registrados en cualquier soporte. Además, se aplica al sector público y al sector privado (artículo 2.1 LOPD).

La ley, en un principio, tiene un sentido omnicomprensivo, y trata de no dejar zonas sin cobertura. Sin embargo, excluye distintas situaciones y remite a disposiciones específicas en otros casos. De esta forma, se excluyen los ficheros de personas físicas en el ejercicio de actividades exclusivamente personales o domésticas, los ficheros sometidos a la normativa sobre protección de materias clasificadas y los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada (artículo 2.2 LOPD). Los ficheros que se remiten a su normativa específica son los regulados por la legislación electoral, los que sirvan a fines exclusivamente estadísticos y los informes personales de calificación que regula la legislación del régimen del personal de las Fuerzas Armadas (artículo 2.3 LOPD). También tienen legislación específica los datos procedentes de imágenes y sonidos obtenidos mediante viodeocámaras por las Fuerzas y Cuerpos de Seguridad; y el Registro Civil y el Registro Central de Penados y Rebeldes.

Por lo tanto, las universidades, tanto públicas como privadas, como el ejercicio de sus funciones propias, que en parte realizan sus profesores, están sometidos a la normativa de protección de datos.

1.3. Conceptos básicos

Resulta útil detenernos para mostrar alguno de los conceptos propios de este ámbito que como profesores, y ciudadanos, deberíamos conocer (para ulteriores aproximaciones puede verse el artículo 3 LOPD y el artículo 5 RELOPD).

18.1 C.E., con quien comparte el objetivo de ofrecer una eficaz protección constitucional de la vida privada personal y familiar, atribuye a su titular un haz de facultades que consiste en su mayor parte en el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos cuya concreta regulación debe establecer la ley (...). La peculiaridad de este derecho fundamental a la protección de datos respecto de aquel derecho fundamental tan afín como es el de la intimidad radica, pues, en su distinta función, lo que apareja, por consiguiente, que también su objeto y contenido difieran." Y en el fundamento siguiente, el 6, se amplía el argumento: "De este modo, el objeto de protección del derecho fundamental a la protección de datos no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual (…)". Así, "el contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso" (fundamento jurídico 7).

Así, por dato personal se entiende cualquier información relativa a personas identificadas o identificables. De esta forma, puede ser un dato de este tipo una información numérica, alfabética, gráfica o acústica. El afectado o interesado es la persona física titular de los datos que son objeto de tratamiento.

Fichero es "todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso". El responsable del fichero es la persona física o jurídica que decide sobre la finalidad, contenido y uso del tratamiento de los datos. Téngase en cuenta que el tratamiento de datos es prácticamente cualquier operación que se realice con los mismos, sea automatizada o no (la normativa cita operaciones que permitan "la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación", y también consulta, utilización, cancelación o supresión). Diferente a responsable es el encargado del tratamiento, que es la persona o servicio que trata los datos personales por cuenta del responsable, existiendo una relación jurídica que le vincula con mismo y delimita su ámbito de actuación.

A su vez, usuarios son los sujetos autorizados para acceder a los datos de un fichero.

En este orden de cosas, con relación a los datos del alumnado, los profesores universitarios somos, en principio, usuarios, aunque en algún caso podríamos convertirnos en encargados de tratamiento. Además, respecto a nuestros propios datos, seríamos afectados o interesados, en el ámbito universitario, cuando nuestras instituciones tratan nuestros datos para la realización de la nómina o para el control de la calidad docente o del horario.

Por fuentes accesibles al público se entiende aquellos ficheros que pueden ser consultados por cualquiera de forma libre. Solo son fuentes de este tipo las cinco que recoge la ley: el censo promocional, los repertorios telefónicos, los diarios y boletines oficiales, los medios de comunicación, y las listas de personas pertenecientes a grupos profesionales (que solo han de contener el nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia a dicho grupo). Por lo tanto, para usar los datos que se obtienen en estas fuentes no se precisa consentimiento ni autorización de ningún tipo.

3. CUESTIONES GENERALES SITUACIONALES

3.1. Los principios de la protección de datos

Existen una serie de principios que rigen toda esta cuestión de la protección de datos, y cuyo conocimiento permite resolver en la práctica el mayor número de situaciones en las que nos encontremos con datos personales. Además, poseen una fuerte relevancia hermenéutica en el momento de analizar también las dudas que se presenten. Como principios jurídicos que son persiguen una vigencia general, que admite gradación en su cumplimiento (a diferencia de las reglas, que o se

cumplen o no, no resulta graduable su cumplimiento). Estos principios son de obligado cumplimiento, de manera que existen sanciones en caso de vulneración. Los responsables de los ficheros o los encargados del tratamiento deben procurar que dicho tratamiento se adapte a tales principios.

El primer principio que citamos es el principio de calidad de los datos (artículo 4 LOPD). En virtud del mismo, solo podrán recogerse datos personales para su tratamiento cuando sean adecuados, pertinentes y no excesivos para el cumplimiento de las finalidades del fichero al que se incorporan semejantes datos. De este modo, se introduce en este ámbito un criterio de proporcionalidad y racionalidad. Esta previsión exige que las finalidades del fichero se hallen claramente explicitadas, además de ser legítimas. No se podrán usar datos para finalidades incompatibles con las que motivaron su recogida, aunque se permite un tratamiento posterior con fines históricos, estadísticos o científicos. Este principio también reclama que los datos de carácter personal sean exactos y puestos al día. De este modo, si resultan inexactos o incompletos, serán cancelados y sustituidos por los datos rectificados o completados. Los datos se cancelarán cuando dejen de ser necesarios o pertinentes para la finalidad para la cual se recabaron. A veces la cancelación, entendida como borrado físico de los datos, no es posible puesto que es necesario mantener los datos durante cierto período, o hasta que prescriban las posibles responsabilidades que se generen en el tratamiento. Cuando esto sea así, los datos deben bloquearse y excluirse de tratamiento. Si la conservación se produce por fines históricos, estadísticos o científicos, los datos deberían conservarse disociados[2].

El segundo principio es de información en la recogida de datos (artículo 5 LOPD). Así, el responsable del fichero debe garantizar la existencia de una fórmula para informar a los afectados de determinadas cuestiones: de la existencia de un fichero, de la finalidad de la recogida de datos y de los destinatarios de la información; de si es obligatoria o no su respuesta a las distintas preguntas que se le planteen; de las consecuencias de la obtención de datos o de su negativa a suministrarlos; de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición; y de la identidad y dirección del responsable del fichero. Esta información que se facilita a los ciudadanos debe ser expresa, precisa e inequívoca.

El tercer principio que traemos a colación es el del consentimiento (artículo 6 LOPD). El tratamiento de datos personales requiere el consentimiento inequívoco del afectado, "salvo que la ley disponga otra cosa". Y, en efecto, la propia LOPD prevé distintas excepciones, en las que no es necesario prestar tal consentimiento, algunas de singular relevancia: cuando los datos son recogidos para el ejercicio de las funciones propias de las administraciones públicas en el ámbito de sus competencias; cuando se refieren a las partes de un contrato o

[2] El procedimiento de disociación es "todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable" (artículo 3.f LOPD)

precontrato de una relación negocial, laboral o administrativa, y los datos personales son necesarios para el mantenimiento y cumplimiento de ésta; cuando el tratamiento tenga como finalidad proteger un interés vital del interesado y éste se encuentre física o jurídicamente incapacitado para dar su consentimiento; cuando los datos figuren en fuentes accesibles al público (ya citadas más arriba). En todo caso, téngase en cuenta que la excepción del consentimiento no exime de otras obligaciones, como la de informar y la de tratamiento de calidad de los datos (adecuados, pertinentes y no excesivos, como ya indicamos).

En cuarto lugar, citamos el principio de datos especialmente protegidos (artículo 7 LOPD). Este principio significa que el tratamiento de cierto tipo de datos conlleva unas exigencias adicionales, unas garantías de refuerzo. En concreto, los relativos a la ideología, la afiliación sindical, la religión o creencias, el origen racial, la salud y la vida sexual[3].

El principio de seguridad de los datos es el quinto de los principios relevantes (artículo 9 LOPD). Es necesario que el responsable del fichero adopte las medidas técnicas y organizativas necesarias para garantizar la seguridad de los datos de sus ficheros.

El deber de secreto también es tratado en la LOPD en el apartado de los principios, en una clara muestra de mala técnica legislativa (artículo 10 LOPD). En función del mismo, el responsable del fichero y quienes intervengan en el tratamiento de datos están obligados al secreto profesional respecto de los mismos.

El principio de comunicación de los datos (artículo 11 LOPD) hace referencia a que en el caso de cesión de datos personales deben cumplirse determinadas obligaciones. La cesión debe conectarse con las funciones legítimas del cedente y del cesionario, e implica darle al interesado información sobre la finalidad y la identidad del cesionario. La regla general es la necesidad de previo consentimiento del interesado para que se pueda efectuar la cesión. Una situación que tiene, de nuevo, excepciones varias[4].

---

[3] Estos refuerzos que contempla la LOPD consisten en prohibir expresamente la creación de ficheros con la finalidad exclusiva de almacenar datos especialmente protegidos; exigir el consentimiento expreso y por escrito del afectado si los datos son de ideología, afiliación sindical, religión o creencias; y consentimiento expreso cuando los datos se refieran al origen racial, la salud o la vida sexual; en el caso de comisión de infracciones en materia de protección de datos, la gravedad de las mismas aumenta en un grado cuando el fichero contiene datos especialmente protegidos; se establecen medidas de seguridad de nivel alto para los ficheros que contienen datos especialmente protegidos, también llamados sensibles; se prevé que los datos personales relativos a la comisión de infracciones penales o administrativas sólo pueden ser incluidos en ficheros de titularidad de las administraciones públicas competentes en los supuestos previstos en las respectivas normas reguladoras. De nuevo hay excepciones, relativas a la prevención o diagnóstico médicos, a la prestación de asistencia sanitaria o a la salvaguarda del interés vital del afectado cuando este se halle incapacitado para prestar consentimiento.

[4] De este modo el consentimiento no será necesario cuando la cesión esté autorizada por una ley; cuando se traten de datos recogidos de fuentes accesibles al público; cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho

Por último, el principio de acceso a los datos por cuenta de terceros (artículo 12) posibilita que los datos sean tratados por personas distintas a los usuarios o responsable del fichero. En este caso la relación que se establece para el tratamiento debe regularse en un contrato que fije determinadas obligaciones, como que este tercero tratará los datos conforme a las instrucciones del responsable o que no utilizará los datos con fines distintos a los que figuren en el contrato.

3.2. Los derechos subjetivos

El genérico derecho a la protección de datos de carácter personal contiene en su interior un conjunto de derechos más concretos. Los cuatro más relevantes son los derechos de acceso, rectificación, cancelación y oposición (conocidos con el acrónimo ARCO).

El derecho de acceso (artículo 15 LOPD) le otorga al interesado la facultad de "solicitar y obtener gratuitamente conocer información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos". El responsable del fichero deberá responder en el plazo máximo de un mes. Este derecho solo puede ser ejercitado a intervalos no inferiores a doce meses.

En cuanto al derecho de rectificación (artículo 16 LOPD), permite al interesado solicitar al responsable del tratamiento tal rectificación cuando sus datos resultan inexactos o incompletos. El responsable tiene diez días para hacer efectivo este derecho.

El derecho de cancelación se regula de forma similar al de rectificación (artículo 16 LOPD). Permite al interesado solicitar la cancelación de sus datos inexactos o incompletos. El responsable tiene también diez días para cumplir con esta solicitud. La cancelación da lugar al bloqueo de los datos, que se conservarán "únicamente a disposición de las administraciones públicas, jueces y tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de estas". Cuando se supera este plazo los datos deberían suprimirse.

El derecho de oposición, a su vez, opera en los supuestos en los que no es necesario el consentimiento del interesado. De este modo, salvo que la ley prevea una excepción, el interesado podrá oponerse al tratamiento

---

tratamiento con ficheros de terceros, siempre que se limite a la finalidad que la justifique; cuando la comunicación tenga por destinatarios al Defensor del Pueblo, el ministerio fiscal o los jueces y tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas (igualmente a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas); cuando la cesión de datos relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero, o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica; cuando la cesión se produzca entre administraciones públicas para el ejercicio de las mismas competencias; cuando la cesión se produzca entre administraciones públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos; y cuando los datos sean obtenidos o elaborados por una administración con destino a otra.

de sus datos "cuando existan motivos fundados y legítimos relativos a una concreta situación personal" (art. 6.4 LOPD).

El ejercicio de estos derechos de acceso, rectificación y cancelación se puede denegar por dos razones, una conectada con la seguridad y otra con temas fiscales (artículo 23 LOPD). Así, se puede denegar en ficheros de Fuerzas y Cuerpos de Seguridad "en función de los peligros que pudieran derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades en las investigaciones que se estén realizando". Y también se puede denegar en ficheros de la Hacienda Pública cuando se obstaculicen "las actuaciones administrativas tendentes a asegurar el cumplimiento de las obligaciones tributarias y, en todo caso, cuando esté siendo objeto de actuaciones inspectoras."

Al margen de estos derechos, que son los más relevantes, también se puede citar el derecho de consulta al Registro General de Protección de Datos, que es un derecho diferente al derecho de acceso. Este Registro es un órgano integrado en la Agencia Española de Protección de Datos, una entidad estatal. Los ficheros de los de las dos agencias autonómicas que existen (la vasca y la catalana) son complementarios de este. En el registro consta la información de los ficheros inscritos, como quién es el responsable del mismo, el tipo de datos que tratan o los colectivos de los que se recabaron los datos.

3.3. Ficheros públicos y privados

Resulta necesario que las personas y entidades que traten datos creen ficheros para ubicar tales datos y registren esos ficheros en la Agencia de Protección de Datos, en el Registro que tiene al efecto (al que aludimos al final del apartado anterior).

El procedimiento de creación y notificación varía en el caso de ficheros de titularidad pública y ficheros de titularidad privada. Los de las universidades públicas son del primer tipo, y los de las universidades privadas del segundo.

Así, los ficheros de titularidad pública (artículos 20 y siguientes LOPD) se crean por disposición general publicada en el Boletín Oficial del Estado o el diario oficial correspondiente. Esta disposición de creación debe tener cierto contenido: la finalidad del fichero, personas sobre las que se pretenda obtener datos, procedimiento de recogida, estructura, cesiones, órganos responsables, servicios ante los que se pueden ejercitar los derechos y medidas de seguridad[5]. Como dijimos, las universidades públicas tienen este tipo de ficheros[6].

[5] Los ficheros de las fuerzas y cuerpos de seguridad tienen unas previsiones específicas en el artículo 23 LOPD.

[6] Se pueden ver en la dirección http://www.agpd.es/portalwebAGPD/ficheros_inscritos/titularidad_publica/indice_organismos/index-ides-idphp.php?tipo_admin=T1RSQVMgUEVSU09OQVMgSlVSSURJQ08tUFVCTElDQVM=&subclasificacion=VU5JVkVSU0lEQURFUw==

En cambio, los ficheros de titularidad privada (artículos 25 y siguientes LOPD) requieren ser notificados previamente a la Agencia Española de Protección de Datos. En esa notificación debe constar el responsable del fichero, la finalidad del mismo, su ubicación, el tipo de datos que contendrá y las medidas de seguridad. El Registro de la Agencia inscribirá el fichero si se ajusta la notificación a los requisitos exigibles.

Téngase en cuenta que los ficheros de asociaciones de antiguos alumnos de una universidad son ficheros privados, aunque sean de una universidad pública, pues una asociación es una entidad privada, no una administración pública.

3.4. Medidas de seguridad

En este ámbito resulta de suma importancia tener en cuenta que existen una serie de medidas de seguridad que se aplicarán a los ficheros, y al tratamiento de datos en general, medidas que suponen una garantía para la protección de los mismos.

Existen tres niveles de medidas de seguridad en función del tipo de datos y de la naturaleza de la información del fichero: nivel básico, medio y alto (artículos 79 y siguientes RELOPD). De lo que se trata es de garantizar la confidencialidad, integridad y disponibilidad de los datos.

Además, el responsable del fichero elaborará un documento de seguridad "que recogerá las medidas de índole técnica y organizativa acordes a la normativa de seguridad vigente que será de obligado cumplimiento para el personal con acceso a los sistemas de información" (artículo 88 RELOPD).

3.5. Infracciones y sanciones

La normativa de protección de datos, como consecuencia de su naturaleza jurídica, está garantiza por medio de infracciones y de sanciones anudadas a tales infracciones. Hay que recordar que una de las características del derecho es su coactividad, es decir, la imposición forzosa del mismo en caso de incumplimiento. Pues bien, el procedimiento sancionador es un ejemplo de ese rasgo de la coactividad.

Por exigencias del principio de legalidad sancionador, las infracciones deber estar claramente recogidas y descritas. La LOPD recoge tres tipos de infracciones, leves, graves y muy graves (artículo 44 LOPD), a las que anuda también tres tipos de sanciones (artículo 45 LOPD), que consisten en multas que pueden llegar hasta los 600.000 euros. El ejercicio de la potestad sancionadora le corresponde a la Agencia de Protección de Datos.

De todos modos, hay que tener en cuenta que las administraciones públicas no serán sancionadas con multas. Si comenten una de las infracciones previstas, la resolución sancionadora impondrá las medidas a adoptar para que cese esa situación o se corrija y, eventualmente, se podrá proponer también la incoación de actuaciones disciplinarias (artículo 46 LOPD).

3.5. La Agencia

La Agencia de Protección de Datos estatal ostenta un papel relevante como garante del derecho fundamental que estamos comentando. Podríamos definirla como el ente de derecho público que supervisa el cumplimiento de la normativa sobre protección de datos personales en todos los ámbitos. Sus actuaciones deben producirse con plena independencia y objetividad. De esta forma, entre otras funciones, vela por el cumplimiento de la legislación de protección de datos, dicta instrucciones para adecuar los tratamientos de datos, atiende peticiones y reclamaciones de la personas afectadas, informa a las personas acerca de sus derechos, requiere a los responsables la adopción de medidas para adecuar el tratamiento de datos a las previsiones legales, ejerce la potestad sancionadora ya comentada, o ejerce el control relativo a los movimientos internacionales de datos (artículo 37 LOPD).

Por lo tanto, al margen de las funciones de control, también ejerce una labor de consultoría y asesoramiento, que incluye resolver consultas puntuales y jornadas informativas para tratar distintos aspectos.

Con relación a los ficheros creados o gestionados por las comunidades autónomas o por la administración local, se pueden crear agencias autonómicas, que tendrán la consideración de autoridades de control y a las que también se garantizará su plena independencia y objetividad en el ejercicio de su cometido (artículo 41.1 LOPD). Así las cosas, en la actualidad existe en Cataluña la Autoridad Catalana de Protección de Datos / Autoritat Catalana de Protecció de Dades, y en el País Vasco la Agencia Vasca de Protección de Datos / Datuak Babesteko Euskal Bulegoa. Al margen de las agencias especializadas en la protección de datos, los órganos garantes de derechos también deben velar por este derecho fundamental a la protección de datos, y supervisar la aplicación de su normativa específica. Entre ellos, podemos citar las defensorías del pueblo, los jueces y tribunales, y el ministerio fiscal.

4. LAS OBLIGACIONES DE LAS UNIVERSIDADES

En materia de protección de datos, como se deriva de lo que hemos comentado hasta el momento, las universidades tienen diversas y concretas obligaciones.

Recordemos que el artículo 27.10 de la Constitución española reconoce la autonomía de las universidades en los términos que la ley establezca. Esta previsión fue desarrollada por diversas leyes orgánicas. En la actualidad la Ley Orgánica 6/2001, de universidades, se refiere a las universidades públicas como instituciones creadas por los órganos legislativos para desarrollar el servicio público de la educación superior mediante la investigación, la docencia y el estudio. La sentencia del Tribunal Constitucional 26/1987 define la autonomía universitaria como un derecho fundamental de la comunidad universitaria (y no como garantía institucional, lo que parecía más adecuado). La vertiente objetiva o institucional de la libertad académica sería la autonomía universitaria. En todo caso, la autonomía universitaria, entendida como parte del contenido

esencial de la libertad académica o como garantía institucional, es de configuración legal. El legislador debe respetar el contenido esencial del derecho, pero tienen libertad para establecer elementos organizativos y funcionales comunes a todas las universidades.

En líneas generales, sin entrar en pormenores, las obligaciones de las universidades en la materia de protección de datos son las siguientes:

- Crear, notificar e inscribir los ficheros
- Recoger y tratar los datos de carácter personal aplicando los principios de la normativa de protección de datos
- Actualizar los ficheros
- Garantizar la seguridad de los datos (e implantar las medidas de seguridad específicas de cada tipo de fichero)
- Elaborar el documento de seguridad
- Facilitar a las personas el ejercicio de sus derechos
- Colaborar con la Agencia en el ejercicio de sus funciones

Hacemos a continuación algún comentario adicional para explicar ciertas cuestiones.

El cumplimiento de las funciones propias de las universidades (de docencia, investigación y estudio) les permite crear ficheros de carácter personal, que resultan necesarios para cumplir las legítimas actividades que realizan. Es obligatorio declarar esos ficheros e inscribirlos en el Registro de la Agencia.

En este tema de los ficheros universitarios sorprenden las diferencias que existen entre las distintas universidades[7]. En la nota 6 de este trabajo recogíamos la dirección web donde se pueden ver los distintos ficheros inscritos. Realmente, desde el consejo de universidades (o la secretaría de universidades) o desde la conferencia de rectores se podría hacer un esfuerzo de coordinación, para arrojar más seguridad en al ámbito de la protección de datos, y avanzar en la pedagogía de este derecho. Incluso podría avanzarse en la realización de un código tipo para las universidades, de los previstos en el artículo 32 LOPD.

Todos los ficheros deben tener medidas de seguridad de nivel básico. Se subirán a nivel medio en los ficheros de infracciones, o los que contengan datos tributarios o de crédito. Y el nivel alto es preciso en ficheros sobre datos especialmente protegidos (información sobre ideología, religión, creencias, origen racial, raza o vida sexual). De esta forma, por ejemplo, si un fichero tiene datos de discapacidad de alguien debería tener nivel de seguridad alto (estos datos se considera que entran dentro de la salud). Así, ficheros de matrícula, de de gestión de becas y ayudas o de servicio médico pueden contener estos datos. Un fichero de usurarios de biblioteca, en cambio, puede contener información sobre sanciones, por lo que su nivel de seguridad debe ser medio.

[7] Es difícil, por lo tanto, esquematizar los ficheros que han creado las universidades. Podemos hablar de fichero de pruebas de acceso, fichero de matrícula, fichero de expediente académico, fichero de becas y ayudas, fichero de tarjeta universitaria, fichero de búsqueda de empleo, fichero de nóminas, fichero de evaluación de la docencia, fichero de biblioteca, fichero de servicio médico, fichero de control horario, fichero de expedientes de personal, etc.

La disposición de carácter general que declare el fichero debería ser aprobada por el rector, por el consejo de gobierno o por el claustro. Dada la heterogeneidad de la práctica no se puede precisar más.

El responsable del fichero, realmente, puede ser cualquier órgano de la universidad (el que decide la finalidad, contenido y uso del tratamiento de datos de carácter personal, como dice el artículo 3.d LOPD). La práctica habitual hace que el responsable sea el órgano centralizado, el que tiene la competencia para la cual el fichero es instrumental (secretaría general, gerente o vicerrectores). Aunque otra opción sería establecer como responsables a órganos descentralizados, como el director de área. La centralización permite coordinar mejor los distintos ficheros e implantar con mayor facilidad y de modo homogéneo las medidas de seguridad. En cambio, la opción de la descentralización puede decirse que es más realista, ya que realmente el que decide sobre la finalidad y usos es el órgano inferior.

Como es sabido, las universidades siempre han tratado datos personales para cumplir con sus actividades, datos que afectan al alumnado, el profesorado y el personal de administración. También interesan a veces otros datos, como los de padres o tutores, de proveedores de servicios, o de pacientes (en el caso de hospitales universitarios). Y desde un tiempo a hasta parte la tecnología digital ha inundado la vida universitaria en todas sus facetas, subrayando la necesidad de tener más control sobre los datos tratados.

Se ha dicho que tradicionalmente no ha habido mucha sensibilidad hacia la protección de datos en el entorno universitario (Troncoso Reigada, 2006, 85) y que existió un cierto retraso en las universidades en el cumplimiento de la LOPD (*ibidem*), por la falta de implicación de los órganos directivos y la carencia de definición de un responsable, la necesidad de modificar hábitos arraigados, la descentralización universitaria que provocaba una fuerte tendencia a la replicación de datos, las dificultades de control sobre tratamientos que desarrollan los profesores, y los déficits administrativos de las universidades. En la actualidad solo en parte se puede decir que hemos superado esos problemas.

En cuanto a las medidas de seguridad, la legislación universitaria subraya la necesidad de las mismas en este campo: la disposición adicional vigésimo primera de la Ley Orgánica 4/2007, por la que se modifica la Ley Orgánica 6/2001, de universidades, en su párrafo primero preceptúa que "las universidades deberán adoptar las medidas de índole técnica y organizativa necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, tratamiento o acceso no autorizados".

Por último, hay que tener en cuenta la diferencia que existe entre las universidades públicas y las privadas. Las primeras, como administraciones públicas que son, poseen un régimen específico con distintas especialidades, algunas de importancia, y que ya vimos *supra*. Las más importantes son: el consentimiento del interesado encuentra más

excepciones, tanto en el tratamiento (artículo 6.2 LOPD) como en la cesión de datos (artículo 11.2 apartado e LOPD); distintos requisitos para la creación, modificación de ficheros (artículo 20.1 LOPD); y diferencias en las infracciones (artículo 46 LOPD). Las universidades públicas son administraciones, de manera que gozan de todas las prerrogativas y potestades de éstas, también en el ámbito de la protección de datos.

5. LA DINÁMICA PRÁCTICA

Los profesores universitarios estamos sometidos a la normativa de protección de datos en la medida en que empleamos habitualmente datos personales en nuestro trabajo, sobre todo en el ámbito de la docencia, pero también en numerosas ocasiones en la investigación. Además, los datos de los propios profesores también son tratados por las universidades de manera regular y continua, como en las nóminas. Por lo tanto, los profesores serán tanto usuarios de los ficheros de su universidad, como interesados cuando sus datos se incorporan a ficheros universitarios (de nóminas, de acceso).

5.1. Recogida

La *recogida de datos*, en principio, no le incumbe al profesor universitario sino a los órganos establecidos al efecto en cada universidad, que son los que deberán cumplir con los principios ya vistos de la protección de datos en el momento de la recogida de los mismos y de su posterior tratamiento.

No obstante, puede haber algún supuesto en el que el profesor realice una verdadera recogida de datos. Estamos pensando en actividades propias que realicen un centro o instituto de investigación determinado. Estos pueden tener colaboradores propios y alumnado específico en alguna actividad no reglada y, por lo tanto, articulada al margen de los mecanismos de matrícula oficial. En ese caso, debe hacer ficheros de datos específicos de ese centro o instituto, y los profesores que lo dirigen y realizan esas actividades serían, cuando menos, encargados de tratamiento. También deberían ser los responsables de esos ficheros, pero la práctica que hemos analizado en España (en los ficheros registrados en la Agencia Española de Protección de Datos) no es proclive a esa posibilidad: lo normal es que el responsable de los ficheros del instituto de investigación sea el vicerrector correspondiente. Sea como fuere, en esos supuestos, los profesores deben cumplir con los principios que rigen la recogida de datos. En ejercicio de derechos se sustanciará ante el responsable del fichero, o sea, normalmente el vicerrector.

También, a veces se hacen ficheros oficiosos (e ilegales), como de alumnos de prácticas que recopilan directamente los profesores, o ficheros de asistentes a cursos y jornadas puntuales. Hay que reclamar el fin de estas prácticas y la acomodación de las mismas a la legislación de protección de datos.

5.2. Tratamiento

El *uso de los datos personales del alumnado* es totalmente habitual en la labor del docente. En ello hay que exigir, de nuevo, el cumplimiento de los principios que rigen esta materia. Además, aconsejo prudencia y razonabilidad teniendo en mente que la finalidad de ese tratamiento es la actividad docente, no otra. Es decir, hay que tener presente el principio de calidad de los datos, que reclama que los datos recogidos no se usen para finalidades incompatibles con aquellas para las que hubieran sido recogidos (los datos del alumnado se recogen para cumplir con la relación jurídica que existe entre universidad y matriculados en ella para recibir formación académica).

En ese uso de los datos de los alumnos cobra singular protagonismo la lista de clase, ahora en formato digital, con lo que las posibilidades de tratamiento son mucho mayores que antaño.

La *publicación de las notas*, tanto parciales como finales, fue un asunto debatido en España a lo largo de años. Sin embargo, ahora la legislación es bastante clara. En efecto, la disposición adicional vigésimo primera de la Ley Orgánica 4/2007, de 12 de abril, de modificación de la Ley Orgánica 6/2001, de 21 de diciembre, de universidades, establece que "no será preciso el consentimiento de los estudiantes para la publicación de los resultados de las pruebas relacionadas con la evaluación de sus conocimientos y competencias ni de los actos que resulten necesarios para la adecuada realización y seguimiento de dicha evaluación". Por lo tanto, las universidades tienen la posibilidad de publicar las notas, aunque el precepto indicado no obliga a ello. Los centros universitarios pueden apreciar la existencia de un interés público en el conocimiento generalizado de los resultados de las evaluaciones, al margen de la opinión del alumnado al respecto. Desde nuestro punto de vista, lo más recomendable es que se haga tal publicación: en su versión digital en la intranet de la universidad, y en su versión analógica en los tablones de la facultad. Además, la nueva cultura de la transparencia, auspiciada por la Ley 19/2013, también refuerza esta idea de la publicación de la notas. No creemos oportuno que se publiquen en abierto en la web por los peligros que conlleva el *data mining*. También hay que recordar que no se pueden publicar datos excesivos. Como algún autor ha recordado, no es necesario publicar el nombre y los apellidos, el DNI y el número de expediente, basta con uno de ellos (Messía de la Cerda Ballesteros, 2015).

Un supuesto diferente sería las notas de un proceso competitivo, es decir, de un proceso en el que se lucha por cierto número de puestos (como en una oposición). En este tipo de procesos la publicación es obligatoria pues prima el principio constitucional de mérito y capacidad. La normativa administrativa obliga a tal publicación[8]. Por lo general, las notas de la actividad docente universitaria no son procesos competitivos

[8] Artículo 59.6 b) de la Ley 30/1992, de 26 de noviembre, de régimen jurídico de las administraciones públicas y del procedimiento administrativo común: la publicación sustituirá a la notificación "cuando se trata de actos integrantes de un procedimiento selectivo o de concurrencia competitiva de cualquier tipo".

(salvo para la concesión de matrículas de honor), por lo que serían de aplicación las reflexiones del párrafo anterior, no las de este.

En todo caso, la publicación de calificaciones debe tener presente, de nuevo, el principio de calidad de los datos, que exige que cuando los datos dejen de ser necesarios se cancelarán.

Las universidades pueden tratar información de sus alumnos sin su consentimiento ya que los datos se refieren a partes de un contrato y son necesarios para su mantenimiento y cumplimiento (artículo 6.2 LOPD). Además, las universidades públicas lo hacen para el cumplimiento de funciones administrativas, lo que también excepciona el consentimiento del interesado. En este orden de cosas, por ejemplo, no es necesario que los alumnos den su consentimiento a que se digitalice su fotografía para el carné del estudiante, que es necesario para distintas actividades universitarias.

5.3. Seguridad

Además de lo dicho, el profesorado universitario debe mantener las *medidas de seguridad* propias de los ficheros que usan. A ello también me refería antes cuando aconsejaba un criterio de prudencia en el uso de los datos de los alumnos. Así, por ejemplo, hay que proteger el acceso a nuestra secretaría virtual, donde estarán datos del alumnado, y custodiar debidamente los exámenes, que también suelen reflejar datos identificativos. Se trata de imbuirse de una cultura de seguridad razonable en nuestras actividades cotidianas en el docencia, el estudio y la investigación.

Recordemos que el *deber de secreto* del artículo 10 LOPD se extiende a los que intervengan en cualquier fase del tratamiento de los datos de carácter personal, que también tienen el deber de guardarlos. Estas obligaciones "subsistirán aun después de finalizar sus relaciones con el titular del fichero".

5.4. Las encuestas académicas de los profesores

Estas encuestas contienen calificaciones y comentarios del alumnado que *evalúan la calidad de la docencia*. Debe existir un fichero específico para esta finalidad. En el cuestionario, en virtud del principio de calidad, solo deberían constar preguntas dirigidas a conocer la calidad de esa docencia, no otras que serían por ello mismo excesivas. Además, los profesores deben ser informados de acuerdo con el principio ya visto de información en la protección de datos. No es preciso pedir el consentimiento de los profesores para desarrollar encuestas de este tipo pues sería de aplicación la excepción ya comentada de la existencia de una relación administrativa o laboral, que hace necesario el tratamiento de estos datos para mantenerla (artículo 6.2 LOPD). Y en las universidades públicas hay todavía otra razón más, la ya señalada presencia de una función propia de la universidad (otra excepción al consentimiento del ya citado artículo 6.2 LOPD, referida al ejercicio de

funciones propias de las administraciones en el ámbito de sus competencias).

5.5. Complementos y evaluaciones del profesorado

La *administración educativa* debe tener los correspondientes ficheros para los distintos tratamientos de los datos de profesores que realiza. Por ejemplo, complementos retributivos autonómicos, o procedimientos de evaluación de la actividad investigadora, habilitaciones o acreditaciones.
Los datos deben ser adecuados y pertinentes para la finalidad del fichero concreto de que se trate. De este modo, en el complemento retributivo, solo se pueden recabar datos que se vayan a utilizar como criterios para dar o no el complemento (Troncoso Reigada, 2006, 119). También hay que cumplir con el principio de información.

En cuanto a la publicación de estos datos, hay que tener en cuenta la normativa específica existente. Así, la disposición adicional vigésimo primera, punto 4, de la Ley Orgánica 4/2007, por la que se modifica la LO 6/2001, de universidades, prescribe que no será preciso el consentimiento del personal de las universidades "para la publicación de los resultados de los procesos de evaluación de su actividad docente, investigadora y de gestión realizados por la universidad o por las agencias o instituciones públicas de evaluación".

En el caso de los complementos retributivos, debemos pensar que se trata de un procedimiento selectivo o competitivo. En este sentido, desde un punto de vista general, los procedimientos selectivos o de concurrencia competitiva tienen que ser objeto de publicidad. En concreto, la notificación del acto administrativo se efectúa publicando dicho acto (según el ya citado artículo 59.6 apartado b de la Ley 30/1992, de régimen jurídico de las administraciones públicas y del procedimiento administrativo común). Esta publicación resulta obligatoria, no potestativa.

Tal publicación es una cesión de datos, que no precisa consentimiento de los afectados por haber habilitaciones legales para ello. De todos modos, recordemos que el principio de calidad reclama que los datos deberán cancelarse cuando hayan dejado de ser necesarios y pertinentes para la finalidad. Si la publicación persigue que terceros conozcan el acto para su posible impugnación, cuando se sobrepasa el plazo de impugnación habrá que proceder a la cancelación de esos datos.

En cambio, la evaluación de la actividad investigadora o la acreditación no son procedimientos selectivos o competitivos porque ni hay un número máximo de sexenios para atribuir ni un número limitado de acreditaciones. Aquí no opera la previsión de la Ley 30/1992, pero sí la de la Ley Orgánica 4/2007, por lo que será posible su publicación.

5.6. Directorios telefónicos y de correo electrónico del profesorado

Las universidades tienen ficheros en los que constan los directorios de teléfono y de correo del profesorado. Se trata de datos personales sometidos a la normativa que regula este sector del ordenamiento jurídico

(identifican a las personas o las hacen identificables). Por lo tanto, estos ficheros deben estar declarados e inscritos.

Ha habido debates acerca de si tales directorios deberían ser reservados o públicos. Incluso se han defendido posiciones intermedias, de publicación en la intranet (Troncoso Reigada, 2006, 140). De hecho, la práctica de las universidades ha sido diversa, aunque parece que primó la publicidad. No cabe duda de que son teléfonos y *mails* pertenecientes al dominio de la universidad, por medio de los cuales se cumplen las funciones públicas que desarrolla un profesor universitario. Pero ello no significa que no sea un dato personal, que sí lo es como ya dijimos. No son datos íntimos, no forman parte de la vida privada, pero son datos personales al referirse a una persona física identificada o identificable.

Las universidades pueden tratar estos datos sin consentimiento de los profesores, pues se aplicarían las excepciones ya vistas del artículo 6.2 LOPD (relación administrativa o laboral, y para las universidades públicas el cumplimiento de funciones administrativas).

En el marco de la nueva cultura de transparencia, que marca la Ley 19/2013, nos inclinamos por la publicación en abierto de estos directorios. En este sentido juegan los deberes de publicidad activa, referidos a la estructura organizativa (artículo 6 de esa Ley 19/2013). Asimismo, el artículo 15 de la Ley 19/2013 pone trabas al derecho de acceso a la información, pero casi exclusivamente para datos especialmente protegidos, que no es el caso de estos directorios.

5.7. Cesión de datos desde las universidades

En el apartado siguiente veremos diversos supuestos de cesión de datos desde las universidades, que fueron objeto de consulta en la Agencia Española de Protección de Datos. Ahora hacemos un par de reflexiones distintas sobre ello.

Las previsiones cesión o comunicación de datos difieren en función de la naturaleza de la universidad, pública o privada, al ser las primeras, como dijimos, administración. Por lo tanto, las excepciones del artículo 11 LOPD al consentimiento del interesado varían en unas universidades u otras. Y el también citado artículo 21 LOPD se aplicaría solo a las públicas.

Así, es posible la comunicación de datos entre administraciones públicas sin consentimiento del interesado para el ejercicio de competencias homogéneas o que versen sobre las mismas materias (artículo 21.1 LOPD). Un ejemplo puede ser la comunicación de datos entre una universidad pública, la consejería de educación de la comunidad autónoma, o el ministerio de educación. Eso sí, para las mismas materias o las mismas competencias. Para competencias diferentes habría que pedirle al alumnado el consentimiento; o referirse a un tratamiento posterior de los datos con fines históricos, estadísticos o científicos. Aunque realmente, en muchas ocasiones, no será necesaria la cesión de información personal para un tratamiento histórico o estadístico, al ser suficiente la información disociada.

Las cesiones de datos de alumnos entre universidades de distintos países se rigen por la normativa de transferencia internacional de datos (que exige un nivel de protección adecuado en el destinatario).

En fin, al margen de lo comentado, puede haber expresas previsiones legales que permitan la cesión sin pedir el consentimiento (lo que es otra excepción del artículo 11.2 apartado a LOPD), lo que rige tanto para universidades públicas como privadas. Por ejemplo, el Estatuto de los Trabajadores prevé la comunicación de algunos datos de los trabajadores de la universidad al comité de empresa. O la legislación también ampara la comunicación de datos a las fuerzas y cuerpos de seguridad del estado. Igualmente, las universidades deben ceder a la policía datos de estudiantes extranjeros no comunitarios a los efectos de obtención y regularización de los permisos de residencia por estudios.

6. EJEMPLOS DE CONSULTAS PLANTEADAS EN ESTE TEMA

Recogemos a continuación algunas de las consultas planteadas ante la Agencia Española de Protección de Datos que tienen que ver con la vida universitaria. Esta selección tiene una mera intención informativa y ejemplificadora, que en parte alude a cosas ya comentadas anteriormente. Los mayores problemas los originan la cesión de datos.

Cesión de datos para la realización de un estudio sociológico (2002)

Se plantea la posibilidad de que sean comunicados datos por parte de varias universidades públicas a una entidad para la realización de un proyecto de investigación sociológico. Se pretende amparar dicha cesión en el artículo 11.2 apartado e) de la LOPD, y que sea posible tal cesión sin contar con el consentimiento de los afectados puesto que la misma se produce entre administraciones públicas y se realiza con fines científicos.

La Agencia Española de Protección de Datos analiza en primer lugar la adecuación subjetiva de los intervinientes al supuesto de hecho. Así las cosas, se exigiría que tanto el cedente como el cesionario fueran administraciones públicas. No hay duda con el decente en este caso, pero sí alguna con relación al cesionario, al ser un instituto universitario de investigación. Se admite el supuesto siempre que el proyecto científico se desarrolle en un instituto universitario a título institucional (no a título personal por docentes del mismo).

Tras ello, se analiza el fin científico que se alega. Se afirma que no todo proyecto intitulado "científico" amparará la cesión de datos sin consentimiento. Hay que tener presente el principio de calidad de los datos, que exige un tratamiento adecuado y proporcionado a la finalidad del estudio. En el caso concreto se entiende que ello es así, y que la materia es científica al integrarse en un proyecto del Plan I+D+I concedido por la Comisión Interministerial de Ciencia y Tecnología.

La conclusión, por lo tanto, es favorable a las intenciones de los que plantearon la consulta: la cesión se podía efectuar sin necesidad de recabar el consentimiento previo de los afectados.

Cesión de datos a defensor universitario (2005)

Esta consulta se pregunta si es conforme a la normativa la comunicación al defensor universitario de los datos necesarios para el ejercicio de sus funciones, tanto por parte del propio centro universitario como por terceras entidades que hubieran contratado servicios con el mismo o incluso otras entidades independientes a la propia universidad.
Se recuerda la normativa que regula al defensor universitario (disposición adicional decimocuarta Ley Orgánica 6/2001, de universidades), que también contempla la legislación de Andalucía (el caso era de esa comunidad), y los estatutos de la universidad respectiva.

Se reflexiona, en el marco de la cesión de datos, sobre las excepciones a la regla del consentimiento del afectado a la hora de recabar datos (el tan citado artículo 11 LOPD), en especial en el caso de que la comunicación esté amparada en una norma con rango de ley. La Agencia entiende que ello es así por la previsión vista de la Ley Orgánica 6/2001. Si no le fuera posible al defensor recabar antecedentes o datos, no podría ejercer sus funciones, por lo que hay que considerar amparada por dicha ley la comunicación por terceros o transmisión por otros órganos de los datos vinculados al cumplimiento de sus funciones.

Se concluye, por un lado, que el defensor universitario podrá recabar de otros órganos de la universidad y de las entidades que tengan la condición de encargado del tratamiento de la misma los datos necesarios para el ejercicio de sus funciones; y por otro, que el artículo 11.2 LOPD ampara la comunicación por terceras entidades de datos al defensor. En todo caso, los datos han de ser adecuados, pertinentes y no excesivos.

Solicitud de datos de alumnos con discapacidad (2009)

Se plantea si una cátedra de accesibilidad, arquitectura y diseño de una universidad puede solicitar a universidades públicas españolas los datos de estudiantes con discapacidad matriculados en las mismas, con objeto de contactar con ellos para la realización de un estudio.

Se entiende que esta comunicación es una verdadera cesión de datos (artículo 3 apartado i LOPD). Además, se considera que el dato de la discapacidad (la Agencia emplea el término minusvalía, totalmente desaconsejable por ser ofensivo con estas personas) es un dato de salud[9].
La cesión de datos de salud tiene un régimen especial en la LOPD en la medida que son datos especialmente protegidos. Como regla general, el artículo 7.3 LOPD estable que el tratamiento y cesión de dichos datos se podrá hacer cuando "así lo disponga una ley o el afectado consiente expresamente". La excepción a ello se ubica en el artículo 7.6 LOPD: "el tratamiento de datos de salud podrá efectuarse si resulta necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia

[9] El art. 5 apartado g RELOPD define a los datos de carácter personal relacionados con la salud de este modo: informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo. A lo que añada que "en particular, se consideran datos relacionados con la salud de las personas los referidos al porcentaje de discapacidad y a su información genética".

sanitaria o tratamientos médico o al gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto". También se podrán tratar si ello es necesario "para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento". Estas excepciones deben interpretarse de manera restrictiva. Así, no cubren el tratamiento posterior que no sea necesario para la prestación directa de la asistencia sanitaria.

Además, el artículo 11.2 apartado f LOPD estable la licitud de la cesión de datos relacionados con la salud si la misma es necesaria "para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica".

En el supuesto analizado la cesión se produce entre administraciones públicas. Por lo tanto, es de aplicación el artículo 21 LOPD, que posibilita la cesión de datos a otras administraciones para el ejercicio de competencias diferentes si la comunicación tiene por objeto el tratamiento con fines históricos, estadísticos o científicos. En el caso que se comenta, la Agencia desconoce si el estudio de accesibilidad ser realiza a título personal por un profesor o si es un proyecto institucional en el marco de un programa de investigación concreto, que le daría el rango de auténtico estudio científico (y permitiría aplicar esa posibilidad citada del artículo 21 LOPD).

Asimismo, se recuerda que el artículo 4.2 LOPD preceptúa que los datos no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. En el presente caso, la finalidad pretendida (realizar un estudio de accesibilidad) es incompatible con la finalidad que motivó la recogida de los datos (los datos fueron recogidos y tratado para el adecuado cumplimiento de la relación jurídica existente ente la universidad y los que se matricularon en la misma para recibir formación académica).

Después de estas reflexiones se concluye que en este supuesto no es aplicable la excepción al consentimiento del citado artículo 11.2 apartado f LOPD. Así, la cesión planteada, en cuanto contenga datos de salud, debe quedar sometida al consentimiento expreso del interesado, con independencia de que el trabajo a desarrollar se inserte o no en el marco de un proyecto institucional.

Cesión de datos alumnado de postgrado a dos profesores de una universidad (2009)

Se analiza un supuesto de cesión de datos de alumnado a dos profesores que están efectuando una base de datos histórica. Se trata de un estudio enmarcado dentro de un proyecto nacional de investigación y docencia universitaria. La Agencia recuerda en la respuesta a la consulta que las cesiones de datos deben estar relacionadas con las funciones

legítimas del cedente y del cesionario, y que la regla general es solicitar el previo consentimiento al interesado. Pero también recuerda que hay supuestos excepcionales que no precisan el consentimiento de los interesados.

En el supuesto que examina, la Agencia trae también a colación la previsión específica sobre la cesión de datos entre administraciones (que se ubica en el artículo 21 LOPD), para decir que la cesión entre administraciones se puede efectuar para el ejercicio de competencias diferentes cuando la comunicación tienen por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos. El caso del que se ocupaba tenía una finalidad estadística. En su opinión, ello debe conectarse con planes oficiales estadísticos, no otros. Así, afirma que la utilización de los datos solo sería posible en caso de que el estudio estadístico estuviera previsto en las normas reguladoras de los planes estadísticos correspondientes a la administración territorial en cuyo ámbito se realizase el estudio. La referencia estatal es Ley 12/1989, de 9 de mayo, reguladora de la función estadística pública, desarrollada por varias normas que aluden al Plan Estadístico Nacional. En la información que remitió el consultante a la Agencia no se hace constar la inclusión del estudio analizado entre los contenidos en dicho plan, por lo que no se sabe si está o no comprendido en esas previsiones normativas. Por lo tanto, la Agencia entiende que habrá que obtener el consentimiento de los interesados de manera específica.

No obstante, cabría la cesión de las calificaciones de los alumnos sin necesidad de recabar este consentimiento si los datos se encuentran debidamente disociados. Sin embargo, matiza que si de la información relativa a las calificaciones que se facilite, puede deducirse la identidad del afectado sin realizar esfuerzos desproporcionados, no estaríamos ante un supuesto de disociación y habría que requerir el consentimiento del interesado[10].

Comunicación de datos por parte de universidades para la elaboración de una tesis doctoral (2010)

La consulta se refiere a la posibilidad de que diversas universidades le comuniquen al consultante datos de carácter personal de profesores para la elaboración de una tesis doctoral.

Se efectúan reflexiones ya recogidas en otras consultas. Con carácter general la cesión de datos está regulada en el artículo 11 LOPD, que establece excepciones al consentimiento en su apartado segundo, entre ellas cuando la cesión se produzca entre administraciones públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos. La cesión de datos entre administraciones tiene un régimen específico en el artículo 21 LOPD, que permite la comunicación a otras administraciones para el ejercicio de competencias diferentes si

[10] Como ejemplo de esfuerzo poco proporcionado se cita el hipotético supuesto de las calificaciones comunicadas manteniendo el orden alfabético de los apellidos, que permitiría establecer una correlación entre las notas y el alumno.

tiene por objeto el tratamiento posterior de los datos con los fines dichos. Ello implica que tanto el cedente como el cesionario deben ser administraciones públicas. En el caso planteado no se aclara si ello es así, ni si la tesis o estudio en cuestión se encuentra financiado por el plan nacional de investigación científica, desarrollo e innovación, o si el cesionario va a desarrollarlo a título personal o si, por el contrario, se trata de un proyecto institucional.

La conclusión va en la línea ya señalada en ejemplos anteriores. En efecto, si el objeto de consulta, la tesis doctoral, se desarrolla por el profesor a título institucional y en el marco de un proyecto de investigación concreto, se podrá aplicar la excepción al consentimiento en la cesión de datos de los artículos 11.2 y 21.1 LOPD. Incluso, en este supuesto si se solicitaran a una universidad privada también se podría prescindir del consentimiento puesto que el artículo 11.2 también prevé una excepción si una ley así lo contempla (esa ley será la Ley Orgánica 6/2001, de universidades, en cuyo artículo 40 se regula la investigación como un derecho y un deber del profesorado universitario). Por el contrario, en el caso de que el trabajo de investigación se desarrollase a título personal por el docente universitario, sería preciso recabar el consentimiento de los interesados, tanto en el caso de que los datos se soliciten a universidades públicas como privadas.

Reconocimiento facial en el control de asistencia a clase y a las pruebas (2011)

El caso examinado se refiere a que en un centro universitario se tratan los datos necesarios para el reconocimiento de los alumnos a través de programas de reconocimiento facial. La finalidad de ello es controlar la asistencia a las clases y la identificación en la realización de pruebas.

La argumentación parte del análisis del tratamiento de datos biométricos. Por los mismos se entiende "aquellos aspectos físicos que, mediante un análisis técnico, permiten distinguir las singularidades que concurren respecto de dichos aspectos y que, resultando que es imposible la coincidencia de tales aspectos en dos individuos, una vez procesados, permiten servir para identificar al individuo en cuestión". Se citan como ejemplo las huellas digitales, el iris del ojo o la voz. Además, se estima que la evolución de la tecnología ha demostrado la utilidad del tratamiento de datos biométricos en el desarrollo de sistemas de identificación única de la población.

Para tratar estos datos es de aplicación el artículo 6 LOPD, que exige consentimiento del afectado salvo que se aplique alguna de las excepciones que ahí se recogen. Entre ellas que lo autorice alguna norma con rango de ley (artículo 10.2 apartado a RELOPD), o que el tratamiento sea necesario para el adecuado mantenimiento de una relación jurídica. En la mayor parte de los supuestos con los que se ha encontrado la Agencia se podía aplicar esta última previsión, referida a la preexistencia de un vínculo contractual (que permite el tratamiento por lo general de una huella dactilar).

Tras ello, se acude al derecho de la Unión Europea para recordar que el tratamiento de datos personales será lícito si es necesario para satisfacer un interés legítimo y si no prevalecen los derechos del interesado (artículo 7 apartado f de la Directiva 95/46/CE). Ello implica que deba aplicarse una regla de ponderación: valorar si en el supuesto concreto existe un interés legítimo del responsable del tratamiento que prevalezca sobre el interés o derechos del interesado; o, por el contrario, si dichos derechos de los interesados han de prevalecer sobre aquel interés legítimo. Se trata de traer a colación el principio de proporcionalidad, que contiene distintos subprincipos que deben cumplirse (idoneidad, necesidad y ponderación o proporcionalidad en sentido estricto).

No hay duda que el tratamiento de datos biométricos es idóneo para la finalidad de control perseguida. Pero el problema estriba en determinar si resulta posible alcanzar la finalidad perseguida a través de medios menos intrusivos en la esfera íntima del afectado con similar eficacia (o sea, no se cumpliría con el subprincipio de la necesidad). Asimismo, resulta problemático ver si el uso de esta medida depara un mayor beneficio al interés general que el perjuicio que eventualmente pueda ocasionarse al afectado (así no se cumpliría tampoco el subprincipio de la ponderación).
En todo caso, habría que analizar la casuística de cada supuesto. De este modo, la Agencia dio el visto bueno al uso de la huella dactilar por trabajadores o empleados públicos en su jornada laboral, a tenor de las circunstancias concurrentes. En cambio, en otro caso, se entendió desproporcionado emplear la huella dactilar para control el acceso de los alumnos a un centro escolar.

Y en el supuesto que sustancia en esta consulta, la Agencia concluye que resulta desproporcionado. La finalidad de control de asistencia podría lograrse igualmente a través de otros mecanismos habitualmente utilizados hasta la fecha, que garantizan seguridad en el logro del objetivo. O sea, que es posible establecer medidas más seguras de control sin necesidad de proceder al tratamiento de datos de reconocimiento facial.

Acceso de los padres a las calificaciones universitarias de sus hijos mayores de edad (2014)

Unos padres consultan a la Agencia si pueden acceder al expediente de su hijo teniendo en cuenta que están sufragando los gastos de su matrícula.

En este sentido, se recuerda la disposición adicional vigésimo primera de la Ley Orgánica 4/2007, de 12 de abril, de modificación de la Ley Orgánica 6/2001, de 21 de diciembre, de universidades, que establece que "no será preciso el consentimiento de los estudiantes para la publicación de los resultados de las pruebas relacionadas con la evaluación de sus conocimientos y competencias ni de los actos que resulten necesarios para la adecuada realización y seguimiento de dicha evaluación". De este modo, el legislador reconoce la posibilidad de que los

centros universitarios aprecien la existencia de un interés público en el conocimiento generalizado de los resultados de las evaluaciones. Ese interés prevalecería sobre la voluntad de los alumnos y permitiría la publicación sin precisar de su consentimiento. Además de ello, también puede existir un interés específico de alguien en conocer dichas calificaciones, que podría ampararse en el artículo 15.3 de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.

En cuanto a los datos relacionados con la obtención de becas, dicha información debe ser objeto de publicidad activa por la administración concedente. Es lo que exige el art. 8.1 apartado c de la citada Ley 19/2013.

Se concluye en este caso que el acceso a las calificaciones está amparado en la normativa.

7. CONCLUSIONES

No cabe duda que la temática de protección de datos presenta aspectos problemáticos. Así es criticable el exceso de especificidades sectoriales y excepciones que contempla, lo que es un riesgo para la seguridad jurídica. O también se puede esgrimir negativamente que la normativa actual debería estar más conectada a la realidad de la tecnología digital, en general, y de internet, en particular. O sea, que debería ser objeto de una actualización para afrontar cuestiones tales como las cookies, las direcciones IP fijas y móviles, o los datos genéticos y los perfiles de ADN.

Sin embargo, y al margen de lo dicho, es evidente que la normativa de protección de datos resulta de cumplimiento obligatorio, incluso puede afirmarse que es una muestra de calidad democrática pues es camino que afianza la dignidad del individuo. De esta forma, los profesores universitarios debemos ser escrupulosos en su cumplimiento. En este sentido también somos ejemplo para nuestro alumnado y colaboraremos en su formación como ciudadanos y ciudadanas.

Esta normativa tiene como finalidad proteger los derechos y libertades de las personas en el tratamiento que se efectúe de sus datos personales. Por ello, desde la universidad tenemos que estar firmemente comprometidos en tal elevada tarea. Nuestras universidades han mostrado lentitud en el asentamiento de la cultura de protección de datos, aunque por encima de otras adminstraciones. Esperemos que el presente supere esas disfunciones anteriores, y que logremos en la institución universitaria equilibrar el derecho fundamental a la protección de datos con las nuevas previsiones de transparencia, que son también una exigencia democrática. Se precisa para ello tanto sensibilización como formación.

8. BIBLIOGRAFÍA

AGENCIA DE PROTECCIÓN DE DATOS DE LA COMUNIDAD DE MADRID (2004). Guía de protección de datos personales para universidades. Madrid.

AGENCIA DE PROTECCIÓN DE DATOS DE LA COMUNIDAD DE MADRID (2008). *Protección de datos personales para universidades*. Thomson-Civitas. Madrid.

FERNÁNDEZ RODRÍGUEZ, J. J. (2004). *Lo público y lo privado en internet. Intimidad y libertad de expresión en la red*. Universidad Nacional Autónoma de México. México D. F.

LUCAS MURILLO DE LA CUEVA, P. L. (1990). *El derecho a la autodeterminación informativa*. Tecnos. Madrid.

MARTÍNEZ MARTÍNEZ, R. (2004). *Una aproximación crítica a la autodeterminación informativa*. Civitas. Madrid.

MESSÍA DE LA CERDA BALLESTEROS, J. A. (2015). "La protección de datos en las universidades: el caso de la publicación de las calificaciones". Disponible en http://porticolegal.expansion.com/pa_articulo.php?ref=317

PIÑAR MAÑAS, J. L. y RODOTÀ, S. (2014). *Transparencia, acceso a la información y protección de datos*. Reus. Madrid.

REBOLLO DELGADO, L. y SERRANO PÉREZ, M. M. (2014). Manual de protección de datos. Dykinson. Madrid.

TRONCOSO REIGADA, A. (2006). "La publicación de datos de profesores y alumnos y la privacidad personal. Acerca de la protección de datos personales en las universidades". *Revista de Derecho Político*, nº 67, pp. 76-163.

TRONCOSO REIGADA, A. (2010). *Comentarios a la Ley Orgánica de protección de datos de carácter personal*. Civitas. Madrid.

WARREN, S. D. y BRANDEIS, L. D. (1890). "The right to privacy". *Harvard Law Review*, vol. 4, nº. 5, pp. 193-219.