La protección de los datos personales en la Universidad a ojos de un defensor universitario

Agustí Cerrillo i Martínez
Síndic de Greuges de la Universitat Oberta de Catalunya

1. Introducción

La protección de los datos personales ha sido objeto de una profunda revisión en los últimos años de la mano del legislador europeo para dar respuesta a los nuevos retos que la evolución tecnológica y la globalización está planteando al derecho fundamental a la protección de los datos personales.

La aprobación del 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 (en adelante, RGPD) que es aplicable desde el 25 de mayo de 2018 sin la necesidad que los estados miembros adopten ninguna norma o medida y, posteriormente, de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD) han introducido una nueva aproximación a la protección de datos lo que se ha concretado en numerosos cambios a los que iremos haciendo referencia en las próximas páginas.

Todo ello tiene lógicamente una repercusión en las Universidades que desde hace décadas han sido conscientes del impacto que la protección de datos tiene en su actividad; de hecho, más allá de la preocupación universitaria por la gestión de los datos personales y la garantía del cumplimiento de la normativa vigente, como ha señalado algún autor, "no es en absoluto aventurado señalar que el derecho fundamental a la protección de datos cuenta su origen en la academia española a través de las pioneras aportaciones" (Martínez Martínez, 2018). No podemos desconocer que las Universidades tienen en su poder numerosos datos personales de un gran volumen de estudiantes, profesores y personal de gestión (desde listados de profesores hasta listados de notas y trabajos; desde datos bancarios del personal de servicios hasta datos de beneficiarios de becas; desde expedientes académicos hasta historiales laborales).

En las próximas páginas, aun siendo conscientes que dejamos fuera de nuestro foco de atención numerosos aspectos de la regulación de la protección de datos, muchos de ellos de gran importancia jurídica y práctica (Véase un amplio y completo análisis de la regulación vigente en materia de protección de datos personales en Rallo Lombarte, 2019 y Troncoso Reigada, 2019), nos proponemos llevar a cabo una lectura de estas normas desde la universidad y, en particular, desde la perspectiva de los defensores universitarios quienes deben velar por el respeto a los derechos y las libertades de los profesores, estudiantes y personal de administración y servicios, ante las actuaciones de los diferentes órganos y servicios universitarios y por la mejora de la calidad universitaria en todos sus ámbitos (disposición adicional decimocuarta Ley Orgánica 6/2001, de 21 de diciembre, de Universidades)

En particular, una vez hayamos determinado qué son los datos personales, centraremos nuestra atención en tres aspectos de la regulación de la protección de datos personales como son los principios que rigen los tratamientos de datos personales, los derechos de los interesados y, finalmente, las obligaciones de los responsables, encargados y delegados de la protección de datos. Finalmente, a modo de reflexión final, expondremos cuál puede ser el papel de los defensores universitarios en relación a la protección de datos personales.

2. Los datos personales en la universidad

Los datos personales son cualquier información sobre una persona física identificada o identificable (artículo 4 RGPD). Tal y como se desprende de este artículo una persona física identificable es aquella cuya identidad pueda ser determinada, directa o indirectamente mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona. De este modo, son datos personales no solo el nombre y los apellidos de los estudiantes o los profesores o su dirección sino también muchos otros datos en poder de las Universidades derivados del desarrollo de sus actividades docentes y de investigación como los datos académicos, la experiencia profesional o el historial laboral o las infracciones disciplinarias cometidas.

Para ilustrar el alcance de la noción de dato personal en la universidad puede resultar de utilidad la lectura de la doctrina de diversas autoridades de protección de datos que se han pronunciado a raíz de las actuaciones realizadas por las Universidades.

Así, es un dato personal el número de Documento Nacional de Identidad. Por ello, no es un sistema adecuado de identificación y autenticación para acceder al campus virtual de una universidad aquel que utiliza el DNI. Tampoco resulta adecuado publicar el número de junto al nombre y los apellidos de un alumno en un listado en un campus virtual sin contar con su consentimiento tal y como se recoge en los dictámenes de la Agencia Catalana de Protecció de Dades al hilo de las consultas formuladas, precisamente, por el síndic de Greuges de una universidad catalana sobre el sistema de identificación y autenticación para acceder al campus virtual de la universidad (CNS 28/2011 y CNS 4/2012).

También es un dato personal la imagen de las personas. Por ello, la grabación de los alumnos durante la realización de los exámenes en una universidad exigirá ponderar adecuadamente los bienes jurídicos protegidos lo que lleva a la conclusión de que difícilmente puede entenderse que el uso generalizado de esta medida sea proporcionado y adecuado para la finalidad perseguida salvo que se lleve a cabo en determinadas circunstancias y con especiales salvaguardas (informe de la Agencia Española de Protección de Datos 0186/2017). Asimismo, en el caso de las imágenes captadas a través de una vídeo cámara instalada en el acceso a un laboratorio de una facultad exige, entre otros, dar cumplimiento al derecho de información (dictamen de la Agencia Catalana de Protecció de Dades PS 55/2010).

Asimismo, son un dato personal las huellas dactilares. Por ello, si se recogen las huellas dactilares en el control de acceso a unas dependencias de la universidad sin proporcionar a las personas afectadas información sobre los tratamientos de datos personales será una infracción de la normativa (dictamen de la Agencia Catalana de Protecció de Dades PS 15/2017 y el expediente de la Agencia Española de Protección de Datos E/02116/2016).

De hecho, la imagen facial o datos dactiloscópicos que se pueda utilizar para identificar a los estudiantes o al personal de la universidad son datos biométricos que junto con otros datos como los relativos a la salud, la afiliación sindical o la ideología son algunos ejemplos de datos especialmente protegidos que pueden también estar en poder de la universidad (artículo 4.14 RGPD). En principio, el tratamiento de estos datos está prohibido a no ser que concurra alguna de las circunstancias previstas en el artículo 9.2 RGPD como que el interesado haya su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados o sea necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado o este haya hecho manifiestamente públicos los datos personales.

Finalmente, también debe considerarse como un dato personal la información sobre la antigüedad de un profesor o el personal de administración y servicios que le identifique directa o indirectamente (dictamen de la Agencia Catalana de Protecció de Dades CNS 14/2009).

3. Los principios relativos al tratamiento

Los principios relativos al tratamiento son aquellas reglas que regulan como se deben llevar a cabo los tratamientos de datos personales con el fin de garantizar la protección de los datos personales. De este modo, los datos personales deben ser necesariamente tratados de acuerdo con los principios previstos en el RGPD. La vulneración de los principios previstos en el RGPD se tipifica en la normativa vigente como infracción muy grave (artículos 83 RGPD y 72 LOPDGDD) (Corral Sastre, 2016). La nueva regulación ha llevado a cabo una actualización de los distintos principios a los que haremos referencia a continuación. Sin embargo, en términos generales, la regulación de los principios del tratamiento tiene un carácter continuista respecto a la regulación anterior (Puyol Montero, 2016, 137). De todos modos, no podemos desconocer que la nueva regulación refleja el desarrollo que estos principios han ido experimentando en los últimos años a la luz de las normas aprobadas por los estados miembros y las sentencias dictadas por el TJUE (Muñoz Ontier, 2018, 347). Asimismo, ha incorporado nuevos principios como el de responsabilidad proactiva al que nos referiremos en una sección posterior.

3.1. Principios de licitud, lealtad y transparencia

Los datos personales deben ser tratados de manera lícita, leal y transparente en relación con el interesado (artículo 5.1.a) RGPD). Para que el tratamiento sea lícito es necesario que se dé alguna de las condiciones previstas en el RGPD (artículo 6.1 RGPD). La principal condición para que el tratamiento sea lícito es que el interesado haya dado su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos. El consentimiento debe ser libre, específico, informado e inequívoco por el que acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen (artículo 4.11 RGPD). Cuando se quiera fundar el tratamiento de los datos en el consentimiento del afectado para una pluralidad de finalidades será preciso que conste de manera específica e inequívoca que dicho consentimiento se otorga para todas ellas (artículo 6.2 LOPDGDD).

En particular, en algunas universidades la ausencia de consentimiento del interesado ha dado lugar a diversas reclamaciones ante las autoridades

de protección de datos. Así, cuando una universidad ha enviado un correo electrónico mostrando la dirección de todos los destinatarios sin haber recabado su consentimiento se ha considerado como una infracción de la normativa (dictamen de la Agencia Catalana de Protecció de Dades PS 2/2010). También cuando se ha incluido la imagen de una persona en una orla sin haber dado su consentimiento para ello (resolución de la Agencia Española de Protección de Datos R/01307/2017). Igualmente cuando la universidad ha publicado a través de un directorio en la intranet los datos de sus alumnos para que los profesores puedan contactar con ellos sin su consentimiento (dictamen de la Agencia Catalana de Protecció de Dades PS 41/2011).

Para que el consentimiento pueda manifestarse adecuadamente, las Universidades deben facilitar a los interesados información sobre el tratamiento en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo (artículo 12 RGPD). Entre otras, se debe facilitar la información relativa a la identidad y los datos de contacto del responsable, los datos de contacto del delegado de protección de datos, los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento o los destinatarios o las categorías de destinatarios de los datos personales (artículo 13.1 RGPD). El RGPD prevé que la información que se deba facilitar al interesado será diferente cuando los datos personales se obtengan del interesado (artículo 13.1) respecto a cuando los datos personales no se hayan obtenido del interesado (artículo 14.1 y 2). En ambos casos, el responsable del tratamiento puede facilitar al afectado la información básica indicándole la dirección de correo electrónico o el medio a su disposición para poder acceder a la restante información (artículo 11 LOPDPGDD). Esta información puede facilitarse a través de un aviso incluido en la página web o portal de la universidad[1]. Asimismo, para facilitarse la comprensión de la información, esta puede transmitirse en combinación con iconos normalizados que permitan proporcionar de forma fácilmente visible, inteligible y claramente legible una adecuada visión de conjunto del tratamiento previsto (artículo 12.7 RGPD).

Además de los supuestos en los que el interesado ha dado su consentimiento, los tratamientos de datos personales pueden ser lícitos si son necesarios para la ejecución de un contrato en el que el interesado sea parte o para la aplicación a petición de este de medidas precontractuales; para el cumplimiento de una obligación legal aplicable al responsable del tratamiento; para proteger intereses vitales del interesado o de otra persona física; para el cumplimiento de una misión realizada en interés público o en

1 Véase como ejemplo, por todos, el aviso de privacidad de la Universitat Oberta de Catalunya. Accesible en: https://www.uoc.edu/portal/es/_peu/avis_legal/politica-privacitat/index.html, última consulta: febrero de 2019.

el ejercicio de poderes públicos conferidos al responsable del tratamiento; o para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales (artículo 6.1 RGPD).

Un supuesto en el ámbito universitario en el que el tratamiento está previsto legalmente sin la necesidad de recabar el consentimiento de los interesados lo encontramos en relación a la publicación de los resultados de las pruebas relacionadas con la evaluación de los conocimientos y competencias de los estudiantes o de los actos que resulten necesarios para la adecuada realización y seguimiento de dicha evaluación o 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 estos casos la Ley Orgánica 4/2007, de 12 de abril, por la que se modifica la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades dispone que no será preciso el consentimiento de los estudiantes o del personal de las Universidades (disposición adicional vigésima primera). De todos modos, a pesar de la habilitación prevista en la LOU, cuando se publican los resultados de la evaluación de la actividad de los profesores puede no estar justificado mantener publicados los resultados obtenidos con anterioridad (dictamen de la Autoritat Catalana de Protecció de Dades CNS 29/2011).

3.2. Principio de limitación de la finalidad

Los datos personales deben ser recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines (Artículo 5.1.b RGPD). Este precepto también dispone que cuando el tratamiento ulterior de los datos personales tenga fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales. Véase al respecto lo previsto en el artículo 26 LOPDGDD.

3.3. Principio de minimización de datos

Los datos personales deben ser adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados (artículo 5.1.c RGPD). De este modo, es necesario asegurar que únicamente se recaban los datos personales necesarios para lograr la finalidad prevista.

Por ello, cuando una universidad ha incluido en la lista de calificaciones de

dos datos identificativos (nombre y apellidos y número identificador del estudiante), la Autoritat Catalana de Protecció de Dades ha considerado que se ha vulnerado el principio de calidad (dictamen de la Agencia Catalana de Protecció de Dades PS 50/2014). Asimismo, cuando se ha publicado el listado de los estudiantes de una asignatura junto a la nota media de su expediente y el número de identificación académico también se ha concluido que con ello se ha vulnerado este principio por ser desproporcionado para la finalidad prevista (dictamen de la Agencia Catalana de Protecció de Dades PS 19/2014). Finalmente, la publicación del censo electoral de las elecciones al claustro con posterioridad a la celebración de las elecciones también supone una vulneración del principio de calidad de los datos (dictamen de la Agencia Catalana de Protecció de Dades PS 7/2013).

3.4. Principio de exactitud

Los datos personales deben ser exactos y, si fuera necesario, actualizados (artículo 5.1.d RGPD). Para ello, las Universidades deben adoptar todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan.

3.5. Principio de seguridad

Los datos personales deben ser tratados de tal manera que se garantice de manera adecuada su seguridad para evitar entre otros el tratamiento no autorizado o ilícito, la pérdida, destrucción o daño accidental. De este modo se persigue garantizar la integridad y la confidencialidad de los datos. Para ello, tal y como expondremos posteriormente se deben aplicar las medidas técnicas u organizativas apropiadas.

4. Los derechos de los miembros de la comunidad universitaria

A fin de garantizar el cumplimiento de estos principios, el RGPD reconoce distintos derechos de los interesados. El RGPD refuerza los derechos de los interesados en materia de protección de datos (Álvarez Caro, 2016). También ha ampliado el elenco de los derechos entre los que podemos destacar el derecho al olvido que con anterioridad a su regulación en el RGPD fue objeto de atención por el Tribunal de Justicia de la Unión Europea en la conocida sentencia del TJUE de 13 de mayo de 2014, asunto C-131/12 Google Spain, S.L. y Google Inc. / Agencia Española de Protección de Datos, Mario Costeja González (Berrocal Lanzarot, 2017); (Simón Castellano, 2015).

Junto a los derechos reconocidos en el RGPD, la LOPDGDD reconoce otros derechos de los ciudadanos en Internet algunos de los cuales pueden tener

un impacto en el ámbito de las Universidades como el derecho a la educación digital, el derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral, el derecho a la desconexión digital en el ámbito laboral; el derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo; el derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral o el derecho al olvido en búsquedas de Internet (título X LOPDGDD).

En las próximas centraremos nuestra atención específicamente en aquellos que pueden tener un mayor impacto en el ámbito universitario. Con carácter previo, podemos destacar algunos aspectos de carácter general. En primer lugar, que el responsable del tratamiento está obligado a indicar al interesado los medios a su disposición para ejercer los derechos. Estos medios deben ser fácilmente accesibles (artículo 12 LOPDGDD).

En segundo lugar, que los derechos reconocidos en el RGPD pueden ser limitados cuando con la restricción se respeten en los derechos y libertades fundamentales y sea una medida necesaria y proporcionada para salvaguardar, entre otros, la seguridad del Estado, la defensa, la seguridad pública, la prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales, la protección de la independencia judicial, la supervisión, inspección, o reglamentación vinculada con el ejercicio de la autoridad pública o la protección del interesado o de los derechos y libertades de otros (artículo 23 RGPD).

En tercer lugar, que en el caso de que no se respeten los derechos reconocidos en el RGPD, el interesado puede presentar una reclamación ante la Agencia Española de Protección de Datos o agencia autonómica de protección de datos competentes quien resolverá al respecto (considerando 141 RGPD así como, entre otros, artículos 12.4, 13.2, 14.2, 15.1 RGPD). Asimismo, el impedimento o la obstaculización del ejercicio de los de los interesados está tipificado como infracción (artículos 83 RGPD y 72.1.k y 74.c y d LOPDGDD).

4.1. Derecho de información

La transparencia en el tratamiento de los datos personales se concreta en el derecho a la información de los interesados. Como ya hemos avanzado anteriormente, los responsables del tratamiento deben informar al interesado de diversos aspectos que variarán en función de si los datos han sido recabados del interesado o no.

Sin embargo, el RGPD dispone algunas excepciones a este derecho como, por ejemplo, cuando la información ya esté a disposición del interesado

(artículo 14.5 RGPD). En términos generales, la información se ha de poner a disposición de los interesados en el momento en el que se le soliciten sus datos o, cuando los datos no se obtengan del propio interesado, en el plazo de un mes (artículo 14.3 RGPD).

4.2. Derecho de acceso

El interesado tiene derecho a saber si se están tratando o no sus datos personales (artículo 15.1 RGPD). El interesado también tiene derecho a acceder a dichos datos y a obtener la información relativa a diferentes aspectos como los fines del tratamiento, las categorías de datos personales de que se trate, los destinatarios o las categorías de destinatarios a los que se comunicaron o serán comunicados los datos personales, el plazo previsto de conservación de los datos personales o, de no ser posible, los criterios utilizados para determinar este plazo, la existencia del derecho a solicitar del responsable la rectificación o supresión de datos personales o la limitación del tratamiento de datos personales relativos al interesado, o a oponerse a dicho tratamiento, el derecho a presentar una reclamación ante una autoridad de control o la información disponible sobre su origen cuando los datos personales no se hayan obtenido del interesado y la existencia de decisiones automatizadas.

Cuando así lo solicite el interesado, el responsable del tratamiento le facilitará una copia de los datos personales objeto de tratamiento sin que ello pueda afectar negativamente a los derechos y libertades de terceros. La LOPDGDD dispone que el derecho se entenderá otorgado si el responsable del tratamiento facilita al interesado un sistema de acceso remoto, directo y seguro a sus datos personales (artículo 13)

4.3. Derecho de rectificación

El interesado tiene derecho a obtener sin dilación indebida la rectificación de los datos personales inexactos que le conciernan (artículo 16 RGPD). El interesado también tiene derecho a que se completen los datos personales que sean incompletos. A estos efectos, el interesado debe indicar de manera clara y detallada a qué datos se refiere y la corrección que quiera que se haga y, cuando sea preciso, acompañar la solicitud de la documentación que justifique la rectificación (artículo 14 LOPDGDD).

4.4. Derecho de supresión

El interesado tiene derecho a obtener sin dilación indebida la supresión de los datos personales que le conciernan (artículo 17 RGPD).

El responsable del tratamiento estará obligado a suprimir los datos personales del interesado cuando estos ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo; el interesado retire el consentimiento en que se basa el tratamiento; el interesado se oponga al tratamiento y no prevalezcan otros motivos legítimos para el tratamiento; los datos personales hayan sido tratados ilícitamente; los datos personales deban suprimirse para el cumplimiento de una obligación legal o se hayan obtenido en relación con la oferta de servicios de la sociedad de la información.

El derecho de supresión puede ser limitado cuando el tratamiento sea necesario para ejercer el derecho a la libertad de expresión e información; para el cumplimiento de una obligación legal o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable; por razones de interés público en el ámbito de la salud pública; con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos o para la formulación, el ejercicio o la defensa de reclamaciones.

4.5. Derecho a la limitación del tratamiento

El interesado tiene derecho a obtener del responsable del tratamiento la limitación del tratamiento de los datos. La limitación del tratamiento se podrá obtener cuando el interesado haya impugnado la exactitud de los datos personales; o el tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso; o el responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones; o el interesado se haya opuesto al tratamiento mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado (artículo 18 RGPD).

Cuando se haya limitado el tratamiento de datos personales, los datos solo podrán ser objeto de tratamiento, con excepción de su conservación, con el consentimiento del interesado o para la formulación, el ejercicio o la defensa de reclamaciones, o con miras a la protección de los derechos de otra persona física o jurídica o por razones de interés público importante.

4.6. Derecho de oposición

El interesado tiene derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular, a que datos personales que le conciernan sean objeto de un tratamiento (artículo 21 RGPD).

En este caso, el responsable del tratamiento debe dejar de tratar los datos personales, salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones.

Una manifestación concreta de este derecho la encontramos en el derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado de los datos personales que produzca efectos jurídicos en él o le afecte significativamente de modo similar (artículo 22 RGPD).

5. Los sujetos que participan en la garantía de la protección de datos personales en la universidad

Las universidades han de garantizar que los tratamientos de datos personales se ajustan a lo dispuesto en la normativa de protección de datos y que se han tomado las medidas necesarias para garantizar los derechos de los interesados y la seguridad de los datos personales. Todo ello lo han de poder demostrar ante las personas interesadas y también ante la autoridad de protección de datos tal y como se desprende del principio de responsabilidad proactiva (artículo 5.2 RGPD). Para ello es necesario que asignen a distintos sujetos las responsabilidades para el cumplimiento de las distintas obligaciones y la garantía de los diversos principios reconocidos en el RGPD atribuyéndoles las funciones específicas y los recursos necesarios para cumplir con lo previsto en la normativa.

5.1. El responsable y el encargado del tratamiento

En primer lugar, las Universidades deben determinar quién es el responsable del tratamiento, es decir, la persona física o jurídica, autoridad pública, servicio u otro organismo que determine los fines y medios de un tratamiento (artículo 4.7 RGPD).

En segundo lugar, las Universidades pueden designar a un encargado del tratamiento que será la persona física o jurídica, autoridad pública, servicio u otro organismo que trate los datos por cuenta del responsable del tratamiento (artículo 4.8 RGPD). El tratamiento que deba realizar el encargado se regirá por un contrato u otro acto que le vincule con el responsable y que defina el tratamiento y determine las obligaciones y derechos del responsable y del encargado (artículo 28 RGPD).

Los responsables y encargados del tratamiento han de determinar las medidas apropiadas que deben adoptar en función de los riesgos que pueda generar el tratamiento. Como se desprende del considerando 75 RGPD, en-

tre los riesgos para los derechos y libertades de las personas físicas se encuentran los daños y perjuicios físicos, materiales o inmateriales, la discriminación, la usurpación de identidad o el fraude, pérdidas financieras, daño para la reputación, la pérdida de confidencialidad de datos sujetos al secreto profesional, la reversión no autorizada de la seudonimización o cualquier otro perjuicio económico o social significativo. Esto constituye un cambio significativo respecto al régimen anterior al no concretar el RGPD las medidas de seguridad que deben adoptar los responsables y encargados del tratamiento sino que estas serán determinadas por el responsable en función de la evaluación de los riesgos. Como observa Costa "el cambio conceptual es tan profundo que va más allá del alcance o ámbito de aplicación objetivo de la norma" (Costa Hernandis, 2018, 419).

De este modo, en la actualidad el responsable y el encargado del tratamiento deben aplicar las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo a la vista del estado de la técnica, los costes de aplicación, la naturaleza, el alcance, el contexto y los fines del tratamiento y los riesgos de probabilidad y gravedad para los derechos y libertades de las personas físicas. El cumplimiento de todo ello puede ser acreditado a través de la adhesión a un código de conducta (artículo 32 RGPD). Los códigos de conducta deben ser aprobados por la Agencia Española de Protección de Datos o agencia autonómica de protección de datos y vinculan a quienes se adhieran a ellos. Cuando un responsable o encargado del tratamiento se adhiera al código también se obligan a someter al organismo o entidad de supervisión las reclamaciones que les formulen los interesados (artículo 38 LOPDGDD). Con carácter previo a la aprobación del RGPD, diversas universidades como la Universidad de Castilla-La Mancha, la Universidad Nacional de Educación a Distancia o la Universidad de Oviedo se habían dotado de códigos de conducta.

Asimismo, el RGPD dispone que los responsables deben emplear las medidas técnicas y organizativas apropiadas para aplicar de manera efectiva los principios de protección de datos. La determinación de estas medidas deberá tener en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento así como los riesgos que entraña el tratamiento para los derechos y libertades de las personas físicas (artículo 25.1 RGPD). Además, el responsable del tratamiento deberá aplicar las medidas técnicas y organizativas apropiadas para garantizar que por defecto solo sean objeto de tratamiento los datos personales que sean necesarios para cada fin del tratamiento (artículo 25.2 RGPD). Para acreditar el cumplimiento de estas obligaciones, se podrá utilizar una certificación (artículo 42 RGPD).

Para ello, las Universidades han de llevar a cabo una evaluación del impacto de los tratamientos en la protección de datos personales cuando sea probable que estos puedan suponer un riesgo alto para los derechos y las libertades de las personas. En particular, el RGPD considera que comportan un alto riesgo los tratamientos que elaboren perfiles para tomar decisiones con efectos jurídicos sobre los interesados o les afecten significativamente, traten a gran escala categorías especiales de datos o sirvan para observar de manera sistemática a gran escala una zona de acceso público. Para su interpretación pueden resultar útiles las Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del Reglamento (UE) 2016/679 adoptadas por Grupo "protección de datos" del artículo 29 el 4 de abril de 2017.

Para poder demostrar la conformidad con el RGPD, los responsables o los encargados del tratamiento deben llevar un registro escrito, que puede tener formato electrónico, de las actividades de tratamiento que lleven a cabo (artículo 30 RGPD). De este modo se concreta el principio de responsabilidad proactiva previsto en los artículos 5.2 y 24 RGPD. El cumplimiento de las obligaciones por parte del responsable del tratamiento también puede ser demostrado a través de la adhesión a los códigos de conducta. Como observa Martínez Martínez, "lo relevante del llamado registro de actividades del tratamiento no reside tanto en su contenido como en el cambio de filosofía de gestión que incorpora. Obliga a un cambio en el modelo de gestión desde un cierto grado de pasividad a un nuevo tipo de proactividad" (Martínez Martínez, 2018). Cuando así lo solicite, este registro de las actividades de tratamiento deberá ponerse a disposición de la autoridad de control. Los responsables y encargados del tratamiento de datos así como todas las personas que intervengan en cualquier fase del tratamiento están sujetas al deber de confidencialidad (artículo 5.1 LOPDGDD).

Las autoridades de protección de datos han considerado que el deber de secreto ha sido vulnerado por las Universidades en ocasiones al configurar una lista de distribución unidireccional permitiendo a los usuarios-suscriptores enviar mensajes a dicha lista lo que comporta el acceso a datos personales (dictamen de la Agencia Catalana de Protecció de Dades PS 45/2014), o enviar mensajes de correo electrónico sin ocultar las direcciones de los destinatarios (resolución de la Agencia Española de Protección de Datos R/03231/2016).

5.2. El delegado de protección de datos

Junto a las figuras del responsable y el encargado del tratamiento, el RGPD

prevé que los responsables y los encargados del tratamiento designarán un delegado de protección de datos. Tanto las Universidades públicas como las privadas deben nombrar un delegado (artículo 34.1 RGPD). Las universidades públicas pueden decidir designar un delegado de protección de datos para varias universidades (artículo 37.3 RGPD).

El delegado de protección de datos debe tener las cualidades profesionales y los conocimientos necesarios para poder desarrollar las funciones asignadas. El delegado puede formar parte de la plantilla o bien actuar en el marco de un contrato. En cualquier caso, el delegado debe actuar con autonomía sin poder recibir instrucción alguna respecto al ejercicio de sus funciones y no puede ser destituido ni sancionado por ello. Al respecto, la LOPDGDD dispone que "se garantizará la independencia del delegado de protección de datos dentro de la organización, debiendo evitarse cualquier conflicto de intereses" (artículo 36.2) El delegado de protección de datos rendirá cuentas directamente al más alto nivel jerárquico del responsable o encargado del tratamiento (artículo 38 RGPD).

El delegado de protección de datos será el encargado de informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben; supervisar el cumplimiento de lo dispuesto en la normativa en materia de protección de datos personales; asesorar acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación; cooperar con la agencia de protección de datos y ser el punto de contacto con ella para cuestiones relativas al tratamiento. Los delegados deben mantener secreto o confidencialidad en el desempeño de sus funciones (artículo 38.5 RGPD).

6. Reflexiones finales: la contribución de los defensores universitarios a la garantía de la protección de los datos personales

Las universidades tienen ante sí el reto de adaptarse a la nueva regulación de la protección de datos personales pero se parte de la experiencia acumulada en el pasado (Martínez Martínez, 2018). Para ello cuentan con distintos sujetos a los que el RGPD atribuye distintas responsabilidades y funciones. Como hemos visto en las páginas anteriores, la garantía de la protección de los datos personales corresponde en primera instancia a los responsables y los encargados del tratamiento quienes deben dar satisfacción a las solicitudes de ejercicio de los derechos de los interesados en materia de protección de datos y adoptar las medidas técnicas y organizativas apropiadas para garantizar el cumplimiento de la normativa vigente (artículos 24 y 28 RGPD).

Asimismo, la garantía de la protección de los datos personales y de los derechos de los interesados también corresponde a los delegados de protección de datos a los que pueden dirigirse los interesados con carácter previo a la presentación de una reclamación ante la Agencia Española de Protección de Datos o agencia autonómica de protección de datos. En este caso, el delegado de protección de datos debe comunicar al interesado la decisión adoptada en el plazo máximo de dos meses (artículo 37 LOPDGDD).

En última instancia, corresponde a la Agencia Española de Protección de Datos y a las agencias autonómicas de protección de datos supervisar la aplicación de la normativa en materia de protección de datos y, en particular, garantizar el respeto de los derechos de los interesados. La Agencia Española de Protección de Datos es una autoridad administrativa independiente de ámbito estatal a quien le corresponde. Junto a ella, algunas Comunidades Autónomas han creado su autoridad de protección de datos (por ejemplo, Andalucía, Cataluña o el País Vasco) (artículos 44 y 47 LOPDPGDD). Entre otras funciones esas entidades deben facilitar información a los interesados en relación al ejercicio de sus derechos y tratar las reclamaciones que estos puedan presentar por el incumplimiento de lo dispuesto en el RGPD (artículo 57 RGPD). Estas funciones podrán ser ejercidas por las agencias autonómicas en relación a los tratamientos llevados a cabo por las Universidades de su ámbito de competencia (artículo 57 LOPDGDD).

Más allá de los sujetos, órganos y entidades que tienen específicamente atribuida en el RGPD y la LOPDGDD la garantía de los derechos de los interesados y, en general, la protección de los datos personales, es evidente que en el ámbito universitario los defensores podemos contribuir a la garantía del derecho de protección de datos personales. Al respecto, debemos recordar que el Estatuto del Estudiante Universitario reconoce como derecho de los estudiantes universitarios el derecho a que sus datos personales no sean utilizados con otros fines que los regulados por la Ley de Protección de Datos de carácter personal (artículo 7.1.v Real Decreto 1791/2010, de 30 de diciembre).

Los defensores universitarios en el marco de nuestras funciones de intervenir ante cualquier vulneración de los derechos de los miembros de la comunidad universitaria y de velar por la calidad de la universidad, podemos instar el cumplimento de la normativa de protección de datos y, en particular, recordar ante las instancias competentes que la universidad debe adoptar las medidas de seguridad necesarias para responder a los riesgos identificados. Asimismo, los defensores podemos contribuir a la difusión de los derechos para que todos los miembros de la comunidad universitaria los conozcan y, en su caso, los ejerzan.

La independencia, la autonomía y confidencialidad que definen nuestra actuación constituyen un sólido fundamento para garantizar nuestra contribución a la protección de los datos personales de los miembros de la comunidad universitaria (disposición adicional decimocuarta Ley orgánica de Universidades y artículo 46.1 Estatuto del Estudiante Universitario) tal y como se ha destacado en relación al delegado de protección de datos al afirmar que "una cuestión esencial a considerar en relación con la figura del delegado de protección de datos es la de su independencia" (...) "es decir, la clave está en considerar la independencia como garantía de la autonomía de actuación del delegado de protección de datos" (Recio Gayo, 2016, 384-385).

En cualquier caso, para reforzar esta contribución sería conveniente que las Universidades bien en los instrumentos de que se doten para el cumplimiento de lo dispuesto en el RGPD y la LOPDGDD (por ejemplo, los códigos de conducta) bien en los reglamentos de los defensores universitarios concretasen el alcance de estas funciones.

Normativa citada

LOPDGDD: Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales, *Boletín Oficial del Estado* nº 294, de 6 de diciembre de 2018.

RGPD: 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 y por el que se deroga la Directiva 95/46/CE (*Reglamento General de Protección de Datos*). *Diario Oficial de la Unión Europea*, L 119/1, de 4 de mayo de 2016.

Bibliografía

Álvarez Caro, M. (2016). El derecho de rectificación, cancelación, limitación del tratamiento, oposición y decisiones individuales automatizadas. En J. L. Piñar Mañas (Dir.), *Reglamento general de protección de datos: hacia un nuevo modelo europeo de privacidad* (pp. 227-240). Madrid: Reus.

Berrocal Lanzarot, A. I. (2017). *Derecho de supresión de datos o derecho al olvido*. Madrid: Editorial Reus.

Corral Sastre, A. (2016). El régimen sancionador en materia de protección de datos en el reglamento general de la Unión Europea. En J. L. Piñar Mañas (Dir.), *Reglamento general de protección de datos: hacia un nuevo modelo europeo de privacidad* (pp. 571-586). Madrid: Reus.

Costa Hernandis, R. (2018). Responsabilidad del responsable del tratamiento. En J. López Calvo (Coord.), *El nuevo marco regulatorio derivado del reglamento europeo de protección de datos* (pp. 419-425). Madrid: Bosch-Wolters Kluwer.

Martínez Martínez, R. (2018). La protección de datos en la universidad: retos para el 25 de mayo de 2018. En A. I. Caro Muñoz (Dir.), *La articulación de la gestión universitaria a debate: XIV Curso de Régimen Jurídico de Universidades y Diez años de inestabilidad : el régimen jurídico del personal docente e investigador en España* (pp. 41-68). Cizur Menor: Thomson-Reuters-Aranzadi.

Muñoz Ontier, J. (2018). Disposiciones generales. En J. López Calvo (Coord.), *El nuevo marco regulatorio derivado del reglamento europeo de protección de datos* (pp. 289-300). Madrid: Bosch-Wolters Kluwer.

Puyol Montero, F. J. (2016). Los principios del derecho a la protección de datos. En J. L. Piñar Mañas (Dir.), *Reglamento general de protección de datos: hacia un nuevo modelo europeo de privacidad* (pp. 135-150). Madrid: Reus.

Rallo Lombarte, A. (Coord.) (2019). *Tratado de Protección de Datos*. Valencia: Tirant lo Blanch.

Recio Gayo, M. (2016). El delegado de la protección de datos. En J. L. Piñar Mañas (Dir.), *Reglamento general de protección de datos: hacia un nuevo modelo europeo de privacidad* (pp. 367-388). Madrid: Reus.

Simón Castellano, P. (2015). *El reconocimiento del derecho al olvido digital en España y en la UE: efectos tras la sentencia del TJUE de mayo de 2014*. Barcelona: Bosch.

Troncoso Reigada, A. (Coord.) (2019). *Comentario al RGPD y a la LOPD*. Cizur Menor: Civitas.