CNS 17/2020

Dictamen en relación con la "Guía sobre la protección de datos personales en el ámbito universitario en tiempos del COVID-19" elaborada por la CRUE

Se pide que la Autoridad emita un dictamen sobre la "Guía sobre la protección de datos personales en el ámbito universitario en tiempos del COVID-19" (en adelante "la Guía") elaborada por la CRUE.

Analizada la consulta, que se acompaña de una copia del borrador de la Guía, y de acuerdo con el informe de la Asesoría Jurídica emito el siguiente dictamen:

(...)

II

Antes de entrar a analizar el contenido de la Guía, se considera necesario realizar algunas consideraciones previas sobre la Guía que se somete a consulta y el contexto en el que aparece.

Debe tenerse en cuenta que a pesar de que desde el pasado 14 de marzo se ha declarado el estado de alarma (con sucesivas prórrogas) de acuerdo con el artículo 116.2 CE, esta declaración no comporta una suspensión general de los derechos de las personas y, más concretamente, del derecho fundamental a la protección de datos personales.

En este sentido, y de acuerdo con la Ley orgánica 4/1981, de 1 de junio, de los estados de alarma, excepción y asedio, la declaración del estado de alarma comporta el sometimiento de la función pública y en especial de las fuerzas y cuerpos de seguridad a la autoridad competente, así como puede comportar limitaciones a la libertad de circulación o de reunión, habilitar requisas o la intervención de empresas y establecimientos, limitar el consumo o uso de servicios o establecer medidas para Sin embargo, el derecho a la protección de datos sigue plenamente vigente. La excepcional situación de crisis en materia de salud pública derivada del COVID19 puede hacer entrar en funcionamiento determinados mecanismos previstos en la legislación en esta materia pero en cualquier caso su incidencia en el derecho a la protección de datos deberá reconducirse a los supuestos ya los límites previstos de acuerdo con la normativa aplicable en materia de protección de datos que, en el caso de las universidades, será el Reglamento (UE) 2016/679) del Parlamento y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que se refiere al tratamiento de datos personales ya la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos (RGPD)). Esta normativa establece mecanismos que permiten hacer frente a las situaciones generadas por este nuevo contexto.

La Guía que se analiza en esta consulta ofrece, bajo la forma de preguntas/respuestas, una serie de pautas a tener en cuenta por las universidades para hacer frente a los principales problemas para su funcionamiento que ha generado la situación derivada de la pandemia por el COVID19. Por ello, sus conclusiones deben entenderse aplicables sólo mientras se mantenga esta situación.
Como se sabe en materia de protección de datos a menudo es necesario llevar a cabo un ejercicio de ponderación para determinar la admisibilidad de una determinada medida o las garantías adecuadas a adoptar. En esta tarea juega un papel relevante el contexto en el que se lleva a cabo el tratamiento (actualmente la excepcionalidad derivada de la crisis por el COVID19 y el estado de alarma). Por tanto, no se puede concluir en ningún caso una aplicabilidad generalizada de las consideraciones que se contienen en la Guía, ni las que se hacen en este dictamen, una vez desaparezca esta si

En cualquier caso, habrá que tener en cuenta que se trata sólo de una primera aproximación a los problemas que se plantean, necesariamente de manera simplificada, que será necesario analizar de forma esmerada por cada responsable del tratamiento a la hora de aplicarla a las situaciones concretas que se plateen, a la vista de las circunstancias del caso concreto.

Teniendo en cuenta estas consideraciones, a todos los efectos se debe valorar positivamente tanto la oportunidad de elaborar un documento de esta naturaleza, como el nivel de análisis y el valor orientativo de las pautas que se ofrecen en la Guía para afrontar los principales problemas derivados de esa situación. Sin perjuicio de ello, en este informe se incluirán algunos comentarios sobre algunos aspectos en los que podría ser aconsejable introducir alguna aclaración o realizar una revisión.

El objeto de este informe no es pues validar todos y cada uno de los posicionamientos que se contienen que, como hemos dicho, sólo se pueden analizar cuidadosamente cuando se disponga de un conocimiento suficiente de las circunstancias del caso concreto que se plantee y del apego para los derechos de las personas que puede producirse en cada caso, sino sólo contribuir a la mejora de estas pautas generales como criterio de orientación. A estos efectos se analizarán las diversas cuestiones siguiendo la agrupación por ámbitos que realiza la Guía

III

Ámbito de la docencia

En la respuesta a la pregunta 2 se recomienda grabar las clases del aula virtual.

Al respecto, la Guía recomienda fomentar las interacciones a través del chat. La medida se considera positiva, dado que seguramente fomentará las interacciones al evitar el efecto disuasivo que podría tener la grabación de la interacción en soporte audiovisual.

Sin embargo, al margen de esto, sería conveniente que la recomendación de grabar las clases virtuales fuese acompañada de una recomendación para que tanto la grabación de la imagen como del sonido se refiera únicamente a la persona docente.

A tal efecto sería bueno que se recomiendas de entrada emplear sistemas que sólo impliquen la grabación de la exposición del docente que incluya también las respuestas a las consultas formuladas a través del chat, primando este sistema sobre la videoconferencia, que resultaría más intrusivo

desde el punto de vista de los estudiantes. En caso de que el formato de la clase requiera la videoconferencia, parecería adecuada la previsión de la respuesta a la pregunta 3, para que sea el propio estudiante quien desconecte, en su caso, el sistema de vídeo o audio.

En cuanto a la pregunta 3, se contienen una serie de previsiones sobre diferentes aspectos de los que hay que informar a las personas afectadas, que se valoran positivamente, pero habría que aclarar que es necesario informar sobre todos los aspectos previstos en el artículo 13 RGPD. En principio, parece que la expresión "condiciones generales del tratamiento" se refiere a esta cuestión, pero ni esa expresión ni la expresión "Se recomienda que exista una capa de información si se usan metodologías que graban las clases.", parecen bastante claras.

En la pregunta 5, algunos de los ejemplos que se ponen sobre el derecho de oposición no parecen suficientemente claros. Así, por ejemplo, el hecho de que aparezca la imagen de familiares no sería un caso de derecho de oposición por parte del estudiante o del profesor, sino, en todo caso, de la tercera persona Convendría aclararlo.

IV

Ámbito de la evaluación

En las respuestas a las preguntas 9 y 10 se trata el deber de información, pero se hace de forma que puede generar alguna confusión.

De entrada, en la pregunta 9, la referencia a tres "capas" puede generar confusión dado que, aunque ni el RGPD ni el LOPDDDD emplean la expresión "información por capas", las Guías elaboradas conjuntamente por las diferentes autoridades de control del estado español emplean esta denominación para referirse a la posibilidad, prevista en el artículo 11 LOPDGDD, de ofrecer por un lado la información básica y por otro la restante información. Por eso sería preferible referirse a que la información deberá darse "..., al menos, por tres medios:".

Esta misma respuesta a la pregunta 9 incorpora dos ejemplos de información gráfica que incluiría la información básica a la que se refiere el artículo 11 LOPDGDD. La información contenida en el mismo resulta bastante clara. No obstante, debería completarse la explicación indicando que el enlace que figura debe llevar a poder conocer de una manera fácil el resto de la información prevista en el artículo 13 RGPD.

Por otra parte, ya efectos de mejorar la sistemática, sería positivo que esta información sobre los medios para informar y sobre la información gráfica se trasladara a la respuesta a la pregunta 10 que versa sobre el deber de informar (la pregunta 9 versa sobre si se puede grabar o no).

En la respuesta a la pregunta 11 se menciona expresamente la conveniencia de conocer la opinión de la autoridad de protección de datos sobre la utilización de datos biométricos para identificar al alumnado en pruebas de evaluación.

Por supuesto que esta Autoridad comparte la respuesta ofrecida en cuanto a la necesidad de que un tratamiento de este tipo requeriría llevar a cabo una evaluación de impacto relativa a la protección de datos. Pero más allá de esto, debemos decir que, tal y como expusimos en nuestros dictámenes CNS 63/2018 y CNS 7/2020, es necesario ser especialmente restrictivo a la hora de utilizar estos sistemas.

Hay que tener en cuenta que la utilización de la huella dactilar o el patrón de la huella dactilar u otro dato biométrico como por ejemplo la imagen facial, para identificar a un alumno mediante sistemas técnicos de reconocimiento, hace que este dato deba ser calificado como dato biométrico, dado que de acuerdo con el artículo 4.14 RGPD tienen esta consideración cuando han sido "obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirman la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos;".

Esto hace que, de acuerdo con el artículo 9.1 RGPD, se les deba aplicar el régimen específico previsto para las categorías especiales de datos previsto tanto en el artículo 9, como en otros artículos del RGPD

En este sentido, el Considerante 51 del RGPD pone de manifiesto el carácter restrictivo con el que se puede admitir los tratamientos de estos datos:

> **"(51) (...)Tales datos personales no deben ser tratados, salvo que se permita su tratamiento en situaciones específicas contempladas en el presente Reglamento, habida cuenta de que los Estados miembros pueden establecer disposiciones específicas sobre protección de datos con objeto de adaptar la aplicación de las normas del presente Reglamento al cumplimiento de una obligación legal o al cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. Además de los requisitos específicos de este tratamiento, deben aplicarse los principios generales y otras normas del presente Reglamento, sobre todo en lo que se refiere a las condiciones de licitud del tratamiento. Se deben establecer de forma explícita excepciones a la prohibición general de tratamiento de estas categorías especiales de datos personales, entre otras cosas cuando el interesado dé su consentimiento explícito o tratando de necesidades específicas, en particular cuando el tratamiento sea realizado en el marco de actividades legítimas por determinadas asociaciones o fundaciones cuyo objetivo sea permitir el ejercicio de las libertades fundamentales.**
>
> **(52) Asimismo deben autorizarse excepciones a la prohibición de tratar categorías especiales de datos personales cuando lo establezca el Derecho de la Unión o de los Estados miembros y siempre que se den las garantías apropiadas, a fin de proteger datos personales y otros derechos fundamentales, cuando sea en interés público, en particular el tratamiento de datos personales en el ámbito de la legislación laboral, la legislación sobre protección social, incluidas las pensiones y fines de seguridad, supervisión y alerta sanitaria, la prevención o control de enfermedades transmisibles y otras amenazas graves para la salud.(...)"**

De acuerdo con estas consideraciones, el tratamiento de datos biométricos requerirá no sólo la concurrencia de una de las bases jurídicas establecidas en el artículo 6 del RGPD sino que, además, deberá concurrir alguna de las excepciones previstas en artículo 9.2 del RGPD.

Esta Autoridad ya había analizado, en dictámenes anteriores a la entrada en vigor del RGPD (por ejemplo, CNS 9/2009, CNS 22/2009 o 22/2011), la adecuación a la normativa en materia de protección de datos personales de los sistemas de control de acceso y horario de los empleados de las administraciones públicas mediante datos biométricos (como la huella dactilar o un patrón biométrico), concluyendo, de acuerdo con diversas decisiones judiciales (STS de 2 de julio de 2007, Auto del Tribunal Constitucional de 26 de febrero de 2007, SAN de 4 de marzo de 2010 o STJUE de la región de Murcia de 25 de enero de 2010), que podía resultar proporcionada la utilización de sistemas de control biométrico con ese fin.

En caso de que nos ocupe, la habilitación prevista en el artículo 6.1.e) RGPD (para las universidades públicas) o la prevista en el apartado 6.1.b) (para las universidades privadas), podrían habilitar el tratamiento de datos de los estudiantes. Ahora bien, con la aprobación del RGPD, y tal como pone de relieve el considerante 51 del propio RGPD, en la medida en que los datos biométricos han pasado a ser considerados como una categoría especial de datos (art. 9.1 RGPD), será necesario que concurra alguna de las excepciones previstas en el artículo 9.2 RGPD que permitan levantar la prohibición general del tratamiento de este tipo de datos establecida en el a

No parece clara cuál de las excepciones previstas en el artículo 9.2 podría ser aplicable en caso de que nos ocupa, ya que no parece que pueda basarse en el consentimiento (en este contexto difícilmente podría considerarse libre). Es obvio que si se establece como sistema obligatorio de identificación no puede basarse en el consentimiento.

Del resto de excepciones, teniendo en cuenta la finalidad de la identificación, la única a la que podría apelarse en principio, sería la prevista en la letra g): "el tratamiento es necesario por razones de un interés público esencial , en base al Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado" . Ahora bien, a fin de que pudiera ser de aplicación esta excepción, debería haber sido establecido sobre la base del derecho del Estado miembro.

En cuanto al rango de la norma de derecho interno, el Considerante 41 establece que "Cuando el presente Reglamento hace referencia a una base jurídica oa una medida legislativa, esto no exige necesariamente un acto legislativo adoptado por un parlamento, sin perjuicio de los requisitos de conformidad del ordenamiento constitucional del Estado miembro de que se trate.".

Hay que tener en cuenta al respecto que, en el derecho español, la norma que establezca el tratamiento deberá ser una norma con rango de ley, tal y como se desprende del artículo 53 CE en la medida en que conlleva la limitación de un derecho fundamental, y tal y como ha venido a reconocer la jurisprudencia constitucional (SSTC 292/2000 y 76/2019, entre otros), del Tribunal de Justicia Europea (STJUE 08.04.2014, Digital Rights Ireland, entre otros) y del Tribunal Europeo de Derechos Humanos (STEDH 07.06.2012, Cetro Europa 7 y Di Stefano vs. Italia, entre otros). En este sentido, el artículo 9.2 de la Ley orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales (LOPDGDD) establece que "Los tratamientos de datos contemplados en las letras g), h) ei) del artículo 9.2 del Reglamento (UE) 2016/679 fundados en el Derecho español deberán estar amparados en una norma con rango de ley, que podrá establecer requisitos adicionales relativos a su seguridad y confidencialidad.". Norma que, además, deberá ser proporcional y formulada en términos que resulten previsibles tanto los requisitos y condiciones para su aplicación, como las garantías adoptadas (STC 76/2009).

Sea como fuere, por la información de que se dispone, no parece que se cuente con una norma con rango de ley que permita llevar a cabo este tratamiento, por lo que debería descartarse. Al respecto parece claro también que existen alternativas al alcance con una eficacia similar a la identificación que puede llevarse a cabo en las pruebas presenciales. Aparte de la identificación directa a través del rostro y la voz de los alumnos (sin utilizar procedimientos técnicos específicos), la posibilidad de pedir la exhibición del documento nacional de identidad, NIE, pasaporte o equivalente, y la posibilidad de comprobarlo posteriormente, debería ser suficiente a estos efect

En cuanto a la pregunta 13, la utilización de la expresión "No obstante lo anterior, deberían considerarse los supuestos de oposición al tratamiento, por ejemplo, cuando deriven de circunstancias relacionadas con la diversidad, funcional, o la violencia de género." podría generar falsas expectativas cuando no parece clara a priori la vinculación de estas situaciones con la estimación del derecho de oposición en un contexto como el que se analiza.

En la respuesta a la pregunta 14 se excluye la posibilidad de que los docentes puedan ejercer su derecho de oposición en la grabación de pruebas de evaluación ("no podrá oponerse a la misma"). No parece que a priori pueda establecerse esta conclusión, especialmente porque, a diferencia de las clases virtuales, en una prueba de evaluación puede no ser esencial la captación del docente. Los docentes tienen este derecho como cualquier otra persona, y la procedencia o no de estimar el ejercicio de ese derecho dependerá de las circunstancias del caso concreto de acuerdo con

La respuesta a la pregunta 17 se remite a las orientaciones de la AEPD sobre la identificación de las personas interesadas en publicaciones. Al respecto cabe decir que las citadas orientaciones fueron adoptadas conjuntamente por la Agencia Española de Protección de Datos, la Autoridad Catalana de Protección de Datos, la Agencia Vasca de Protección de Datos y el Consejo de Transparencia y Protección de Datos de Andalucía. Por ello, la remisión debería estar en las orientaciones publicadas por las diferentes autoridades de protección de datos. En concreto en el caso del APDCAT, estas orientaciones están publicadas en su web https://apdcat.gencat.cat/web/.content/ autoridad/normativa/documentos/VAR-9-2019-orientacio-disposicio-addicional-7-cat.pdf .

Estas consideraciones pueden hacerse extensibles a la pregunta 20. En este caso la lista de la APDCAT de tratamientos que deben someterse a AIPD se puede encontrar en https:// apdcat.gencat.cat/web/.content/02 -derechos_y_obligaciones/obligaciones/documentos/Lista DPIA-CAT.pdf

V

Ámbito de la investigación

En este apartado se recoge en diferentes preguntas diversos aspectos relativos a la utilización de datos con fines de investigación. En realidad, si bien la situación derivada del COVID19 presenta alguna problemática específica, las consideraciones que se recogen en la Guía no se refieren en su mayor parte a la situación derivada del COVID19 sino al régimen ordinario aplicable a la

investigación. Pero además, al dividirse en varias preguntas los distintos aspectos del régimen aplicable, puede dar la sensación leyendo separadamente cada una de ellas que sólo se recoge de forma parcial el régimen aplicable y esto puede dar lugar a confusiones. Sería más esclarecedor centrar este tema haciendo referencia a los artículos 5.1.b) 9.2.j), 89 RGPD y DA 17a del LOPDDDD y quizás refundir alguna de las preguntas.

Más allá de esto, conviene realizar algunas observaciones concretas:

En la pregunta 24, en el cuarto punto, se hace referencia a la protección de los intereses vitales como excepción para permitir el tratamiento de categorías especiales de datos (entre ellas las de salud). Sin embargo, es necesario tener en cuenta no sólo el carácter subsidiario de esta excepción (Considerando 46 del RGPD), es decir, que sólo sería aplicable si no existe alguna otra excepción que pueda permitir el tratamiento, sino también, especialmente, el hecho de que la posibilidad de utilizar categorías especiales de datos para la investigación está prevista en la letra j) del artículo 9.2 RGPD, que requiere una norma con rango de ley que establezca las garantías adecuadas.
En este sentido, para la investigación con datos de salud es necesario atender a la regulación específica prevista en la DA 17 LOPDGDD.

En concreto, y como situación estrechamente vinculada a la situación sanitaria actual, conviene tener presente la posibilidad prevista en la letra b) del apartado segundo de la DA 17a de la LOPDDDD, que ya prevé un régimen excepcional para la investigación en situaciones de excepcional gravedad por motivos de salud pública. La aplicación de este supuesto está prevista pero para las autoridades sanitarias y autoridades públicas con competencias en vigilancia de la salud pública.

La pregunta 26 se refiere a esta cuestión, pero lo hace de forma bastante confusa y situando la posibilidad prevista en la letra b) del apartado 2 de la DA 17a como una posibilidad subsidiaria cuando las universidades no cuenten con el consentimiento ni se pueda realizar la investigación con datos seudonimizados. La posibilidad prevista en la letra b) pero no sería una vía para que las universidades lleven a cabo sus propios proyectos de investigación, sino sólo para las autoridades sanitarias y autoridades públicas con competencias en vigilancia de la salud pública, sin perjuicio que las universidades puedan participar en los proyectos de estas autoridades. En estos casos, la participación de las universidades podría articularse a través de los mecanismos a que se refiere la respuesta a la pregunta 22.

Por otra parte, en el punto 5 de la misma pregunta 24 se observa una confusión entre el consentimiento en materia de protección de datos y el consentimiento establecido en la normativa reguladora de los ensayos clínicos, que debería diferenciarse.

VI

Ámbito laboral

En la respuesta a la pregunta 29 se da una especial relevancia al interés vital como habilitación para el tratamiento de datos de los trabajadores, sin tener en cuenta, como ya se ha expuesto, que se

trata de una habilitación subsidiaria (Considerando 46 RGPD). Hay que tener en cuenta que la normativa vigente ya establece previsiones que habilitan el tratamiento, no sólo la normativa de prevención de riesgos laborales que se cita en la respuesta, sino también la normativa de salud pública (p. ej. art. 33 de la Ley 33/2011, de 4 de octubre, general de salud pública).

Estas consideraciones son extensibles también a la pregunta 32, dado que en buena medida duplica la respuesta a la pregunta 29.

La pregunta 30 y su respuesta resulta confusa, dado que no queda claro ni a qué información se refiere la pregunta, ni se indica en la respuesta cuál sería la base jurídica y la excepción del artículo 9.2 que habilitaría la comunicación.

En el segundo párrafo de la respuesta a la pregunta 31, se considera que las universidades pueden preguntar a los visitantes de la universidad datos sobre los países que han visitado anteriormente o si presentan sintomatología relacionada con el coronavirus. Según se expone, esto se basaría en la protección del interés vital de la comunidad universitaria.

No parece sin embargo que la habilitación del interés vital pueda habilitar una medida como ésta con carácter obligatorio, tanto en lo que se refiere a la falta de competencias de las universidades en esta materia (en principio correspondería establecerlo, en su caso, a las autoridades en materia de salud pública), como por la falta de proporcionalidad de la medida. En caso de que la universidad permita el acceso a la Universidad de personas identificables distintas a sus trabajadores, deberá hacerse de acuerdo con los requisitos que hayan establecido las autoridades en materia de salud pública.

A la respuesta a la pregunta 35 podría ser bueno añadir la conveniencia de que se haya establecido un protocolo para tratar los casos que en el control de entrada den resultado positivo al control de temperatura, de forma segura desde el punto de vista de salud pública, pero garantizando también en cualquier caso la confidencialidad.

VII

Ámbito del teletrabajo

En la pregunta 37, si bien es cierto que los riesgos en materia de seguridad son muy relevantes en materia de teletrabajo, podría ser conveniente hacer referencia también a otros riesgos como los riesgos para la privacidad de los trabajadores y de las personas que conviven con ellos o la exactitud de los datos. Por otra parte, podría ser conveniente remarcar que la referencia a la seguridad de la información debe entenderse hecha no sólo a la confidencialidad frente a accesos indebidos, sino también a la disponibilidad y la integridad.

La respuesta a la pregunta 46 establece la no aplicabilidad de la suspensión de plazos prevista en el R. Decreto 463/2020 a las notificaciones de violaciones de seguridad ya la atención del ejercicio de los derechos previstos en el RGPD por parte de las universidades .

Si bien esta Autoridad comparte plenamente la conclusión en cuanto a la no suspensión del plazo para la notificación de las violaciones de seguridad (por el interés público en el cese de los efectos de la violación y por la propia naturaleza de ese plazo, dado que una notificación realizada meses después pierde toda su efectividad especialmente en una situación en la que los riesgos asociados al teletrabajo pueden acabar poniendo en cuestión esta medida vinculada al estado de alarma), no parece que se pueda llegar a la misma conclusión respecto a la no suspensión del término para el cuidado de los derechos.

De entrada, está claro que a las universidades privadas no les es de aplicación la suspensión de plazos dado que el R. Decreto 463/2020, limita la aplicabilidad de sus previsiones sobre suspensión de plazos (DA 3a) a las entidades del sector público (art. 2 de la Ley 39/2015).

En cuanto a las universidades públicas, que forman parte del sector público institucional, sí les sería de aplicación la regulación de la DA 3a del Real Decreto, y además no parece que concurra ninguna de las excepciones previstas para que no sea de aplicación la suspensión:

- **Adopción de medidas de instrucción y ordenación para evitar perjuicios graves en los derechos de el interesado, cuando exista conformidad de las personas interesadas.**
- **Situaciones estrechamente vinculadas al estado de alarma.**
- **Que sean indispensables para el interés general o el funcionamiento básico de los servicios.**

En el caso de las solicitudes de ejercicio de derechos, en principio no parece que concurra ninguna de estas circunstancias, por lo que no parece que pueda sostenerse con carácter general la no suspensión de los plazos. Ello sin perjuicio de que si en algún caso concurre alguna de estas circunstancias, el órgano competente pueda adoptar mediante resolución motivada la no suspensión.

De acuerdo con las consideraciones hechas en estos fundamentos jurídicos en relación con la consulta planteada en relación con la "Guía sobre la protección de datos personales en el ámbito universitario en tiempos del COVID-19", se realizan las siguientes,

Conclusiones

La "Guía sobre la protección de datos personales en el ámbito universitario en tiempos del COVID-19", puede constituir una herramienta útil para gestionar los tratamientos de datos personales que deban llevarse a cabo por las universidades durante la situación de crisis sanitaria COVID19, sin perjuicio de que convendría revisar los aspectos a que se refiere este informe.

Barcelona, 29 de abril de 2020