Referencias Jurídicas CMS | Artículo de fondo

TMC | Protección de Datos

Mayo 2020

Celebración de reuniones *online* por órganos de gobierno y administración de personas jurídicas y protección de datos de carácter personal

José Luis Piñar | *Of Counsel* CMS, Catedrático de Derecho Administrativo

1. Posible celebración de reuniones *online* por órganos colegiados aun sin estar previsto en sus Estatutos

La situación de confinamiento derivada de la declaración del estado de alarma en virtud del Real Decreto 463/2020 ha supuesto que, sin perjuicio del desarrollo de las distintas fases en que va a llevarse a cabo la llamada desescalada, no sea siempre posible celebrar reuniones presenciales de los órganos de gobierno y administración de las personas jurídicas.

Para hacer frente a esta situación, el Real Decreto-ley 8/2020, de 17 de marzo, de medidas urgentes extraordinarias para hacer frente al impacto económico y social del COVID-19, establece una serie de medidas extraordinarias aplicables al funcionamiento de los órganos de gobierno de las personas jurídicas de derecho privado y de las sociedades anónimas cotizadas. En particular los artículos 40 (parcialmente modificado por la disposición final primera, 13ª del Real Decreto-ley 11/2020) y 41, respectivamente permiten con carácter general la celebración de reuniones por videoconferencia, aun cuando no estuviese previsto por los Estatutos.

En la *Guía sobre el Real Decreto-ley 8/2020, de 17 de marzo, de medidas urgentes extraordinarias para hacer frente al impacto económico y social de COVID-19* elaborada por CMS se analizan con detalle tanto el régimen especial para sociedades cotizadas como para las no cotizadas. En cualquier caso, el Real Decreto-ley se refiere también, con carácter más amplio, a asociaciones, sociedades civiles y mercantiles, sociedades cooperativas y fundaciones.

2. Aplicación de la legislación de protección de datos

Sin entrar en todos los detalles de las medidas adoptadas (que como digo ya han sido analizadas en la Guía citada), nos centraremos ahora en el régimen de la celebración de reuniones y en el de adopción de acuerdos por vía telemática desde el punto de vista de la legislación de datos de carácter personal, en particular el Reglamento (UE) 2016/679, de protección de datos (RGPD) y la Ley Orgánica 3/2018 de Protección de Datos de Carácter Personal y garantía de los derechos digitales de los ciudadanos (LOPD-GDD).

La situación no solo se plantea en España, como es obvio, si no a nivel global. De hecho la preocupación por el uso de herramientas o aplicaciones que permiten la celebración de videoconferencias *online* ha sido analizada por numerosas autoridades con competencias en materia de protección de datos y privacidad no solo en Europa sino más allá de su territorio. Basta hacer referencia, por ejemplo, a los puntos que ha señalado la F*ederal Trade Commission* y que deberían tenerse en cuenta a la hora de celebrar reuniones *online* utilizando herramientas colaborativas (*Video conferencing: 10 privacy tips for your business*).

Tengamos en cuenta en cualquier caso que no hablamos ahora de reuniones más o menos informales celebradas por medios telemáticos, sino de reuniones formales con un régimen jurídico muy preciso en cuanto a las reglas de convocatoria, celebración y adopción de acuerdos. Lo que puede exigir un tratamiento de datos más intenso, pero que al mismo tiempo ha de llevarse a cabo con todas las garantías.

3. Principios del derecho a la protección de datos

Ante todo debe partirse de que la celebración de reuniones por videoconferencia implica el tratamiento de datos de carácter personal: en todo caso la voz y a veces los datos de identificación de los participantes, así como su imagen. Este tratamiento de datos debe cumplir los principios de protección de datos, es decir licitud, lealtad y transparencia, limitación de la finalidad, minimización de datos, exactitud, limitación del plazo de conservación, seguridad y responsabilidad proactiva. Veamos cómo operan alguno de ellos.

a. Licitud del tratamiento

En cuanto al principio de licitud es imprescindible que se dé alguno de los supuestos que legitiman el tratamiento de datos de carácter personal. El consentimiento de los afectados puede ser título habilitante pero no hay que excluir que pueda así mismo considerarse aplicable el título de interés legítimo o incluso el de interés público dada la necesidad de que se acrediten las circunstancias que en su caso sean necesarias para considerar válidamente celebrado la reunión y válidamente adoptados los acuerdos a los que en su caso se llegue. En particular puedes resultar imprescindible identificar a los participantes para evitar que puedan participar quiénes no forman parte del órgano colegiado, garantizar la validez de la constitución del órgano acreditando el quórum de constitución o garantizar la validez de los acuerdos adoptados acreditando para ello el quórum de adopción de acuerdos. Estas circunstancias implican que en ciertos casos sea imprescindible identificar a los asistentes sin que ello pueda estar condicionado a que estos otorguen su consentimiento. Asimismo no puede ser el consentimiento el que habilite el tratamiento para la elaboración de las actas correspondientes.

b. Transparencia: información a los afectados

Una de las claves del derecho a la protección de datos es que los interesados cuenten con la información que exigen facilitar los artículos 13 y 14 del RGPD así como el artículo 11 de la LODPDGDD. En particular acerca de la identidad de quién trata los datos, qué tipos de datos van a ser recabados o la finalidad.

c. Finalidad del tratamiento y principio de minimización de los datos

Distinto es el tema de qué datos pueden o deben ser recabados para las anteriores finalidades, lo que nos lleva a plantear el tema, por un lado, de la limitación de la finalidad y por otro el de la minimización de datos.

Además del principio de licitud y transparencia tiene especial importancia el principio de finalidad. En efecto la finalidad del tratamiento de datos que se lleva a cabo con ocasión de la celebración *online* de reuniones, bien sea la voz o también imagen, sólo puede ser la de poder llevar a cabo o facilitar la celebración de reuniones *online*, así como la elaboración de las actas correspondientes, sin que los datos puedan ser utilizados para finalidades distintas.

En cuanto a los datos que pueden ser tratados, plantea especial interés la posibilidad de utilizar categorías especiales de datos, especialmente datos biométricos, para identificar a los participantes. Según el artículo 9 del Reglamento los datos biométricos son considerados categorías especiales de datos si permiten identificar de manera unívoca a una persona física. En este sentido no cabe duda de que la utilización de sistemas de reconocimiento facial implicaría el uso de datos biométricos con la finalidad de reconocer o identificar de manera unívoca a las personas intervinientes en las reuniones. Cabe entonces plantear si el uso de tales sistemas es legítimo o si por el contrario deberían utilizarse otros sistemas menos intrusivos para la privacidad que permitiesen alcanzar la misma finalidad (identificar a los asistentes a la reunión).

Pese a que no se refiere a la organización de videoconferencias o reuniones *online*, puede ser relevante el *Informe de la Agencia Española de Protección de Datos 0036/2020 sobre utilización del reconocimiento facial para la realización de exámenes online*, que se refiere entre otras cosas a la posibilidad de utilizar técnicas de reconocimiento facial para identificar a los asistentes al examen, con conclusiones que pueden trasladarse a la celebración de reuniones *online*.

Ante todo debe señalarse que el uso de categorías especiales de datos está en principio prohibido por la legislación de protección de datos, lo que no impide que en ciertos casos tal prohibición pueda ser levantada con el consentimiento de los afectados. Esto es lo que ocurre con los datos biométricos. Significa esto, como dice la Agencia,

que el consentimiento del afectado podrá permitir el tratamiento de sus datos biométricos, pero siempre que el mismo sea explícito, previo, libre e informado. El principal problema que plantea el consentimiento para el tratamiento de datos biométricos de cara a la celebración de reuniones de órganos colegiados *online* es que podría considerarse que su otorgamiento no es libre. En este sentido el considerando 42 del RGPD destaca que el consentimiento no debe considerarse libremente prestado cuando el interesado no goza de verdadera o libre elección o no puede denegar o retirar su consentimiento sin sufrir perjuicio alguno. La anterior consideración nos puede llevar a la conclusión de que no sería posible exigir en todo caso el reconocimiento facial para la identificación de quienes asisten a una reunión *online*. En particular sería dudoso poder considerar libre el consentimiento en caso de que existiendo varias posibilidades para tal identificación además del reconocimiento facial, algunas de las cuales pueden ser menos intrusivas para la protección de datos, no se diese posibilidad a los interesados de poder optar por ese otro medio de identificación.

Por otra parte, y al objeto de poder demostrarlo, es preciso tener constancia del consentimiento otorgado, en particular si se tratan datos biométricos. En este sentido son relevantes algunas de las consideraciones que el Comité Europeo de Protección de Datos ha recogido en sus recientes *Directrices 5/2020 sobre el consentimiento en el Reglamento 2016/79* adoptadas el pasado 4 de mayo. En ellas se afirma que el hecho de que el consentimiento deba ser explícito (en particular cuando se pretenden tratar categorías especiales de datos) no implica que sea necesario que en todo caso deba ser escrito. Especialmente, al referirse al consentimiento en un contexto *online*, señala que puede acreditarse, por ejemplo, a través de la "*conservación de información sobre la sesión en la que el consentimiento ha sido expresado*". Lo que el Comité Europeo exige es que los responsables del tratamiento apliquen el principio de responsabilidad proactiva en relación con la obtención válida del consentimiento de los afectados.

En conclusión cabría afirmar que la exigencia del reconocimiento facial podría ser lícita si el interesado otorga su consentimiento expreso para ello y además se articulan sistemas alternativos menos intrusivos para su identificación.

Las anteriores consideraciones pueden ser trasladables al hecho de que se graben las sesiones. Esta circunstancia puede ser no solo conveniente sino incluso imprescindible para la constancia del desarrollo del debate y de los acuerdos adoptados así como para la elaboración del correspondiente acta. En este sentido los asistentes deben ser informados de que la sesión se va a grabar, bien en audio o también en imágenes, para garantizar el principio de transparencia. El hecho de que la plataforma utilizada advierta además de forma expresa de que la sesión está siendo grabada incrementa aún más la transparencia en el tratamiento de datos.

d. Principio de integridad y confidencialidad: medidas de seguridad

En fin es especialmente relevante el cumplimiento estricto del principio integridad y confidencialidad de los datos, es decir, la exigencia de adoptar estrictas medidas de seguridad. En la celebración de reuniones *online* cobra especial importancia en efecto garantizar, tal como establece el artículo 5.1 f del RGPD, una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida destrucción o daño accidental. Por tanto el responsable del tratamiento deberá adoptar tales medidas o, en caso de que la reunión se celebre utilizando herramientas de terceros, exigir que estas reúnan todas las garantías de seguridad que sean necesarias. No es necesario ahora recordar que, como en más de una ocasión se ha puesto de manifiesto, parece que ciertas plataformas colaborativas tienen o han tenido fallos de seguridad que desaconsejarían su uso o cuando menos y en todo caso el de versiones que no fuesen las últimas y más actualizadas. Incluso alguna institución relevante ha acordado suspender las reuniones *online* por temor a posibles ataques informáticos que incrementarían el riesgo de que las mismas pudiesen ser intervenidas y hechas públicas.

4. Derechos de los interesados. En particular el derecho de acceso

En otro orden de cosas deben estar plenamente garantizados los derechos de los afectados tal como están regulados en los artículos 15 a 22 del RGPD y artículos 12 a18 de la LOPDGDD. De entre ellos puede plantear alguna duda el cómo atender el derecho de acceso, teniendo en cuenta que el mismo podría afectar a datos personales de terceros tal como ocurriría si se pretendiese el acceso íntegro a grabaciones de voz o de imagen. En este sentido cabe traer a colación la Resolución de la Agencia Española de Protección de Datos nº R/00558/2019, referida al acceso a grabaciones de voz. En ella la Agencia advierte que "*dichas grabaciones pueden contener, además de sus datos [del interesado], información relativa a terceras personas que no le podría ser comunicada, ya que, en caso contrario, podría constituir una cesión de datos sin consentimiento*". Y permite expresamente que "*el derecho de acceso a la grabación de su voz solicitado por la parte reclamante sí está amparado por la normativa vigente en materia de protección de datos, facilitando la copia de la grabación solicitada a la parte reclamante o, en su defecto, transcripción de su contenido*".

5. Relación entre responsable y encargado del tratamiento

Un aspecto especialmente relevante del régimen jurídico de la celebración de reuniones *online* es el de la relación entre quién organiza la reunión y el prestador del servicio, plataforma o herramienta que va a ser utilizado para dicha reunión. Con carácter general estaremos ante una relación entre un responsable del tratamiento –quien organiza la

reunión– y un encargado –quien presta el servicio–. En estos casos debe aplicarse en su totalidad el artículo 28 del RGPD, en particular lo que establece su apartado primero según el cual cuando se vaya a realizar un tratamiento por cuenta de un responsable éste elegirá únicamente un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiadas de manera que el tratamiento sea conforme con los requisitos del Reglamento y garantice la protección de los derechos de los interesados. Además dicho artículo exige que el tratamiento por el encargado se rija por un contrato u otro acto jurídico que vincule al encargado y el responsable y establezca el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados y las obligaciones y derechos del responsable. Por su parte el artículo 33 de la LOPDGDD se refiere asimismo a la relación entre responsable y encargado.

Es evidente que en no pocas ocasiones la celebración de videoconferencias utilizando las plataformas generalmente usadas, más que en un contrato se basara en la aceptación de los términos y condiciones de quién presta el servicio. En este sentido es muy importante señalar que deben revisarse con mucha atención tales términos y condiciones al objeto de comprobar que están en línea con lo que exige el Reglamento y la Ley. En particular deberá tenerse especial cuidado con la ubicación de los servidores del prestador, que en principio deberían estar alojados en territorio de la Unión Europea o en su caso en territorio de algún Estado que cuente con declaración de adecuación por parte de la Unión Europea. Si no fuese así, debería darse alguna de las garantías que regulan los artículos 46 y 47 del Reglamento o basarse en alguno de los supuestos excepcionales que prevé su artículo 49. De lo contrario podríamos encontrarnos con un caso de transferencias internacionales de datos no acordes al Derecho de la Unión Europea.

Por otra parte el responsable debe exigir al encargado que adopte las medidas de seguridad que sean necesarias para evitar violaciones tales como el acceso a los datos por parte de terceros.

6. Celebración de reuniones *online* por órganos colegiados de las Administraciones Públicas

Pese a que el Real Decreto-ley 8/2020, en lo que ahora estamos analizando, no es de aplicación a las Administraciones Públicas, cabe hacer una breve referencia a alguna cuestión que debe ser puesta de relieve.

Ante todo debe señalarse que el artículo 17 de la Ley 40/2015, de régimen jurídico del sector público, permite las reuniones de órganos colegiados "a distancia": "*todos los órganos colegiados se podrán constituir, convocar, celebrar sus sesiones, adoptar acuerdos y remitir actas tanto de forma presencial como a distancia, salvo que su reglamento interno recoja expresa y excepcionalmente lo contrario*". Y añade que "*en las sesiones que celebren los órganos colegiados a distancia, sus miembros podrán encontrarse en distintos lugares siempre y cuando se asegure por medios electrónicos, considerándose también tales los telefónicos, y audiovisuales, la identidad de los miembros o personas que los suplan, el contenido de sus manifestaciones, el momento en que éstas se producen, así como la interactividad e intercomunicación entre ellos en tiempo real y la disponibilidad de los medios durante la sesión. Entre otros, se considerarán incluidos entre los medios electrónicos válidos, el correo electrónico, las audioconferencias y las videoconferencias*".

Por otra parte, no sólo las Administraciones Públicas que celebren las reuniones han de tomar las medidas de seguridad establecidas en el Esquema Nacional de Seguridad regulado mediante Real Decreto 3/2010, de 8 de enero, sino que los proveedores que en su caso les presten el servicio de videoconferencia deberán asimismo cumplir con medidas de seguridad semejantes. Así lo dispone la disposición adicional primera de la Ley Orgánica 3/2018 según la cual en los casos en los que un tercero preste un servicio en régimen de contrato a alguna de las administraciones públicas (por ejemplo el servicio de organización o gestión de reuniones telemáticas) las medidas de seguridad se corresponderán con las de la Administración Pública de origen y se ajustarán al Esquema Nacional de Seguridad.

La presente publicación no constituye asesoramiento jurídico de sus autores.