https://doi.org/10.1344/REYD2020.22.32348

Repercusiones de la docencia online en el estatuto jurídico del profesorado universitario

Repercussions of online teaching on the legal status of university teachers

David Sanz Esteban
Director Técnico en Materia de Privacidad
Universidad de Valladolid, España
E-mail: david.sanz@uva.es

Resumen: La propagación de la pandemia causada por la enfermedad COVID-19 precipitó la suspensión de la docencia presencial en la Universidad. La transición desde una modalidad esencialmente presencial a una totalmente online ha supuesto un reto para las universidades españolas, quienes han debido adaptarse en un tiempo récord. Esto ha generado para el profesorado nuevas obligaciones para las cuales las instituciones universitarias no los habían preparado. La carencia de normativa específica ha hecho que los procesos se hayan debido adaptar a la ya existente, contando únicamente con cierto margen en lo que respecta a la reglamentación propia de las universidades. Este trabajo hace un recorrido por los distintos escenarios modificados por la docencia online y las implicaciones que ha tenido para las instituciones universitarias y su profesorado.

Palabras clave: Derecho a la propia imagen, Docencia online, Evaluación online, Voto electrónico, Reuniones órganos colegiados, Imágenes, Pandemia, Protección de datos, Universidades, Seguridad de la información.

Abstract: The spread of the pandemic caused by the COVID-19 disease sped up the suspension of face-to-face teaching at University. The transition from an essentially face-to-face modality to a totally online one has been a challenge for Spanish universities, who have had to adapt in record time. This has generated new obligations for teachers for which university institutions had not prepared them. The lack of specific regulations has meant that the processes have had to be adapted to the existing ones, with only a certain margin with

regard to the regulations of the universities. This work takes a tour of the different scenarios modified by online teaching and the implications it has had for university institutions and their teachers.

Keywords: Right to one´s own image, Online teaching, Online evaluation, Electronic voting, Professional body meetings, Images, Pandemic, Data protection, Universities, Information security

ÍNDICE: 1. INTRODUCCIÓN. 1.1. Insuficiencia de medios y brecha digital. 1.2. Dificultades de aplicación de la Ley de Prevención de Riesgos Laborales en el Teletrabajo. 1.3. Derecho a la intimidad en los dispositivos. 1.4. Compromiso del derecho a la desconexión digital. 2. MODALIDADES DE CONEXIÓN EN EL TELETRABAJO Y MEDIDAS DE SEGURIDAD APLICABLES. 2.1. Modalidades de conexión. 2.2. Herramientas en la nube de terceros. 2.3. Medidas de seguridad. 3. DOCENCIA ONLINE. 4. EVALUACIONES ONLINE. 5.INVESTIGACIÓN. 6. REUNIONES TELEMÁTICAS DE ÓRGANOS COLEGIADOS. 7. PROCESOS ELECTORALES TELEMÁTICOS. 8. RETORNO A LA PRESENCIALIDAD. 8.1. Obligatoriedad de comunicación de la enfermedad. 8.2. Evitar aglomeraciones mediante control de acceso, cita previa y control de aforo. 8.3. Prevención de riesgos laborales en la nueva presencialidad. 8.4. Cesión de datos al sistema de salud. 9. CONCLUSIONES.

1. INTRODUCCIÓN[1]

La situación de emergencia de salud pública ocasionada por la expansión de la Covid-19 precipitó la adopción de una serie de medidas drásticas destinadas a contener su propagación. Entre ellas, debido a la gravedad de la situación, incluso se llegó a la restricción de derechos y libertades fundamentales de la ciudadanía.

Se ha acudió a la limitación de la libertad de circulación como medio fundamental para evitar los contactos directos entre ciudadanos y, por ende, la propagación de la enfermedad. La autoridad gubernativa materializó esta restricción con la declaración del estado de alarma mediante el Real Decreto 463/2020, de 14 de marzo, por el que se declara el estado de alarma para la gestión de la situación de crisis sanitaria ocasionada por el COVID-19.

Por otro lado, se incluían medidas específicas de contención en el ámbito educativo y de la formación. El artículo 9 del Real Decreto 463/2020 ordenó la suspensión de la actividad educativa presencial a todos los niveles, incluyendo la enseñanza universitaria, toda vez que se recomendaba acudir a las modalidades de docencia a distancia y "on line", siempre que esto resultase posible.

Toda actividad universitaria presencial no esencial fue suspendida de inmediato. Solo se permitiría acudir al centro de trabajo cuando la actividad resultase indispensable, especialmente para el mantenimiento de las infraestructuras o para la atención y el cuidado de seres vivos.

Estas circunstancias provocaron que una Universidad esencialmente presencial tuviese que adaptarse a un modelo de prestación remota en todos sus ámbitos. Este modelo de prestación del servicio público de educación[2] superior a distancia, propició la aparición de una nueva serie de obligaciones para todo su personal. Sin embargo, en este documento nos centraremos especialmente en aquellas que vinculan al personal docente e investigador.

[1] Este trabajo surge como fruto de la colaboración con el Delegado de Protección de Datos de la Universidad de Valladolid, el Dr. Ricard Martínez Martínez de la Universitat de València.

[2] Según el art. 1 de la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades, La Universidad realiza el servicio público de la educación superior mediante la investigación, la docencia y el estudio.

2. UNA TRANSICIÓN NO EXENTA DE DIFICULTAD AL TRABAJO ONLINE

Acudir a una fórmula de trabajo a distancia[3] o *teletrabajo*, siempre y cuando la naturaleza del puesto de trabajo lo permitiese, pretendía dotar de continuidad a la actividad universitaria y garantizar así el derecho fundamental a la educación de los estudiantes, pilar básico de la Universidad. Sin embargo, esto presentaba ciertas dificultades no solo de índole técnico y legal, sino también cultural. Hasta ese momento, nuestro país contaba con una escasa cultura de teletrabajo, siendo visto como una modalidad marginal, hasta el punto de carecer en nuestro ordenamiento jurídico de una regulación específica[4]. Por otro lado, la brecha digital entre ciudadanos ya fuese por insuficiencia de medios materiales por motivos económicos o por diferencias en la dotación de infraestructuras entre regiones, dificultaba la conectividad. La ausencia de una normativa laboral específica de teletrabajo requirió la flexibilización de las condiciones laborales[5]. Esta transición se produjo sin una oposición significativa del profesorado que, con carácter general, contribuyó solidariamente en un contexto de lucha contra la pandemia. No obstante lo anterior, esta transición no estaba exenta de una serie de problemas que examinaremos a continuación.

2.1. Insuficiencia de medios y brecha digital

i) Personal universitario

Es conocido el deber de la Universidad como empleador de poner a disposición de sus trabajadores los medios necesarios para el desarrollo de su actividad laboral, incluida la ejercida a distancia. Sin embargo, debido al volumen que representaba la transición de la totalidad de la plantilla, la Universidad ha se ha visto obligada a facilitar los recursos necesarios de distintos modos.

Parte de personal docente e investigador contaba con equipos portátiles propiedad de la universidad que podrían utilizar; en otros casos se posibilitó el traslado de equipos informáticos a los domicilios; y en los menos, algunas universidades recurrieron a programas

[3] 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 en su artículo 5 el carácter preferente de la modalidad laboral a distancia.

[4] Durante el periodo del estado de alarma decretado por el RD-Ley 463/2020, no se contaba con legislación específica del teletrabajo. En estos momentos el ordenamiento jurídico español ha incorporado una regulación específica para el teletrabajo en el Real Decreto-ley 28/2020, de 22 de septiembre, de trabajo a distancia.

[5] Las condiciones laborales se flexibilizaron al decretarse como modalidad laboral preferente el trabajo a distancia en el artículo 5 del Real Decreto-ley 8/2020.

de préstamo de material informático y de comunicaciones[6]. A pesar de todos estos métodos, el uso de los propios dispositivos personales de los trabajadores fue la medida que se impuso, ya que esta constituía la solución más sencilla, más rápida de implementar y con menos costes para la Universidad. Adicionalmente, en todos los casos, se requería que el personal contase con una conexión a Internet en su domicilio. Esto planteaba el reto de dimensionar la seguridad en estos dispositivos.

Toda vez que se recomendaba el trabajo online, no existía predeterminación normativa alguna que forzase a los trabajadores a utilizar sus propios medios. Una vez más se dependía, en la mayoría de los casos, de la buena voluntad de los trabajadores para continuar con su actividad poniendo a disposición de la universidad sus propios medios, como eran los dispositivos electrónicos y la conexión a internet, sufragados con sus medios. Solamente para aquellos que no contasen con los medios suficientes, la universidad los debería poner a su disposición como única opción.

ii) Alumnado

En este caso, el alumnado en su práctica totalidad se vio obligado a la utilización de sus propios medios. No obstante, entre el alumnado se ha apreciado la significativa presencia de una brecha digital que se traduce, en unos casos en la carencia de ordenadores adecuadamente actualizados, derivada de factores económicos, y en otros, en la falta de conexión a Internet en el lugar donde se hubiesen visto obligados a retornar. Anteriormente, los alumnos podían disfrutar de un equipamiento y conexión a la Red en dependencias universitarias, que con motivo de la pandemia dejaron de tener disponibles.

2.2. Dificultades de aplicación de la Ley de Prevención de Riesgos Laborales en el Teletrabajo

Según el artículo 13.4 del Estatuto de los Trabajadores, los trabajadores a distancia tienen derecho a una adecuada protección en materia de seguridad y salud, resultando de aplicación en todo momento lo establecido en la Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales (en adelante, Ley de Prevención de Riesgos Laborales), y su normativa de desarrollo.

[6] En varias universidades se pusieron en marcha programas de préstamo de equipos informáticos a estudiantes y profesorado, como en la Universidad de Valladolid [Disponible en: http://bibecouva.blogs.uva.es/2020/04/20/conectateuva-es/] o en la Universidad de Almería [Disponible en https://cms.ual.es/UAL/universidad/serviciosgenerales/stic/servicios/servicio/SERVICIO14755].

Para conseguirlo, 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 facilitó la evaluación de los riesgos laborales en el domicilio. Esta se entendería cumplida cuando el trabajador, de forma voluntaria se sometiese a una autoevaluación, en los términos previstos en el artículo 16 de la Ley de Prevención de Riesgos Laborales.

Se asumía que, debido al carácter voluntario de la misma, un gran número de los trabajadores ni tan siquiera la presentaría, ya que la práctica totalidad de los trabajadores contarían con unas condiciones en su puesto de trabajo aceptables. Sin embargo, interesaba con este medio poder prestar apoyo a todos aquellos que considerasen que sus condiciones laborales en el domicilio representaban algún tipo de riesgo para su salud.

2.3. Derecho a la intimidad en los dispositivos

La facultad de control del empresario y el derecho a la dignidad, integridad e intimidad trabajador recogidos en Estatuto de los Trabajadores[7] en los artículos. 20.3 y 17, respectivamente, se vieron modulados con la publicación de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante LOPDGDD). De este modo se precisaron los derechos digitales de los trabajadores en el ámbito laboral, trasladándose tanto las políticas específicas en materia de protección de datos como concretándose garantías en los supuestos de vigilancia digital del trabajador y derecho a la desconexión.

A partir de este régimen jurídico debía establecerse si el equipamiento propiedad de la universidad podía utilizarse exclusivamente para un uso profesional o si se admitía además un uso personal. En cuando a los dispositivos personales, deberían determinarse las condiciones para proporcionar un entorno de trabajo que permitiese maximizar la seguridad y control de los sistemas sin intervenir de modo directo en el equipo del trabajador[8].

Las condiciones singulares de la Universidad determinan que la monitorización empresarial se proyecte sobre aspectos muy diferentes de aquellos que habitualmente se utilizan en el marco convencional de las relaciones laborales. La Universidad tiene por misión esencial la

[7] Véase al respecto el Informe 0615/2009 AEPD Control por la Administración de los medios electrónicos a disposición de los empleados públicos para el ejercicio de sus funciones y las STC. 173/2011, de 7 de noviembre y STSJ CLM 1735/2019.

[8] Pueden utilizarse los sistemas del trabajador como medio de conexión a una infraestructura VDI "Virtual Desktop Infraestructure" en la que se han virtualizado los equipos de los trabajadores. Las funciones se desarrollan completamente en remoto, pudiendo monitorizarse el terminal virtual si fuese necesario. Véase Sistemas VDI y teletrabajo, la dupla perfecta en tiempos del COVID-19 Publicado el 02/04/2020, por INCIBE, [Disponible en: https://www.incibe.es/protege-tu-empresa/blog/sistemas-vdi-y-teletrabajo-dupla-perfecta-tiempos-del-covid-19]

docencia, la investigación y a la divulgación de la cultura y de la ciencia, de tal modo que la medición de la productividad en estos ámbitos se basa en parámetros como los sexenios de investigación o en la evaluación de los estudiantes en cuanto a la calidad docente, que no requieren una monitorización individual de cada trabajador.

Adicionalmente existía un segundo problema consecuencia de la dificultad de traslado del terminal telefónico del puesto de trabajo al domicilio. Deberán ofrecerse soluciones que permitan a los trabajadores estar conectados, pero minimizando riesgos.

La revelación de un numero personal, que cobra especial importancia cuando ese tercero sea un estudiante, ya que supone un especial riesgo para el profesorado compartir un espacio de vida privada con sus estudiantes. Se trata de un riesgo en doble sentido, ya que podría utilizarse malévolamente para causar un perjuicio o por el riesgo desde la ética que debería regir las relaciones entre un profesor y un estudiante universitario. A modo de ejemplo, mediante el número de teléfono podría observarse la fotografía de perfil de WhatsApp tanto del profesor como del alumno.

Debe acudirse, por tanto, a fórmulas que no comprometan el número de teléfono personal del profesorado. Fórmulas como el traslado de los clientes de telefonía IP a los terminales del profesorado o la utilización de herramientas para videoconferencias se postulan como medios adecuados para paliar este riesgo.

2.4. Derecho a la desconexión digital

La Universidad en tiempo récord tuvo que hacer un ingente esfuerzo de adaptación a la docencia online que suponía una modificación de las normativas, de los planes de ordenación docente, incluidas las guías docentes de las asignaturas, de los criterios de evaluación y examen y de las estrategias docentes convencionales.

Desde la perspectiva de la experiencia subjetiva próxima de quien realiza este trabajo, lo cierto es que esto supuso un nivel de exigencia que desbordó sobremanera la prestación laboral. En algunos puestos especialmente relevantes, como los relacionados con la gestión académica, la seguridad, el soporte de infraestructuras o la protección de datos, implicó una disponibilidad horaria casi total.

El personal universitario con hijos en edad escolar encontró una dificultad adicional. en la conciliación de la vida laboral, obligando a padres e hijos a atender las obligaciones del teletrabajo, del colegio online y las domésticas de manera simultánea, incluso compartiendo espacios.

El teletrabajo, provocó una distorsión en la jornada laboral para el personal universitario[9]. La ventaja que a priori supondría esta modalidad laboral, flexibilizando los horarios con el fin de facilitar la conciliación de la vida laboral y familiar, resultó en todo lo contrario. La permanente presencialidad en el domicilio y continua disponibilidad que permite la tecnología supuso que en no pocos casos la rigidez habitual de los horarios se diluyese, manteniéndose constantemente disponible.

El sobresfuerzo de adaptación a todos los niveles que supuso la pandemia, en determinados momentos hizo a veces olvidar el derecho a la desconexión digital en el ámbito laboral, con el fin de garantizar el correspondiente tiempo de descanso y facilitar conciliación de la personal y familiar. Se observaba claramente aquí la carencia de un marco regulatorio[10].

A pesar de todo, en la mayoría de los casos el personal universitario contribuyó con su firme voluntad a mitigar los efectos de la grave situación sobrevenida para que los estudiantes pudiesen seguir disfrutando de su derecho a la educación.

3. MODALIDADES DE CONEXIÓN EN EL TELETRABAJO Y MEDIDAS DE SEGURIDAD APLICABLES

3.1. Modalidades de conexión

En un escenario de migración al teletrabajo la Universidad viene obligada a evaluar los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas y a aplicar las medidas técnicas y organizativas apropiadas para garantizar el derecho a la protección de datos[11]. Este compromiso es atribuido al responsable del tratamiento por artículo 24 del RGPD[12] y resultará particularmente relevante la aplicación de cuantas medidas de seguridad de las propuestas en el artículo 32 del RGPD sean necesarias.

---

[9] Según un estudio del portal de empleo InfoJobs, 3 de cada 10 españoles afirma que el teletrabajo dificulta la desconexión digital, "Estudio Infojobs sobre la desconexión digital" [disponible en: https://nosotros.infojobs.net/wp-content/uploads/2020/09/200805_NP.InfoJobs_La-desconexi%C3%B3n-digital-en-Espa%C3%B1a.docx]

[10] Actualmente el Real Decreto-ley 28/2020, de 22 de septiembre, de trabajo a distancia, incluye una previsión específica que regula el derecho a la desconexión digital en su artículo 18.

[11] Tal y como expone el preámbulo de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, "La protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental protegido por el artículo 18.4 de la Constitución española. De esta manera, nuestra Constitución fue pionera en el reconocimiento del derecho fundamental a la protección de datos personales cuando dispuso que «la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos»".

[12] Art. 24) RGPD "Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas

Las categorías de interesados respecto de los cuales la Universidad requiere tratar datos comprenden principalmente tanto a trabajadores, como alumnos, sin perjuicio de otras categorías que pudieran existir. El profesorado, indudablemente requiere tratar datos de alumnos para la correcta prestación del servicio educativo: gestión de alumnos, impartición de docencia y evaluación online, calificaciones, tutorías, etc.

La seguridad de la información se entiende desde un punto de vista multidimensional, integrado por la confidencialidad, integridad, autenticidad, disponibilidad y trazabilidad. En la modalidad laboral no presencial el mayor riesgo puede presentarse en cuanto a lo que una pérdida de confidencialidad supone. En cuanto a la trazabilidad y la autenticidad, si bien en un entorno seguro pueden no resultar excesivamente preocupantes, el acceso remoto a la información por multitud de usuarios hace que esta dimensión cobre relevancia. Por otro lado, la integridad y la disponibilidad de la información son factores que descansarían en este caso en sistemas internos de la organización.

El análisis de riesgos en este contexto resultará particularmente relevante en materia de seguridad, conforme al artículo 32 del RGPD. En este sentido, resulta necesario distinguir distintos escenarios tentativos de teletrabajo, teniendo en cuenta los medios técnicos de los que dispone el trabajador y el modo de acceso a la información corporativa.

a) Propietario de los sistemas utilizados por el empleado

Teniendo en cuenta la propiedad de los dispositivos que utiliza el empleado a distancia, pueden distinguirse las siguientes modalidades.

i) Medios propiedad de la universidad (COPE, COBO[13])

Estos términos son utilizados en el caso de que el dispositivo sea propiedad de la universidad, quien retiene su control total. La principal diferencia entre ambos radica en la posibilidad de cierto uso personal que se admite en el modelo COPE. En COBO el uso personal del equipamiento está prohibido.

En ambos modelos, al retener la universidad el control sobre el equipo, esta puede establecer las políticas de uso y de seguridad de manera efectiva, desplegando en el

físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento"

[13] COPE y COBO son los acrónimos de Corporate Owned Personal Enabled y Corporate Owned Business Only. Una definición precisa de esta terminología puede encontrarse en la guía del CCN-CERT Medidas de seguridad para acceso remoto [Disponible en: https://www.ccn-cert.cni.es/informes/abstracts/4880-medidas-de-seguridad-para-acceso-remoto/file.html]

dispositivo el software que para ello estime conveniente. Las medidas de seguridad deberán ser también adecuadas para el uso privado.

COBO resulta en el modelo que ofrece mayores garantías de seguridad para el teletrabajo, sin embargo, puesto que tradicionalmente se ha admitido en el entorno del profesorado cierto uso personal de los dispositivos, el sistema COPE sería la opción preferida.

ii) Medios propiedad del trabajador (BYOD)

Con el término BYOD (Bring Your Own Device) se denomina el escenario donde el dispositivo es propiedad del trabajador. En este caso la universidad no puede ejercer un control efectivo sobre el terminal, apelando a la responsabilidad del usuario para cumplimiento efectivo de las normas de seguridad que esta hubiese determinado. De este modo, únicamente podrían hacerse comprobaciones de seguridad en las máquinas a las que el empleado se conecte.

Este método ha sido el que ha tenido mayor éxito en tiempos de pandemia, ya que para las universidades no requirió inversión alguna y el despliegue fue inmediato. Como desventaja evidente, la adopción de este sistema constituye el modo de organización más inseguro de todos los expuestos, todo ello si perjuicio de quien sufrague el coste de los equipos y conexión a Internet.

b) Modo de acceso a los datos corporativos

Independientemente de quien ostente la propiedad de los dispositivos utilizados por el empleado, teniendo en cuenta la propiedad de los dispositivos que utiliza el empleado en el trabajo a distancia, pueden distinguirse las siguientes modalidades.

i) Sin posibilidad de descarga de datos ni trabajo en el terminal

La universidad establecerá un mecanismo de conexión mediante el cual toda la actividad laboral se pueda llevar a cabo mediante la conexión a un equipo remoto de la red interna corporativa. El terminal cliente del trabajador actuará exclusivamente como medio de conexión, técnicamente denominado cliente ligero[14] o "Thin client".

[14] Cliente ligero o "thin client" es aquella máquina de usuario que únicamente se limita a actuar como medio para la captura de datos y visualización del servidor al que se conecta, el cual realiza el grueso del proceso. En contraposición, un cliente pesado o "thick client" es capaz de realizar cierto procesado de datos por sí mismo para su transmisión al servidor. [Disponible en: https://techlib.net/definition/thinclient.html]

Este sistema resulta en el que expone en menor medida la información de la universidad, siempre que la conexión se efectúe de manera cifrada mediante técnicas asistidas criptográficamente como VPN[15] o HTTPS[16]. Las condiciones de seguridad del equipo remoto serán similares a las existentes con carácter previo. En el equipo cliente deberá prestarse especial vigilancia en la custodia de las credenciales o certificados de conexión.

ii) Con posibilidad de descarga de datos y trabajo en el terminal

Esta opción se presenta como la más delicada respecto a la posibilidad de una pérdida de confidencialidad de la información. La información como tal se transfiere desde los servidores de la universidad hasta el equipo cliente del usuario, el cual cuenta con software instalado para uso profesional e incluso para uso personal (COPE y BYOD). En contraposición con el concepto de cliente ligero, estos suelen denominarse clientes pesados o "Thick client".

Los equipos cliente deberán implementar medidas de seguridad destinadas a mitigar posibles incidentes de seguridad que comprometan la información de la universidad.

A modo de resumen, se presenta en la *Tabla 1* una matriz de riesgo para la seguridad de la información, de manera genérica, en función del tipo y el propietario del dispositivo.

RIESGO	**PROPIETARIO DEL DISPOSITIVO**		
CONEXIÓN	**COBO**	**COPE**	**BYOD**
Cliente ligero	Muy bajo	Bajo	Bajo
Cliente pesado	Bajo	Medio	Alto

Tabla 1: Matriz de riesgo de seguridad de la información

[15] La Guía de Seguridad de las TIC CCN-STIC 836 ENS. Seguridad en VPN define una Red Privada Virtual (VPN) como aquella que proporciona conexiones virtuales seguras, construidas sobre una red física no segura. [Disponible en: https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/2299-ccn-stic-836-seguridad-en-vpn-en-el-marco-del-ens/file.html]

[16] HTTPS (Hyper Text Transfer Protocol Secure o protocolo seguro de transferencia de hipertexto) se trata del protocolo HTTP estándar protegido por un certificado SSL (Secure Socket Layer). [Disponible en: https://www.websecurity.digicert.com/es/es/security-topics/what-is-ssl-tls-https]

3.2. Herramientas en la nube de terceros

Las universidades en numerosas ocasiones pueden recurrir a herramientas ofrecidas por proveedores externos, siendo frecuente contratar con ellos servicios de correo electrónico, almacenamiento Cloud o software de videoconferencia[17]. En cualquier escenario que implique el uso de herramientas en la nube (Cloud Computing) deberán tenerse en cuenta que, tanto en el caso de tratarse de servicios contratados como de servicios gratuitos ofrecidos por la industria, ni la vigencia de un estado de alarma, ni tampoco de excepción o sitio, relaja en absoluto las garantías del derecho fundamental a la protección de datos. Por ello, cualquier servicio proporcionado por terceros deberá contar con el correspondiente contrato de encargado del tratamiento en los términos previstos por el artículo 28 RGPD.

Según el párrafo primero del citado artículo 28 RGPD, uno de los requisitos impuestos a la hora de escoger un encargado del tratamiento es el de actuar de modo diligente en su elección, contratando solo aquellos que aporten unas garantías adecuadas desde el punto de vista del cumplimiento normativo y de la seguridad de la información, de conformidad con el artículo 32 RGPD, para la correcta protección de los derechos de los interesados.

El uso por parte de los miembros de la comunidad universitaria de software no licenciado por la institución conlleva un serio riesgo de incumplimiento normativo. Se estaría llevando a cabo un tratamiento por un tercero sin ningún tipo de vínculo jurídico con la universidad, por lo que no existiría obligación alguna por su parte.

La universidad cometería en este caso varias infracciones de las catalogadas como muy graves o graves, de acuerdo con la calificación establecida respectivamente por los artículos 72 y 73 de la LOPDGDD. y la Agencia Española de Protección de Datos (en adelante AEPD) podrá proponer la iniciación de actuaciones disciplinarias a título individual o, en su caso, amonestaciones a los cargos responsables para personal de universidades públicas.

En una situación de emergencia, donde la celeridad por contar con los medios adecuados resultaba esencial, el riesgo de acudir a soluciones gratuitas se multiplicó. Por este motivo

[17] Las preguntas frecuentes sobre la sentencia del Tribunal de Justicia de la Unión Europea en el asunto C-311/18 — Comisaria de Protección de Datos vs Facebook Irlanda y Maximillian Schrems, resuelven las dudas sobre la sentencia que invalida las transferencias internacionales de datos a EE.UU. bajo el denominado Privacy Shield. Las universidades deberían tener esto presente dada la gran cantidad de proveedores de ese país. [Disponible en; https://www.aepd.es/sites/default/files/2020-08/faqs-sentencia-SCHREMS-II-es.pdf]

resultaba necesario informar a todos los miembros de la comunidad universitaria de esta prohibición toda vez que se acompañaba de las opciones autorizadas de las que se disponía.

3.3. Medidas de seguridad

La Universidad Pública, viene obligada a la aplicación en toda su extensión del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (en adelante, ENS). En él se regulan las medidas técnicas y organizativas que deben aplicarse a los activos de la universidad para procurarsu seguridad en los términos referidos por el artículo 32 RGPD. En Universidad Privada, esto es más flexible, ya que puede aplicar cualquier medida que garantice adecuadamente la seguridad de la información en los términos del referido artículo.

Para dotar a los sistemas de medidas de seguridad, la universidad deberá establecer en primer lugar las medidas organizativas necesarias que posibiliten el teletrabajo:

a) Definir los métodos y tecnologías mediante los cuales los trabajadores pueden acceder a la información corporativa.
b) Establecer los recursos disponibles para los empleados.
c) Concretar los modelos de uso de los terminales utilizados por los usuarios (COBO, COPE o BYOD)[18]
d) Delimitar los medios de conexión y los usuarios que pueden hacer uso.
e) Precisar las medidas de seguridad aplicables a los equipos que se utilizarán por parte de los trabajadores.

Los manuales correspondientes a la normativa y configuración de herramientas no deberían estar accesibles en abierto ya que con independencia de que esta información no contenga datos estratégicos que permitan identificar servidores, o información sobre procedimientos de seguridad, se intuye la posibilidad de que terceros emulen los documentos con la finalidad de atacar a los sistemas.

Un sistema de comunicación como los descritos para le conexión remota en ambientes de teletrabajo involucra esencialmente tres actores: el terminal del usuario, el canal de

[18] Puede encontrarse información detallada en las siguientes guías e informes del CCN-CERT e INCIBE: Informe del CCN-CERT "IA-21/13 de Riesgos y Amenazas del Bring Your Own Device (BYOD)" [Disponible en: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/677-ccn-cert-ia-21-13-riesgos-y-amenazas-del-byod-1/file.html] y Guía INCIBE "Dispositivos móviles personales para uso profesional (BYOD): una guía de aproximación para el empresario"[Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_dispositivos_moviles_metad.pdf]

comunicación y el "endpoint[19]" remoto que provee el servicio. Para cada uno de ellos se deberán proporcionar las correspondientes medidas de seguridad.

i) Redes

En este caso, la interconexión de los sistemas se lleva a cabo mediante el uso de redes públicas[20] – Internet – por lo que, de no implementarse mecanismos de seguridad, la información sería transportada en claro y podría ser accedida por terceros. La aplicación de técnicas criptográficas[21] para el cifrado de conexiones resulta fundamental para salvaguardar la confidencialidad de la información en tránsito entre el hogar del trabajador y los servidores de la universidad[22], independientemente del hecho de que este se encuentre alojado dentro de la infraestructura universitaria o contratado a un prestador de servicios tercero.

ii) Servidores

En cuanto a los servidores corporativos, las medidas de seguridad no variarán esencialmente respecto a las que se viniesen aplicando, si bien la universidad proporcionará un nivel de seguridad adicional para las conexiones que provengan del exterior, de modo transparente para él.

iii) Clientes

Cuando el mantenimiento de un equipo dependa del personal del departamento de tecnologías de la información y comunicaciones (TIC) de la universidad, este será el encargado de la instalación del software necesario para el trabajo y de la configuración del sistema que le proporcionarle una seguridad adecuada.

---

[19] Un endpoint es un dispositivo informático remoto que se comunica con una red a la que está conectado. Los ejemplos de enpoint incluyen ordenadores, portátiles, tablets, servidores o estaciones de trabajo. [Disponible en https://admware.es/que-es-un-endpoint/]

[20] Art. 22) ENS, aporta una definición de lo que se consideran redes públicas. "Se entenderá por red pública de comunicaciones la red de comunicaciones electrónicas que se utiliza, en su totalidad o principalmente, para la prestación de servicios de comunicaciones electrónicas disponibles para el público, de conformidad a la definición establecida en el apartado 26 del anexo II, de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

[21] Pueden establecerse conexiones seguras mediante VPN, HTTPS u otros protocolos cifrados.

[22] Art. 21) ENS regula la protección de información almacenada y en tránsito. "En la estructura y organización de la seguridad del sistema, se prestará especial atención a la información almacenada o en tránsito a través de entornos inseguros. Tendrán la consideración de entornos inseguros los equipos portátiles, asistentes personales (PDA), dispositivos periféricos, soportes de información y comunicaciones sobre redes abiertas o con cifrado débil. (…)"

Si se trata de un equipo de uso particular, será el propio usuario quien deberá instalar las aplicaciones necesarias que establezca la universidad para poder desarrollar su actividad laboral, las cuales deberán limitarse a las imprescindibles. Se instalará el software necesario para conectarse a la red corporativa y aquel requerido por las características del puesto de trabajo. Adicionalmente, este deberá utilizar el software y aplicar las configuraciones del equipo que se definan como adecuadas al nivel de seguridad que la universidad establezca. Debido a la dificultad que esta configuración puede suponer para el usuario, la universidad debería proveer manuales de instrucciones e incluso un soporte telefónico para ello.

El cumplimiento de las medidas de seguridad requiere del compromiso por parte del trabajador, por tanto, se antoja necesaria la formalización de una declaración responsable en la que este adquiera un compromiso con el correcto uso del software corporativo y la aplicación de las medidas de seguridad establecidas, En este documento deberían detallarse las políticas de uso y las medidas de seguridad a aplicar, que se alinearían a las que a su vez se establecen para dispositivos BYOD.

En la *Tabla 2: Medidas de seguridad en el teletrabajo* se presenta el conjunto de medidas de seguridad aplicable a los equipos de trabajo del personal de la universidad[23].

MEDIDAS DE SEGURIDAD EN EL TELETRABAJO	
CONDICIONES GENERALES DEL EQUIPO DE TRABAJO	
1	Conectarse a la universidad exclusivamente mediante herramientas autorizadas
2	Utilizar software autorizado obtenido de fuentes de confianza.
3	El sistema operativo y aplicaciones deben estar siempre actualizadas
4	Contar con software de detección de malware y antivirus, siempre actualizados
SEGURIDAD EN REDES	
5	Establecer contraseñas y métodos criptográficos en el router WiFi
6	No realizar conexiones a redes WiFi abiertas o publicas
7	No utilizar equipos de uso público

[23] Pueden ampliarse las medidas dictadas por el CCN-CERT para situaciones de teletrabajo en la Guía CCN-CERT BP/18 "Recomendaciones de seguridad para situaciones de teletrabajo y refuerzo en vigilancia" [Disponible en: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/4691-ccn-cert-bp-18-recomendaciones-de-seguridad-para-situaciones-de-teletrabajo-y-refuerzo-en-vigilancia-1/file.html]

MANEJO DE INFORMACIÓN	
8	Evitar descargar información en el dispositivo local
9	Realizar copias de seguridad de los datos, preferiblemente en los sistemas remotos de la universidad.
10	Cifrar los archivos que contengan datos personales o información confidencial
11	Suprimir los datos de manera segura una vez dejan de ser necesarios
CREDENCIALES Y SESIONES	
12	Extremar las precauciones en la custodia de credenciales
13	Escoger contraseñas robustas
14	Evitar almacenar en los navegadores contraseñas de forma automática
15	Utilizar una cuenta de usuario diferenciada del resto de los miembros de la familia
16	Bloquear el terminal cuando no esté en uso de manera manual o automáticamente tras un periodo sin uso
17	Cerrar las sesiones al finalizar el trabajo
18	Proteger el equipo mediante contraseña cuando este almacene certificados digitales.
DISPOSITIVOS REMOVIBLES Y SOPORTE PAPEL	
19	Evitar el uso de dispositivos removibles como USB o discos duros extraíbles. En caso de necesidad, cifrar su contenido.
20	No etiquetar los dispositivos de manera que desvele su contenido
21	Evitar imprimir y transportar la información en soporte papel
EMAIL	
22	Utilizar el email corporativo
23	Cifrar los adjuntos que contengan datos personales o información confidencial
24	Evitar abrir emails sospechosos y reenviar spam
NOTIFICACIÓN DE INCIDENTES	

25	Notificar cualquier incidente de seguridad al Servicio TIC
FINALIZACIÓN DEL TELETRABAJO	
26	Eliminar la información del equipo de manera segura una vez finalizado el teletrabajo

Tabla 2: Medidas de seguridad en el teletrabajo

4. DOCENCIA ONLINE

La suspensión de la docencia presencial provocó el traslado a una modalidad a distancia en la que su impartición se realizaría utilizando medios telemáticos "online". La Universidad, con el soporte de la tecnología se encontraba ante el reto de seguir prestando el servicio de educación superior a los estudiantes bajo estas nuevas condiciones.

Impartir la docencia de este modo hizo que se incorporasen una serie de obligaciones que alcanzaban a todos los implicados, tanto al profesorado como al alumnado. Debe recordarse en este punto que una clase no es un entorno abierto, lo que requiere el cumplimiento de las nuevas condiciones por todas las partes, asegurándose así el derecho a la educación desde el respeto a la intimidad de las personas, materializado en la protección de sus datos.

Para garantizar la intimidad personal cuando exista una interacción en un entorno online deben establecerse ciertas cautelas ha de ser la propia universidad, quien en virtud del principio de responsabilidad proactiva o *accountability*, provea las condiciones adecuadas para el cumplimiento de las obligaciones.

La impartición de la docencia online introduce una serie de nuevos tratamientos de datos, siendo el más destacable aquél que involucra la difusión de la imagen y la voz de los participantes en videoconferencias, por lo que, para que la universidad pueda tratar estos datos, debe buscarse una base legitimadora entre las propuestas en el artículo 6 RGPD.

Al entrar en conflicto el derecho a la educación con el derecho a la propia imagen, a la intimidad de la vida privada y familiar y a la protección de datos, no fueron pocos los que entendieron que el consentimiento de los profesores y alumnos era condición necesaria y suficiente para poder captar sus imágenes. Sin embargo, esta base de legitimación no sería posible, ya que el consentimiento (6.1.a RGPD) en este contexto se no se estaría prestando de manera libre[24], ya que no existía una alternativa a su negativa, por no ser admisible la posibilidad de la docencia presencial. Además, la retirada del consentimiento, de ser

[24] Puede consultarse más información sobre las características del consentimiento el documento del Grupo de trabajo del artículo 29 Directrices sobre el consentimiento en el sentido del Reglamento (UE) 2016/679, [Disponible en: https://www.aepd.es/sites/default/files/2019-12/wp251rev01-es.pdf]

voluntario este, podría llevarse a cabo en cualquier momento, sin que existiese, como decíamos, una alternativa a esta modalidad docente.

El consentimiento debía basarse, por tanto, en el cumplimiento de la prestación del servicio público de educación superior, misión realizada en interés público (6.1.e RGPD), dentro de la relación contractual conformada en la matrícula que une al estudiante con la universidad (6.1.b). De este modo, se asume la existencia de un compromiso educativo entre la universidad y el estudiante que no decaería ante la circunstancia sobrevenida de la impartición de la docencia a distancia.

No debe perderse de vista que la docencia virtual es algo que existía previamente a la pandemia y el impacto que supondría no va más allá de la videoconferencia. La limitación del derecho a la propia imagen del profesorado en estas circunstancias se vería justificada ya que, utilizando este medio, resulta conditio sine qua non que el profesor se muestre en pantalla.

La universidad, por tanto, debe evaluar el impacto en la esfera de los derechos del profesorado y del alumnado. El requisito de predeterminación normativa exige a su vez que el deber de retransmitir una clase se fundamente en el estatuto jurídico del profesor y en su modulación, siempre que esta salve el juicio de proporcionalidad. Desde este punto de vista, la medida sería adecuada, y resultaría complicado encontrar otra medida más moderada para la consecución del propósito de garantizar la docencia online. Al mismo tiempo se estima que de ella derivan más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto. Indudablemente, existe un impacto en los derechos del profesorado, pero también un evidente interés público.

Debían definirse igualmente una serie de políticas dirigidas a que tanto profesorado como alumnado, como sujetos de derechos y obligaciones, dispusieran de la información necesaria que les permitiese conocer sus responsabilidades y sus derechos y la justificación de la aparente limitación de alguno de ellos.

Respecto al trabajador, debería establecerse:

a) Una definición clara de sus funciones y de las razones que limitan su derecho fundamental.
b) Unas políticas que definan el alcance de estas obligaciones.
c) Información previa al trabajador y a la representación sindical, quienes podrán alegar lo que estimen conveniente.

d) Una definición de las condiciones en las que esta limitación del derecho a la propia imagen se produce en relación con[25]:

- la esfera privada y familiar al impartir docencia desde su hogar
- las condiciones de uso y explotación de esas imágenes: espacio de publicación, finalidades admisibles, posibilidad de grabación o no, reutilización, autoría y derechos de propiedad intelectual.

e) El uso de equipos con acceso remotos requería la implantación de una serie de medidas de seguridad. Resulta fundamental que el profesorado cuente con cierta cultura en el uso de datos y seguridad, lo que debe haber sido adquirido mediante formación.

Respecto del estudiante:

a) La definición de reglas de uso para los estudiantes, unos términos de uso claros y vinculantes.

b) Una definición de las condiciones en las que esta limitación del derecho a la propia imagen se produce en relación con la esfera privada y familiar al participar de forma activa en las clases con la captación de su imagen desde su hogar.

c) Información sobre las consecuencias que el uso y difusión de las imágenes captadas en el aula pueda acarrearle. La universidad debería activar procedimientos disciplinarios o emprender acciones legales ante usos como subir grabaciones a redes de compartición de apuntes, ridiculizar al profesorado, manipular las imágenes, etc.

En todos los casos, la información a todos los implicados se considera fundamental para que cada uno pueda conocer las obligaciones existentes.

Adicionalmente, la formación del profesorado cobra especial relevancia a fin de que pueda manejar con soltura el entorno y posea las debidas capacidades. El profesorado debería comprender que la docencia online no se limita a la colocación de una cámara, sino que ello

[25] En este ámbito, el Tribunal Supremo, en su sentencia núm. 304/2019, de 10 de abril, corrobora que, cuando la cesión del derecho de imagen venga requerida por la ejecución de un contrato laboral entre las partes, no será necesario el consentimiento expreso del afectado para su tratamiento. Y se apoya para ello en la normativa de protección de datos de carácter personal, remitiéndose al artículo 6.1.b) del RGPD en el que se recoge como base jurídica para la legitimación del tratamiento la ejecución de un contrato suscrito por el interesado. El Grupo de trabajo del artículo 29, en su Dictamen 2/2017, sobre el tratamiento de datos en el trabajo y en sintonía con lo expuesto, establece que "es muy poco probable que el consentimiento constituya una base jurídica para el tratamiento de datos en el trabajo, a no ser que los trabajadores puedan negarse sin consecuencias adversas". El Comité Europeo de Protección de Datos (EDPB, por sus siglas en inglés) en sus Directrices actualizadas sobre el consentimiento al amparo del RGPD, de 4 de mayo de 2020, señala que cuando el tratamiento de datos es necesario, el consentimiento para el tratamiento de datos personales no puede considerarse una base legal apropiada.

conlleva una serie de obligaciones que debe cumplir, de acuerdo con los procedimientos que la propia universidad indique.

En este sentido, y dentro de lo que la pandemia ha supuesto, la formación al profesorado en los propios entornos de aula virtual de la universidad se ha mostrado como un medio eficaz para adquirir los conocimientos necesarios en cuanto a los procedimientos de docencia y evaluación online, uso de herramientas y aplicación de la normativa relacionada.

Cabe destacar, por último, que el profesorado no puede utilizar cualquier herramienta software para impartir docencia online. Debe hacerse uso exclusivamente de herramientas autorizadas por la universidad que estén licenciadas y que ceunten con un contrato de encargado del tratamiento (art. 28 RGPD). El uso de otras aplicaciones no es posible y estaría expresamente prohibido. Todo aquel que tuviese una propuesta, deberá consultarla con el delegado de protección de datos y el responsable de seguridad de la información de la universidad.

A modo de corolario, podemos extraer un conjunto de recomendaciones a seguir por el profesorado:

a) Seguir las recomendaciones de la universidad para el cumplimiento de las obligaciones de la institución en materia de protección de datos. En particular, en relación con los deberes de transparencia o información.
b) El profesorado en ningún caso está autorizado ni a definir políticas propias en materia de protección de datos, ni a utilizar formularios o procedimientos distintos de los expresamente establecidos por la universidad.
c) Durante la realización de tareas vinculadas a la docencia que impliquen tratamientos de datos personales de imágenes procurarán garantizar la ausencia de terceras personas no concernidas y del estado de la estancia. La universidad no será responsable del visionado incidental de imágenes que afecten a su esfera de vida privada y familiar no se adoptaron las recomendaciones de configuración de la estancia.
d) Las eventuales grabaciones o visionado de imágenes deberán realizarse y conservarse en los entornos destinados a ellas. No podrán descargarse en ordenadores personales o espacios que no hayan sido expresamente habilitados.
e) Utilizar exclusivamente aplicaciones autorizadas.
f) Aplicar las medidas de seguridad que establezca la universidad y guardar secreto profesional

5. EVALUACIONES ONLINE

Mientras que la docencia online en cierto modo no suponía una gran novedad, ya que en las universidades hacía tiempo que se utilizaban videoconferencias para eventos o cursos de formación extracurricular, la evaluación de los alumnos en remoto supuso un gran reto para el profesorado. La conjugación de la protección de los derechos de los estudiantes confrontaba en algunos aspectos con la lucha contra el fraude académico.

Algunas universidades españolas elaboraron guías con metodología sobre la evaluación online en las que se recogían las principales recomendaciones metodológicas al respecto[26]

A su vez, a través de los grupos de trabajo de la Conferencia de Rectores de las Universidades Españolas (CRUE), se redactó una guía específica orientadas a las necesidades que la protección de datos imponía a las evaluaciones online[27].

La grabación o visualización de alumnos utilizando cámaras introduce serie de requisitos que debían ser trasladados tanto al profesorado como al alumnado. Para ello debían formularse una serie de procesos, que incluirían el cumplimiento de la normativa académica de evaluaciones preexistente junto con la de protección de datos.

No se va más allá en el desarrollo de las obligaciones jurídicas que origina la evaluación online en este documento, ya que será tratado en un artículo específico en esta misma publicación.

6. INVESTIGACIÓN

La propagación de la COVID-19 ha provocado una situación de alerta sanitaria a nivel mundial sin precedentes en tiempos recientes, afectando a múltiples facetas de la sociedad en su conjunto. A modo de ejemplo, es evidente la afectación en mayor o menor grado que han sufrido las personas a nivel psicológico, económico, de salud, laboral, etc.

---

[26] Entre estas guías destaca en cuanto a métodos docentes la Guía de recomendaciones para la evaluación online en las Universidades Públicas de Castilla y León Grupo de Responsables de Docencia Online de las Universidades Públicas de Castilla y León [Disponible en http://portaldetransparencia.uva.es/ documentos/rubrica/29-Recomendaciones-evaluacion-online-Universidades-Publicas.pdf] y CRUE, Informe sobre Procedimientos de Evaluación no Presencial. Estudio del Impacto de su Implantación en las Universidades Españolas y Recomendaciones, publicado el 16 de abril de 2020 [Disponible en: https://tic.crue.org/wp-content/uploads/2020/05/Informe-procedimientos-evaluaci%C3%B3n-no-presencial-CRUE-16-04-2020.pdf].

[27] Guía sobre la protección de datos personales en el ámbito universitario en tiempos del COVID-19, adoptada el 24 de abril de 2020 [Disponible en https://www.crue.org/2020/04/crue-universidades-espanolas-elabora-una-guia-sobre-la-proteccion-de-datos-personales-en-el-ambito-universitario-en-tiempos-del-covid-19/]- Destacan a su vez las Guías relativas a la evaluación online de la Universidad de Valladolid: Guía sobre protección de datos en la evaluación online de la Uva y resúmenes y preguntas frecuentes [Disponible en: http://www.uva.es/protecciondedatos/]

Los investigadores de las universidades españolas, conscientes de esta situación, dentro su compromiso con la sociedad, han emprendido numerosos proyectos de investigación relacionados con la COVID-19 desde la perspectiva de sus áreas de conocimiento o mediante colaboraciones multidisciplinares. Muchas de estas investigaciones tenían a personas como objeto de estudio, requiriendo en no pocos casos el tratamiento de datos personales.

Como todo tratamiento de datos, deben cumplirse una serie de condiciones, que en numerosas ocasiones suponen un grado de dificultad no despreciable en su aplicación para los investigadores. Sin embargo, la Universidad, Pública y la mayoría de las privadas tienen la obligación de contar con un delegado de protección de datos, quien entre sus funciones encuentra la de asesoramiento al responsable del tratamiento.

Las principales obligaciones que implica investigar con datos personales, de manera general pueden resumirse en las siguientes:

a) Tratar datos personales siempre que se cuente con legitimación suficiente. Merece especial atención el tratamiento de datos de categorías especiales, el cual solamente puede efectuarse afrontando condiciones específicas.
b) Obtener el consentimiento cuando esto sea necesario.
c) Informar a los interesados sobre los tratamientos y los derechos que les asisten.
d) Definir roles y responsabilidades en caso de corresponsabilidad en el tratamiento.
e) Diseñar el sistema de información conforme a las reglas de protección de datos desde el diseño y por defecto.
f) Analizar los riesgos asociados al tratamiento, y en su caso, realizar una evaluación de impacto en la protección de datos.
g) Analizar riesgos y diseñar e implementar medidas de seguridad.
h) Obtener asesoramiento delegado de protección de datos.
i) Actuar según el proceso de declaración y autorización del tratamiento e integrarlo en el registro de actividades de tratamiento.
j) Considerar las prestaciones por terceros, o la universidad como sujeto prestador y formalizar el correspondiente contrato de encargado del tratamiento
k) Prestar atención a los posibles flujos internacionales de datos personales.

En la aceleración de los tiempos en los procesos de investigación se han puesto de manifiesto carencias en los procesos de formación, divulgación y conocimiento para los investigadores de las obligaciones jurídicas en materias de investigacion. De hecho y con carácter general, en la investigación ordinaria en las universidades, los investigadores suelen confundir los requisitos de consentimiento informado con el cumplimiento global de la materia, sin tener

en cuenta que el conjunto de requerimientos jurídicos en materia de protección de datos y otras correlacionadas como el mantenimiento de la seguridad de la información son particularmente exigentes.

Los investigadores tienden a considerar al dato personal como uno más de todos los datos, sin tener en cuenta que detrás de estos se encuentran personas, quienes son realmente las propietarias de sus datos y la existencia de una obligación inherente de conservar indemne en todo momento su derecho fundamental a la protección de datos[28].

De acuerdo con la experiencia personal de quien escribe, las incorrecciones más comunes detectados suelen ser las siguientes:

a) Tratar datos personales sin ponerlo en conocimiento de la autoridad académica competente o sin notificarlo al delegado de protección de datos para su asesoramiento.
b) Desconocer que corresponde a la Universidad el papel de responsable del tratamiento en virtud de la relación laboral que vincula al trabajador.
c) No definir las responsabilidades de los intervinientes en un convenio con respecto a los datos a tratar.
d) Utilizar software de cualquier tipo que trate datos personales sin contar la Universidad con un contrato de encargado del tratamiento del artículo 28 RGPD, especialmente softwares de uso gratuito.
e) No aplicar las medidas de seguridad de la información adecuadas en sus equipos informáticos. Ello puede deberse a la inexistencia de una política de seguridad o al desconocimiento de la normativa aplicable, o a la falta de formación para la correcta aplicación.
f) Efectuar contrataciones de productos software que no ofrezcan las debidas garantías para los tratamientos de datos.
g) Llevar a cabo transferencias internacionales de datos por desconocimiento y sin el conocimiento del delegado de protección de datos.
h) No seguir los procedimientos para la declaración, autorización e inclusión en el Registro de actividades del tratamiento de la Universidad.
i) No llevar a cabo un análisis de riesgos o evaluaciones de impacto cuando exista un grave riesgo para los derechos y deberes de los interesados.
j) No distinguir entre los conceptos de datos anonimizados y confidencialidad de la información. En numerosas ocasiones se detectan encuestas que tratan datos de

[28] En este sentido se dirige el lema con el que el Dr. Martínez suele comenzar sus conferencias, "La protección d e datos protege personas, no datos".

personas identificables a través de sus respuestas, pero que se declaran como anónimas.

k) No informar correctamente sobre todo aquello que concierne al tratamiento, como su finalidad, la base jurídica habilitante o derechos de los interesados.
l) Almacenar los datos por un tiempo superior al necesario.
m) Utilizar los datos para una finalidad que no era la inicialmente prevista. Aunque estos casos son los menos.

Con todo esto, la protección de datos es percibida como una formalidad más que consume tiempo al investigador y que le impide desarrollar plenamente su investigación. Sin embargo, esta resulta fundamental cuando de proteger personas se trata y el cumplimiento normativo debería contemplarse como un valor añadido al proyecto por la seguridad jurídica que aporta para los investigadores y para las personas participantes en los estudios. Por otro lado, no sería justo atribuir la responsabilidad de estos errores directamente a los investigadores ya que la escasez de recursos y la falta de formación adecuada hacen que, desafortunadamente, estos errores sean recurrentes.

7. REUNIONES TELEMÁTICAS DE ÓRGANOS COLEGIADOS

Como es conocido, el gobierno y la representación de la Universidad se articula a través de órganos colegiados y unipersonales. Los órganos colegiados son aquellos que adoptan sus decisiones de manera conjunta entre todos sus integrantes. La Universidad encuentra en su estructura varios de estos órganos, resultando su funcionamiento esencial para el desarrollo de la actividad universitaria. Estos están integrados principalmente por el Claustro, el Consejo de Gobierno, el Consejo Social y los Juntas de Facultad o Escuela y los Consejos de Departamento.

La suspensión de la actividad docente trasladó la celebración de las reuniones de los estos órganos a un entorno virtual. Sus miembros tuvieron que reunirse mediante videoconferencia, lo que generó una serie de nuevas obligaciones que provocó que debiesen definirse los deberes derechos y responsabilidades de cada una de las personas integrantes del órgano.

La celebración de reuniones online de órganos colegiados comporta indudablemente un tratamiento de datos en las que se utilizan los datos de imagen de los participantes. Al igual que sucede en la docencia y evaluaciones online, se pone en conflicto el derecho de los trabajadores a la intimidad personal, a la propia imagen y a la protección de datos con el derecho a la educación de los alumnos, el cual depende del normal funcionamiento de la institución universitaria a través de sus órganos colegiados.

Debe comprobarse, por tanto, si existe base legal suficiente para tratar sin consentimiento los datos personales de los miembros de los órganos de la Universidad, mediante la difusión y grabación de las imágenes. Una vez más, basar el tratamiento en el consentimiento de los participantes en las reuniones no sería válido ya que, como en otras ocasiones, no existiría una alternativa presencial. No contar con el consentimiento de alguno de los integrantes inhabilitaría su funcionamiento.

No obstante, encontraríamos base legitimadora en la obligación legal aplicable al responsable del tratamiento, siquiera indirecta, cuando se trata de garantizar el derecho de acceso a la información pública. Y, en todo caso, la sección 3ª del Capítulo II de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, confiere a la Universidad los necesarios poderes públicos a los que se refiere el RGPD. Por tanto, legitimación basada en los artículos 6.1.c y 6.1.e RGPD respectivamente.

De manera adicional, la universidad podría decidir utilizar las imágenes obtenidas en la celebración de las reuniones como videoactas, con plena validez. Para que esto sea posible, la universidad debería establecer un procedimiento en el que se atribuyese validez oficial a las grabaciones, se estableciesen los medios utilizables para la celebración de las reuniones, junto con sus medidas de seguridad, y se definiesen los mecanismos mediante los cuales las actas pueden ser consultadas.

a) Para la celebración de las reuniones solo deben utilizarse las herramientas designadas por la propia universidad, por ser estas las que han sido validadas desde el punto de vista técnico y jurídico.
b) Debe existir un procedimiento que otorgue validez a las actas en el que a su vez se defina el encargado de su custodia, que normalmente recaerá sobre el secretario del órgano.
c) Las actas se almacenarán en los espacios designados para ello, de acuerdo con el procedimiento que establezca la universidad, contando con las adecuadas medidas de seguridad para garantizar su confidencialidad e integridad.
d) Se deben establecer las políticas de privacidad e informarse sobre ellas a los miembros de los órganos con carácter previo a la celebración de las reuniones. Como buena práctica se recomienda proyectar una diapositiva informativa con la información básica sobre protección de datos y un enlace o código QR que lleven a la información detallada.
e) Se deben establecer los mecanismos de acceso para los miembros del órgano y para aquellos que, aun no perteneciendo, soliciten acceso a la videoacta en virtud de lo

dispuesto por la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.

Durante la celebración de las reuniones puede producirse una afectación de la vida privada y familiar. Por lo que, con carácter previo a la celebración de las reuniones online, deben adoptarse criterios de preservación de la vida privada y familiar en las reuniones celebradas online así como impedir el acceso por terceros no autorizados a cualquier información incluidas las deliberaciones del órgano. De ello derivarían obligaciones como las que siguen:

a) Durante la celebración de la reunión en ningún caso podrá estar presente en la estancia ni, sobre todo, tener acceso ni siquiera mediante una mera visualización ninguna persona ajena. Ello no sólo concierne a familiares o personas con las que se conviva, sino también a cualquier tercero, incluido personal de la universidad no relacionado con la reunión.

b) El miembro del órgano será responsable del mantenimiento del debido decoro de la estancia y de evitar el acceso de personas no autorizadas. La universidad carecerá de responsabilidad respecto de la captación incidental de imágenes de terceras personas, o que pudieran afectar a la vida privada, la imagen o el honor de las personas objeto de visualización o registro con motivo de la reunión.

c) Las grabaciones deberán realizarse y conservarse en los entornos destinados a ello. No podrán descargarse en ordenadores personales o espacios que no hayan sido expresamente habilitados.

d) Em las deliberaciones que deban ser tomadas mediante votación secreta de los miembros del órgano, se articularán sistemas que permitan emitir el voto sin que sea conocido por los restantes miembros.

Las reuniones de órganos colegiados pueden involucrar deliberaciones y toma de decisiones que involucren a individuos particulares. En tales casos, deberían definirse reglas de actuación que, aplicando por ejemplo los criterios de ponderación del artículo 15 de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, definan el modo en el que se presentarán al órgano los datos de la persona concernida o, en su caso, acordar limitaciones en la grabación y publicación de los contenidos.

Con el fin de preservar su intimidad, deben articularse medios para que estas deliberaciones no sean mostradas al público. Para ello puede optarse por dividir la sesión en parte “a puerta cerrada”, donde se mantenga esta parte del debate y parte pública para los restantes asuntos. Por otra parte, es necesario considerar la potencial grabación de terceras personas que, no teniendo la condición de miembros del órgano de representación, puedan comparecer en las

sesiones del mismo cuando tal posibilidad se encuentre prevista en el Reglamento de funcionamiento. Por ejemplo, se trataría de comparecencias de expertos, o de miembros de la comunidad universitaria representativos de intereses. En tales casos debería preverse las condiciones de tratamiento de sus datos.

Habida cuenta del funcionamiento ordinario de este tipo de órganos no resulta inusual la presencia en la sala de reuniones de personal de administración y servicios desarrollando tareas de soporte, como por ejemplo la puesta a disposición de los miembros del órgano de documentación de la reunión. Lo mismo sucedería de modo mucho más directo en el caso de resultar necesaria la presencia de una persona intérprete de signos.

En tales casos, resulta tan impensable obtener el consentimiento para el tratamiento, como paralizar la grabación cada vez que de modo incidental un PAS fuese registrado en el video. Cabe considerar que tal grabación resulta de modo ineludible vinculada con el puesto de trabajo que se desempeña. Por tanto, la base jurídica para el tratamiento sería el propio contrato o la relación funcionarial con la Universidad.

En cuanto al periodo de conservación de las videoactas, debemos atenernos a su valor histórico en aplicación de lo previsto por el considerando (50) del RGPD en el que se dice que "Las operaciones de tratamiento ulterior con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos deben considerarse operaciones de tratamiento lícitas compatibles. La base jurídica establecida en el Derecho de la Unión o de los Estados miembros para el tratamiento de datos personales también puede servir de base jurídica para el tratamiento ulterior", trasladándose este al artículo 89 del RGPD,

Cabe considerar, que en nuestro Ordenamiento las grabaciones en video o video-actas se acomodan tanto al concepto de información pública de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, como al de patrimonio documental de la Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español.

Estas normas conformarían una base jurídica para la conservación indefinida de las grabaciones en video o video-actas y su uso con fines históricos. A mayor abundamiento, las propias funciones de la universidad conforme a la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades apuntan precisamente a un quasi-deber institucional de conservación.

8. PROCESOS ELECTORALES TELEMÁTICOS

La Universidad cuenta con la obligación legal atribuida por el artículo 13 de la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades, de celebrar elecciones destinadas a la elección

de sus representantes en los órganos de gobierno y representación. El mismo artículo confía a las universidades el establecimiento de sus normas electorales de forma estatutaria.

En un contexto de no presencialidad sobrevenido, la celebración de los procesos electorales telemáticamente supone una opción que salvaría el derecho de sufragio en esta situación. No es extraño, no obstante, que en determinadas universidades el sistema de voto electrónico ya se encuentre en funcionamiento, debido a las ventajas que se estima que este aporta: la reducción de costes y la comodidad para el votante, que se traduciría en un aumento de la participación.

Sin embargo, como principal dificultad, se enfrenta al reto de conseguir la confianza de los electores[29], ya que todo sistema informático, por su naturaleza, resulta potencialmente inseguro y podría ser manipulado. Es importante, por tanto, articular los procedimientos adecuados y dotar a la tecnología subyacente de medidas de seguridad para salvaguardar la confidencialidad e integridad del voto emitido, garantizar la disponibilidad de la plataforma de votación mediante sistemas resilientes, avalar la autenticidad de la identidad del votante y procurar que el sistema sea trazable y auditable, a la par que anónimo, para que el proceso pueda ser fiable y transparente.

Es incuestionable que un proceso electoral conlleva un tratamiento de datos en los términos que lo define el artículo 4 RGPD. La base jurídica habilitante del tratamiento se encontraría en el cumplimiento de la obligación legal de celebración de comicios atribuida a la Universidad (art. 6.1.c) RGPD). Sin embargo, el hecho de que para ello se utilicen medios electrónicos debería estar contemplado de manera específica en la normativa electoral propia de la universidad. Por otro lado, al ser el derecho de sufragio un derecho a disposición del elector, el consentimiento que este presta (6.1 a) RGPD) al emitir el voto se convertiría en base legitimadora.

El tratamiento de referencia exige casar en realidad dos derechos fundamentales, el derecho a la protección de datos y el derecho a participar en los asuntos públicos, directamente o por medio de representantes, libremente elegidos en elecciones periódicas por sufragio universal. Si bien es obvio que, desde un punto de vista material la finalidad no es otra que

[29] Según la Recomendación Rec (2004) 11 del Comité de Ministros del Consejo de Europa a los Estados miembros sobre los estándares legales, procedimentales y técnicos de los sistemas de votación electrónica, firmada en Estrasburgo el 30 de septiembre de 2004 [Consultable en: https://www.coe.int/t/dgap/goodgovernance/Activities/Key-Texts/Recommendations/E-votingRec_Spanish.asp], "El voto electrónico ha de respetar todos los principios predicables de las elecciones y los referéndums democráticos. El voto electrónico ha de ser tan seguro e inspirar la misma confianza que los sistemas de votación que, utilizados tradicionalmente en las elecciones y referéndum democráticos, no conllevaban el uso de medios electrónicos. Este principio general afecta a todos los aspectos electorales" […] "ha de tenerse en cuenta la necesaria interrelación entre los aspectos jurídicos, o legales, procedimentales, o de gestión, y técnicos del voto electrónico […]"

promover el derecho del artículo 23 de la Constitución Española ofreciendo nuevas modalidades de voto, no lo es menos que en cualquier caso la aplicación de los principios de protección de datos del artículo 5 RGPD, y el principio de protección de datos desde el diseño y por defecto del artículo 24 exigen del delegado de protección de datos un juicio de ponderación que asegure la existencia de adecuadas garantías de los derecho de las personas interesadas.

Sin embargo, antes de finalizar con el juicio de ponderación debe recordarse que reiterada jurisprudencia del Tribunal Europeo de Derechos Humanos exige un elemento adicional. No sólo se trata de que la medida limitativa cumpla una función necesaria en una sociedad democrática para conseguir ciertos derechos, bienes o valores fundamentales, sino que se exige adicionalmente la predeterminación normativa de la limitación. Esta última recaerá en la normativa electoral específica de cada universidad, la cual debe haber consensuado el electrónico como medio admisible para la finalidad.

Desde el punto de vista del juicio de ponderación resulta evidente que la medida es necesaria en relación con el fin y resultaría idónea. Por otra parte, habida cuenta de la naturaleza de la población, miembros de la comunidad universitaria con conocimientos y medios adecuados, no supone un gravamen desproporcionado para el ejercicio del derecho sino, antes al contrario, un modo natural de realizarlo.

No obstante, no es ocioso recordar que la Recomendación Rec (2004) 11 del Comité de Ministros del Consejo de Europa a los Estados miembros sobre los estándares legales, procedimentales y técnicos de los sistemas de votación electrónica, firmada en Estrasburgo el 30 de septiembre de 2004[30], al definir los principios del derecho de sufragio en el párrafo A de su Anexo I sobre estándares legales señala como elemento esencial que los sistemas de votación electrónica se diseñen de tal modo que no se excluya de su uso a personas con algún tipo de discapacidad.

Debe tenerse en cuenta que, de no garantizar el sistema la accesibilidad, las personas concernidas podrían ejercer legítimamente un derecho de oposición al tratamiento lo que, ineludiblemente obligaría a disponer de urna opción física, toda vez que se asegura que no exista duplicidad de voto.

[30] Recomendación Rec(2004) 11 del Comité de Ministros del Consejo de Europa a los Estados Miembros sobre los estándares legales, procedimentales y técnicos de los sistemas de votación electrónica, firmada en Estrasburgoel día 30 de septiembre de 2004, [Consultable en: https://www.coe.int/t/dgap/goodgovernance/Activities/Key-Texts/Recommendations/E-votingRec_Spanish.asp#P100_6113]

El artículo 35 RGPD establece que ante la probabilidad de que un tratamiento "entrañe un alto riesgo para los derechos y libertades de las personas físicas" será necesario llevar a cabo una evaluación de impacto (EIPD) con carácter previo. Al análisis de necesidad de EIPD aconseja su realización, ya que puede considerarse que el tratamiento involucraría la utilización de nuevas tecnologías[31] a gran escala[32].

En cuanto al sistema de voto, este deberá estar construido teniendo presente la protección de datos desde el diseño y por defecto mediante la aplicación de medidas técnicas y organizativas apropiadas, como la seudonimización, que contribuyan con la minimización en el uso de datos. Esto permitirá disminuir los riesgos que se deriven para los derechos y libertades de las personas (artículo 25 RGPD).

La Universidad Pública, aplicará las medidas contenidas en el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica[33], y en este caso no cabe la menor duda que el nivel de seguridad será el máximo previsto, el recomendable seguimiento de los criterios del Anexo III sobre estándares técnicos de la citada la Recomendación Rec (2004) 11 del Comité de Ministros del Consejo de Europa. Estándares no sólo referidos a la seguridad sino a los distintos elementos que garantizan un adecuado desarrollo de la aplicación.

De recurrirse a un subcontratista que preste el servicio de voto electrónico, este deberá aplicar las medidas técnicas y organizativas adecuadas que permitan desarrollar el tratamiento con las máximas garantías. Deberá atender todas las condiciones impuestas por lo dispuesto en el artículo 28 RGPD, De manera adicional, este prestador de servicios deberá acreditar que su sistema es capaz de cumplir con todas las condiciones requeridas a un

[31] Según la guía del Grupo de Trabajo del Artículo 29 WP248 "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 RGPD", [Consultable en https://www.aepd.es/sites/default/files/2019-09/wp248rev01-es.pdf] requieren una evaluación de impacto en protección de datos tratamientos que impliquen la utilización de nuevas tecnologías o un uso innovador de tecnologías consolidadas, incluyendo la utilización de tecnologías a una nueva escala, con un nuevo objetivo o combinadas con otras, de forma que suponga nuevas formas de recogida y utilización de datos con riesgo para los derechos y libertades de las personas.

[32] Para determinar si un tratamiento se puede considerar a gran escala se considerarán los criterios establecidos en la guía WP243 "Directrices sobre los delegados de protección de datos (DPD)" del Grupo de Trabajo del Artículo 29. [Consultable en https://www.aepd.es/sites/default/files/2019-09/wp243rev01-es.pdf] En este caso, consideramos que el tratamiento se produce a gran escala teniendo en cuenta que el tratamiento afecta prácticamente a la totalidad de la comunidad universitaria.

[33] Según la disposición adicional primera LOPDGDD en los casos en los que un tercero preste un servicio en régimen de concesión, encomienda de gestión o contrato, las medidas de seguridad se corresponderán con las de la Administración pública de origen y se ajustarán al Esquema Nacional de Seguridad.

proceso electoral y que ha efectuado una EIPD a su sistema para garantizar estas condiciones, al margen de las propias de seguridad.

En todo procedimiento electoral pueden distinguirse varias fases. A continuación, presentamos las condiciones de cumplimiento normativo que deberían cumplirse en cada una de ellas.

- **Fase 1: Publicación de censos**

La publicación de los censos deberá hacerse según el procedimiento dictado por el reglamento electoral correspondiente. Este indicará los datos a publicar y el lugar de publicación. En especial:

a) Debería contener los datos imprescindibles para su finalidad[34], que no es otra que la de garantizar la completa corrección y veracidad de los datos censales para poder ejercer el derecho de sufragio y ser correctamente identificado en la mesa electoral[35]
b) Preferentemente se utilizarán medios que no expongan los datos de los electores, siendo aconsejable el uso de medios informáticos, atendiendo al principio de protección de datos desde el diseño y por defecto (art. 32 RGPD), a los que cada votante pudiera acceder para consultar exclusivamente su información.
c) La exposición pública se configura como un medio alternativo ante la carencia de recursos informáticos. Esta debería hacerse en un entorno controlado que impidiese accesos a personas no interesadas, además de evitar sustracciones y manipulaciones del censo.
d) Acompañando al censo, deberá informarse sobre el modo de ejercer los derechos de los votantes.

- **Fase 2: Gestión de candidaturas**

La gestión de candidaturas implica de igual modo un tratamiento de datos personales. El derecho de sufragio pasivo requiere las mayores garantías de transparencia. Por tanto, deberá velarse por la exactitud de los datos, al igual que en todo el proceso, para dotarle de las máximas garantías.

[34] Debe procurarse manejar los mínimos datos, de acuerdo con el principio de minimización de datos del artícul 5 RGPD.

[35] A estos efectos, no resultaría aplicable la disposición adicional séptima de la LOPDGG para la ofuscación de documentos de identidad, ya que en este supuesto no se trata de diferenciar entre personas con el mismo nombre y apellidos, una corrección del número del documento de identidad erróneo podría ser necesaria.

- **Fase 3: Votación**

Para la votación se seguirá el procedimiento establecido por el reglamento electoral, el cual establecerá las condiciones particulares que implica un entorno electrónico. En particular:

a) Los miembros de mesa y operadores deberán contar con instrucciones claras y precisas sobre el funcionamiento del sistema y de resolución de incidencias.
b) Deberá informarse a los votantes sobre el procedimiento general de voto y sobre los tratamientos de datos con carácter previo a la votación.
c) Es fundamental, por razones de transparencia y eficiencia, poner la documentación a disposición de los electores en la web institucional o mediante envío por correo electrónico, además de incluirla accesible en el propio sistema de voto.
d) Deberán establecerse los medios de identificación válidos para acceder al sistema de votación. En este sentido serán preferibles todos aquellos basados en sistemas de identificación y firma criptográficos.
e) Todos los sistemas de identificación basados en sistemas no criptográficos deberán haber sido aprobados como sistemas de identificación seguros y válidos[36].
f) Debido a la naturaleza del medio electrónico a utilizar, el procedimiento de voto deberá incluir información específica con las características técnicas y medidas de seguridad que deben reunir los equipos de los electores.
g) Se establecerá un procedimiento de resolución de incidencias con las votaciones, las cuales ahora pueden ser técnicas. Dicho procedimiento deberá incluir medidas de contingencia para los casos en los que no pueda emitirse el voto de forma electrónica.
h) Deberán preverse sistemas para que las personas en situación de diversidad funcional puedan emitir su voto.
i) Deberán generarse recibos de voto que permitan acreditar el depósito del voto en la urna virtual y poder trazar el voto en caso de que exista algún tipo de problema.

- **Fase 4: Recuento**

[36] En aplicación de lo dispuesto en el artículo 10.4 de la Ley 39/2015, de 1 de octubre, que faculta a las Administraciones Públicas a admitir los sistemas de identificación contemplados en esta Ley como sistema de firma cuando permitan acreditar la autenticidad de la expresión de la voluntad y consentimiento de los interesados, siempre que así lo disponga la normativa reguladora, la Resolución de 14 de julio de 2017, de la Secretaría General de Administración Digital, por la que se establecen las condiciones de uso de firma electrónica no criptográfica, en las relaciones de los interesados con los órganos administrativos de la Administración General del Estado y sus organismos públicos.
Puede consultarse un ejemplo de autorización de este tipo de sistemas en:
https://sede.uva.es/opencms/opencms/es/Tablones/Tablon_de_Anuncios/RESOLUCIONES_ORGANOS_UNIP EI
SONALES/DocTablon_0201/Sellado_RRsistemasidentificacionyfirmanocriptograficos.pdf

El sistema de votación, como es de esperar, debería ser anónimo, a la vez que trazable, por lo que sería deseable que este hubiese sido sometido a auditorías efectuadas por terceros que avalasen su correcto funcionamiento para que, de este modo, el recuento ofrecería las máximas garantías.

En esta fase se atenderán las reclamaciones que tanto votantes como electores pudiesen formular. El sistema debería poder hacer frente a reclamaciones referentes a votos no emitidos, votos manipulados o errores en el recuento de los votos.

- **Fase 5: Supresión de datos**

Una vez transcurrido el plazo de impugnación, las papeletas serán destruidas, dándose así por concluido el proceso.

9. RETORNO A LA PRESENCIALIDAD

Una vez finalizado el estado de alarma decretado por el Real Decreto 463/2020, de 14 de marzo, por el que se declara el estado de alarma para la gestión de la situación de crisis sanitaria ocasionada por el COVID-19, la autoridad gubernativa trazó un plan de vuelta a la normalidad, en el que se permitía volver a la actividad presencial adoptando ciertas cautelas para impedir nuevas infecciones. Las medidas que debían adoptarse se publicaron en el Real Decreto-ley 21/2020, de 9 de junio, de medidas urgentes de prevención, contención y coordinación para hacer frente a la crisis sanitaria ocasionada por el COVID-19, el cual fue completado con las correspondientes ordenes de las autoridades sanitarias autonómicas.

9.1. Obligatoriedad de comunicación de la enfermedad

El Real Decreto-Ley 21/2020 en su artículo 22 cataloga a la enfermedad COVID-19, provocada por el coronavirus SARS-CoV-2, como una enfermedad de declaración obligatoria urgente, a efectos de lo previsto en el Real Decreto 2210/1995, de 28 de diciembre, por el que se crea la red nacional de vigilancia epidemiológica

Por su parte, el artículo 26 del citado Real Decreto establece la obligatoriedad de facilitar a las autoridades sanitarias la información de la que dispongan o que les sea solicitada relativa a la identificación y datos de contacto de las personas potencialmente afectadas, provisión de información esencial para la trazabilidad de contactos con la finalidad de realizar una trazabilidad de contactos.

Como puede observarse, correspondería exclusivamente a las autoridades sanitarias y en quienes estas deleguen la trazabilidad de los contactos. Ninguna otra entidad pública o

privada podría recoger datos personales con la finalidad de rastreo, debido a la inexistencia de una predeterminación normativa habilitante.

Si bien es cierto que desde todos los ámbitos se desea combatir con la lucha de la pandemia contribuyendo al rastreo de los casos positivos, recabar datos con fines de rastreo no sería posible para la Universidad. Los datos para aportar a las autoridades sanitarias serían aquellos que se hubiesen obtenido en el ejercicio de su actividad ordinaria[37].

9.2. Evitar aglomeraciones mediante control de acceso, cita previa y control de aforo

Junto con la desinfección, la limpieza y la ventilación, la distancia interpersonal y la adopción de medidas organizativas para evitar aglomeraciones se mostraban como algunas de las medidas más eficaces para evitar la propagación de contactos[38]. Con la finalidad de evitar aglomeraciones y controlar el aforo en los centros administrativos y docentes se establecieron sistemas de control de acceso y de cita previa.

Existe base legal suficiente para que la universidad pueda llevar a cabo un control de acceso a sus dependencias, ya sea de manera automatizada mediante tarjeta inteligente o mediante control de identidad por personal auxiliar con la finalidad de evitar aglomeraciones en dependencias universitarias, en virtud de lo dispuesto por el art. 7 del Real Decreto-ley 21/2020.

Del mismo modo, se consideraría lícito el tratamiento de datos para evitar aglomeraciones mediante la implantación de un sistema de cita previa en base al artículo 7 del Real Decreto-Ley 21/2020 o en base al principio de eficiencia en el funcionamiento de la Administración Pública, principio informador de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas y de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

El control de aforo de las aulas encontraría su justificación en el deber de cumplir con las normas de distanciamiento social requeridas a los responsables de los centros educativos, según el artículo 9 del Real Decreto-Ley 21/2020.

A mayor abundamiento, la Ley de prevención de Riesgos Laborales introduce el derecho a la salud del trabajador y el correlativo deber del empleador para procurarlo. Atendiendo a este requerimiento de velar por la salud de los trabajadores que hace la Ley 31/1995, vistas

[37] En este sentido se pronuncia la medida 1.3 del ACUERDO 29/2020, de 19 de junio, de la Junta de Castilla y León, por el que se aprueba el Plan de Medidas de Prevención y Control para hacer frente a la crisis sanitaria ocasionada por la COVID-19.

[38] El artículo 7 y el artículo 9 del Real Decreto-ley 21/2020, de 9 de junio, de medidas urgentes de prevención, contención y coordinación para hacer frente a la crisis sanitaria ocasionada por el COVID-19, establecen las medidas a adoptar en centros de trabajo y centros docentes, respectivamente.

las especiales circunstancias provocadas por la pandemia de la COVID-19, los sistemas de cita previa, control de acceso y control de aforo, podrían considerarse como un medio adicional que permitiría velar por la salud de los trabajadores ya que, de este modo se impedirían las aglomeraciones.

No debe olvidarse que, atendiendo al principio de minimización de datos, todos estos sistemas deben recabar la menor cantidad de datos posibles para cumplir con su finalidad.

Con independencia de su función principal, estos medios contribuirán en el control de la propagación de la enfermedad, aportándose los datos obtenidos en su actividad a requerimiento de las autoridades sanitarias, lo que les facilitará la trazabilidad de los casos positivos.

9.3. Prevención de riesgos laborales en la nueva presencialidad

Algunas universidades, comprometidas con la vigilancia de la salud, han resuelto procurar a sus trabajadores la posibilidad de realizarse test de COVID-19, de manera voluntaria, dentro del modelo de vigilancia de la salud previsto en el artículo 22 de la Ley de prevención de Riesgos Laborales.

La toma de muestras biológicas que se produce en la analítica conlleva un tratamiento de datos personales de salud, catalogados como categoría especial. Acompañando a este, existirá a su vez tratamiento de datos como consecuencia de la gestión administrativa de las citas y comunicación de resultados.

En esta materia resulta de aplicación el artículo 9 de la LOPDGDD que determina en qué casos será posible el tratamiento de categorías especiales de datos sobre la base del consentimiento.

Por tanto, sería lícito el tratamiento de datos personales con fines de medicina preventiva o laboral. No obstante, este tratamiento deberá ser realizado por un profesional sujeto a la obligación de secreto profesional, o bajo su responsabilidad. Y deberá acudirse a la legislación sectorial a fin de determinar si se requiere o no del consentimiento del trabajador.

Un tratamiento de datos de este tipo, en el que se tratan datos de salud a gran escala[39], requiere de una evaluación de riesgos que determine si el tratamiento tal y como está formulado puede llevarse a cabo sin que por ello se vean perjudicados los derechos y libertades de los interesados.

[39] Este tratamiento a gran escala no sería por número, sino por porcentaje respecto al total, tal y como establece el informe Directrices sobre los delegados de protección de datos (DPD) el Grupo de trabajo sobre protección d datos del artículo 29. [Consultable en: https://www.aepd.es/sites/default/files/2019-09/wp243rev01-es.pdf]

La universidad que contando con Servicio de Prevención de Riesgos Laborales propio subcontrate exclusivamente los servicios de análisis clínicos a los trabajadores requerirá la formalización de un contrato de encargado del tratamiento del art. 28 RGPD, ya que la entidad prestadora del servicio tendrá la consideración de encargado del tratamiento[40]. Esto no será necesario si la universidad cuenta con un Servicio de Prevención Ajeno subcontratado que se encuentre en condiciones de realizar las analíticas, ya que este tendría la consideración de responsable.

A su vez, es el propio trabajador quien puede venir obligado a declarar situaciones de riesgo. Tal tal y como establece el artículo 29.2.6º de la Ley 31/1995, el trabajador debe cooperar con el empresario para que éste pueda garantizar unas condiciones de trabajo que sean seguras y no entrañen riesgos para la seguridad y la salud de los trabajadores.

Por último, el Procedimiento de actuación para los servicios de prevención de riesgos laborales frente a la exposición al SARS-CoV-2, del Ministerio de trabajo de 8 de junio de 2020, no incluye el cribado entre las medidas de carácter colectivo y en su Anexo V se ofrece una Guía de actuación para la gestión de la vulnerabilidad y el riesgo en el ámbito en ámbitos no sanitarios o sociosanitarios. Por tanto, un este sistema no se correspondería en absoluto con un modelo que requiere de la individualización del riesgo y, como medida de control, de la intervención de los representantes de los trabajadores para la adopción de una medida de esta naturaleza.

9.4. Cesión de datos al sistema de salud

Debido al carácter voluntario de la analítica de detección de infección por COVID-19, derivada de la opcionalidad de la participación en la vigilancia de la salud de la Universidad (art. 22 Ley 31/1995), dependerá de la voluntad de este la comunicación del resultado de la prueba a la universidad en caso de resultar positiva. No obstante, no podemos olvidar que, como hemos visto, en virtud del 29 de la misma Ley, el trabajador estaría obligado a comunicar cualquier situación que ponga en peligro su salud o la del resto de compañeros. De no hacerlo, podría enfrentarse a sanciones disciplinarias.

Una vez que el trabajador ha comunicado la infección a la universidad, esta deberá comunicarlo a las autoridades sanitarias, según dispone el artículo 26 del Real Decreto-Ley, toda vez que puede desplegar el protocolo de prevención correspondiente para proteger al resto de los empleados.

[40] Puede consultarse el criterio seguido por la AEPD en la atribución a las mutuas del carácter de responsable del tratamiento en los informes jurídicos 112/2008 y 0299/2009.

Como cláusula de cierre, el Real Decreto-Ley 21/2020 en su artículo 25 obliga a todos los laboratorios autorizados en España para la realización de pruebas diagnósticas para la detección de SARS-CoV-2 mediante PCR u otras pruebas moleculares a remitir diariamente al Ministerio de Sanidad y a la autoridad sanitaria de la comunidad autónoma en la que se encuentren los datos de todas las pruebas realizadas a través del Sistema de Información establecido por la administración respectiva.

10. CONCLUSIONES

A lo largo del presente artículo se ha pretendido abarcar el conjunto de nuevos escenarios motivados por la irrupción de la docencia online con motivo de la propagación de la enfermedad COVID-19. Esto ha supuesto que los trabajadores de la Universidad se hayan visto sujetos a una serie de nuevas obligaciones. Estas situaciones han sido abordadas a partir de la normativa preexistente aplicable, si fuera esta general o específicamente universitaria y a partir de los criterios motivados por la nueva normativa relacionada con la pandemia.

El marco jurídico de la prestación del servicio de educación superior a través de herramientas de teletrabajo se enfrentó a una situación de debilidad e incertidumbre que debió ser paliada a mediante tres estrategias.

En primer lugar, resulta muy loable la buena voluntad de colaboración del profesorado, que aplicó los criterios de seguridad y confidencialidad que razonablemente derivaban del sentido común. Sin perjuicio de ello, las universidades hicieron un significativo esfuerzo en la definición de criterios jurídicos y materiales que garantizasen el cumplimiento normativo en el despliegue de esta prestación.

En segundo lugar, no menos importante fue el enorme esfuerzo de disciplina de esta materia a partir de la interpretación de un marco jurídico previo prácticamente inexistente e insuficiente.

Por último, las directrices implantadas por las universidades, esencialmente a partir de las aportaciones de los delegados de protección de datos, contaron con la predisposición colaborativa del profesorado.

La transición al teletrabajo enfrentada por la Universidad no contó con ningún tipo de criterio objetivo, lo que requirió un ingente esfuerzo en la adaptación. Actualmente, con la promulgación del Real Decreto-ley 28/2020, de 22 de septiembre, de trabajo a distancia, se pone fin a la incertidumbre vivida.

En cuanto a las obligaciones específicas que hemos visto para cada uno de los escenarios a lo largo del texto, podemos resumirlas a continuación.

El teletrabajo de forma genérica implica obligaciones en cuanto a los medios materiales y quién los facilita, respecto a la prevención de riesgos laborales o a preservación de los derechos a la intimidad y a la desconexión digital. El uso de medios digitales introducía la necesidad de aplicación de medidas que garantizasen la seguridad de los datos. Todo esto conlleva la necesidad de formar al profesorado.

A su vez, la docencia y la evaluación online suponen un tratamiento de datos de imágenes de los estudiantes, por lo que estos deben ser protegidos. Para ello el profesorado debe informarles sobre los tratamientos que se produzcan, las medidas de seguridad que deben aplicar y sobre los usos tolerados de la información. Además, deben seguir en todo momento las instrucciones dictadas por la universidad en cuanto al uso exclusivo de los medios disponibles y aplicar todas aquellas medidas de seguridad y organizativas que les sean dictadas.

En cuanto a la celebración de reuniones de órganos colegiados, el medio virtual introduce de igual modo una serie de obligaciones para los miembros de los órganos. Existe un deber de información, de aplicación de las instrucciones que al respecto se dicten por la universidad, aplicar las medidas de seguridad correspondientes y hacer uso exclusivamente de las herramientas autorizadas. Las universidades deberán establecer en su normativa los procedimientos organizativos y técnicos habilitantes de esta modalidad.

Las elecciones online suponen un reto para la Universidad, desde un punto de vista organizativo y de la seguridad de la información. La universidad debería contar con los procedimientos aprobados en normativa interna para que esta modalidad electoral cuente con la debida validez. validado.

Respecto a la investigación, debería prestarse atención al cumplimiento normativo por parte de los investigadores para aportar seguridad jurídica a sus estudios. Debería incidirse en la información que al respecto se les proporciona y aumentar la calidad y cantidad de formación al respecto.

Por último, la nueva normalidad ha impuesto una serie de obligaciones que escapan en cierto modo al ámbito universitario, y que corresponden mayormente al sanitario. La declaración de la enfermedad COVID-19 es una obligación del personal de la Universidad, no solo a los servicios de salud autonómicos, sino a la propia universidad para que pueda desplegar sus políticas de prevención, persistiendo en todo momento la obligación de preservación de la salud del resto de trabajadores y de la suya propia.