INFORME SOBRE LA COMPETENCIA CONSISTENTE EN EL ANÁLISIS Y TRATAMIENTO DE DATOS PERSONALES EN LAS PRACTICAS UNIVERSITARIAS

ANTECEDENTES:

En el proceso de acreditación de determinados títulos de grado y máster ante la Agencia Nacional de Evaluación de la Calidad y Evaluación (ANECA), la Universidad de las Hespérides ha recibido la notificación de ANECA indicando lo siguiente en relación con la competencia *"utilizar datos personales y confidenciales de las empresas a través de plataformas colaborativas en el desarrollo de la actividad empresarial":*

Se observa que la competencia específica "Utilizar y analizar datos personales y confidenciales de las empresas a través de plataformas colaborativas en el desarrollo de la actividad empresarial" puede no ser adquirida por todos los estudiantes ya que no es realista considerar que las empresas compartan sus datos personales y confidenciales a través de plataformas colaborativas debido a los requerimientos de seguridad y normativa de protección de datos.

Se echa en falta un hipervínculo que enlace con la normativa específica que tiene la universidad sobre de desarrollo de las prácticas académicas externas, que debe ser acorde a lo planteado en el artículo 11 del RD 822/2021.

CONTEXTO NORMATIVO ACADÉMICO

El Estatuto del Estudiante Universitario, aprobado por Real Decreto 1791/2010, de 30 de diciembre, reconoce en su artículo 8 el derecho de los estudiantes de Grado a «disponer de la posibilidad de realización de prácticas, curriculares o extracurriculares, que podrán realizarse en entidades externas y en los centros, estructuras o servicios de la Universidad, según la modalidad prevista y garantizando que sirvan a la finalidad formativa de las mismas» (apartado f) y a «contar con tutela efectiva, académica y profesional (…) en las prácticas externas que se prevean en el plan de estudios» (apartado g).

El Real Decreto 592/2014, de 11 de julio, por el que se regulan las prácticas académicas externas de los estudiantes universitarios indica en su exposición de motivos que se ha de promover la incorporación de estudiantes en prácticas en el ámbito de las administraciones públicas y en el de las empresas privadas, impulsando la empleabilidad de los futuros profesionales, fomentando su capacidad de emprendimiento, creatividad e innovación y dando respuesta al compromiso con la transformación económica basada en la sociedad del conocimiento.

El mismo Real Decreto define a la práctica externas en su artículo 2 como “una actividad de naturaleza formativa realizada por los estudiantes universitarios y supervisada por las Universidades, cuyo objetivo es permitir a los mismos aplicar y complementar los conocimientos adquiridos en su formación académica, favoreciendo la adquisición de competencias que les preparen para el ejercicio de actividades profesionales, faciliten

su empleabilidad y fomenten su capacidad de emprendimiento" (definición que también acoge en su artículo 11 el Real Decreto 822/2021, de 28 de septiembre, por el que se establece la organización de las enseñanzas universitarias y del procedimiento de aseguramiento de su calidad).

Asimismo, el citado RD 822/2021, recuerda que "el andamiaje" de la formación universitaria se focaliza en el *estudiantado* y en sus *competencias,* entendidas estas como el conjunto de conocimientos, capacidades y habilidades académicamente relevantes, que le confiere el título universitario alcanzado. Estas competencias, explica el RD, *permiten al estudiantado su inserción en el mundo laboral y, lógicamente, formar parte activa de la sociedad*.

Ello enlaza y tiene relación con los fines que de acuerdo con lo establecido en el RD 592/214 se pretende alcanzar con la realización de las prácticas, que son en definitiva, que el estudiantado obtenga una experiencia práctica que facilite la inserción en el mercado de trabajo y mejore su empleabilidad futura.

En conclusión: las prácticas universitarias forman parte de la formación universitaria y mediante estas prácticas se pretende que el estudiantado, como parte igualmente de su formación académica adquiera las competencias (conocimientos, capacidades y habilidades) que permitirán al estudiantado su inserción en el mundo laboral y, lógicamente, formar parte activa de la sociedad.

La normativa reguladora de dichas prácticas no recoge en todo caso ningún tipo de prohibición ni limitación al hecho de que el estudiantado, durante el ejercicio y realización de sus prácticas, accede y trate datos de carácter personal contenidos en ficheros y tratamientos responsabilidad de la entidad colaboradora que acoge al estudiante en prácticas.

EL CONTEXTO EUROPEO DE LA ACTIVIDAD PÚBLICA Y PRIVADA

En la Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre "Una Estrategia Europea de Datos" se pone de manifiesto que en los últimos años, las tecnologías digitales han transformado nuestra economía y nuestra sociedad, afectando a todos los sectores de actividad y a la vida diaria de todos los europeos. Los datos están en el centro de esta transformación.

La ciudadanía y los actores públicos o privados deben estar empoderados para tomar mejores decisiones sobre la base de los conocimientos que se desprenden de los datos y por tanto, estos datos deben estar disponibles para todos. Esto ayudará a la sociedad a sacar el máximo partido de la innovación y la competencia y a garantizar que todos se beneficien de un "dividendo digital".

La Comunicación insta a la Unión Europea (UE) a crear un entorno político atractivo a fin de que, de aquí a 2030, la cuota de la UE en la economía de los datos al menos se corresponda con su peso económico y ello no por imposición, sino por libre elección.

El objetivo es crear un espacio único europeo de datos, un verdadero mercado único de datos, abierto a datos procedentes de todo el mundo, en el que los datos personales y no personales, incluidos los datos sensibles de empresas, estén seguros y las empresas también tengan fácil acceso a una cantidad casi infinita de datos industriales de alta calidad, de manera que se impulse el crecimiento y se cree valor, minimizando al mismo tiempo la huella humana medioambiental y de carbono.

Debe ser un espacio en el que la legislación de la UE pueda aplicarse con eficacia y en el que todos los productos y servicios basados en los datos cumplan las normas pertinentes del mercado único de la UE. Al efecto, Europa ha de combinar una legislación y una gobernanza adaptadas al fin perseguido para garantizar la disponibilidad de datos, con inversiones en normas, herramientas e infraestructuras, así como en competencias para el manejo de los datos.

Asimismo, en el marco de la Estrategia Europea de Datos la Comisión Europea ha elaborado una propuesta de Reglamento relativo a la Gobernanza Europea de los Datos con el objetivo de ampliar la disponibilidad de los datos con miras a su utilización en condiciones proporcionadas, no discriminatorias y justificadas objetivamente habida cuenta de las categorías de datos, los fines de la reutilización y la naturaleza de los datos cuya reutilización se permita.

Esta propuesta completa la Directiva (UE) 2019/1024 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, relativa a los datos abiertos y la reutilización de la información del sector público (Directiva sobre datos abiertos), donde se explica con detalle como el sector público de los Estados miembros recoge, produce, reproduce y difunde una amplia gama de información en numerosos ámbitos de actividad, como el social, político, económico, jurídico, geográfico, medioambiental, meteorológico, sísmico, turístico, empresarial, educativo y de las patentes.

En el contexto explicativo de la propuesta, “razones y objetivos de la propuesta” se indica que el objetivo de este instrumento es ampliar la disponibilidad de datos con miras a su utilización, mediante el aumento de la confianza en los intermediarios de datos y el refuerzo de los mecanismos para el intercambio de datos en el conjunto de la Unión Europea, abordando por tanto las situaciones que se exponen a continuación:

- La cesión de datos del sector público para su reutilización, en los casos en que esos datos estén sujetos a derechos de terceros.
- El intercambio de datos entre empresas a cambio de algún tipo de remuneración.
- La cesión de datos personales con ayuda de un «intermediario de datos personales», cuya labor consistirá en ayudar a los particulares a ejercer los derechos que les confiere el Reglamento General de Protección de Datos.
- La cesión de datos con fines altruistas.

Por tanto, indica la propuesta, la interacción con la legislación sobre datos personales reviste especial importancia. En este sentido, existen técnicas que permiten realizar análisis, respetando la privacidad, en las bases de datos que contienen datos personales, como la anonimización, la seudoanonimización, la privacidad diferencial, la generalización, o la supresión y la aleatorización.

La aplicación de estas tecnologías de protección de la privacidad, junto con enfoques globales de protección de datos, garantiza la reutilización segura de los datos personales y los datos comerciales confidenciales con fines de investigación, innovación y estadísticos. En muchos casos, esto implica que la utilización y la reutilización de los datos en este contexto solo puedan realizarse en un entorno de tratamiento seguro creado y supervisado. De hecho, a nivel de la Unión, existe experiencia con estos entornos de tratamiento seguros que se utilizan para la investigación sobre microdatos estadísticos.

En este sentido, los documentos elaborados por los organismos del sector público de carácter ejecutivo, legislativo o judicial constituyen un conjunto amplio, diverso y valioso de recursos que pueden beneficiar a la sociedad puesto que, al ofrecer esta información, tanto las personas ciudadanas como las personas jurídicas pueden hallar nuevas formas de utilizarla y crear productos y servicios nuevos e innovadores.

El empleo inteligente de los datos, incluido su tratamiento a través de aplicaciones de inteligencia artificial, a buen seguro tendrá un efecto transformador en todos los sectores de la economía.

Por ello, Europa tiene claro que, en este escenario, se requiere una estructura de gobernanza que garantice la mayor participación de partes interesadas posible, esto es, a las organizaciones de consumidores e interlocutores sociales, empresas, investigadores y organizaciones de la sociedad civil, sobre la aplicación y futuro desarrollo del marco.

Además, esta estructura de gobernanza debe establecer vínculos estrechos con otras autoridades competentes nacionales y de la UE en los distintos sectores, a fin de completar los conocimientos técnicos y de ayudar a las autoridades actuales a controlar y supervisar las actividades de los agentes económicos en lo que respecta a los sistemas de inteligencia artificial y los productos y servicios provistos de inteligencia artificial.

En conclusión: Entre los objetivos de la Unión Europea está convertirse en líder de una sociedad impulsada por los datos, apoyándose en un mercado único digital donde los datos se compartan libremente entre los países miembros, lo cual hace que las competencias digitales y de tratamiento de datos sean un elemento relevante en la formación universitaria.

EL TELETRABAJO EN EL CONTEXTO DE LOS SECTORES PÚBLICO Y PRIVADO

Más localmente, en la exposición de motivos de la Ley 10/2021, de 9 de julio, de trabajo a distancia cuyo objeto es regular el trabajo a distancia que se preste por cuenta ajena así como el teletrabajo como forma de trabajo a distancia, explica que este sistema de trabajo está cogiendo auge frente a la organización empresarial tradicional, lo que sin duda trae consigo prácticas novedosas y más flexibles, estimula cambios organizativos en las empresas y fortalece la formación y empleabilidad de las personas trabajadoras.
En la misma línea, el Real Decreto-ley 29/2020, de 29 de septiembre, de medidas urgentes en materia de teletrabajo en las Administraciones Públicas y de recursos humanos en el Sistema Nacional de Salud para hacer frente a la crisis sanitaria

ocasionada por la COVID-19 introduce en el texto refundido de la Ley del Estatuto Básico del Empleado Público, un nuevo artículo 47 bis regulando el teletrabajo en la Administración Pública entendido este como aquella modalidad de prestación de servicios a distancia en la que el contenido competencial del puesto de trabajo puede desarrollarse, siempre que las necesidades del servicio lo permitan, fuera de las dependencias de la Administración, mediante el uso de tecnologías de la información y comunicación.

En este sentido, la propia exposición de motivos de dicha norma establece que la prestación del servicio a distancia mediante teletrabajo en el ámbito público fomenta así el uso de las nuevas tecnologías de la información y el desarrollo de la administración digital con las consiguientes ventajas tanto para las empleadas y empleados públicos, como para la administración y la sociedad en general prestando una especial atención a los deberes en materia de confidencialidad y protección de datos.

A mayor abundamiento, el Proyecto de Real Decreto por el que se regula el teletrabajo en la Administración del Estado y cuyo texto legal está sometido a trámite de información pública con fecha 15 de diciembre de 2021 explica que el compromiso adquirido con la transformación digital del sector público enmarcado en la estrategia España Digital 2025, así como la identificación de la Administración del Siglo XXI como una de las diez políticas palanca de reforma estructural para un crecimiento sostenible e inclusivo de las que se compone el Plan de Recuperación, Transformación y Resiliencia, evidencian cómo la generalización de los sistemas que permiten el teletrabajo supone un punto de partida sobre el que apoyar este impulso de la digitalización. Para hacer realidad esta transformación el teletrabajo constituye una herramienta clave, ya que contribuye a modernizar las formas de organización, a través de la fluidez de los intercambios de información y la comunicación en tiempo real por medios telemáticos, así como la gestión del espacio en entornos cada vez más flexibles; suponiendo además la introducción de formas de dirección orientada a la consecución de objetivos y la evaluación del rendimiento para la correcta supervisión del trabajo realizado en remoto.

Añade la exposición de motivos que únicamente podrán autorizarse las solicitudes de teletrabajo en el sector público de personas que cumplan los requisitos de situación administrativa, de antigüedad, o de *competencias digitales*. Todo ello sin perjuicio de otros requisitos que puedan fijar los departamentos ministeriales u organismos públicos o entidades de derecho público.

En todo caso, y de acuerdo con los textos reguladores vigentes, entre las obligaciones formales del acuerdo de trabajo a distancia tanto por la empresa o Administración Pública como por el personal teletrabajador debe garantizar que el tratamiento de la información facilitada estará sometido a los principios y garantías previstos en la normativa aplicable en materia de protección de datos.

Finalmente traemos a colación en este contexto laboral y estatutario de los sectores privado y público la exigencia establecida en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante LOPDGDD) ex artículo 83 “Derecho a la educación digital” a través del cual se exige que el sistema educativo garantice la plena inserción del alumnado en la sociedad digital y el aprendizaje de un uso de los medios digitales que sea seguro y respetuoso con la

dignidad humana, los valores constitucionales, los derechos fundamentales y, particularmente con el respeto y la garantía de la intimidad personal y familiar y la protección de datos personales.

En este sentido, mantiene el citado artículo que las Administraciones educativas deben incluir en el diseño del bloque de asignaturas de libre configuración la competencia digital a la que se refiere el apartado anterior, indicando en el apartado tercero que los planes de estudio de los títulos universitarios, en especial, aquellos que habiliten para el desempeño profesional en la formación del alumnado, garantizarán la formación en el uso y seguridad de los medios digitales y en la garantía de los derechos fundamentales en Internet (entre ellos claro está, el de la protección de los datos de carácter personal)[1].

En la misma línea, la Carta de los Derechos Digitales adoptada por el Gobierno de España, dispone en su apartado XVII "Derecho a la educación digital" *que el sistema educativo debe tender a la plena inserción de la comunidad educativa en la sociedad digital y un aprendizaje del uso de los medios digitales dirigido a una transformación digital de la sociedad centrada en el ser humano. [….] Se potenciará que el profesorado reciba formación para adquirir competencias digitales y para la enseñanza y transmisión de los valores y derechos referidos en el número anterior.*

La Carta, que no tiene valor normativo, sin embargo ofrece un marco de referencia para garantizar los derechos de la ciudadanía en la nueva realidad digital y tiene como objetivo reconocer los retos que plantea la adaptación de los derechos actuales al entorno virtual y digital.

En conclusión: La competencia digital así como la competencia consistente en utilizar y analizar datos personales es una competencia esencial en el contexto laboral tanto del sector privado como en el ámbito de la prestación de servicios públicos.

LA COMPETENCIA CONSISTENTE EN UTILIZAR Y ANALIZAR DATOS PERSONALES Y CONFIDENCIALES DE LAS EMPRESAS A TRAVÉS DE PLATAFORMAS COLABORATIVAS EN EL DESARROLLO DE LA ACTIVIDAD EMPRESARIAL EN EL CONTEXTO DE LA REALIZACIÓN DE PRÁCTICAS FORMATIVAS UNIVERSITARIAS

De acuerdo con la normativa reguladora de las prácticas universitarias, estas podrán realizarse en la propia universidad o en entidades colaboradoras, tales como, empresas, instituciones y entidades públicas y privadas en el ámbito nacional e internacional pudiendo incorporarse el estudiante a la plantilla de la entidad colaboradora al término de los estudios[2].

Visto todo lo expuesto anteriormente la competencia específica consistente en "*utilizar y analizar datos personales y confidenciales de las empresas a través de plataformas colaborativas en el desarrollo de la actividad empresarial*" deviene esencial en el

[1] Incluso en la misma línea el artículo 83 de la LOPDGDD en su apartado cuarto señala que las Administraciones Públicas incorporarán a los temarios de las pruebas de acceso a los cuerpos superiores y a aquéllos en que habitualmente se desempeñen funciones que impliquen el acceso a datos personales materias relacionadas con la garantía de los derechos digitales y en particular el de protección de datos.

[2] Sin que el tiempo de las prácticas se compute a efectos de antigüedad ni se exima el período de prueba salvo que en el oportuno convenio colectivo aplicable estuviera expresamente estipulado algo distinto.

contexto social y laboral actual y futuro y por tanto debe formar parte de los objetivos de las prácticas universitaria.

Ello además debe ponerse en relación con el hecho de que, de acuerdo con el RD 592/2014, entre sus fines, con la realización de las prácticas académicas externas se pretende que los estudiantes universitarios obtengan una experiencia práctica y las competencias y habilidades necesarias para facilitar su inserción en el mercado de trabajo y mejora de su empleabilidad futura.

La propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establece el programa Europa Digital para el periodo 2021-2027 expone que la transformación digital afecta a todos los sectores de la economía y transforma ámbitos clave de la sociedad para los próximos diez años como mínimo, a saber, la computación avanzada, el tratamiento de datos, la ciberseguridad y la inteligencia artificial. Por ello, la inversión en la adquisición de las capacidades más avanzadas en estos ámbitos, adquiriendo las competencias necesarias para desarrollarlas y utilizarlas, proporcionará un impulso esencial a la transformación digital de nuestras áreas de interés público y nuestra industria.

En el artículo 7 de la propuesta "Competencias digitales avanzadas" se indica específicamente que en el marco del Programa Europa Digital para el periodo 2021-2027 se contribuirá a la financiación del desarrollo de competencias digitales avanzadas en las áreas que reciban ayuda del citado programa, contribuyendo de este modo a aumentar la reserva de talento de Europa, fomentando una mayor profesionalidad, especialmente con respecto a la informática de alto rendimiento, el análisis de macrodatos, la ciberseguridad, la tecnología de cadena de bloques, la robótica y la inteligencia artificial. En consecuencia, la intervención financiera perseguirá los siguientes objetivos operativos:

a)favorecer la concepción e impartición de formación y cursos a largo plazo a estudiantes, profesionales informáticos y trabajadores en general;
b)favorecer la concepción e impartición de formación y cursos a corto plazo a empresarios, dirigentes de pequeñas empresas y trabajadores en general;
c)fomentar la formación en el puesto de trabajo y las prácticas para estudiantes, jóvenes empresarios y graduados.

El mercado de trabajo y empleabilidad futura por tanto va a requerir profesionales formados en el uso y tratamiento de información, incluidos datos personales, con conocimientos y habilidades en el marco normativo vigente en esta materia, incluida la normativa de datos personales.

Ello hace necesario que competencia específica consistente en "*utilizar y analizar datos personales y confidenciales de las empresas a través de plataformas colaborativas en el desarrollo de la actividad empresarial*" forme parte de los objetivos de las prácticas universitarias tanto en instituciones públicas como privadas.

El ejercicio de las prácticas universitarias para la adquisición de esta competencia es perfectamente viable tanto en el sector público como en el privado tanto se desarrollen estas de forma presencial como a través de medios y plataformas a distancia.

En la actualidad, tanto las empresas como las Administraciones Públicas ya disponen de herramientas de organización o realización del trabajo a distancia mediante el uso exclusivo o prevalente de medios y sistemas informáticos, telemáticos y de telecomunicación plenamente adaptados a los requerimientos de seguridad exigidos por la normativa de protección de datos de carácter personal.

De hecho, estas medidas de seguridad y confidencialidad no son exclusivas del trabajo a distancia o a través de plataformas y sistemas informáticos, telemáticos y de telecomunicación, sino que son exigencias derivadas de la normativa de protección de datos aplicables también al uso de sistemas de tratamiento de datos personales a nivel local[3] así como sistemas manuales o no automatizados. En definitiva, cualquier persona que, dentro de una organización pública o privada tenga acceso a datos personales, en su condición de "persona usuaria" de dichos datos está obligada a respetar todas las medidas de seguridad y confidencialidad que, el responsable del tratamiento de dichos datos (empresa privada o Administración Pública) haya establecido.

En estos términos, la vigente normativa sobre protección de datos de carácter personal constituida por el Reglamento General de Protección de Datos y la anteriormente citada LOPDGDD exige a los llamados responsables y encargados del tratamiento (esto es las empresas o Administraciones Públicas donde lo estudiantes realizan sus prácticas) el cumplimiento de una serie de principios en el tratamiento de los datos, como medida previa para que cualquier persona de su organización pueda acceder y tratar dichos datos personales en el marco de su actividad laboral, estatutaria o de prácticas, con independencia de que el acceso a los datos se realice por las personas usuarias a través de plataformas a distancia o soportes manuales (papel).

Estos principios que las entidades acogedoras de estudiantes en prácticas deben cumplir son los siguientes:

- *Responsabilidad del responsable del tratamiento:* 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 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 RGPD.

  Cuando sean proporcionadas se incluirá la aplicación, por parte del responsable del tratamiento, de las oportunas políticas de protección de datos.

- *Protección de datos desde el diseño y por defecto*: Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la

[3] Es decir, en el propio entorno interno de la organización.

minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del RGPD y proteger los derechos de los interesados.

El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento.

Esta obligación se aplicará a la cantidad de datos personales recogidos, (i) a la extensión de su tratamiento, (ii) a su plazo de conservación y (iii) a su accesibilidad.

Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas.

- *Seguridad del tratamiento*: Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

  a)la seudonimización y el cifrado de datos personales;

  b)la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;

  c)la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;

  d)un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

  Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

Pero las obligaciones de confidencialidad de los datos personales, no solo recaen sobre el llamado “responsable del tratamiento” sino que el propio RD 592/2014 establece que entre los deberes de los estudiantes (artículo 9.2.g) está el de guardar confidencialidad en relación con la información interna de la entidad colaboradora y guardar secreto profesional sobre sus actividades, durante su estancia y finalizada esta y entre los deberes del tutor de la entidad colaboradora (artículo 11.2.c, g y k) está (i) el de informar al estudiante de la organización y funcionamiento de la entidad y de la normativa de interés, (ii) proporcionar al estudiante los medios materiales indispensables para el desarrollo de la práctica y (iii) prestar ayuda y asistencia al estudiante, durante su

estancia en la entidad, para la resolución de aquellas cuestiones de carácter profesional que pueda necesitar en el desempeño de las actividades que realiza en la misma.

Este deber de confidencialidad que se exige al estudiante en prácticas presupone por tanto que este tendrá acceso a información confidencial de la empresa (incluyendo aquella que contenga datos personales) y se le exige, no solo durante su estancia y sino también, finalizada esta.

En conclusión: Tanto la normativa de protección de datos como la normativa que regula las prácticas universitarias contemplan un marco legal que permite el tratamiento de datos personales y otras informaciones de carácter confidencial empresarial por parte del estudiantado, previa implantación de medidas de seguridad de carácter técnico y organizativo las cuales, en todo caso suponen una exigencia legal para las partes intervinientes (empresa, universidad y estudiante).

La adquisición de esta competencia deviene esencial en el contexto social y económico actual donde como se ha visto, el mercado de trabajo y empleabilidad futura requiere de profesionales formados en el uso y tratamiento de información, incluidos datos personales, con conocimientos y habilidades en el marco normativo vigente en esta materia, incluida la normativa de datos personales.

GUÍA SOBRE PROTECCIÓN DE DATOS PARA ESTUDIANTES QUE REALIZAN PRÁCTICAS EXTERNAS

El pasado 4 de noviembre de 2019, la Universitat de València y la Cátedra de Privacidad y Transformación Digital Microsoft-UV presentaron la «Guía sobre protección de datos para estudiantes que realizan Prácticas Externas».

[4]Esta guía, desarrollada por Ricard Martínez, director de la Cátedra, en colaboración con los vicerrectorados de Empleo y Programas Formativos, de Innovación y Transferencia y de Estudios y Política Lingüística, y con el soporte técnico del Instituto de Robótica, explica que su objetivo esencial es aportar un elemento adicional de formación para las y los estudiantes universitarios en prácticas y su utilidad alcanza a todo el estudiantado del país en cualquier nivel educativo, ofreciendo indicaciones sobre cómo los estudiantes deben cumplir con sus deberes en materia de protección de datos en el desarrollo de la actividad de prácticas tanto en entidades privadas como públicas.

Su segundo objetivo consiste en concienciar sobre la garantía de los derechos de las personas cuyos datos eventualmente pudieran tratar durante sus prácticas y entre otros fines, busca informar a los estudiantes sobre los riesgos y expone las razones en las que se basa su necesaria implicación, formándole en el conocimiento de sus obligaciones básicas. El documento presta una particular atención a situaciones en las que pueden existir riesgos significativos y trata de concienciar respecto de la especial significación que tiene el acceso a datos especialmente protegidos en el sector de la salud, de las

[4] Fuente: https://www.uv.es/uvweb/catedras-institucionales/es/novedades-del-departamento/catedra-privacidad-transformacion-digital-microsoft-uv-presenta-guia-proteccion-datos-estudiantes-realizan-practicas-externas-1285923261505/Novetat.html?id=1286101162499

implicaciones de tratar datos de menores en edad escolar y, finalmente, sobre la especial trascendencia que tienen algunos desempeños profesionales como los despachos de abogados.

El desarrollo de esta Guía se enmarca en las actividades vinculadas al programa de cátedras institucionales de la Universitat de València, cubriendo una necesidad en la formación y supone una manifestación de la responsabilidad proactiva de la Universitat en la formación y preparación de sus estudiantes en prácticas y ha contado con la colaboración de distintas universidades y de otras instituciones.

En dicha guía, publicada en la página web institucional de la Universitat de València con una licencia Creative Commons[5], se informa al estudiante de cuestiones como las siguientes:

1.-¿Por qué deberías leer esta Guía?

Vivimos en una época de transformación digital. La sociedad de nuestro tiempo funciona gracias al procesamiento masivo de datos personales y de todo tipo de información complementaria.

[…] cuando nos insertamos en un entorno laboral pasamos al otro lado, tratamos datos de los demás asumimos ciertos compromisos legales y se espera de nosotros la capacidad de manejar adecuadamente los datos personales y garantizar la seguridad de la información corporativa.

4.- ¿Tengo derechos en protección de datos? ¿Y obligaciones?

[…] *se imponen deberes a las personas que trabajan y/o prestan un servicio en la organización para asegurar un tratamiento adecuado de los datos. Si en el marco de tus prácticas no cumples con estas obligaciones pones en peligro a la empresa y a los derechos de los clientes. En los siguientes apartados exponemos algunos de estos deberes que te afectarán durante tus prácticas.*

5*.-¿Por qué debo guardar secreto?*

El deber de secreto se exige prácticamente en todas las profesiones. Este secreto que se exige al funcionario, al trabajador, o al profesional o al estudiante en prácticas cumple funciones muy diversas.

El secreto puede ser fundamental para la supervivencia de la empresa. Así, cuando nos insertamos en un entorno laboral en el que existe algún tipo de I+D+i (investigación, desarrollo e innovación), o cuando se obtienen ventajas competitivas por adoptar cierto tipo de procesos o localizar a determinados proveedores, o cuando se va a lanzar un nuevo producto, el secreto puede ser crucial para la supervivencia de la organización. Si asistes a una reunión estratégica de la empresa, o a un curso de formación sobre una nueva actividad o producto, o te encuentras en un lugar restringido y por ejemplo publicas un tuit, una foto en Instagram, o un comentario en una red social, o te

[5] Permite su reutilización por todo el sector educativo nacional previa mención de su autor.

geolocalizas ofreciendo información a terceros, podrías estar filtrando sin querer información muy valiosa para la competencia. En otras ocasiones, es la propia naturaleza de la actividad la que exige ese deber de secreto. En el ejercicio de funciones públicas las personas que prestan sus servicios en la Administración tienen un deber de secreto. […] Si mientras realizas prácticas en una clínica, alguien llama por teléfono y le facilitas información sobre el paciente o se la proporcionas a un tercero sin verificar que está autorizado, estás vulnerando el derecho a la intimidad de la persona enferma.

*En protección de datos también existe deber de secreto. Y este resulta más exigente incluso que los anteriores. Este derecho afecta a cualquiera que trate datos personales, esto es, es cualquier tipo de información referida a una persona identificada o identificable. Por tanto, no depende ni del tipo de empresa, ni de su actividad, ni del tipo de dato, ni de tu perfil profesional. Basta con el simple hecho de que accedas a datos para tener que cumpl*ir con este deber.

6.-¿Para qué sirve la seguridad?

Uno de los recursos estratégicos que maneja toda organización es la información, tanto personal como de cualquier otra naturaleza. Cada vez es más común apreciar que lo verdaderamente valioso no se encuentra tanto en un plano físico o material sino en algo tan intangible como la información y el conocimiento.

[…] En la seguridad el elemento más importante, y también el eslabón más débil, son los usuarios, las personas. En el desarrollo de tus prácticas debes prestar mucha atención y aplicar rigurosamente las políticas de seguridad de la entidad. Antes de empezar la actividad pregunta por ellas si no te las han proporcionado.

7.-¿Cómo puedo contribuir a cumplir el RGPD y la LOPDGDD y garantizar la seguridad? ¿Cuáles son mis obligaciones?

Al integrarnos en el equipo de trabajo de una organización asumimos un conjunto de obligaciones. Es posible que nuestro lugar de prácticas cuente con un protocolo de bienvenida o de formación. Si es así, debemos prestar la mayor atención e interiorizar las normas y procedimientos de actuación establecidos.

En cualquier caso, existe un conjunto de medidas de seguridad que deberíamos conocer y aplicar, ya que responden al sentido común.

A continuación, se enumeran algunas de ellas.

Acceso a instalaciones Deberemos respetar las prohibiciones de acceso si las hubiera, limitarnos a nuestros permisos y, en todo caso, aplicar las condiciones que existan para ello. No es inusual que el acceso a las zonas de archivo clínico o el emplazamiento del equipamiento informático resulte restringido. En ocasiones, en función de la naturaleza de la información, podrían existir reglas de actuación como, por ejemplo, no apagar ciertos equipos, o no introducir un Smartphone con cámara. Cuando necesitemos acceder a un área restringida, seguiremos siempre los procedimientos internos para obtener autorización.

Controles de acceso lógico En nuestra incorporación lo usual debería ser que nos asignen permisos de acceso a los sistemas de información, habitualmente mediante algún tipo de validación de usuario y contraseña. Estas claves suelen ser facilitadas por algún responsable de la entidad y deberían ser individuales. Al usarlas debemos acceder exclusivamente a los recursos y sistemas autorizados y únicamente desde el puesto o terminal asignados. […]. Debemos proteger nuestra contraseña, no compartirla nunca, cambiarla periódicamente o cuando se nos requiera, y activar contraseñas seguras.

Acceso remoto y dispositivos propios Si está prevista alguna fórmula de teletrabajo con acceso remoto a los sistemas de información, o si se permite llevar a casa dispositivos portátiles o usar los propios, debemos extremar la seguridad. Es preferible que la información permanezca en el sistema de la empresa o en el del proveedor autorizado. Debemos renunciar a prácticas de riesgo con estos dispositivos, como compartirlos con terceros, instalar software no verificado, llevarnos información en un pendrive para seguir trabajando en casa, o usar programas peer to peer.

En definitiva y puesto que no están limitadas las prácticas formativas a través de medios a distancia o plataformas colaborativas o de trabajo, la propia guía partiendo de este punto advierte al estudiante de su obligación de garantizar y extremar la seguridad en estos casos

CONCLUSIONES

Primera.- Las prácticas académicas externas constituyen una actividad de naturaleza formativa realizada por los estudiantes universitarios y supervisada por las Universidades, cuyo objetivo es permitir a los mismos aplicar y complementar los conocimientos adquiridos en su formación académica, favoreciendo la adquisición de competencias que prepare al estudiantado para el ejercicio de actividades profesionales, faciliten su empleabilidad y fomenten su capacidad de emprendimiento.

Segunda.- Las tareas que desarrollará el estudiantado durante el curso de las prácticas contribuirán a su formación integral como complemento de su aprendizaje teórico y práctico, a facilitar el conocimiento de la metodología de trabajo adecuada a la realidad profesional, a favorecer el desarrollo de competencias técnicas, metodológicas, personales y participativas, y a favorecer los valores de innovación, creatividad y emprendimiento. En todo caso, la finalidad última de las prácticas será obtener una experiencia práctica que facilite la inserción en el mercado de trabajo y mejore su empleabilidad futura.

Tercera.- Es la empresa quien determina la modalidad de las prácticas y adopta las medidas y logística necesarias para la preparación implementación y el correcto desarrollo de las prácticas del estudiantado.

Cuarta.- La actividad del estudiantado en prácticas se ajustará a un proyecto formativo que procure que el estudiante ponga en práctica sus conocimientos asumiendo tareas y responsabilidades acordes con su cualificación y experiencia, y pudiendo tener como objetivo la competencia específica de utilizar y analizar datos personales y

confidenciales de las empresas a través de plataformas colaborativas en el desarrollo de la actividad empresarial.

Quinta.- La información que las empresas pueden poner a disposición del estudiantado está protegida por diversas norma legales que a título general caracterizan o definen la información como confidencial y sujeta al deber de secreto pero, en particular, centramos nuestro interés en tres normas como son Ley de Secretos Empresariales, el Reglamento General de Protección de Datos y la Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales.

Sexta.- Ninguna de estas tres normas es impeditiva del acceso a la información protegida por parte de personas que forman parte de una organización (personal laboral, estatutario o en prácticas universitarias) y por tanto, ninguna de estas tres normas es impeditiva de la realización de prácticas formativas que requieran el tratamiento de datos personales (a través de cualquier medio y forma que determine la empresa) ni impeditiva de la adquisición de la competencia específica consistente en uutilizar y analizar datos personales y confidenciales de las empresas a través de plataformas colaborativas en el desarrollo de la actividad empresarial.

Séptima.- Tanto las normas citadas en la conclusión quinta como los reales decretos que regulan las practicas universitarias, establecen "*obligaciones de hacer"* consistentes en la implantación de medidas de seguridad y "*obligaciones personales"* consistentes en el deber de secreto así como otro tipo de medidas de carácter organizativo para garantizar la seguridad y la confidencialidad de los datos, protegiendo así, en particular, los datos de carácter personal.

Octava.- Estas obligaciones de seguridad y confidencialidad no se exigen en virtud del medio de acceso a los datos (plataformas colaborativas, técnicas de comunicación a distancia, o soportes manuales) sino que son aplicables a cualquier medio de acceso y tratamiento de los datos personales. Por tanto, se aplicarán tanto en el caso en que las prácticas universitarias se realicen a distancia como in situ en las organizaciones.

Novena.- No parece realista considerar que la competencia específica consistente en "*utilizar y analizar datos personales y confidenciales de las empresas a través de plataformas colaborativas en el desarrollo de la actividad empresarial*" no puede ser adquirida por los estudiantes porque las empresas establezcan impedimentos en cuanto a la compartición de sus datos personales y confidenciales a través de plataformas colaborativas debido a los requerimientos de seguridad y normativa de protección de datos, puesto que como se ha visto, la normativa de protección de datos no contiene ningún impedimento y además es igualmente aplicable a cualquier otra forma de trabajo a distancia o teletrabajo tanto en organizaciones públicas como privadas.

En este sentido, las organizaciones que acojan estudiantes en prácticas están obligadas a garantizar la seguridad de los datos a los que dichos estudiantes accedan, cualquiera que sea la modalidad o forma de acceso a los mismos que la empresa haya establecido.

La empresa es quien decide el nivel de acceso a los datos aplicando las medidas de seguridad que correspondan en las bases de datos que contienen datos personales,

como la anonimización, la seudoanonimización, la privacidad diferencial, la generalización, o la supresión y la aleatorización.

Hay casos donde la adquisición de esta competencia durante la realización de prácticas no deja lugar a dudas, como es el caso de la realización de prácticas en empresas de base tecnológica y startups. Véase que, de acuerdo con el proyecto de Ley de fomento del ecosistema de las empresas emergentes aprobado por el Gobierno de España, estas empresas emergentes favorecen especialmente el establecimiento teletrabajadores y "nómadas digitales" y fomentan la colaboración con las administraciones públicas, las universidades, organismos públicos de investigación y centros tecnológicos, previéndose la creación de sandboxes o licencias de pruebas en sectores regulados, respondiendo a la singularidad de este tipo de empresas y a las principales demandas del sector.

Décima.- La propia autoridad de control española, la AEPD, en su doctrina reconoce el teletrabajo como una fórmula de organización de la actividad del trabajo en las empresas que si bien se extendió durante la primera ola de la pandemia de la COVID-19, en la actualidad se ha consolidado en muchas empresas.

Así lo manifiesta la AEPD en el artículo publicado en su blog "Teletrabajo y protección de datos en el ámbito digital" al manifestar lo siguiente:

La situación excepcional derivada de la pandemia de la COVID-19 hace ya más de un año puso sobre la mesa de toda clase de organizaciones la urgente necesidad de un cambio no programado en los modelos de negocio tradicionales. Una de las más importantes fue la puesta en marcha de políticas del teletrabajo. En cuestión de pocas semanas fue necesario tomar decisiones a corto plazo y hacer uso intensivo de accesos remotos, plataformas online y virtualizando las relaciones laborales. Lo que se presuponía temporal se ha quedado, cuanto menos de forma parcial, en buena parte de las entidades, dando paso a un nuevo modelo económico que forma parte de la digitalización.

Décimo primera.- No podemos olvidar que, entre los objetivos de la Unión Europea está convertirse en líder de una sociedad impulsada por los datos, apoyándose en un mercado único digital donde los datos se compartan libremente entre los países miembros, lo cual hace que las competencias digitales y de tratamiento de datos sean un elemento relevante en la formación universitaria para la capacitación e inserción de los estudiantes en el mercado laboral. Competencias que lógicamente serán adquiridas no solo en el proceso de estudio sino también en el proceso de las prácticas.

Décimo segunda.- Añadido a lo anterior, la LOPDGDD exige que el sistema educativo garantice la plena inserción del alumnado en la sociedad digital y el aprendizaje de un uso de los medios digitales que sea seguro y respetuoso con la dignidad humana, los valores constitucionales, los derechos fundamentales y, particularmente con el respeto y la garantía de la intimidad personal y familiar y la protección de datos personales.

Décimo tercera.- En la misma línea, la Carta de los Derechos Digitales elaborada por el Gobierno de España dispone que el sistema educativo debe tender a la plena inserción de la comunidad educativa en la sociedad digital y un aprendizaje del uso de los medios

digitales dirigido a una transformación digital de la sociedad centrada en el ser humano potenciándose que el profesorado reciba formación para adquirir competencias digitales y para la enseñanza y transmisión de los valores y derechos fundamentales, entre los cuales se encuentra, el derecho fundamental a la protección de datos.

Décimo cuarta.- En consecuencia, la competencia digital así como la competencia consistente en utilizar y analizar datos personales es una competencia esencial en el contexto laboral tanto del sector privado como en el ámbito de la prestación de servicios públicos.

Décimo quinta.- Entre las medidas que la Universidad de las Hespérides contempla para garantizar que las prácticas se lleven a cabo con todas las garantías y exigencias legales en materia de seguridad y confidencialidad de los datos personales, se encuentran las siguientes:

- Firma del Convenio de Cooperación Educativa con la entidad colaboradora (empresa privada o Administración Pública) con la inclusión del deber de confidencialidad exigible al estudiante.

- Entrega de la información necesaria al estudiante al respecto de la organización y funcionamiento de la entidad y de la normativa de interés, especialmente en materia de seguridad y confidencialidad de la información y datos personales que pueda conocer en el ejercicio de su prácticas formativas.

- Aportación de la "Guía sobre protección de datos para estudiantes que realizan prácticas externas" que recoge las recomendaciones sobre los aspectos básicos relativos a la protección de datos y en particular a la seguridad y confidencialidad de los datos personales que deben cumplir los estudiantes en prácticas.

  Dicha guía ha contado además con la colaboración de distintas universidades[6] y de otras instituciones y está publicada en la página web institucional de la Universitat de València con una licencia Creative Commons que permite su reutilización por todo el sector educativo nacional.

  La guía supone una manifestación de la responsabilidad proactiva de las universidades usuarias de la misma en la formación y preparación de los estudiantes en prácticas.

- Elaboración de políticas y normativas específicas de desarrollo de las prácticas académicas externas, que será aprobada por los órganos de gobierno de la Universidad de las Hespérides, relacionadas con el cumplimiento de los principios de protección de datos en el tratamiento de datos personales y normas de confidencialidad y seguridad de la información.

[6] Universitat de Valencia, Universidad de Alcalá, Universidad de Burgos, Universidad de La Laguna, Universitat Jaume I, Universidad de Murcia, Universitat de Lleida, Universidad de Oviedo, Universidad Politécnica de Valencia, Universidad de La Rioja, Universidad de Salamanca.