VISIÓN PRACTICA DE LA PROTECCIÓN DE DATOS EN UN DEPARTAMENTO DE RECURSOS HUMANOS

Máster de Dirección de Recursos Humanos.

Escuela de Posgrado y Doctorado

Universidad de La Laguna

Curso 2020-2021 convocatoria Septiembre

Autoras: Isabelle R. Camesella Duarte y Silvia Rodríguez Maestre

Tutorizado por el profesor: D. Luis Fajardo López

RESUMEN

Con la entrada en vigor del Reglamento UE 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de personas físicas en lo que respecta al tratamiento de datos personales y la libre circulación de estos datos y por la que se deroga la Directiva 95/46 CE, comúnmente denominado como Reglamento General de Protección de Datos, los países miembros de la unión Europea se enfrentan a un cambio en la gestión de la Protección de Datos.

En el caso de España, se adecúan las normas existentes, se aprueba la Ley Orgánica de Protección de Datos y Garantías de los Derechos Digitales y la Agencia Española de Protección de Datos toma un papel más relevante en el que algunas de sus prácticas más importantes hasta ese momento pasan al texto de esta última norma, tratando de acercar a la ciudadanía esta legislación a la vez que realiza un seguimiento de su cumplimiento.

Este trabajo trata de realizar un acercamiento a los aspectos más relevantes del régimen jurídico relativo a la Protección de Datos, especialmente en aquellos elementos más relevantes desde la óptica de los Recursos Humanos.

ABSTRAC

With the entry into force of EU Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and the free movement of such data and repealing Directive 95/46 EC, commonly known as the General Data Protection Regulation, the member countries of the European Union are faced with adapting their legislation to it.

In the case of Spain, the existing regulations are being adapted, a new Organic Law on Data Protection and Digital Guarantees is being created and, through the Spanish Data Protection Agency, an attempt is being made to bring this legislation closer to the public while monitoring compliance with it.

This work attempts to approach the most relevant aspects of the legal regime relating to Data Protection, especially those elements that are most relevant from the perspective of Human Resources.

With the entry into force of EU Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and the free movement of such data and repealing Directive 95/46 EC,

commonly known as the General Data Protection Regulation, the member countries of the European Union are facing a change in the management of Data Protection.

In the case of Spain, the existing regulations were adapted, the Organic Law on Data Protection and Guarantees of Digital Rights was passed and the Spanish Data Protection Authority took on a more relevant role in which some of its most important practices up to that time were included in the text of the new legislation, trying to bring this regulation closer to the citizens while monitoring its compliance.

This work attempts to approach the most relevant aspects of the legal regime relating to Data Protection, especially those elements that are most relevant from the point of view of Human Resources.

PALABRAS CLAVE

Protección de datos, Responsable del tratamiento, Encargado de tratamiento, Tratamiento de datos personales, Registro de Actividades de tratamiento, datos personales.

KEYWORDS

Data Protection, Data Controller, Data Processor, Personal Data Processing, Register of Processing Activities, Personal Data

ÍNDICE

Contenido

ABREVIATURAS

AEPD: Agencia Española de Protección de Datos

C.E.: Constitución Española

EAC: Estatuto de Autonomía de Canarias, reformado por Ley Orgánica 1/2018, de 5 de noviembre.

LET: Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores

LOPD: Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

LOPDgdd: Ley Orgánica 3/ 2018 de 5 de diciembre de Protección de Datos personales y de garantía de los derechos digitales

RGPD: Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)

RRHH: Recursos Humanos

1. INTRODUCCIÓN

Es la segunda década del siglo XXI el mundo se encuentra inmerso en la era digital, que rige todo tipo de procedimientos, actuaciones e incluso relaciones sociales.

Debido a ello, los diferentes ordenamientos jurídicos han tratado de irse actualizando, en un mundo en el que todo cambia mucho más rápido de lo esperado. En palabras de José Luís Rodríguez Álvarez[1] se esperaba que los datos fuesen el petróleo de esta nueva era, sin embargo, esas predicciones ya han sido superadas, teniendo en cuenta que en el año 2018 las cuatro mayores empresas digitales del mundo superaron a las inversiones realizadas por las cuatro mayores compañías petroleras, poniendo así de manifiesto la denominada datificación de las sociedades.

Esto nos lleva a pensar que los datos que fluyen por la red, no solo aportan beneficios a los usuarios que las utilizan, pudiendo mejorar su forma de trabajar, de estudiar, de investigar o de incluso relacionarse, sino que comportan un gran beneficio económico. Las empresas que ofrecen el servicio para explotar económicamente los datos recabados con éste, en lo que se viene a denominar capitalismo de la vigilancia.

En palabras de Shoshana Zuboff, "el capitalismo de la vigilancia reclama unilateralmente para sí la experiencia humana, entendiéndola como una materia prima gratuita que puede traducir en datos de comportamiento. Aunque algunos de dichos datos se utilizan para mejorar productos o servicios, el resto es considerado como un excedente conductual privativo («propiedad») de las propias empresas capitalistas de la vigilancia y se usa como insumo de procesos avanzados de producción conocidos como inteligencia de máquinas, con los que se fabrican productos predictivos que prevén lo que cualquiera de ustedes hará ahora, en breve y más adelante. Por último, estos productos predictivos son comprados y vendidos en un nuevo tipo de mercado de predicciones de comportamientos que yo denomino mercados de futuros conductuales. Los capitalistas de la vigilancia se han enriquecido inmensamente con esas operaciones comerciales, pues son muchas las empresas ansiosas por apostar sobre nuestro comportamiento futuro".[2]

[1]RODRÍGUEZ ÁLVAREZ, J.L. y FAJARDO LÓPEZ, L. "La defensa de libertades ante la vigilancia y tratamiento masivo de datos", XII Congreso Nacional de la Abogacía, Consejo General de la Abogacía Española, 2019 (material de acceso restringido, cedido por el ponente para este trabajo). Otras referencias: Abogacía (Revista del Consejo General de la Abogacía Española), n.º 115, mayo 2019.

[2] ZUBOFF, S., *La era del capitalismo de la vigilancia*, Paidós (2020, Spanish edition) p.11 y s.s

En base a ello, la sociedad y por ende las empresas y la ciudadanía, se encuentra ante una nueva forma de gestionar los datos que maneja, especialmente aquellos de carácter personal y de ahí la intencionalidad de este TFM de realizar un acercamiento a las diferentes normativas relacionas con la protección de datos de carácter personal, específicamente en el ámbito de los Recursos Humanos (en adelante, RRHH), donde existe una gran amplitud de gestiones que conllevan la recepción, manejo y envío de datos sensibles de las personas que desarrollan su actividad en una determinada empresa. Es por ello, que el objetivo que se persigue es crear una pequeña guía que fuera de utilidad para los departamentos de RRHH, llegando a concretar las cuestiones prácticas de implementación de esta normativa.

2. LA PROTECCIÓN DE DATOS EN EL ORDENAMIENTO JURÍDICO ESPAÑOL

El derecho a la protección de datos no aparece recogido como tal, en la Constitución Española de 1978 (en adelante, C.E)[3], sin embargo, sí que la norma fundamental del Ordenamiento Jurídico español reconoce en su artículo 18.1 que "se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen" estando dichos conceptos, íntimamente ligados al concepto de protección de datos de carácter personal. Así mismo cabe destacar como en el apartado 4 de dicho artículo se establece 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."

Con todo ello, si bien podemos observar que no existe mención expresa al derecho fundamental a la protección de datos personales, sí que el Tribunal Constitucional ha sido el encargado de construir este precepto mediante sentencias, pudiendo destacar la Sentencia 292/2000 de 30 de noviembre en la que en su fundamento jurídico número 7 establece que "De todo lo dicho resulta que el contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular. Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos.

En fin, son elementos característicos de la definición constitucional del derecho fundamental a la protección de datos personales los derechos del afectado a consentir

[3] Publicada en el BOE número 311 de 29 de diciembre de 1978

sobre la recogida y uso de sus datos personales y a saber de los mismos. Y resultan indispensables para hacer efectivo ese contenido el reconocimiento del derecho a ser informado de quién posee sus datos personales y con qué fin, y el derecho a poder oponerse a esa posesión y uso requiriendo a quien corresponda que ponga fin a la posesión y empleo de los datos. Es decir, exigiendo del titular del fichero que le informe de qué datos posee sobre su persona, accediendo a sus oportunos registros y asientos, y qué destino han tenido, lo que alcanza también a posibles cesionarios; y, en su caso, requerirle para que los rectifique o los cancele."[4]

En base a Sentencias del Tribunal Constitucional relativas a la protección de datos, así como al desarrollo de normas en base a ello, nuestro ordenamiento jurídico ha demostrado una vez más su capacidad de no quedar obsoleto ante situaciones inexistentes en el momento de la creación de la propia Constitución.

Debido a la rapidez con la que ha ido avanzando la denominada era digital, ha sido necesario crear normas que se traten de ajustar a la realidad. Así hemos visto en breve tiempo (para la estabilidad habitual de las normas) tres leyes reguladoras de la protección de datos de carácter personal: La Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal[5]; la Ley Orgánica de 15/1999 de 13 de diciembre de Protección de datos de carácter personal (conocida como LOPD)[6], y la vigente Ley Orgánica 3/ 2018 de 5 de diciembre de Protección de Datos personales y de garantía de los derechos digitales (LOPDgdd)[7].

El ámbito regulatorio de esta materia es de carácter europeo, siendo la norma de mayor rango el Reglamento UE 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de personas físicas en lo que respecta al tratamiento de datos personales y la libre circulación de estos datos y por la que se deroga la Directiva 95/46 CE (Reglamento General de Protección de Datos)[8], y al que nos referiremos como RGPD.

[4] STC 292/2000, de 30 de noviembre, (Recurso número 1.463/2000) FJ 7º.
[5] Publicada en el BOE número 262 de 31 de octubre de 1992
[6] Publicada en el BOE número 298 de 14 de diciembre de 1999
[7] Publicada en el BOE número 294 de 6 de diciembre de 2018
[8] Publicado en DOUE número 119 de 4 de mayo de 2016

El RGPD, define un nuevo marco de garantía y tutela de tan importante derecho fundamental[9] y sustituyó a todas las disposiciones de la LOPD contrarias al mismo vigente en ese momento y cualquier otro derecho nacional que entrara en conflicto con este. Para complementar al RGPD, se aprueba la LOPDgdd, antes referida, sobre las que ahondaremos a lo largo de este trabajo, ya que regula específicamente algunos derechos en relación a la protección de datos personales en el ámbito laboral e incorpora a nuestro ordenamiento jurídico un nuevo derecho digital de contenido laboral como es el derecho a la desconexión digital, todo ello parte de estudio de este trabajo.

Haciendo un recorrido por la legislación relacionada con la protección de datos, cabe destacar su inclusión en el Estatuto de Autonomía de Canarias aprobado por la Ley Orgánica 1/2018 de 5 de noviembre[10] (en adelante, EAC), concretamente en su Título I, Capítulo II, dedicado a los Derechos y Deberes. En el artículo 30 de dicha norma, establece a tenor literal "Se garantiza el derecho efectivo de todas las personas la privacidad y protección de sus datos personales contenidos en archivos y ficheros que son competencia de las administraciones públicas canaria, así como el derecho a acceder a los mismos, a su examen, corrección y cancelación".

En este caso, se observa como el estatuto canario, siguiendo la senda comenzada por los Estatuto valenciano y catalán[11], denominados de nueva generación, inserta en su norma institucional básica nuevos derechos, entre los que se encuentran recogidos los relacionados con la protección de datos.

El hecho de que el EAC ancle la protección de datos en el Capítulo II del Título I, hace que no quede como un principio rector, sino que se trate de un auténtico derecho, ejercitable frente a las Administraciones Públicas canarias y que conlleva para la ciudadanía la posibilidad de acudir a los Tribunales en caso de entender vulnerados tales derechos.

Todo ello conlleva a las Administraciones Públicas canarias, no solo a adecuar su actuación sino, a garantizar la protección de los datos que utiliza en ellas. [12]

---

[9] PIÑAR MAÑAS, J.L.,"Reglamento General de Protección de Datos, hacia un nuevo modelo europeo de privacidad"1º ed., Reus (Madrid, 2016) pag 19-20

[10] Publicado en el BOE número 268 de 6 de noviembre de 2018

[11] Artículo 31 del Estatuto catalán, aprobado por L.O. 6/2006, de 19 de julio (BOE n.º 172, del 20).

[12] FAJARDO LÓPEZ, L.: "Título I. Capítulo II. Derechos y deberes; artículos de 25, 28 Y 30", en AA.VV. (SUAY RINCÓN, J. VILAR ROJAS, F.) *El Estatuto de Autonomía de Canarias, Ley Orgánica 1/2018, de 5 de noviembre, 1ºed., Ed. Aranzadi, Navarra,2019, pág. 164-173*

Teniendo en cuenta que este trabajo se realiza desde una óptica basada en los Recursos Humanos, se hace necesario comprender la relación existente entre todas las normas citadas anteriormente y el Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores[13] (en adelante, LET) ya que se trata de la principal norma de aplicación en el ámbito laboral. El LET establece en su artículo 1 que la aplicación de esta norma es dentro del ámbito de organización y dirección del empresario o empleador, por lo que podemos deducir que dentro de los márgenes de este ámbito, el empleador tendrá capacidad para tomar ciertas decisiones, sin embargo, cabe destacar que la normativa laboral no exime del cumplimiento de la normativa relativa a la Protección de Datos, ni viceversa.

Tal y como veremos, existen ciertos flujos de información de datos personales, que no quedan a disposición de las partes, sino que son de carácter obligatorio para poder desarrollar la actividad laboral y que por tanto *de facto* legitiman al empresario o empleador a su uso.

Debido a su importancia, es necesario mencionar a la Agencia Española de Protección de Datos (en adelante, AEPD) al ser la autoridad pública independiente encargada de velar por el cumplimiento de la normativa sobre protección de datos. Garantiza y tutela el derecho fundamental a la protección de datos de carácter personal de los ciudadanos".[14] Esta autoridad se creó para velar por el respeto al derecho al honor, a la intimidad y a la propia imagen. La AEPD se define como un ente de derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con total independencia de las Administraciones Públicas en el ejercicio de sus funciones.

El marco normativo de la AEPD está constituido por el RGPD, LPDPgdd, el Real Decreto 389/2021 de 1 de junio, por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos [15], la Ley 40/2015, de 1 de octubre, de régimen Jurídico del Sector Público[16] y la Ley 39/2015, de 1 de octubre, del procedimiento Administrativo Común de las Administraciones Públicas[17]

[13] Publicada en el BOE número 255 de 24 de octubre de 2015.
[14] Agencia Española de Protección de Datos. Disponible en Agencia Española de Protección de Datos | AEPD (fecha de última consulta 31 de agosto de 2021)
[15] Publicado en el BOE número 131 de 2 de junio de 2021
[16] Publicado en el BOE número 236 de 2 de octubre de 2015
[17] Publicado en el BOE número 236 de 2 de octubre de 2015

En relación al régimen jurídico aplicable, la AEPD está sujeta al Derecho Administrativo tanto en el ejercicio de sus competencias como en su régimen patrimonial y de contratación.

Las funciones de la AEPD se encuentran recogidas en el artículo 5 de su estatuto, pudiendo destacar entre ellas, la supervisión de la aplicación de la normativa vigente relativa a la protección de datos personales relativas al RGPD, supervisar la aplicación de la normativa relativa a los derechos digitales de la LOPDgdd y su desarrollo, así como la elaboración de informes de carácter preceptivo ante los supuestos establecidos en el mismo.

3. PRINCIPALES CONCEPTOS SOBRE LA PROTECCIÓN DE DATOS

Con la finalidad de acercar a un contexto práctico los contenidos del RGPD, se debe proceder en primer lugar, a conocer algunos de sus conceptos más relevantes para lo que de forma puntual también serán reseñados preceptos clave de la LOPDgdd, y de la AEPD

3.1. Datos personales

Recogido en el artículo 4, del RGPD establece que se entenderá por datos personales toda información sobre persona física identificada o identificable; se considerará persona física identificable a toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dichas personas.

3.2. Principales sujetos

En el mismo artículo 4 RGPD se define a los sujetos que participan en estos procesos, pudiendo así identificar a interesado, responsable del tratamiento, encargado del tratamiento, destinatario y tercero.

El Interesado, corresponde a la persona física identificada o identificable de cuyos datos personales se realizará el tratamiento.

Cuando se trata del Responsable del Tratamiento, se refiere a la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto a otros, determine los fines y medios del tratamiento de los datos.

Sujeto diferenciado en el Encargado de Tratamiento, siendo la persona física o jurídica, autoridad pública, servicio u otro organismo que trate los datos personales por cuenta del responsable del tratamiento. En este caso cabe destacar que es el artículo 28.3 de este mismo Reglamento establece que dicho encargo se regirá por un contrato u otro acto jurídico que así lo acredite, por el que se vincule al encargado respecto del responsable y quede de manifiesto el objeto, naturaleza, finalidad del tratamiento, obligaciones y derechos etc.

Cuando se hace mención al Destinatario, se hace referencia a la persona física o jurídica, autoridad pública, servicio u otro organismo al que se comuniquen los datos personales, se trate o no de un tercero.

Por último, cuando el Reglamento hace mención a un Tercero, se refiere a la persona física o jurídica, autoridad pública, servicio u organismo distinto del interesado, del responsable, del encargado y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o encargado.

Una vez definidos los principales sujetos, podemos pasar a analizar algunos preceptos de este Reglamento que serán de vital importancia para su correcta aplicación.

3.3. Legitimación del tratamiento de datos de carácter personal

El tratamiento que se da a los datos personales, debe contener una base legal que lo legitime y para ello es necesario que se cumplan los requisitos del RGPD, de esta forma podemos encontrar en el artículo 6 del mismo, los supuestos en los que dicho tratamiento se considera lícito, debiendo cumplir cualquiera de las causas de legitimación que se enumeran a continuación.

En primer lugar, el RGPD hace referencia a la necesidad de contar con el consentimiento del interesado para los fines específicos del tratamiento.

En segundo lugar, establece que el tratamiento que se trate tenga que ser necesario para la ejecución de un contrato en el que elinteresado es parte o para la aplicación a petición de este de medidas precontractuales.

En tercer lugar, establece que el tratamiento sea necesario para el cumplimiento de una obligación legalaplicable al responsable del tratamiento.

En cuarto lugar, nos encontramos con el supuesto en el que el tratamiento sea necesario para proteger intereses vitales del interesado o deotra persona física.

En quinto lugar, hace referencia a aquellos supuestos en los que el tratamiento sea necesario para el cumplimiento de una misión realizada eninterés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.

En sexto lugar, establece los supuestos en los que el tratamiento sea necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobredichos intereses no prevalezcan los intereses o los derechos

y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.

En este mismo artículo podemos observar como la norma establece que el interés legítimo se puede utilizar como base de licitud de un tratamiento siempreque no prevalezcan los intereses o los derechos y libertades de los interesados y teniendo en cuenta las expectativas razonables de las personas afectadas por el tratamiento, basadas en la relación que tienen con el responsable del tratamiento.

Por otro lado, establece que los casos en que la base jurídica de los tratamientos sea el consentimiento, éstedeberá tener las características previstas por el RGPD, entendiendo por estas el consentimiento, que analizaremos a continuación.

3.4. Legitimación del tratamiento en el ámbito de las relaciones laborales

Tal y como establece la AEPD en la guía de protección de datos en las relaciones laborales[18], el empresario tiene legitimidad para el tratamiento de los datos de las personas trabajadoras, ya que será necesario para la ejecución de un contrato. Igualmente, será lícito el tratamiento de esos datos para poder cumplir con las obligaciones legales por parte del responsable del tratamiento, como puede ser para las cotizaciones de la seguridad social u obligaciones tributarias, entre otras. Así mismo podrá contar con toda la información necesaria para la satisfacción de intereses legítimos perseguidos por el tratamiento.

3.5. El consentimiento

El consentimiento aparece recogido en el artículo 7 del RGPD y tal y como hemos ido desarrollando, para los tratamientos cuya base legal sea basada en la prestación del consentimiento, el responsable debe asegurarse que éste sea inequívoco, entendiendo por éste, aquel que se ha prestado mediante manifestación del interesado o mediante una clara acción afirmativa.

Los consentimientos conocidos como tácitos, basados en la inacción de los interesados, dejan de ser válidos a partir de la aprobación de este reglamento, incluso para tratamientos iniciados con anterioridad, que tendrán que proceder a su adecuación a éste, en base a las

[18] Guía de Protección de Datos en las Relaciones Laborales publicada por la Agencia Española de Protección de Datos. Disponible en La protección de datos en las relaciones laborales (aepd.es) (fecha de última consulta: 31 de agosto de 2021)

opciones que esta propia norma pone a su alcance para ello, destacando el considerando 42 del RGPD donde podemos encontrar de forma clara y concisa las principales características del mismo, entre la que debemos destacar que el consentimiento no se considera libremente prestado cuando el interesado no goce de verdadera o libre elección o no puede denegar o retirar su consentimiento sin sufrir perjuicio alguno.

Ahondando en el artículo 7 del RGPD, encontramos las características que debe poseer el consentimiento para ser lícito y que pasamos a analizar a continuación.

Se trata de un consentimiento prestado de forma que tiene que poder ser revocable en cualquier momento. Es necesario que, en todo momento, el responsable pueda acreditar la forma mediante la que ha obtenido el consentimiento.

Para que el consentimiento sea válido es necesario que haya sido utilizado en un lenguaje, claro y sencillo.

Si la obtención del consentimiento se hubiese realizado de forma escrita, debe quedar claramente diferenciadala parte referente a la protección de datos del resto de declaraciones que pudiese contener el documento, no creando error o confusión.

Asimismo, en el supuesto de datos sensibles, en la adopción de decisiones automatizadas y en transferencias internacionales, el consentimiento, además deinequívoco, ha de ser explícito.

Cabe destacar que los menores de edad tienen capacidad para consentir el tratamiento de sus datos de carácter personal, determinando el RGPD, los Estados miembros pueden establecer por ley el consentimiento de los menores siempre que la edad no sea inferior a 13 años ni superior a 16. En España, esa edad está fijada en los 14 años (artículo 7 LOPDgdd). Por tanto, desde tan temprana edad, es fundamental el uso responsable de internet.[19]

Para finalizar, debemos considerar que el propio RGPD establece la posibilidad de prestar el consentimiento de forma agrupada en caso de vinculaciones entre los fines, siempre y cuando no se trate de tratamientos de datos que implicasen conductas diferenciadas, ante lo cual, deberías ser prestado de forma independiente.

[19] Pérez, A. (2016). La protección de los derechos fundamentales de los menores en Internet desde la perspectiva europea. Ius Et Praxis (Talca, Talca, Chile), 22(1), 377-415.

3.6. El consentimiento en el ámbito de las relaciones laborales

El consentimiento de las personas trabajadoras, además de ser individual libre y específico, no puede ser sustituido por un consentimiento plural o indirecto, mediante la negociación colectiva, tal y como establece el Tribunal de Justicia de la Unión Europea.[20]

Debemos destacar que las relaciones laborales se encuentran sujetas a las leyes que le sean de aplicación, así como a los contratos de trabajo mediante los que se haya formalizado la misma, por lo que la principal legitimación del empresario par el uso de sus datos viene enmarcado por el cumplimiento de estos. En otros casos, bastará con la información a los trabajadores de ciertas medidas o acciones que realizará el empresario, por ejemplo, de supervisión y siempre que las mismas solo conlleven tal fin. Todo ello pone de manifiesto que el consentimiento como tal, queda en un ámbito limitado dentro de las relaciones laborales.

3.7. Datos especialmente protegidos

Como hemos podido observar a lo largo de este trabajo, los datos personales son la base de la protección, sin embargo, existen una serie de datos que son considerados especialmente protegidos, debido a su relación con derechos fundamentales, que merecen una especial atención.

De esta manera el RGPD en su artículo 9 recoge la prohibición general del tratamiento de estos datos de mayor sensibilidad, tales como las opiniones políticas, convicciones religiosas, afiliación sindical, sobre raza o etnia, la salud, orientación sexual o datos genéticos o biométricos.

Sin embargo, cabe destacar una serie de excepciones contenidas en este mismo artículo entre las que destacaremos las siguientes, por estar relacionadas con el ámbito de estudio de este trabajo.

Cuando el tratamiento sea necesario para el cumplimiento de las obligaciones y para el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del derecho laboral y de la seguridad social y protección social, en la medida en que así lo autorice el derecho de la Unión Europea de los Estados miembros o un

[20] Según Sentencia de TJUE (Gran Sala), de 5 de octubre de 2014. Consultado en CURIA - Documentos (europa.eu)

Convenio Colectivo con arreglo a tal derecho, que establezca garantías adecuadas al respeto de los derechos fundamentales y de los intereses del interesado,

Así mismo cuando sea con fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia sanitario o social.

3.8. Registro de actividades de tratamiento

El registro de actividades de tratamiento está regulado en el artículo 30.1. del RGPD. Dicho artículo indica que "*cada responsable y, en su caso, su representante llevará un registro de las actividades de tratamiento efectuadas bajo su responsabilidad*".

Este registro es un documento que recoge los flujos de datos que se están llevando a cabo en la empresa. En la guía de la Guía práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD[21], el tratamiento se considera como "*el conjunto de operaciones dirigidas a conseguir una determinada finalidad que se legitiman en una misma base jurídica*". Cada tratamiento debe incluir operaciones tales como la recogida, el registro, la organización, la estructuración, la consulta o la utilización de los datos.

Dicho registro deberá contener la siguiente información:

- el nombre y los datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable, y del delegado de protección de datos;
- los fines del tratamiento;
- una descripción de las categorías de interesados y de las categorías de datos personales;
- las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales;
- en su caso, las transferencias de datos personales a un tercer país o una organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el

[21] https://www.aepd.es/sites/default/files/2019-09/guia-analisis-de-riesgos-rgpd.pdf

artículo 49, apartado 1, párrafo segundo2, la documentación de garantías adecuadas;

- cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos;
- cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad

Para que este documento sea eficaz y cumpla con las funciones que impone la ley, el Registro tiene que ser siempre actualizado, sujeto a una revisión continua y actualización imprescindible cada vez que se produzca un cambio relevante en alguna actividad de tratamiento registrada o se produzca una incidencia como puede ser una brecha de seguridad o una queja.

No existe un modelo de registro de actividades de tratamiento en el RGPD y es aconsejable tener este registro de forma escrita, que puede ser tanto en papel como electrónica (principio de la equivalencia funcional de la forma electrónica). La empresa tiene que escoger el método más adecuado a su perfil. Tendrá que ser redactado en un formato claro y legible que facilite su comprensión.

Entendemos que el formato más indicado es el formato electrónico puesto que se trata de un documento vivo que sufrirá cambios o anotaciones, reflexiones, planteamientos distintos. Está claro que frente a una brecha de seguridad nos tendremos que plantear que medidas se deben de tomar de ahora en adelante para evitar que la situación se vuelva a producir.

4. PRINCIPALES DERECHOS DE PROTECCIÓN DE DATOS

El Capítulo III del RGPD es el relativo a los derechos del interesado, en este caso ahondaremos en algunas de las cuestiones más relevantes para la realización de este trabajo, ya que al igual que en los apartados anteriores, sería imposible incidir en cada uno de ellos.

A. El derecho de acceso del interesado, recogido en el artículo 15 del RGPD establece que el interesado tendrá derecho a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen y, en tal caso, derecho de acceso a los datos personales y a información como, los fines del tratamiento, los destinatarios o categorías de destinatarios a los que se comunicaron sus datos o a los que serán comunicados, la existencia del derecho que posee el interesado a solicitar al responsable la rectificación, supresión o limitación del tratamiento de sus datos o si existen decisiones automatizadas incluyendo la elaboración de perfiles, entre otras.

   Para el ejercicio de estos derechos, la AEPD pone a disposición de los interesados modelos de solicitud[22]

B. El derecho de rectificación**,** se recoge en el artículo 16 de RGPD donde establece que el interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la rectificación de los datos personales inexactos que le conciernan. Teniendo en cuenta los fines del tratamiento, el interesado tendrá derecho a que se completen los datos personales que sean incompletos, inclusive mediante una declaración adicional.

   La propia AEPD cuenta con modelos para el ejercicio de estos derechos[23]

C. Derecho de supresión, también denominado derecho al olvido, podemos encontrarlo en el artículo 17 de RGPD y establece que El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a

[22] Agencia Española de Protección de Datos. Disponible en formulario-derecho-de-acceso.pdf (aepd.es) (fecha de última consulta: 31 de agosto de 2021)
[23] Agencia Española de protección de Datos. Disponible en formulario-derecho-de-rectificacion.pdf (aepd.es) (fecha de última consulta 31 de agosto de 2021)

suprimir sin dilación indebida los datos personales cuando concurra alguna de las circunstancias recogidas en el mismo, tales como que esos datos ya no sean necesarios para los fines que fueron recogidos, por retirada del consentimiento por parte del interesado, porque los datos hayan sido tratados ilícitamente etc.

Para el ejercicio de este derecho, la AEPD pone a disposición de los interesados un modelo base[24]

D. Derecho a la limitación del tratamiento, recogido en el RGPD en su artículo 18 establece que los interesados podrán obtener la limitación del tratamiento de sus datos cuando se cumpla alguna de las condiciones establecidas en el mismo, como por inexactitud, por la ilicitud del tratamiento o porque los datos ya no sean necesarios por parte del responsable para el fin que fueron obtenidos, pero se solicita que no sean cancelados, para poder ejercer reclamaciones.

   La AEPD cuenta con un modelo para el ejercicio de este derecho de limitación del tratamiento[25]

E. Derecho a la portabilidad de los datos, establecido en el artículo 20 RGPD como el derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado, cuando se cumplan los requisitos contemplados en el mismo.

   Para su ejercicio es posible consultar la página de la AEPD ya que cuenta con un modelo para ello.[26]

F. El derecho de oposición recogido en el artículo 21 del RGPD, es el derecho del interesado a que no se lleve a cabo el tratamiento de sus datos personales o que cese el mismo en algunos casos concretos como cuando no sea necesario su consentimiento para el tratamiento, como consecuencia de la concurrencia de un motivo legítimo y fundado, referido a su concreta situación personal, que lo

[24] Agencia Española de protección de Datos. Disponible en formulario-derecho-de-supresion.pdf (aepd.es) (fecha de última consulta: 31 de agosto de 2021)
[25] Agencia Española de protección de Datos. Disponible en formulario-derecho-de-limitacion.pdf (aepd.es) (Fecha de última consulta: 31 de agosto de 2021)
[26] Agencia Española de protección de Datos. Disponible en formulario-derecho-de-portabilidad.pdf (aepd.es) (Fecha de última consulta: 31 de agosto de 2021)

justifique, siempre que una Ley no disponga lo contrario. También en el caso de que se trate de ficheros que tengan por finalidad la realización de actividades de publicidad y prospección comercial y cuando el tratamiento tenga por finalidad la adopción de una decisión referida al afectado y basada únicamente en un tratamiento automatizado de sus datos de carácter personal.

En la guía del ciudadano de la AEPD[27] , para ejercer el derecho de oposición no se necesita justificar ningún motivo, es decir, "los interesados tendrán derecho a oponerse, previa petición y sin gastos, al tratamiento de los datos que les conciernan, en cuyo caso serán dados de baja del tratamiento, cancelándose las informaciones que sobre ellos figuren en aquél, a su simple solicitud". En la AEPD podemos encontrar modelo para ejercitar el derecho[28]

G. Derecho a no ser objeto de decisiones individuales automatizadas**,** recogido en el artículo 22 RGPD, establece que todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar.[29]

H. Derecho de cancelación, definido como el procedimiento en virtud del cual el responsable cesa en el uso de los datos, es recogido también en el artículo 16.3 de la LOPD donde establece que "La cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión" Es por ello que aquí se incluye el derecho de supresión de los datos

   En este caso también se trata de un derecho personalísimo por lo que solo podrá ser el interesado quien debe realizar la petición de cancelación de sus datos personales ante el responsable del tratamiento, en ella deberá aportar la documentación que justifique el motivo de cancelación de algún dato en caso de

[27] Agencia Española de Protección de Datos: Guía para el ciudadano. Disponible en Guía para el Ciudadano (aepd.es) (Fecha de última consulta: 31 de agosto de 2021)
[28] Agencia Española de Protección de Datos. Disponible en formulario-derecho-de-oposicion.pdf (aepd.es) (Fecha de última consulta: 31 de agosto de 2021)
[29] Agencia Española de Protección de Datos. Disponible en formulario-derecho-de-oposicion-decisiones-automatizadas.pdf (aepd.es) (Fecha de última consulta: 31 de agosto de 2021)

ser erróneo o inexacto, o indicar si lo que se pretende es el cese del consentimiento del tratamiento de sus datos, cuando esto sea posible. En este caso, a diferencia del derecho a cancelación, no se trataría de modificar aquellos datos que fuesen inexactos o incorrectos, sino de su desaparición.

4.1. LA LEY ORGÁNICA 3/ 2018 DE 5 DE DICIEMBRE DE PROTECCIÓN DE DATOS PERSONALES Y DE GARANTÍA DE LOS DERECHOS DIGITALES

Esta Ley recoge una serie de derechos específicos relacionados con los Recursos Humanos de las empresas, por lo que merecen una especial mención en este trabajo

4.1.1. Intimidad en dispositivos digitales

El artículo 87 de esta Ley establece "el derecho a la intimidad y el uso de dispositivos digitales en el ámbito laboral" lo que genera dos tipos de acciones diferenciadas. En primer lugar, conlleva que las empresas deban elaborar una política clara de uso de los dispositivos digitales y por otro lado, el deber de informar a los trabajadores sobre los criterios de uso de los mismos. Cabe destacar que es necesario que se cuente con la participación de los trabajadores para la elaboración de las normas empresariales de uso de estos dispositivos digitales, teniendo que "respetar en todo caso, los estándares mínimos de protección de la intimidad de acuerdo con los usos sociales y los derechos reconocidos constitucional y legalmente". En todo caso, el control empresarial deberá realizarse con respeto al principio de proporcionalidad.

4.1.2. Dispositivos de vigilancia en centros de trabajo

Cuando hablamos de datos personales debemos recordar que la imagen es también uno de ellos, ya que hace claramente identificable al sujeto, por lo que las grabaciones en el marco de las relaciones laborales también se recogen dentro de esta Ley, ya que este tipo de dispositivos son cada vez más habituales para la verificación del correcto desempeño de las funciones.

El artículo 89 establece "el derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en lugar de trabajo", este artículo regula la videovigilancia con fines de control empresarial del cumplimiento por parte de los trabajadores y trabajadoras de sus obligaciones laborales. Para ello se exige que antes de su colocación estos sean informados, de forma expresa, clara y concisa, así como la

representación legal de los trabajadores, si la hubiese. Cabe destacar que queda expresamente excluido la posibilidad de instalar este tipo sistemas en los lugares de destinados al descanso o esparcimiento de los trabajadores.

El empleador podrá tratar las imágenes, siempre que se trate de imágenes obtenidas a través de sistemas de cámaras o videocámaras para el ejercicio de las funciones de control de los trabajadores reconocido en LET y que le son inherentes y siempre que dichas funciones no extralimiten su marco legal. Igualmente es necesario destacar que la colocación de esta serie de dispositivos debe ser proporcional a aquello que el empleador desea vigilar, tanto en su número como ubicación, enfoque y duración de conservación. Deberá ser establecido un protocolo de borrado, así como de acceso a las imágenes en el que quede constancia de las personas que accedan a las mismas y los motivos para ello.

Los sistemas de grabación de sonido solo podrán ser utilizados cuando resulten relevantes parala seguridad de instalaciones, personas o bienes, derivados de la actividad laboral

4.1.3. Sistemas de geolocalización

Artículo 90 regula la utilización de sistemas de geolocalización con fines de control en el ámbito laboral, para lo que se exige la obligación por parte del empleador a informar de la existencia de estos sistemas y de su forma de uso de forma clara, expresa e inequívoca a los trabajadores y a la representación legal de los trabajadores, en caso de que la hubiese.

Es legal instalar sistemas de geolocalización para conocer la ubicación de los trabajadores durante su jornada laboral, siempre que se informe correctamente a éstos sobre la existencia de los mismos. Por otro lado, es preferible que los citados sistemas de geolocalización se instalen en dispositivos que sean propiedad de la empresa y no de los trabajadores, para evitar posibles disputas ante los tribunales. Por último, será necesario recabar el consentimiento expreso de los trabajadores para obtener sus datos personales fuera de su jornada laboral a través de los citados sistemas de geolocalización.[30]

4.1.4. Derecho a la desconexión digital

[30] ARIAS BENITEZ, R., ¿Puede un empresario obligar a sus trabajadores a estar geolocalizables?, *Aranzadi digital*. num 1 (2021)

El artículo 88 establece el reconocimiento al derecho a la desconexión digital, siendo una de las novedades más mediáticas de esta Ley que copó los titulares de la prensa en el momento de su aprobación.

Quizá, más que de un nuevo derecho, podríamos hablar de la concreción de derechos tanto de intimidad como de aquellos relacionados con el descanso, estableciendo "los trabajadores tendrán derecho a la desconexión digital a fin de garantizar, fuera del tiempo de trabajo legal o convencionalmente establecido, el respeto de su tiempo de descanso, permisos y vacaciones, así como de la intimidad personal y familiar, debiéndose preservar dicho derecho"

5. PRINCIPALES FLUJOS DE INFORMACIÓN EN LOS DEPARTAMENTOS DE RECURSOS HUMANOS

El departamento de Recurso Humanos es el departamento que recibe y atesora la mayor cantidad de datos personales correspondientes a las personas trabajadores que forman parte de la organización y también aquella información perteneciente a candidatos a alguna selección de personal. Es por ello que para la elaboración de este trabajo, se haga indispensable un análisis de los principales flujos de información que conllevan este tipo de datos personales.

5.1. La Selección

De tal manera que las primeras informaciones que llegan al departamento de Recursos Humanos son las correspondientes a personas externas a la organización quienes a la ocasión de un anuncio de oferta de empleo postulan al puesto enviando su Curriculum Vitae (en adelante CV) con o sin fotografía, así como copias de Títulos y diplomas.

En numerosas ocasiones, para finalizar y decidirse por el candidato/a ideal, se suele hacer una última entrevista en la que intervendrá el jefe del departamento en el que se tiene que insertar. En este caso, se le facilitará también una copia del CV.

Si la selección se hace a través de una agencia de colocación o una empresa de selección, la empresa les hará llegar los CV que tiene en su poder y que desea sean considerados en la selección. A la empresa le llegará la información de los mejores postulantes que no suelen superar las tres o cuatro personas.

5.2. La contratación

En el momento de la contratación es cuando se suele generar la mayor aportación de información puesto que el trabajador para poder concertar un contrato de trabajo suele aportar mucha documentación que suele ser:

- DNI
- Numero de afiliación
- Dirección
- Cuenta bancaria
- Modelo 145

- CV
- Títulos, certificaciones de curso, formación contenida en el CV valorados en el proceso de selección.

El modelo 145 es el documento denominado "Comunicación de datos al pagador" que se utiliza para conocer la situación personal de la persona trabajadora para poder calcular el porcentaje de IRPF que le corresponde en función de sus ingresos y de su situación personal.

En este documento, la persona trabajadora informa de cuál es su situación personal dando detalles sobre:

- Si mismo (situación familiar, Discapacidad). Es más, si su situación familiar es la de "casado/a y no separado/a legalmente cuyo cónyuge no obtiene rentas superiores a 1.500 euros anuales", tendrá que facilitar el número de NIF de su cónyuge.

- Sus descendientes si conviven con él (año de nacimiento, discapacidad)

- Sus ascendientes si conviven con él (año de nacimiento, discapacidad)

- Si por decisión judicial, está abonando pensiones compensatorias en favor del cónyuge o anualidades por alimentos en favor de los hijos

Luego dependiendo del puesto o de la actividad de la empresa se suele solicitar, además, otros documentos que la empresa considera imprescindibles para el cumplimiento del contrato de trabajo.

- Certificado de vida laboral actualizado y expedido por la Seguridad Social

En este caso, la empresa solicita la entrega de este certificado para corroborar la información facilitada en el CV y/o comprobar la experiencia previa alegada.

- Certificado de Delitos de naturaleza sexual negativo

Este certificado es solicitado cuando la actividad de la empresa está relacionada con menores de edad.

- Cuota sindical y cuenta bancaria donde hacer el ingreso

Esta información, nunca es solicitada por la empresa, sino que es el trabajador quien la entrega de forma voluntaria para que la empresa se haga cargo de pagar su cuota a su sindicato después de retrotraerlo cada mes de su nómina.

- Carnet de manipulador de alimentos

Este documento se solicita en aquellas empresas cuya actividad está relacionada con la producción, elaboración, manipulación y/o suministros de alimentos,

- Carnet de carretillero

Este carnet es exigido a aquellas personas que conduzcan carretillas elevadoras para reposición y aprovisionamiento de productos, operaciones de mantenimiento y seguridad, carga y descarga de vehículos y productos, preparación de pedidos

- Carnet de conducir y copia de póliza de seguro de coche

El carnet de conducir es solicitado si el empleo está directamente relacionado con un puesto de transporte (reparto) y también cuando el puesto requiere desplazamientos durante la jornada de trabajo y se suelo solicitar la póliza de seguro de coche cuando dicha actividad se realiza con el coche propio de la persona trabajadora.

- Darde
- Certificado de discapacidad
- Información acerca de la calificación de "Víctima de Violencia de Genero" (orden de alejamiento, sentencia condenatoria)
- Certificado de Exclusión social

Estos últimos documentos se pedirán cuando se trate de alguna contratación subvencionada o bonificada, se habrá de aportar la documentación acreditativa que permita a la empresa aplicarse las bonificaciones o recibir la subvención correspondiente.

Si la empresa tiene externalizada la gestión de las relaciones laborales como por ejemplo las nóminas, altas y bajas en la seguridad social, contratos y registro en el SEPE, la documentación que se le hace llegar desde la empresa son las necesarias para estos trámites (DNI, NUMERO DE AFILIACION, DIRECCIÓN,

MODELO 145, y la documentación correspondiente a la justificación de bonificaciones o reducciones.

5.3. Durante la relación laboral:

5.3.1. Comunicación de datos con la Administración Pública:

- **con la Seguridad Social:**

La relación con esta entidad es continua en el tiempo y a lo largo de los años se irán dando información de forma periódica a la misma.

Tanto la empresa como la Asesoría que puede representar a la empresa informarán a la Seguridad Social a través del Sistema Red[31]. Previamente la empresa habrá tenido que obtener su Certificado Digital (que garantiza la seguridad de las comunicaciones y otorga validez legal a cualquier transacción electrónica que realice). Con este certificado, se tiene que solicitar la autorización a la TGSS para poder operar a través del sistema RED.

Para ello, se usará el modelo TA2 para comunicar a la Seguridad Social el alta o la baja de un trabajador en la empresa o comunicar alguna variación relativa a contrato, grupo de cotización…etc.

Mensualmente, la empresa presentará los seguros sociales a través del Recibo de Liquidación de Cotizaciones (RLC, antiguo TC1) y la Relación Nominal de trabajadores (RNT, antiguo TC2). Además, también se presentará la Comunicación de Conceptos Retributivos Abonados (CRA).

Otras de las comunicaciones de la empresa se refieren a los partes de alta, baja o confirmación de Incapacidad Temporal por contingencias comunes o accidente de trabajo.

- **con el SEPE:**

La empresa cuando celebra un contrato con un/a trabajador/a, tiene la obligación de comunicar esa contratación en el plazo de 10 días hábiles al SEPE. En la actualidad, en que los registros presenciales son cuasi nulos, se usa el programa

[31] Orden ESS/484/2013 de 26 de marzo por la que se regula el Sistema de remisión Electrónica de datos en el ámbito de la Seguridad Social

Contrat@ para estos trámites. Esta obligación se mantiene a la hora de comunicar una prórroga de contrato temporal.

En este caso también se necesitará una autorización de los Servicios Públicos de Empleo. Una vez concedida, se accede a Contrat@ con Certificado Digital o con el Identificador de la empresa y una clave personal que se ha sido asignada al realizar la solicitud.

En la comunicación de contrato de trabajo, los datos del trabajador son bastantes exhaustivos tales como nombre y apellidos, DNI, Numero Afiliación, fecha nacimiento, nivel de estudios, lugar de residencia y todos los datos relativos al contrato: tipo, duración, porcentaje de jornada, categoría.

De la misma manera, otra comunicación de datos de trabajadores que se tiene con el SEPE es en el momento de la finalización de la relación laboral cuando la empresa tiene la obligación de comunicar el Certificado de Empresa. En este la información que se entrega son los datos de identificación del trabajador, los datos de contrato (inicio y fin, Porcentaje de jornada, causa de finalización) y las bases de cotización correspondiente a los 180 últimos días.

- **Con la Agencia Tributaria**

La empresa retiene la aportación al IRPF de los trabajadores en su nómina y su misión es entregar ese dinero retenido de forma trimestral a través del modelo 111. Una vez al año, en el mes de enero, la empresa tiene que preparar el modelo 190 donde se recoge trabajador por trabajador lo que se le ha retenido todo el año, así como su aportación a la Seguridad Social. Si bien en el modelo 111 no aparecen datos de los trabajadores, en el modelo 190 la información personal de los trabajadores se corresponde con su DNI y su nombre y apellidos.

La empresa debe disponer de un Certificado Digital para poder presentar esas declaraciones y si se trata de una Asesoría debe estar en posesión una autorización para presentar declaraciones en nombre de terceros (normalmente por estar dado de alta como colaborador).

En otros momentos, se trata de contestar a requerimientos de embargo de nómina de algún/a trabajador/a. Si el trabajador sigue en la empresa y tiene una nómina lo

suficientemente alta para poder ser embargada, la empresa tendrá que informar del importe neto de la misma, así como de la cantidad que se le embargará.

- **Con Juzgados**

En estos casos, también suele tratar de comunicación de embargo sobre los salarios de la persona trabajadora y se hará entrega del mismo tipo de información que en el apartado anterior.

- **Con la Inspección de trabajo**

La empresa puede ser objeto de inspección por parte de los Inspectores de trabajo y de la seguridad social. En estos casos para poder realizar su cometido y hacer la investigación pertinente, los Inspectores pueden solicitar todo tipo de documentación que la empresa debe de entregarle tales como:

- Partes de alta y baja
- Nominas
- Contratos
- Justificante de formación de riesgos laborales
- Control de presencia

Esta documentación se suele aportar de forma presencial en el despacho del Inspector o últimamente se les hace llegar vía mail.

- **Con la Autoridad Laboral**

En materia de prevención de riesgos laborales, desarrollada por la Ley 31/1995 de Prevención de riesgos laborales, según el art. 23, la empresa deberá conservar a disposición de la Autoridad laboral tanto la relación de accidentes de trabajo y enfermedades profesionales que hayan causado al trabajador una incapacidad laboral superior a un día de trabajo, así como la práctica de los controles del estado de salud de los trabajadores y las conclusiones obtenidas de los mismos.

También es necesario registrar los accidentes de trabajo con baja médico como los aquellos sin baja médica en el Sistema Delta. Cada declaración tiene que recibir el visto bueno de la Mutua de Accidentes y por último de la Autoridad Laboral.

5.3.2. Comunicación con los representantes de la empresa:

El artículo 64 del Estatuto de los trabajadores establece los derechos de información y consulta y competencias de los representantes de los trabajadores tanto bajo la forma de delegados de personal como de comité de empresa.

A lo largo del mandato de la representación de los trabajadores se le va a entregar mucha documentación tanto acerca de la empresa tales como resultados, balance, previsiones, pero también acerca de la contratación de los trabajadores y las trabajadoras, las prórrogas de contrato, la prevención de riesgos laborales, etc.

- La copia básica de los contratos:

El artículo 8.4 LET dice que "*El empresario entregará a la representación legal de los trabajadores una copia básica de todos los contratos que deban celebrarse por escrito, a excepción de los contratos de relación laboral especial de alta dirección sobre los que se establece el deber de notificación a la representación legal de los trabajadores.*

Con el fin de comprobar la adecuación del contenido del contrato a la legalidad vigente, esta copia básica contendrá todos los datos del contrato a excepción del número del documento nacional de identidad o del número de identidad de extranjero, el domicilio, el estado civil, y cualquier otro que, de acuerdo con la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, pudiera afectar a la intimidad personal. El tratamiento de la información facilitada estará sometido a los principios y garantías previstos en la normativa aplicable en materia de protección de datos.

La copia básica se entregará por el empresario, en plazo no superior a diez días desde la formalización del contrato, a los representantes legales de los trabajadores, quienes la firmarán a efectos de acreditar que se ha producido la entrega.".

- Acerca de las sanciones muy graves

La representación de los trabajadores tendrá derecho a ser informada de las sanciones muy graves impuestas por la empresa.

- En todos aquellos procedimientos que necesitan un periodo de consulta con la representación de los trabajadores y donde se hará entrega de información acerca de los trabajadores:

Esto se produce cuando la empresa necesita sancionar por falta grave o muy grave a un trabajador representante de los trabajadores o algún afiliado al sindicato.

En los procedimientos de despido colectivo y de suspensión de contratos y reducción de jornada por causas económicas, técnicas, organizativas y de producción también se tiene que proceder a un periodo de consulta.

- Elecciones sindicales

Es un momento álgido de las relaciones con la representación de los representantes donde se entrega de forma pública es decir con publicación en tablones de anuncios varios documentos donde aparecen información de los trabajadores, entre ellos:

- Composición de la mesa electoral con nombre y apellidos de los miembros de la misma, así como su número de DNI.
- Censo electoral donde figuran datos tales como nombre y apellidos, sexo, DNI, fecha de nacimiento, antigüedad en la empresa, categoría profesional.
- Lista de candidaturas con nombres y apellidos y afiliación

5.3.3. Comunicación con otras empresas:

- **con la Mutua colaboradora con la Seguridad Social:**

Cuando se crea una empresa, uno de los primeros tramites a realizar es la solicitud de Código de Cuenta de Cotización (en adelante CCC). En este mismo modelo, en su séptimo apartado, la empresa comunica cual es la Entidad de Accidentes de trabajo es decir la Entidad con la que se ha concertado la cobertura de las contingencias de accidentes de trabajo y enfermedades profesionales así cual es la Entidad con la que se cubre la Incapacidad Temporal por Contingencias Comunes.

A partir de este momento, se establece una estrecha relación con la Mutua colaboradora con la Seguridad Social quien tendrá acceso a los datos de los trabajadores dados de alta en la empresa, así como a los mismos trabajadores.

La Mutua no solo se hará cargo de la prestación por accidente de trabajo, sino que también atenderá a nuestros trabajadores desde un punto de vista médico. Cuando se produce el accidente de trabajo, la empresa tiene que rellenar un parte de asistencia donde aparecerán los datos de la empresa y para el trabajador, la empresa tendrá que facilitar nombre y apellidos, DNI, Número de afiliación, Dirección, así como las circunstancias del accidente y los posibles síntomas y lesiones.

Cuando la Mutua ha atendido a la persona trabajadora y ha formalizado un parte de Incapacidad Temporal por Contingencias Profesionales (comúnmente conocido como parte de accidente de trabajo), la empresa tendrá que volcar todos estos datos en el programa DELTA que es el Sistema de Declaración Electrónica de Accidentes de trabajo. El parte de accidente de trabajo deberá llevar el visto bueno de la Mutua de Accidentes y de la Autoridad Laboral. Para poder usar el sistema Delta, la empresa usará su certificado digital y luego se dará de alta en el sistema Delta.

Además, si concertamos con la Mutua, la cobertura de las prestaciones de Incapacidad Temporal por contingencias comunes, ésta controlará esos procesos de baja directamente a través de sus equipos médicos.

Muchas veces, los trabajadores de la empresa tienen que solicitar prestaciones de forma directa a la Mutua. El departamento de RRHH es quien les ayuda a preparar la documentación solicitada. Son trámites relacionados con el pago directo de prestación tanto por contingencias profesionales como contingencias comunes, por las cuales, el trabajador tendrá que presentar solicitud de pago directo y acompañarla de una serie de documentos tales como copia del DNI, documento bancario, nóminas en caso de trabajadores a tiempo parcial.

Si se trata de una prestación por cuidado de menores afectados por cáncer y otra enfermedad grave, la solicitud deberá ir acompañada además de una copia del libro de familia, una declaración médica.

- **Con Los bancos**

El artículo 29 del LET establece que *"la liquidación y el pago del salario se harán puntual y documentalmente en la fecha y lugar convenidos o conforme a*

los usos y costumbres". Es por ello que las empresas, en regla general, optan por el pago del salario a través de transferencia bancaria.

La empresa mensualmente hace llegar un fichero con los datos de los trabajadores y el importe de su nómina para que el banco realice la transferencia preceptiva para el pago del salario.

Este fichero contiene en regla general nombre y apellidos, DNI y Número de cuenta bancaria de la persona trabajadora.

- **Con la empresa de prevención de riesgos laborales:**

La empresa podrá concertar un contrato con un servicio de prevención ajeno y para ello dará acceso a datos de sus trabajadores cuando se trate de organizar la formación de los mismos o en el momento de la vigilancia de la salud cuando se procede a efectuar los reconocimientos médicos preceptivos.

Y siguiendo a Isabel De Marcos, los datos relativos a la salud, como datos personales sensibles, tendrán que cumplir con los principios y derechos relativos a la protección de datos, buscando el equilibrio entre la necesidad de tratar estos datos y la protección de la persona para evitar discriminaciones o tratamientos ilícitos.[32]

- **Con empresas de formación:**

La empresa dentro de su plan de formación de la plantilla llegará a concertar cursos de formación donde también dará información de sus trabajadores tales como nombres y apellidos y DNI.

Si la formación es bonificada existirá además una remisión de información a la Fundación Estatal para la Formación en el Empleo (en adelante FUNDAE). Tenemos que saber que la empresa se tiene que dar de alta en la aplicación de Formación Programada por las empresas de FUNDAE usando para ello su certificado digital o lo hará la empresa de formación en su lugar.

[32] De Marcos, I. (2012). Breve aproximación a las implicaciones jurídicas y operativas del tratamiento de datos de salud. *Gaceta Médica de México*, 148(5), 480-486

- **Con compañías de seguro**

Muchos convenios colectivos recogen en sus mejoras sociales la toma de seguros diversos que cubren a sus trabajadores tales como seguros de vida, de accidentes, de pensiones donde tendrán que facilitar los datos de sus trabajadores para que sean incluidos en las pólizas necesarias.

- **Con las empresas clientes**

Muchas veces parte de los servicios se desarrollan en los centros de trabajo de los clientes de la empresa como pueden ser el caso de transporte, merchandising, limpieza. Para ello, la empresa tendrá que comunicar datos de los trabajadores que van a desempeñar alguna labor en esos centros. En regla general serán datos identificativos tales como datos de identificación como nombre y apellidos y número de DNI.

Además, muchas empresas nos solicitan de forma mensual tanto el recibo de liquidación de cotizaciones como la relación nominal de trabajadores donde aparecen los trabajadores asignados a su centro de trabajo.

- **Contratas y subcontratas**

En los casos de contrata y subcontrata, la información que se cede acerca de nuestros trabajadores es muy abundante empezando por la relación del personal adscrito a la obra donde tiene que figurar los nombres y apellidos, DNI, número de afiliación a la seguridad social y categoría.

En estos casos, se solicitará mensualmente los recibos de liquidación de los seguros sociales, así como las relaciones nominales de trabajadores adscrito a la contrata o subcontrata, así como declaración firmada por cada trabajador que certifique estar al corriente en el cobro de su salario.

Desde el punto de vista de la prevención de riesgos laborales se necesita entregar información tal como el justificante de entrega de EPIS de cada trabajador, el justificante de información sobre el plan de seguridad y salud, el certificado de aptitud médica, un listado de personal autorizado a utilizar determinadas maquinas.

6. CUMPLIMIENTO DE LA PROTECCIÓN DE DATOS EN EL DEPARTAMENTO DE RECURSOS HUMANOS.

Después de conocer los movimientos y flujos de datos en el departamento de Recursos Humanos, así como el tipo de datos que se están manejando, es imprescindible canalizar esta información para cumplir con la protección de datos.

En la actualidad y siguiendo el espíritu del RGPD, cumplir con la protección de datos significa plantearse y razonar lo que la empresa está haciendo con los datos, como lo está haciendo y que tiene previsto hacer en caso de fuga de datos y también establecer un ciclo de revisión. La idea es que la empresa tiene que cumplir con la ley, no siguiendo unas reglas rígidas, sino que tiene que hacerlo de forma adecuada y adaptada a la organización.

La idea que queremos hacer llegar en este trabajo Fin de Máster es que la protección de datos es una obligación que tenemos que llevar de forma viva, adaptada a nuestra organización y siempre actualizada siguiendo el marco obligatorio de la legislación vigente.

En este sentido, lo que proponemos es que la organización lleve un registro de actividades de tratamiento que hemos definido anteriormente en el apartado 3.8 de este trabajo.

También nos parece muy importante que se tenga siempre presente que la protección de datos se establezca desde el primer momento un ciclo de revisión sobre todo cuando se recibe una queja. El concepto es que la protección de datos establecida se vaya nutriendo de la experiencia y la reflexión para ir mejorando y poder conseguir el mejor sistema para nuestra organización.

Atendiendo a lo que acabamos de describir, vamos a trabajar esta información según tres bloques de relaciones, siendo estos:

1) Relaciones del Departamento de Recurso Humanos con las Administraciones Publicas
2) Relaciones del Departamento de Recursos Humanos con empresas proveedoras de servicios
3) Relaciones del Departamento de Recursos Humanos con los trabajadores

En nuestra empresa, el responsable del Tratamiento será siempre la empresa y por ello tendremos que hacer figurar los siguientes datos: Razón social, CIF y la Dirección.

Por regla general será nuestro departamento quien lleve la responsabilidad de ejecutar todo el trabajo relacionado con el flujo de datos personales.

6.1. Relaciones del departamento de Recursos Humanos con las Administraciones Publicas

NOMBRE DEL FICHERO	**GESTION INTEGRAL DEL PERSONAL, NOMINAS Y SEGURIDAD SOCIAL**
Base jurídica	Cumplimiento de una obligación legal: Legislación laboral y de Seguridad Social, Estatuto de los trabajadores, Convenio Colectivo
Fines del tratamiento	Contratación de personal, Elaboración de nóminas, Seguros sociales, Finiquitos, Apertura de centros de trabajo
Colectivo	Personal de la organización
Datos	Identificativos Económicos Salud (Certificado discapacidad, Bajas IT, Accidentes Laborales Situación Familiar
Destinatarios	Organismos Públicos: Tesorería General de la Seguridad Social, Servicios Públicos de Empleo (autonómica y estatal, AEAT…)
Período de conservación	Los datos se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se obtuvieron y para determinar las posibles responsabilidades que se pudieran derivar de dicha finalidad y del tratamiento de los datos. El plazo de conservación de documentos contables, fiscales, laborales o mercantiles, con carácter general es de 6 años según el articulo 30 del Código de Comercio. Los datos económicos se conservarán al amparo de lo dispuesto en la Ley 58/2003 de 17 de diciembre, General Tributaria (mínimo 4 años). Los documentos de pago de cuotas a la Seguridad Social se custodiarán durante 5 años a contar desde la fecha en la que debieron ser ingresadas.
Medidas de Seguridad	En los archivos en papel, será necesario anonimizar la información (uso títulos generales tales como “nóminas”, “Seguros Sociales” o tener un sistema de códigos para que

	personas ajenas al departamento no averigüen a quien corresponde la información contenida. Para la información electrónica, es importante garantizar la información. Los medios utilizados pueden ser "copia de seguridad en disco duro sin conexión", guardar la información en una nube privada (nunca pública). Garantizar que solamente el personal del Departamento de Recursos Humanos acceda a la información custodiada. Se instaura el uso de usuario y contraseña para el acceso a la información.

En este apartado la empresa tiene que usar las plataformas puestas a disposición por la Administración General del Estado. Las empresas están trabajando con Certificados digitales emitidos por la Fabrica Nacional de Moneda y Timbre y acreditada la identidad en una Oficina de Acreditación de Identidad.

6.2. Relaciones del Departamento de Recursos Humanos con las empresas proveedoras de Servicios

NOMBRE DEL FICHERO	**SELECCIÓN, FORMACION, DESARROLLO DE PERSONAL**
Base jurídica	Cumplimiento de una obligación legal: Legislación laboral y de Seguridad Social para Mutuas, Prevención de Riesgos Laborales) Convenio Colectivo (Seguros y pólizas de vida y/o accidente) Cumplimiento de una obligación contractual: Consentimiento de los trabajadores (selección) Contrato con las empresas (bancos)
Fines del tratamiento	Selección, formación, Reconocimientos médicos del personal, Orden de transferencia al banco
Colectivo	Personal de la organización Candidatos/as interesados/as en trabajar en la organización
Datos	Identificativos Económicos Salud (Certificado discapacidad, Bajas IT, Accidentes Laborales) Académicos y profesionales
Destinatarios	Mutuas de Accidentes Empresas de Prevención de Riesgos Laborales Bancos Asesoría Laboral Compañías de Seguro

	Empresas de formación Empresas de selección
Período de conservación	Los datos se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se obtuvieron y para determinar las posibles responsabilidades que se pudieran derivar de dicha finalidad y del tratamiento de los datos. El plazo de conservación de documentos contables, fiscales, laborales o mercantiles, con carácter general es de 6 años según el artículo 30 del Código de Comercio. Los datos económicos se conservarán al amparo de lo dispuesto en la Ley 58/2003 de 17 de diciembre, General Tributaria (mínimo 4 años). Los documentos de pago de cuotas a la Seguridad Social se custodiarán durante 5 años a contar desde la fecha en la que debieron ser ingresadas Documentación laboral a contar desde el fin de la relación laboral será de 4 años (Art. 21 RD legislativo 5/2000 de 4 de agosto, Sobre infracciones y Sanciones en el Orden Social (LISOS) Documentación en materia de prevención de riesgos laborales, 5 años
Medidas de Seguridad	En los archivos en papel, será necesario anonimizar la información (uso títulos generales tales como "nóminas", "Seguros Sociales" o tener un sistema de códigos para que personas ajenas al departamento no averigüen a quien corresponde la información contenida. Para la información electrónica, es importante garantizar la información. Los medios utilizados pueden ser "copia de seguridad en disco duro sin conexión", guardar la información en una nube privada (nunca pública). Garantizar que solamente el personal del Departamento de Recursos Humanos acceda a la información custodiada. Se instaura el uso de usuario y contraseña para el acceso a la información.

En este apartado y dependiendo del destinatario, muchas veces, no podremos estar seguro ni tener la plena confianza que los datos que le transferimos estén realmente protegidos y salvaguardados.

La primera duda surge acerca de la herramienta utilizada para el traspaso de dicha información. En la realidad, se suelen usar cuentas de correo de mail para hacerla llegar o muchas veces, las empresas usan el mismo WhatsApp para hacer llegar DNI, Partes de alta y/o baja IT para que la Asesoría cumpla con su cometido.

En el caso de los bancos, podemos estar razonablemente seguros que los datos viajan de forma segura a través de las herramientas internet facilitadas por los mismos con varios códigos de identificación para realizar los movimientos necesarios para las transferencias de nóminas.

Por otro lado, tampoco tenemos constancia del método de archivo de las mismas, del lugar de archivo como tampoco sabemos quien puede tener acceso a esa documentación escrita.

Es necesario verificar que nuestras empresas proveedoras cumplan con los requisitos de la protección de datos, estableciendo protocolos de actuación, usando medios técnicos más seguros. Podemos exigir a nuestra asesoría que trabaje con un portal del cliente donde solamente se puede acceder con contraseña. En que este sistema sea el único método de subir documentación identificativa de nuestros trabajadores.

Otro instrumento que se puede exigir para garantizar nuestros datos es que el vehículo de comunicación no sea ofrecido por una empresa de la economía de datos es decir una empresa cuyo modelo de negocio se basa en la explotación de datos que para conseguir esa información ofrece correos gratuitos (Gmail, Hotmail, Yahoo!).

6.3. Relaciones del Departamento de Recursos Humanos con los trabajadores

NOMBRE DEL FICHERO	**SELECCIÓN, GESTION INTEGRAL DE PERSONAL, CONTROL DE PRESENCIA**
Base jurídica	Cumplimiento de una obligación legal o contractual: Legislación laboral y de Seguridad Social. Convenio Colectivo Consentimiento expreso de los candidatos
Fines del tratamiento	Selección, contratación, mantenimiento del expediente personal, control de presencia, prevención de riesgos laborales, gestión de nominas, finiquitos. Seguimiento de ausencias, vacaciones y permisos, Gestión de la actividad sindical
Colectivo	Personal de la organización Candidatos/as en procesos selectivos
Datos	Identificativos Económicos Salud (Certificado discapacidad, Bajas IT, Accidentes Laborales) Académicos y profesionales Situación personal Afiliación Sindical
Destinatarios	Dirección de la empresa Departamento de Recursos Humanos Trabajadores

Período de conservación	Los datos se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se obtuvieron y para determinar las posibles responsabilidades que se pudieran derivar de dicha finalidad y del tratamiento de los datos. El plazo de conservación de documentos contables, fiscales, laborales o mercantiles, con carácter general es de 6 años según el artículo 30 del Código de Comercio. Los datos económicos se conservarán al amparo de lo dispuesto en la Ley 58/2003 de 17 de diciembre, General Tributaria (mínimo 4 años). Los documentos de pago de cuotas a la Seguridad Social se custodiarán durante 5 años a contar desde la fecha en la que debieron ser ingresadas Documentación laboral a contar desde el fin de la relación laboral será de 4 años (Art. 21 RD legislativo 5/2000 de 4 de agosto, Sobre infracciones y Sanciones en el Orden Social (LISOS) Documentación en materia de prevención de riesgos laborales, 5 años
Medidas de Seguridad	En los archivos en papel, será necesario anonimizar la información (uso títulos generales tales como "nóminas", "Seguros Sociales" o tener un sistema de códigos para que personas ajenas al departamento no averigüen a quien corresponde la información contenida. Para la información electrónica, es importante garantizar la información. Los medios utilizados pueden ser "copia de seguridad en disco duro sin conexión", guardar la información en una nube privada (nunca pública). Garantizar que solamente el personal del Departamento de Recursos Humanos acceda a la información custodiada. Se instaura el uso de usuario y contraseña para el acceso a la información.

En este apartado, la empresa tiene plena autonomía para poner medios para trabajar de forma segura y evitar cualquier tipo de fuga de información. En este caso, estamos diciendo que la empresa tiene que tener la certeza que el lugar (electrónico y/o físico) tenga un acceso limitado a las personas autorizadas al manejo de los mismos.

En el caso de la gestión y recepción de Curriculum, la empresa puede trabajar de forma muy fácil a través de formularios o registros directamente en la página web. Existe software específico que lo incluye en un ERM (Enterprise Resources Management o

Gestión de Riesgos empresariales, y otros de propósito general con formularios o recepción de documentación que también podría cumplir, dependiendo del tamaño de la empresa. Un ejemplo con ambas opciones (formulario y gestión de documentación es Nextcloud.[33]

En cuanto al movimiento diario con sus trabajadores con respecto a intercambio de información y documentación, la empresa puede disponer de muchas herramientas que le permite trabajar de forma totalmente segura al generar procesos de comunicación. Podemos encontrar algunas redes sociales descentralizadas y basadas en código abierto, como Mastodon[34], mediante las cuales podemos comunicarnos de manera segura, por ejemplo, con un grupo concreto de trabajo o una comunidad específica. Especialmente útil, dentro de una sociedad mercantil, es el programa de código abierto **Mattermost[35]** o Rocket.chat[36] para el intercambio de archivos y las comunicaciones internas. Creada específicamente para empresas, equipos de TI y desarrollo de *softwares* a los que les preocupan diversas cuestiones de seguridad; siendo esta una alternativa a otros tipos de programas con funciones similares, pero que no prestan la misma importancia en salvaguardar los datos que en ellas se intercambian. Los programas de código abierto permiten que las empresas limiten o pongan ciertas restricciones en su uso, facilitando con ello la adaptación a las necesidades de la organización y proporcionando una mayor seguridad a nuestros datos, al no estar este bajo control del propietario de la aplicación. Una posible herramienta podría ser Slack[37] que es una aplicación de mensajería para el trabajo en equipo, donde todos los miembros autorizados pueden acceder a información y comunicarse. Habrá que evaluar esa posibilidad teniendo en cuenta que es un servicio ofrecido por un tercero, del que desconocemos la gestión de los datos. Debe ser evaluado por el DPD en cada caso, teniendo en cuenta los tratamientos que van a realizarse.

También tenemos aplicaciones de mensajería instantánea basado en esos mismos fundamentos de seguridad y privacidad, como el programa **Ricochet Refresh[38], (**es un proyecto de código abierto para la mensajería instantánea que aún está en experimentación). Este último no solo incluye una única opción de seguridad, con el

[33] https://nextcloud.com/ (Fecha de última consulta: 31 de agosto de 2021)
[34] https://joinmastodon.org (Fecha de última consulta: 31 de agosto de 2021)
[35] https://mattermost.com (Fecha de última consulta: 31 de agosto de 2021)
[36] https://rocket.chat/es/ (Fecha de última consulta: 31 de agosto de 2021)
[37] https://slack.com/intl/es-es/ (Fecha de última consulta: 31 de agosto de 2021)
[38] https://www.ricochetrefresh.net (Fecha de última consulta: 31 de agosto de 2021)

cifrado de mensajes de extremo a extremo, sino que también mantiene los metadatos de los usuarios ocultos, haciendo imposible la extracción de información o su identificación. En los últimos tiempos, a raíz de los nuevos términos que se aplicaron en el programa Whatsapp, han cogido cierta popularidad otros programas de mensajería instantánea motivando que instituciones como el Consejo de la Unión Europea haya recomendado su descarga, para mantener a buen recaudo cierta privacidad. De manera específica recomendaron la descarga de **Signal**[39] , siendo mediante esa aplicación con la que se empezaron a comunicar con los periodistas que desarrollan su actividad en la alta institución europea.

Otra de las opciones existentes, para portales del empleado con una mayor seguridad, es la de **OrangeHRM,**[40] aunque esta opción para la gestión de Recursos Humanos es más útil en aquellas empresas con un tamaño mediano o pequeño. En este caso, el programa apuesta por el desarrollo mediante módulos para adaptarse a las necesidades societarias, abarcando desde la gestión de las vacaciones, a la creación de informes o uno donde almacenar una base de datos con toda la información necesaria sobre cada uno de los trabajadores (tipo de contrato, número de la Seguridad Social, etcétera).
Las pymes pueden acceder a paquetes ofimáticos como **Libreoffice**[41], que lo tienen todo, y sus versiones en nube con **Cryptpad**[42] o **Nextcloud**. Todas ellas tienen bases de datos, e incluso gestión de proyectos con metodología Canvas.

En definitiva, lo que se necesita para la protección de los datos que nos han sido confiados es usar medios técnicos que permitan a la empresa, huir y no caer en las garras de las empresas que "regalan" programas e instrumentos digitales (bases de datos, nubes, mensajería). para poder acceder a los datos ahí guardados para luego cederlos y venderlos en el mercado digital.

[39] https://bit.ly/3yqMGZU (Fecha de última consulta: 31 de agosto de 2021)
[40] https://www.orangehrm.com/es/ (Fecha de última consulta: 31 de agosto de 2021)
[41] https://es.libreoffice.org/ (Fecha de última consulta: 31 de agosto de 2021)
[42] https://cryptpad.fr/ (Fecha de última consulta: 31 de agosto de 2021)

7. APLICACIÓN DE LA NORMATIVA EN PROTECCIÓN DE DATOS

Una vez analizada la legislación relativa a la protección de datos de carácter personal, incidiendo en aquella que tiene especial relación con las relaciones laborales y los principales flujos de información de un departamento de RRHH, es posible tratar de acercar esta normativa a los procesos y procedimientos que se realizan desde un departamento de Recursos Humanos.

Con la intención de que este trabajo sirva como una pequeña guía genérica de apoyo a este tipo de departamentos, la realizamos como si te tratara de una pequeña y mediana empresa (en adelante, PYME) cuyo objeto social no se trate de elaboración de perfiles ni fines publicitarios, especificados como no incluidos en el RGPD.

7.1. Persona encargada de tratamiento de datos

Como pudimos analizar anteriormente, no solo existen los responsables de tratamiento de datos, sino que la figura de encargado también aparece recogida en el RGPD siendo este siendo la persona física o jurídica, autoridad pública, servicio u otro organismo que trate los datos personales por cuenta del responsable del tratamiento.

Las relaciones entre responsable y encargado deben formalizarse en un contrato o en un acto jurídico que vincule al encargado respecto al responsable. Por lo que el responsable tiene la obligación de formalizar la relación si aún no se ha formalizado.

Los contratos de encargo deben incluir aspectos como los que se muestran a continuación:

- Objeto, duración, naturaleza y la finalidad del tratamiento.
- Tipo de datos personales y categorías de interesados.
- Obligación del encargado de tratar los datos personales únicamente siguiendoinstrucciones documentadas del responsable.
- Condiciones para que el responsable pueda dar su autorización previa, específica ogeneral, a las subcontrataciones.
- Asistencia al responsable, siempre que sea posible, en la atención al ejercicio dederechos de los interesados.
- El deber de confidencialidad.
- Las medidas de seguridad que debe de adoptar el encargado para

garantizar elcumplimiento con el RGPD.

- El destino de los datos al finalizar la prestación del servicio.

Ambos, encargado y responsable del tratamiento, pueden ser sancionados de acuerdo con el RGPD si incumplen sus obligaciones, aunque la responsabilidad última sobre el tratamiento sigue estando atribuida al responsable, que es quien determina la existencia del tratamiento y su finalidad.
Será responsabilidad del responsable, la elección de encargados de protección de datos que ofrezcan las garantías suficientes para aplicar las medidas jurídicas, técnicas y apropiadas para cumplir con los requisitos establecidos por el RGPD.

Cabe destacar que son numerosas las empresas y organizaciones que externalizan este tipo de funciones a empresas especializadas en la protección de datos.

7.2. Análisis de riesgos y medidas de seguridad

Como hemos podido analizar a lo largo de este trabajo, la protección de datos no es algo que solamente sea responsabilidad de los departamentos de RRHH, es por ello, que la propia empresa deberá contar con una serie de procesos que le permitan garantizar la seguridad de los datos que maneja, como pueden ser los de proveedores y clientes. Cada empresa u organización deberá realizar un análisis de riesgos tal y como establece el RGPD.

El RGPD introduce el análisis de riesgo con la finalidad de que los responsables lleven a cabo una valoración del riesgo sobre los tratamientos que realizan. Este análisis de riesgo variará en función de:

- Los tipos de tratamiento.
- La naturaleza de los datos.
- El número de interesados.
- La cantidad y variedad de tratamientos que realice una misma organización.

Por otra parte, el RGPD no solo tiene en cuenta que el análisis de riesgo que debe abarcar las amenazas que se ciernen sobre la organización, sino también al riesgo existente en aplicar actividades de tratamiento sobre los datos personales de los interesados.

La AEPD en su guía práctica de análisis de riesgo en los tratamientos de datos

personales[43] sujetos al RGPD, detalla una hoja de ruta a seguir para realizar un correcto análisis de riesgo:

a) Implantar la protección de datos desde el diseño y por defecto.

   Entendiendo que el análisis de riesgo se debe de tener en cuenta desde el mismo momento en el que se están definiendo las actividades de tratamiento. El responsable debe establecer procedimientos de control y seguridad que garanticen los principios de protección de datos.

b) Definición y el diseño de las actividades de tratamiento.

La definición de una actividad de tratamiento es un paso que requiere tener claro cuáles son las finalidades del tratamiento de datos personales. Corresponde a cada organización, de acuerdo con el principio de responsabilidad proactiva, decidir el nivel de agregación o segregación para elaborar el registro de actividades de tratamiento ydebe valorar hasta qué punto esa agregación o segregación corresponde con las finalidades, las bases jurídicas y los grupos de individuos distintos.

La definición de las actividades de tratamientos permite obtener un conocimiento sobre el ciclo de vida de los datos, de las actividades realizadas y de cualquier elemento que interviene en las mismas.

c) Una vez se han definido todas las actividades de tratamiento, se deben atender a las obligaciones que describe el RGPD sobre los responsables y los encargados, y analizar si es necesario incluir nuevas actividades de tratamiento.

El artículo 5 del RPGD establece que el responsable del tratamiento deberá garantizar el cumplimiento de los principios relativos al tratamiento y ser la figura responsable de demostrarlo. Por tanto, es fundamental definir adecuadamente las actividades de tratamiento y documentar los análisis realizados,así como, dejar trazabilidad de estos y de las conclusiones que los soportan para poder garantizar la responsabilidad proactiva.

Llegados a este punto, en el que se tiene definidas las actividades, se podrá proceder a

[43] Guía práctica de análisis de riesgo en los tratamientos de datos personales elaborada por la Agencia Española de Protección de Datos. Disponible en guia-analisis-de-riesgos-rgpd.pdf (aepd.es) (Fecha de última consulta: 31 de agosto de 2021)

analizar el riesgo que puede conllevar cada una de ellas, tratando de dirimir cuáles de ellas puedan conllevar un escaso riesgo o por el contrario, conllevar un riesgo elevado y por tanto tener que proceder a realizar una evaluación de impacto sobre estas.

El artículo 35.3 del RGPD describe los siguientes casos en los cuales se ha considerado que un tratamiento puede derivar en alto riesgo:

- Evaluación sistemática y exhaustiva de aspectos personales de personas físicas quese basan en un tratamiento automatizado como la elaboración de perfiles y sobre cuyabase se toman decisiones que producen efectos jurídicos para las personas físicas o que les afectan de modo similar.
- Tratamiento a gran escala de las categorías especiales de datos personales, o datos sobre condenas e infracciones penales o medidas de seguridad conexas.
- Observación sistemática a gran escala de una zona de acceso público.
- Los riesgos son variables y pueden cambiar ante variaciones en las actividades de tratamiento. Para garantizar una adecuada gestión de riesgos se debe tener en cuenta una monitorización continua de los riesgos y una evaluación periódica de la efectividad de las medidas de control definidas para reducir el nivel de exposición al riesgo.

En caso de que se determine que no es necesario realizar una evaluación de impacto, se debe documentar adecuadamente los motivos por los cuales se ha llegado a esa conclusión. En cualquier caso, se debe mantener evidencia de que se ha llevado a cabo este análisis.

En el caso que nos ocupa de los RRHH se deberá realizar un análisis, ya no solo los flujos de información como tal, que vimos anteriormente, sino los soportes en los que se realizan, los tipos de ficheros en los que se almacena, las personas que deben tener acceso a los mismos, personas con capacidad de visualizar y o de modificar datos, creación de usuarios y contraseñas adecuadas, seguridad de los propios dispositivos de acceso, certificados digitales, apoderamientos de acceso a los mismos, traspaso de información a terceros, copias de seguridad, … Pero no solo hablamos de la seguridad de estos datos en formato digital, es necesario analizar todos los flujos de información y de tratamiento de los datos en formato papel que pueden existir en las dependencias del departamento, las nomenclaturas que puedan estar a la vista de otros trabajadores o terceros que acudieran a ella, proteger el acceso a archivos, registros etc. y por supuesto contemplar la

destrucción de documentos cuando fuese necesario cumpliendo con los requisitos de la propia normativa relativa a la protección de datos.

Realizar este análisis de las actividades que se realizan en el departamento y el posible riesgo, así como tomar medidas de seguridad para paliar cada una de ellas, es indispensable para poder desarrollar una correcta aplicación de la protección de datos.

Desde el punto de vista de las medidas de seguridad, se debe tener en cuenta, que dichas medidas de seguridad deben ser acordes con el fin que buscan, la empresa u organización que las gestiona y el tipo de datos de que se trate y para ello, se debe tener en cuenta para la adopción de tales medidas cuestiones como:

- El coste de la técnica.
- Los costes de aplicación.
- La naturaleza, el alcance, el contexto y los fines del tratamiento.
- Los riesgos para los derechos y libertades.

El responsable tiene la obligación de implicarse en la definición, difusión y control delas normas de seguridad entre el personal encargado de llevarlas a cabo o simplemente de respetarlas.

Otra obligación que tienen los responsables y los encargados es la de redactar un documento de seguridad. En la guía de seguridad de datos de la AEPD se muestran los apartados mínimos que debe incluir el documento de seguridad entre los que podemos destacar:

- Medidas, normas, procedimientos, reglas y estándares de seguridad.
- Funciones y obligaciones del personal, estructura y descripción de los ficheros y sistemas de información.
- Procedimiento de notificación, gestión y respuesta ante incidencias.
- Procedimiento de copias de respaldo y recuperación de datos.
- Medidas adoptadas en el transporte, destrucción yo reutilización de soportes y documentos.
- Identificación del responsable de seguridad y control periódico del cumplimiento del documento.

7.3. Deber de confidencialidad

El RGPD establece en sus artículos 28 y 90 la exigencia de guardar secreto profesional de los datos, a aquellas personas que intervengan en cualquier fase del proceso de tratamiento de datos. Por ello, el responsable de los datos debe garantizar la confidencialidad de las personas autorizadas para el tratamiento de datos, normalmente mediante cláusulas contractuales con consecuencias jurídicas y laborales en caso de incumplimiento.

En el caso de los RRHH será necesario delimitar las funciones de tratamiento de cada una de las personas que formen parte del departamento, bien sean de acceso, de archivo, de modificación, de consulta etc., como ya vimos anteriormente, para poder establecer las personas con las que se debe fijar cláusulas de confidencialidad específicas, sin dejar de lado el hecho de que se trata de un departamento que ya de por sí, maneja todo tipo de información especialmente sensible y que conlleva la confidencialidad de manera intrínseca.

7.4. Notificación de violaciones de seguridad

El RGPD define violaciones de seguridad de los datos o quiebras de datos como todo incidente que ocasione la destrucción, pérdida, o alteración accidental o ilícita de datos personales transmitidos, conservados, o tratados de otra forma, o la comunicación, o acceso no autorizado a dichos datos.

Casos que pudieran darse en un departamento de RRHH como el robo o extravío de ordenadores, el acceso no autorizado a una base de datos incluso cuando fuese por personal del propio departamento o el borrado accidental de ficheros, serán consideradas violaciones de seguridad y por tanto deberán ser tratadas como tal bajo la normativa del RGPD, cumpliendo los siguientes requisitos.

En primer lugar, el responsable debe notificar a la autoridad de protección de datos competente, a menos que se considere improbable que la violación suponga un riesgo para los derechos y libertades de los afectados. Si se realizara tal comunicación deberá producirse sin dilación indebida, en el plazo de 72 horas desde su conocimiento por parte del responsable y conteniendo al menos la siguiente información:

- Naturaleza de la violación
- Categoría de datos y de interesados afectados

- Medidas adoptadas por el responsable para solventar la violación
- Si procede, medidas aplicadas para paliar los posibles efectos negativos sobre los interesados

Se deberá notificar a los interesados afectados por tal violación sin dilación indebida, así como recomendaciones sobre las medidas que pueden tomar para hacer frente a las posibles consecuencias de esta quiebra de seguridad.

7.5. Medidas de responsabilidad proactiva

Es necesario que cada empresa u organización realice una valoración de los riesgos que puede conllevar el tratamiento de los datos de carácter personal que realiza, realizar un registro de las actividades de tratamiento que realiza y mantenerlo actualizado.

Es necesario revisar las medidas de seguridad a medida que se actualizan las actividades o de que haya sucedió algún tipo de incidente, así como establecer mecanismos para conocer con rapidez posibles violaciones de seguridad y medidas de reacción.

Será necesario que el departamento de RRHH realice esta valoración en base a las actividades de tratamiento que realiza. En este caso, para este trabajo se ha tratado de analizar las actividades más comunes que se desarrollan en el departamento para visualizar la complejidad de las mismas.

7.6. Resumen de las principales obligaciones en relación al cumplimiento del RGPD, en relación a un departamento de Recursos Humanos

Tras haber realizado un análisis de la normativa en relación a la protección de datos de carácter personal, ahondando en cada una de las partes más relevantes, haremos un resumen de cada uno de los pasos que se deben tener en cuenta, desde la óptica de un departamento de RRHH, con la intención de facilitar la comprensión y cumplimiento de esta normativa. Para ello se utiliza de base la Guía del Reglamento de Protección de Datos para responsables de tratamiento, elaborada por la AEPD.[44]

7.6.1. Legitimación y consentimiento

[44] Guía de directrices para la elaboración de contratos entre responsables y encargados del tratamiento elaborada por la Agencia Española de protección de datos. Disponible en guia-directrices-contratos.pdf (aepd.es) (Fecha de última consulta: 31 de agosto de 2021)

Establecer claramente cuál es la base legal de los tratamientos que se vayan a realizar y contar con el consentimiento de los interesados es la base para poder cumplir con la protección de datos.

En el ámbito de los RRHH la base jurídica que legitima para poder tratar los datos es la ejecución de un contrato de trabajo, así como cumplir con las obligaciones legales aplicables al responsable del tratamiento, como podría ser cumplir con las exigencias de cotizaciones de la Seguridad Social, para lo que es imprescindible y necesario contar con los datos de la persona trabajadora y tratarlos.

Cuando sea necesario el consentimiento del trabajador, éste deberá ser inequívoco, libre y específico.

Se debe tener en cuenta que el consentimiento individual no puede ser sustituido por uno indirecto y plural, como podría ser a través de la negociación colectiva.

7.6.2. Información y derechos

Es necesario proporcionar a los interesados toda la información relativa a la protección de datos de forma clara, concisa, transparente y de fácil acceso cumpliendo con los requisitos del RGPD. Así mismo es necesario contar con mecanismos para poder hacer valer cada uno de los derechos de los interesados y todos los formularios para ello.

Será necesario que los departamentos de RRHH cuenten con toda la documentación necesaria para que los interesados puedan tener conocimiento en todo momento el tratamiento que se le da a sus datos, sus derechos y la forma en que pueden ser ejercidos.

Existen multitud de formularios para ello, la AEPD pone a disposición de las empresas y organizaciones modelos tipo que pueden servir de base como los que se han ido exponiendo en este trabajo y que pueden ser consultados en los anexos,

7.6.3. Relaciones entre responsable y encargado

Existe la posibilidad de contar con encargados de protección de datos, siendo personas físicas o jurídicas que se encargan del tratamiento de los datos y con los que habría que formalizar un contrato, aunque la responsabilidad del tratamiento seguirá recayendo sobre el responsable, por lo que este deberá velar porque cumpla con los requisitos establecidos en el RGPD de datos para ello.

Es posible que los departamentos de RRHH contraten servidores o programas para la realización de nóminas o por ejemplo que recurran a la externalización de los procesos selectivos. El responsable de los datos seguirá siendo de la empresa, ya que es a quien los trabajadores le han cedido sus datos.

8. CONCLUSIONES

A tenor de las conclusiones generales que emanan de la investigación realizada sobre las normas que regulan actualmente la protección de datos en España y, tras el análisis realizado en este trabajo, se puede afirmar que es posible organizar los recursos humanos de una empresa con total seguridad siguiendo las directrices del RGPD.

Esta aseveración se basa en que la normativa vigente pone a disposición de las empresas y administraciones las herramientas necesarias para garantizar la gestión adecuada de la protección de datos dentro de cualquier departamento de recursos humanos, sea cual sea su tamaño. Además, el coste económico es muy bajo en comparación con la seguridad y garantías que aporta e incluso su implantación puede llegar a ser gratuita a través de algunas herramientas que pone a disposición la AEPD y que presentamos en este trabajo.

El origen del problema actual por el que muchas empresas continúan sin contar con un sistema propio de protección de datos vinculado de forma directa a su concepto de Recursos Humanos se debe al desconocimiento que existe sobre cómo aplicarlo y a dónde acudir para hacerlo correctamente y de forma eficiente. Sin embargo, cada vez son más las empresas que se muestran favorables a realizar sus registros de actividades para conocer cuáles pueden ser sus posibles brechas de seguridad en materia de protección de datos.

En resumen, la legislación en materia de protección de datos aplicada concretamente a los Recursos Humanos es el mejor instrumento que tienen a su alcance las empresas e instituciones para contar con una eficiente protección de datos que además permita prevenir posibles problemas y todo ello sin tener que realizar un esfuerzo económico, puesto que cada sociedad podría adaptar su sistema a sus necesidades a su ámbito de actuación y a sus medios.

Los objetivos planteados a la hora de iniciar un trabajo de estas características obligan a conocer en profundidad las diferentes normativas vinculadas a la protección de datos de carácter personal para, a continuación, poder establecer con rigor cuánto se ha tenido que avanzar en el marco normativo para no quedar obsoleto ante una materia íntimamente ligada a la era digital, que avanza a pasos mucho más rápidos que la propia sociedad.

Este análisis ha contribuido a poner de manifiesto cómo nuestro ordenamiento jurídico cuenta con las herramientas necesarias para no dejar sin contenido nuevos derechos, tal y como ha demostrado al interpretar el artículo 18.4 CE, relativo al uso de la informática para garantizar el honor y la intimidad personal, a través de Sentencias del Tribunal Constitucional, reconociendo como un derecho fundamental el garantizar a las personas un poder de control y de disposición sobre sus datos personales.

Como establece el propio preámbulo de la LOPDgdd nos encontramos ante una sociedad cada vez más globalizada, lo que ha hecho necesario lograr una regulación de carácter uniforme supranacional y de ahí que el RGPD se haya conformado como la base para la legislación de esta materia en la Unión Europea.

A lo largo de este trabajo se exponen de forma detallada los aspectos más importantes de la normativa vigente en relación a la protección de datos personales con la intención de contribuir al conocimiento de este tipo de normativa, incidiendo en los aspectos relacionados con los RRHH. Cabe destacar que, en los departamentos de RRHH de las empresas u organizaciones, independientemente de su tamaño, se realizan multitud de tratamientos de datos, muchos de ellos especialmente sensibles y, por tanto, es de vital importancia tener conocimiento de al menos sus aspectos básicos para poder realizarlos correctamente.

Existe cierto desconocimiento en lo relativo a la protección de datos en el ámbito empresarial, pero sobre todo en el ámbito social, siendo una materia que afecta directamente a la ciudadanía en su día a día, sin ser conscientes de la misma. No nos referimos solo a los derechos que tengan los trabajadores como tal en el seno de una organización, sino a la ausencia de conocimientos básicos por parte de la ciudadanía sobre la cesión de datos, su confidencialidad, el uso y tráfico de los mismos, ni el alcance de los derechos de los que es titular y cuyo ejercicio está completamente recogido en la legislación vigente, contando incluso con la AEPD que pone a su disposición diferentes explicaciones y modelos para ello.

A pesar de contar con un conjunto de normas y herramientas que tratan de garantizar los derechos de la ciudadanía inmersa la era digital, se desconoce su alcance, a pesar de relacionarse y trabajar cada día de forma más habitual, mediante medios digitales sin conocer su grado de seguridad.

Whatsapp, Google, Gmail, Hotmail, Facebook, Instagram, Telegram, Meet, son algunas de las aplicaciones que de forma más habitual son utilizadas no solo por la ciudadanía en su esfera personal, sino en el ámbito organizacional e incluso académico. Sin embargo, este tipo de aplicaciones no son caracterizadas por el cumplimiento exhaustivo de la privacidad de sus usuarios y teniendo en cuenta que los datos han sido catalogados como el petróleo de nuestra era, cabe pensar que los datos utilizados al hacer uso de ellas, pasan a formar parte de ese nuevo mercado. Es por ello, que sin más afán que tratar de ofrecer otras alternativas de comunicación más seguras, se han expuesto algunas alternativas, especialmente pensadas en el ámbito de los Recursos Humanos, pero válidas para todos ellos.

Recordemos que el ámbito organizacional ha realizado un esfuerzo de adaptación a la legislación relativa a la protección de datos , en la que se fomenta la actitud de mejora y de cumplimiento mediante los Registros de Actividades de Tratamiento de Datos y donde cada día existen más empresas y asesorías especializadas en adecuar los medios de éstas al cumplimiento de la misma, pero eso no evita que aún quede un largo camino por recorrer, ya que, para poder desarrollar una sociedad consciente de la importancia de la protección de sus propios datos personales, se hace necesario incidir en la importancia de la formación relacionada con la misma.

Quizás la clave de todo radique en que la gran mayoría de los usuarios y usuarias de tecnología, da igual su localización, nivel de estudios, sexo o conocimientos académicos confían e incluso dan por hecho que el problema de la protección de su privacidad no es algo que les atañe a ellos como sujetos interesados, sino a las marcas, programas informáticos, apps, etc. Por eso cuando salta a la luz algún escándalo vinculado al uso fraudulento de datos personales no es usual extremar la precaución ni proceder a informarse con detalle de las políticas de privacidad de los productos que se consumen o utiliza, ni de los derechos de los que se es titular. Muchos de nosotros pensamos que seguridad equivale de forma automática a privacidad. Muchas de las plataformas, páginas internet ofrecen sus servicios de forma gratuita por un lado y usar nuestros datos para fines de mercadotecnia, elaboración de perfiles, trazado de modelos conductuales a pesar de ser actividades casi prohibidas en el Reglamento de protección de datos.

En la medida en que las organizaciones, así como los usuarios y usuarias vayan siendo cada vez más proactivos y, por tanto, conscientes de las repercusiones que derivan de la

utilización de espacios virtuales poco seguros e incluso a reconocerlos para evitarlos, se podrá seguir avanzando en la denominada cultura de la privacidad.

Creemos que, en nuestra sociedad, los individuos no están realmente concienciados de la importancia de la protección de sus datos, de tener conocimiento de quien los tiene, donde los tienen y que se hace con los mismos. Entendemos que, para llegar a la cultura de la privacidad, el único camino es la formación e información de todos y todas.

Creemos que las Universidades y Centros de formación tienen que tener en sus planes de estudio una asignatura contundente que dé la formación necesaria para que las futuras personas trabajadoras, empresarias, autónomas puedan tomar consciencia de la importancia de esta faceta de las organizaciones.

También crear formaciones universitarias para formar un elenco de profesionales del mundo de la protección de datos que puedan acometer, informar y asesorar a las futuras empresas.

9. BIBLIOGRAFÍA Y OTRAS REFERENCIAS BIBLIOGRÁFICAS

A. Bibliografía

ARIAS BENITEZ, R., ¿Puede un empresario obligar a sus trabajadores a estar geolocalizables?, Aranzadi digital. núm. 1 (2021)

DE MARCOS, I. (2012). Breve aproximación a las implicaciones jurídicas y operativas del tratamiento de datos de salud. *Gaceta Médica de México*, 148(5), 480-486.

FAJARDO LÓPEZ, L.: "Título I. Capítulo II. Derechos y deberes; artículos de 25, 28 Y 30", en AA.VV. (SUAY RINCÓN, J. VILAR ROJAS, F.) El Estatuto de Autonomía de Canarias, Ley Orgánica 1/2018, de 5 de noviembre, 1ºed., Ed. Aranzadi, Navarra,2019, pág. 164-173.

PÉREZ, A. (2016). La protección de los derechos fundamentales de los menores en Internet desde la perspectiva europea. Ius Et Praxis (Talca, Talca, Chile), 22(1), 377-415.

PIÑAR MAÑAS, J.L.,"Reglamento General de Protección de Datos, hacia un nuevo modelo europeo de privacidad"1º ed., Reus (Madrid, 2016) pag 19-20

RODRÍGUEZ ÁLVAREZ, J.L. y FAJARDO LÓPEZ, L. "La defensa de libertades ante la vigilancia y tratamiento masivo de datos", XII Congreso Nacional de la Abogacía, Consejo General de la Abogacía Española, 2019 (material de acceso restringido, cedido por el ponente para este trabajo). Otras referencias: Abogacía (Revista del Consejo General de la Abogacía Española), n.º 115, mayo 2019.

ZUBOFF, S., *La era del capitalismo de la vigilancia*, Paidós (2020, Spanish edition) p.11 y s.s.

Guía de Protección de Datos en las Relaciones Laborales publicada por la Agencia Española de Protección de Datos. Disponible en La protección de datos en las relaciones laborales (aepd.es)

Guía de la Guía práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD. Disponible en https://www.aepd.es/sites/default/files/2019-09/guia-analisis-de-riesgos-rgpd.pdf

Guía para el ciudadano por la Agencia Española de Protección de Datos. Disponible en Guía para el Ciudadano (aepd.es)

Guía práctica de análisis de riesgo en los tratamientos de datos personales elaborada por la Agencia Española de Protección de Datos. Disponible en guia-analisis-de-riesgos-rgpd.pdf (aepd.es)

Guía de directrices para la elaboración de contratos entre responsables y encargados del tratamiento elaborada por la Agencia Española de protección de datos. Disponible en guia-directrices-contratos.pdf (aepd.es)

B. Otras referencias Bibliográficas y webs

https://www.aepd.es/es

https://www.mac-mutua.org/

https://www.sepe.es/

https://delta.mites.gob.es/Delta2Web/main/nuevoUsuario.jsp

https://sepe.es/HomeSepe/empresas/servicios-para-empresas/comunica-contratacion.html

https://www.sepe.es/HomeSepe/empresas/servicios-para-empresas/certificados.html

C. Referencias legislativas

Real Decreto de 22 de agosto de 1885 por el que se publica el Código de Comercio

Constitución Española. Cortes Generales «BOE» núm. 311, de 29 de diciembre de 1978

Ley Orgánica 2/1984, de 26 de marzo, reguladora del derecho de rectificación. Jefatura del Estado. «BOE» núm. 74, de 27 de marzo de 1984

Real Decreto 428/1993 de 26 de marzo por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos.

Ley 31/1995, de 8 de noviembre, de prevención de Riesgos Laborales. Jefatura del Estado. «BOE» núm. 269, de 10 de noviembre de 1995.

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Jefatura del Estado. «BOE» núm. 298, de 14 de diciembre de 1999

Real Decreto legislativo 5/2000 de 4 de agosto, Sobre infracciones y Sanciones en el Orden Social (LISOS). Ministerio de Trabajo y Asuntos Sociales. «BOE» núm. 189, de 8 de agosto de 2000.

Ley 58/2003, de 17 de diciembre, General Tributaria. Jefatura del Estado. «BOE» núm. 302, de 18 de diciembre de 2012.

Real Decreto 625/2014, de 18 de julio, por el que se regulan determinados aspectos de la gestión y control de los procesos por incapacidad temporal en los primeros trescientos sesenta y cinco días de su duración. Ministerio de Empleo y Seguridad Social. «BOE» núm. 176, de 21 de julio de 2014

Ley 40/2015, de 1 de octubre, de régimen Jurídico del Sector Público. «BOE» núm. 236, de 2 de octubre de 2015.

Ley 39/2015, de 1 de octubre, del procedimiento Administrativo Común de las Administraciones Públicas. «BOE» núm. 236, de 2 de octubre de 2015.

Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores. Ministerio de Empleo y Seguridad Social. «BOE» núm. 255, de 24 de octubre de 2015

Ley Orgánica 1/2018, de 5 de noviembre, de reforma del Estatuto de Autonomía de Canarias.

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Jefatura del Estado. «BOE» núm. 294, de 06 de diciembre de 2018

D. Otras referencias normativas

REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)

10.ANEXOS

EJERCICIO DEL DERECHO DE ACCESO

DATOS DEL RESPONSABLE DEL TRATAMIENTO.

Nombre / razón social: ..... Dirección de la Oficina / Servicio ante el que se ejercita el derecho de acceso: C/Plaza ..... nº ..... C.Postal ..... Localidad ..... Provincia ..... Comunidad Autónoma .....

DATOS DEL AFECTADO O REPRESENTANTE LEGAL.

D./ Dª. ....., mayor de edad, con domicilio en la C/Plaza ..... nº....., Localidad ..... Provincia ..... C.P. ..... Comunidad Autónoma ..... con D.N.I....., con correo electrónico……..por medio del presente escrito ejerce el derecho de acceso, de conformidad con lo previsto en el artículo 15 del Reglamento UE 2016/679, General de Protección de Datos (RGPD).

SOLICITA

Que se le facilite gratuitamente el derecho de acceso por ese responsable en el plazo de un mes a contar desde la recepción de esta solicitud, y que se remita, a la dirección arriba indicada, la siguiente información:

-Copia de mis datos personales que son objeto de tratamiento por ese responsable.

-Los fines del tratamiento, así como las categorías de datos personales que se traten.

-Los destinatarios o categorías de destinarios a los que se han comunicado mis datos personales, o serán comunicados, incluyendo, en su caso, destinatarios en terceros u organizaciones internacionales.

-Información sobre las garantías adecuadas relativas a la transferencia de mis datos a un tercer país o a una organización internacional, en su caso.

-El plazo previsto de conservación, o de no ser posible, los criterios para determinar este plazo.

-Si existen decisiones automatizadas, incluyendo la elaboración de perfiles, información significativa sobre la lógica aplicada, así como la importancia y consecuencias previstas de dicho tratamiento.

-Si mis datos personales no se han obtenido directamente de mí, la información disponible sobre su origen.

-La existencia del derecho a solicitar la rectificación, supresión o limitación del tratamiento de mis datos personales, o a oponerme a dicho tratamiento.

-El derecho a presentar una reclamación ante una autoridad de control.

En .....a.....de.....de 20.....

EJERCICIO DERECHO DE RECTIFICACIÓN

DATOS DEL RESPONSABLE DEL TRATAMIENTO.

Nombre / razón social: ..... Dirección de la Oficina / Servicio ante el que se ejercita el derecho de rectificación: C/Plaza ..... nº ..... C.Postal ..... Localidad ..... Provincia ..... Comunidad Autónoma ..... **DATOS DEL AFECTADO O REPRESENTANTE LEGAL.**

D./ Dª. ....., mayor de edad, con domicilio en la C/Plaza ..... nº....., Localidad ..... Provincia ..... C.P. ..... Comunidad Autónoma ..... con D.N.I....., con correo electrónico……..por medio del presente escrito ejerce el derecho de rectificación, de conformidad con lo previsto en el artículo 16 del Reglamento UE 2016/679, General de Protección de Datos (RGPD).

SOLICITA

Que se proceda a acordar la rectificación de los datos personales, que se realice en el plazo de un mes a contar desde la recepción de esta solicitud, y que se me notifique de forma escrita el resultado de la rectificación practicada.

Datos sobre los que solicito el derecho de rectificación:
……
……
……..

Que en caso de que se acuerde que no procede practicar la rectificación solicitada, se me comunique motivadamente a fin de, en su caso, reclamar ante la Autoridad de control que corresponda.

Asimismo, en caso de que mis datos personales hayan sido comunicados por ese responsable a otros responsables del tratamiento, se comunique esta rectificación a los mismos.

En .....a.....de.....de 20.....

Firmado:

EJERCICIO DEL DERECHO DE SUPRESIÓN

DATOS DEL RESPONSABLE DEL TRATAMIENTO

. Nombre / razón social: ..... Dirección de la Oficina / Servicio ante el que se ejercita el derecho de supresión: C/Plaza ..... nº ..... C.Postal ..... Localidad ..... Provincia ..... Comunidad Autónoma ..... **DATOS DEL AFECTADO O REPRESENTANTE LEGAL.**

D./ Dª. ....., mayor de edad, con domicilio en la C/Plaza ..... nº....., Localidad ..... Provincia ..... C.P. ..... Comunidad Autónoma ..... con D.N.I....., con correo electrónico……..por medio del presente escrito ejerce el derecho de supresión, de conformidad con lo previsto en el artículo 17 del Reglamento UE 2016/679, General de Protección de Datos (RGPD).

SOLICITA

Que se proceda a acordar la supresión de sus datos personales en el plazo de un mes a contar desde la recepción de esta solicitud, y que se me notifique de forma escrita el resultado de la supresión practicada.

Que en caso de que se acuerde que no procede practicar total o parcialmente la supresión solicitada, se me comunique motivadamente a fin de, en su caso, reclamar ante la Autoridad de control que corresponda.

Que en caso de que mis datos personales hayan sido comunicados por ese responsable a otros responsables del tratamiento, se comunique esta supresión.

En .....a.....de.....de 20.....

Firmado:

EJERCICIO DEL DERECHO A LA LIMITACIÓN DEL TRATAMIENTO

DATOS DEL RESPONSABLE DEL TRATAMIENTO.

Nombre / razón social: ..... Dirección de la Oficina / Servicio ante el que se ejercita el derecho de limitación: C/Plaza ..... nº ..... C.Postal ..... Localidad ..... Provincia ..... Comunidad Autónoma

DATOS DEL AFECTADO O REPRESENTANTE LEGAL.

D./ Dª. ....., mayor de edad, con domicilio en la C/Plaza ..... nº....., Localidad ..... Provincia ..... C.P. ..... Comunidad Autónoma ..... con D.N.I....., con correo electrónico ……,por medio del presente escrito ejerce el derecho de limitación, de conformidad con lo previsto en el artículo 18 del Reglamento UE 2016/679, General de Protección de Datos (RGPD).

SOLICITO

Que se limite el tratamiento de mis datos personales, teniendo en consideración: (marcar)

Que el tratamiento es ilícito y me opongo a su supresión.

Que el responsable ya no necesita mis datos personales para los fines para los cuales fueron recabados, pero los necesito para la formulación, ejercicio o defensa de mis reclamaciones.

Que sea atendida mi solicitud en los términos anteriormente expuestos en el plazo de un mes, y que se comunique esta limitación a cada uno de los destinatarios que ese responsable del tratamiento haya comunicado mis datos personales.

En .....a.....de.....de 20.....

Firmado

EJERCICIO DEL DERECHO A LA PORTABILIDAD DE LOS DATOS

DATOS DEL RESPONSABLE DEL TRATAMIENTO.

Nombre / razón social: ..... Dirección de la Oficina / Servicio ante el que ejercita el derecho a la portabilidad de los datos: C/Plaza ..... nº ..... C.Postal ..... Localidad ..... Provincia ..... Comunidad Autónoma ..... **DATOS DEL AFECTADO O REPRESENTANTE LEGAL.**

D./ Dª. ....., mayor de edad, con domicilio en la C/Plaza ..... nº....., Localidad ..... Provincia ..... C.P. ..... Comunidad Autónoma ..... con D.N.I....., con correo electrónico ..... por medio del presente escrito ejerce el derecho la la portabilidad de los datos, de conformidad con lo previsto en el artículo 20 del Reglamento UE 2016/679, General de Protección de Datos (RGPD).

SOLICITA

Que se le faciliten en el plazo de un mes sus datos personales en un formato estructurado, de uso común y lectura mecánica.

En su caso, que los citados datos personales sean transmitidos directamente al responsable ……(especifíquese nombre o razón social), siempre que sea técnicamente posible.

En .....a.....de.....de 20.....

Firmado