N/REF: 0073/2020

Examinada su solicitud de informe urgente, remitida a este Gabinete Jurídico, referente al Anteproyecto de Ley por el que se regula el trabajo a distancia, solicitado de esta Agencia Española de Protección de Datos de conformidad con lo dispuesto en los artículos 57.1.c) del 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 por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) y 5 b) del Estatuto de la Agencia, aprobado por Real Decreto 428/1993, de 26 de marzo, cúmpleme informarle lo siguiente:

Antes de entrar a analizar el texto sometido a informe es preciso señalar que, habida cuenta de la fundamentación legal del informe que inmediatamente va a evacuarse y su carácter preceptivo, a tenor de lo dispuesto en las normas que acaban de señalar, debería indicarse en la Exposición de Motivos de la norma que la misma ha sido sometida al previo informe de la Agencia Española de Protección de Datos. Asimismo, deberá recogerse la emisión del presente informe y su valoración en la Memoria de Análisis de Impacto Normativo.

Por otro lado, habiéndose autorizado por Acuerdo del Consejo de Ministros del pasado 23 de junio la tramitación administrativa urgente prevista en el artículo 27.1.b) de la Ley 50/1997, de 27 de noviembre, del Gobierno, y habiéndose solicitado el informe el 11 de septiembre, se procede a su emisión a la mayor brevedad, sin perjuicio de que hubiera sido deseable un análisis más detenido del mismo, dada la implicación que su regulación tiene en el derecho fundamental a la protección de datos de carácter personal.

I

El Anteproyecto remitido tiene por objeto la regulación del trabajo a distancia, entendido como “forma de organización del trabajo o de realización de la actividad laboral conforme a la cual esta se presta en el domicilio de la persona trabajadora o en el lugar elegido por esta, durante toda su jornada o parte de ella, con carácter regular” y del que es una subespecie el “teletrabajo”, definido como “aquel trabajo a distancia que se lleva a cabo mediante el uso exclusivo o prevalente de medios y sistemas informáticos, telemáticos y de telecomunicación”, siendo de aplicación, según su artículo 1, a las relaciones de trabajo “en las que concurran las condiciones descritas en el artículo 1.1 del texto refundido de la Ley del Estatuto de los Trabajadores aprobado por Real Decreto Legislativo 2/2015, de 23 de octubre, que se

desarrollen a distancia con carácter regular. Se entenderá que el trabajo a distancia es regular cuando, en un periodo de referencia de tres meses, un mínimo del 30 por ciento de la jornada, o el porcentaje proporcional equivalente en función de la duración del contrato, sea prestada bajo esta modalidad".

La norma proyectada pretende adecuar la regulación del trabajo a distancia a las nuevas relaciones laborales, influidas por el mayor uso de las nuevas tecnologías y que se han incrementado como consecuencia de la pandemia del COVID-19, tal y como señala su Exposición de Motivos:

> "2. El trabajo a distancia, en su concepción clásica de trabajo a domicilio, como aquel que se realiza fuera del centro de trabajo habitual y sin el control de la empresa y vinculado a sectores y ámbitos geográficos muy concretos, se ha visto superado por la realidad de un nuevo marco de relaciones y un impacto severo de las nuevas tecnologías.
>
> En la actualidad, más que trabajo a domicilio lo que existe es un trabajo remoto y flexible, que permite que el trabajo se realice en nuevos entornos que no requieren la presencia de la persona trabajadora en el centro de trabajo.
>
> Esta virtualización de las relaciones laborales desvincula o deslocaliza a la persona trabajadora de un lugar y un tiempo concretos, lo que sin duda trae consigo notables ventajas, entre otras, mayor flexibilidad en la gestión de los tiempos de trabajo y los descansos; mayores posibilidades, en algunos casos, de una autoorganización, con consecuencias positivas, en estos supuestos, para la conciliación de la vida laboral. personal y familiar; reducción de costes en las oficinas y ahorro de costes en los desplazamientos; productividad y racionalización de horarios; compromiso y experiencia de la persona empleada; atracción y retención de talento o reducción del absentismo.
>
> Sin embargo, también presenta posibles inconvenientes: protección de datos, brechas de seguridad, tecnoestrés, horario continuo, fatiga informática, conectividad digital permanente, mayor aislamiento laboral, pérdida de la identidad corporativa, deficiencias en el intercambio de información entre las personas que trabajan presencialmente y aquellas que lo hacen de manera exclusiva a distancia, o traslado a la persona trabajadora de costes de la actividad productiva sin compensación alguna, entre otros.
>
> El impacto real de estas formas de prestación u organización del trabajo se vio incrementada de manera exponencial por el impacto de la pandemia de la COVID-19, lo que ha puesto de manifiesto sus ventajas y debilidades, así como la necesidad de que se aborde su regulación desde un marco jurídico de seguridad, certeza y transparencia."

La insuficiencia del marco legislativo actual se destaca en la MAIN, por transcripción del Acuerdo del Consejo de Ministros de 23 de junio:

"El Anteproyecto de Ley que se propone tiene por objeto cubrir el vacío legal sobre condiciones mínimas aplicables al trabajo a distancia, dada la insuficiencia del marco regulatorio actual constituido por el artículo 13 del Estatuto de los Trabajadores.

Dicha insuficiencia se ha puesto de manifiesto recientemente, debiendo abordarse con carácter urgente a través del artículo 5 del Real Decreto-ley 8/2020, de 17 de marzo, de medidas urgentes extraordinarias para hacer frente al impacto económico y social del COVID-19, en el que se estableció el carácter preferente del trabajo a distancia debiendo la empresa adoptar las medidas oportunas si ello es técnica y razonablemente posible y si el esfuerzo de adaptación necesario resulta proporcionado. Como resulta de las exposiciones de motivos de dicha norma y del Real Decreto-ley 15/2020, en la crisis de la COVID-19 el teletrabajo constituye un medio preferente para garantizar la continuidad de la actividad empresarial, para garantizar las medidas de contención y la protección de las personas trabajadoras y para seguir atendiendo a las necesidades de conciliación de la vida laboral y familiar. Dicho precepto ha sido prorrogado en su vigencia durante los dos meses posteriores al cumplimiento de la vigencia prevista en el párrafo primero de la disposición final décima del presente Real Decreto-ley 8/2020, de 17 de marzo.

En definitiva, la crisis sanitaria ha normalizado el uso del trabajo a distancia y ha acelerado una tendencia que ya se advertía con anterioridad, pero, sobre todo, ha permitido advertir no solo las potencialidades, sino también los retos de una forma de trabajo que hasta ahora ha sido peculiar en nuestro país, pero que probablemente no lo será tanto a partir de ahora. En países de nuestro entorno las cifras reflejan claramente el aumento exponencial del uso de estas formas de prestación no presenciales situándose por encima del 50%.

La extensión y normalización del trabajo a distancia sin un marco legal suficiente que permita establecer las certezas y garantías necesarias puede distorsionar el marco de las relaciones laborales, y afecta a condiciones que se incorporan como esenciales de acuerdo con nuestro marco constitucional (artículo 35 CE y el Estatuto de los Trabajadores) y el acervo de normas internacionales y comunitarias que integran "un suelo social mínimo" (entre otras, Capítulo II del Pilar Social Europeo, Directiva 2003/88/ CE, de 4 de noviembre de 2003, Carta Social Europea, Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, la Directiva Marco 89/391/ CEE del Consejo, de 12 de junio de 1989, relativa a la aplicación de medidas para promover la mejora de la seguridad y de la salud de los trabajadores en el trabajo y el propio Texto refundido de la Ley del Estatuto de los Trabajadores)."

Por consiguiente, el propio texto tiene en cuenta la incidencia que el trabajo a distancia y, singularmente, el teletrabajo, va a tener en el derecho

fundamental a la protección de datos de carácter personal, lo que considera en su exposición de motivos como un “inconveniente”.

La necesidad de garantizar la protección de datos de carácter personal, sin perjuicio de venir impuesta por la normativa vigente a la que posteriormente se hará referencia, ya había sido prevista en el Acuerdo Marco Europeo sobre Teletrabajo en su apartado 5:

> 5) Protección de datos
> El empresario es responsable de tomar las medidas que se imponen, especialmente en lo que
> se refiere a software, para garantizar la protección de los datos utilizados y procesados por el
> teletrabajador para fines profesionales.
> El empresario informa al teletrabajador de toda legislación o normativa de la empresa
> referente a la protección de datos.
> Es responsabilidad del teletrabajador el cumplimiento de estas normas.
> El empleador deberá informar al trabajador especialmente sobre:
> 1. Cualquier limitación en la utilización del equipo o de herramientas informáticas
> tales como internet.
> 2. Las sanciones en caso de incumplimiento.

Teniendo en cuenta que la necesidad de garantizar la protección de los datos personales deriva de un derecho fundamental de los ciudadanos, **esta Agencia considera oportuno que se cite de manera separada en la Exposición de Motivos, destacando que el trabajo a distancia requiere la adopción de las medidas necesarias para garantizar el derecho fundamental a la protección de datos de carácter personal.**

En este sentido hay que señalar cómo con la finalidad de dar seguridad jurídica y ante los acontecimientos derivados del COVID-19 y el establecimiento del carácter preferente del trabajo a distancia por el Real Decreto-ley 8/2020, esta Agencia publicó en el pasado mes de abril las “Recomendaciones para proteger los datos personales en situaciones de movilidad y teletrabajo”.

II

En lo que a la materia de protección de datos personales se refiere, la norma a la que debe ajustarse el Anteproyecto sometido a consulta es el 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 por el que se deroga la Directiva 95/46/CE (RGPD en lo sucesivo) y a la Ley Orgánica

3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD en lo sucesivo).

Atendiendo a dicha normativa y al ámbito estricto de competencias de esta Agencia, que no se extiende a la totalidad de los derechos digitales regulados en la LOPDGDD sino únicamente a los que implican un tratamiento de datos de carácter personal regulados en los artículos 89 a 92 de la misma (no comprende, por tanto, el derecho a la desconexión digital, citado en el Anteproyecto), el texto remito plantea numerosas cuestiones referidas al tratamiento de datos de carácter personal, si bien la mayoría de ellas comunes a otras modalidades de relaciones laborales, aunque en el presente caso con nuevas implicaciones por el empleo de las tecnologías en el trabajo a distancia.

Por consiguiente, en el presente informe se van a analizar algunas de estas implicaciones, sin poder realizar una análisis exhaustivo dada la abundante casuística y la urgencia en la emisión del mismo, partiendo de la necesidad de cumplir, en todo caso, con la normativa de protección de datos personales, sistematizada en los principios recogidos en el artículo 5 del RGPD:

> Artículo 5. Principios relativos al tratamiento
>
> 1. Los datos personales serán:
>
> a) tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»);
>
> b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales («limitación de la finalidad»);
>
> c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»);
>
> d) exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan («exactitud»);
>
> e) mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de

investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado («limitación del plazo de conservación»);

f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»).

2. El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»).

Asimismo, hay que tener en cuenta que el RGPD dedica un artículo específico al tratamiento de los datos personales en el ámbito de las relaciones laborales:

Artículo 88 Tratamiento en el ámbito laboral

1. Los Estados miembros podrán, a través de disposiciones legislativas o de convenios colectivos, establecer normas más específicas para garantizar la protección de los derechos y libertades en relación con el tratamiento de datos personales de los trabajadores en el ámbito laboral, en particular a efectos de contratación de personal, ejecución del contrato laboral, incluido el cumplimiento de las obligaciones establecidas por la ley o por el convenio colectivo, gestión, planificación y organización del trabajo, igualdad y diversidad en el lugar de trabajo, salud y seguridad en el trabajo, protección de los bienes de empleados o clientes, así como a efectos del ejercicio y disfrute, individual o colectivo, de los derechos y prestaciones relacionados con el empleo y a efectos de la extinción de la relación laboral.

2. Dichas normas incluirán medidas adecuadas y específicas para preservar la dignidad humana de los interesados así como sus intereses legítimos y sus derechos fundamentales, prestando especial atención a la transparencia del tratamiento, a la transferencia de los datos personales dentro de un grupo empresarial o de una unión de empresas dedicadas a una actividad económica conjunta y a los sistemas de supervisión en el lugar de trabajo.

3. Cada Estado miembro notificará a la Comisión las disposiciones legales que adopte de conformidad con el apartado 1 a más tardar el 25

de mayo de 2018 y, sin dilación, cualquier modificación posterior de las mismas.

III

En primer lugar, procede analizar la licitud de los distintos tratamientos de datos personales, lo que requiere diferenciar entre el tratamiento por el empresario de los datos personales de los trabajadores y el tratamiento, por estos últimos, de datos personales en el desarrollo de su trabajo.

En este último caso, teniendo en cuenta que el tratamiento de los datos personales por los trabajadores en el desarrollo de sus funciones y, consecuentemente, como parte del propio responsable, no se requiere la existencia de una base jurídica distinta de la que legitima el tratamiento por el propio responsable, suscitándose las principales cuestiones en materia de seguridad y protección de la integridad y confidencialidad de los datos, a las que nos referiremos posteriormente, y que van a determinar la necesidad de incluir en el acuerdo de trabajo a distancia, las "Instrucciones dictadas por la empresa, previa información o consulta a la representación de personas trabajadoras, para la protección de datos y seguridad de la información específicamente aplicables en el trabajo a distancia" (artículo 6.j del Anteproyecto).

En cuanto al tratamiento de los datos personales por el empleador, el artículo 4 del Anteproyecto parte de la voluntariedad del trabajo a distancia, que requerirá la firma del acuerdo de trabajo a distancia regulado en la ley, sin que esta modalidad pueda ser impuesta en aplicación del artículo 41 del Estatuto de los Trabajadores.

En este mismo sentido, la Exposición de Motivos recalca que "[…] esta modalidad de organización o prestación de la actividad laboral no resulta de los poderes de dirección y organización empresariales ni de la figura de la modificación sustancial de condiciones de trabajo, artículo 41 del Estatuto de los Trabajadores, sino que es una opción voluntaria para ambas partes".

No obstante, la voluntariedad del trabajo a distancia no implica que el tratamiento de los datos personales del trabajador por parte del empleador derivados de dicha situación se fundamente en el consentimiento del propio trabajador.

En este punto, es preciso recordar, como ya se ha indicado en reiteradas ocasiones por esta Agencia, que la reforma operada por el Reglamento general de protección de datos respecto del régimen contenido en la Ley Orgánica 15/1999 exige un cambio de perspectiva en lo que respecta a los principios articuladores del derecho fundamental a la protección de datos de carácter personal y, en particular, a aquél que hacía del "principio de consentimiento" el eje central del derecho a la protección de datos.

En efecto, si bien la Ley Orgánica y el Reglamento no difieren excesivamente en lo que atañe a la enumeración de las causas legitimadoras del tratamiento, se produce una modificación sumamente relevante en el modo en que dichas causas aparecen recogidas por los textos aplicables: así, mientras del tenor de la Ley Orgánica 15/1999 parecía deducirse que la regla básica de legitimación era, con carácter general, el consentimiento, resultando las restantes causas legitimadoras excepcionales en relación con el consentimiento, que como regla general debía regir el tratamiento, en el texto del artículo 6.1 del Reglamento general de protección de datos el consentimiento se recoge como una de las seis causas de legitimación para el tratamiento sin ostentar mayor o menor importancia que las restantes que en a norma se enumeran.

A mayor abundamiento, el propio Reglamento general de protección de datos pone de manifiesto que el consentimiento del afectado no debe constituir la base legal del tratamiento en determinados supuestos. Así, el considerando 42 señala en su última frase que “El consentimiento no debe considerarse libremente prestado cuando el interesado no goza de verdadera o libre elección o no puede denegar o retirar su consentimiento sin sufrir perjuicio alguno” y el considerando 43 añade que “Para garantizar que el consentimiento se haya dado libremente, este no debe constituir un fundamento jurídico válido para el tratamiento de datos de carácter personal en un caso concreto en el que exista un desequilibro claro entre el interesado y el responsable del tratamiento, en particular cuando dicho responsable sea una autoridad pública y sea por lo tanto improbable que el consentimiento se haya dado libremente en todas las circunstancias de dicha situación particular”.

De este modo, no procede recabar en ningún caso el consentimiento del afectado en los supuestos en los que el tratamiento se encuentre amparado por cualquiera de las causas incluidas en las letras b) a f) del artículo 6.1 del Reglamento general de protección de datos.

En este sentido, en las relaciones entre empleador y trabajador se viene considerando que la base jurídica del tratamiento no puede ser el consentimiento, dada la situación de desigualdad que se produce, lo que impide considerar que el mismo sea libre.

Así se recoge, actualmente en las Directrices del Comité Europeo de Protección de Datos 05/2020 sobre el consentimiento con arreglo al Reglamento 2016/679:

> 21. También en el contexto del empleo se produce un desequilibrio de poder. Dada la dependencia que resulta de la relación entre el empleador y el empleado, no es probable que el interesado pueda negar a su empleador el consentimiento para el tratamiento de

> datos sin experimentar temor o riesgo real de que su negativa produzca efectos perjudiciales. Parece poco probable que un empleado pudiera responder libremente a una solicitud de consentimiento de su empleador para, por ejemplo, activar sistemas de vigilancia por cámara en el lugar de trabajo o para rellenar impresos de evaluación, sin sentirse presionado a dar su consentimiento. Por tanto, el CEPD considera problemático que los empleadores realicen el tratamiento de datos personales de empleados actuales o futuros sobre la base del consentimiento, ya que no es probable que este se otorgue libremente. En el caso de la mayoría de estos tratamientos de datos en el trabajo, la base jurídica no puede y no debe ser el consentimiento de los trabajadores [artículo 6, apartado 1, letra a)] debido a la naturaleza de la relación entre empleador y empleado.

Por consiguiente, el tratamiento por el empleador de los datos personales del trabajador no se puede fundamentar en el consentimiento de este último, debiendo estar amparado en otra base jurídica del artículo 6.1. del RGPD que legitime dicho tratamiento.

Con carácter general, en el ámbito de las relaciones laborales, dicha base jurídica vendrá determinada por la existencia de una relación contractual conforme a lo señalado en el artículo 6.1.b) del RGPD: el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales.

Esta base jurídica legitima, en particular, los tratamientos de datos personales del trabajador a fin de que el empresario pueda ejercer el poder de dirección y control que le atribuye el artículo 20.3 del Texto Refundido del Estatuto de los Trabajadores, aprobado por Real Decreto Legislativo 2/2015 de 23 de octubre, conforme al cual “El empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad y teniendo en cuenta, en su caso, la capacidad real de los trabajadores con discapacidad”. En este sentido se ha venido pronunciando esta Agencia, así como el Tribunal Supremo (Sentencia de 2 de julio de 2007 (Rec. 5017/2003), reiterada en otras posteriores como la de 16 octubre 2012 (Rec. 231/2010) y el Tribunal Constitucional, tal y como señala en la Sentencia del Pleno del Tribunal Constitucional de 3 marzo 2016, recurso de amparo 7222/2013:

> “Aplicando la doctrina expuesta al tratamiento de datos obtenidos por la instalación de cámaras de videovigilancia en el lugar de trabajo, que es el problema planteado en el presente recurso de amparo, debemos concluir que el empresario no necesita el consentimiento expreso del trabajador para el tratamiento de las imágenes que han sido obtenidas a través de las cámaras instaladas en la empresa con la finalidad de

seguridad o control laboral, ya que se trata de una medida dirigida a controlar el cumplimiento de la relación laboral y es conforme con el art. 20.3 TRLET , que establece que “el empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad humana”. Si la dispensa del consentimiento prevista en el art. 6 LOPD se refiere a los datos necesarios para el mantenimiento y el cumplimiento de la relación laboral, la excepción abarca sin duda el tratamiento de datos personales obtenidos por el empresario para velar por el cumplimiento de las obligaciones derivadas del contrato de trabajo. El consentimiento se entiende implícito en la propia aceptación del contrato que implica reconocimiento del poder de dirección del empresario.

En definitiva, la exigencia de finalidad legítima en el tratamiento de datos prevista en el art. 4.1 LOPD viene dada, en el ámbito de la videovigilancia laboral, por las facultades de control empresarial que reconoce el art. 20.3 TRLET, siempre que esas facultades se ejerzan dentro de su ámbito legal y no lesionen los derechos fundamentales del trabajador”.

Incide sin embargo dicha resolución en la necesaria observancia del principio de proporcionalidad:

“Por ello, como hemos señalado, aunque no se requiere el consentimiento expreso de los trabajadores para adoptar esta medida de vigilancia que implica el tratamiento de datos, persiste el deber de información del art. 5 LOPD. Sin perjuicio de las eventuales sanciones legales que pudieran derivar, para que el incumplimiento de este deber por parte del empresario implique una vulneración del art. 18.4 CE exige valorar la observancia o no del principio de proporcionalidad. Debe ponderarse así el derecho a la protección de datos y las eventuales limitaciones al mismo justificadas en el cumplimiento de las obligaciones laborales y las correlativas facultades empresariales de vigilancia y control reconocidas en el art. 20.3 TRLET, en conexión con los arts. 33 y 38 CE. En efecto, la relevancia constitucional de la ausencia o deficiencia de información en los supuestos de videovigilancia laboral exige la consiguiente ponderación en cada caso de los derechos y bienes constitucionales en conflicto; a saber, por un lado, el derecho a la protección de datos del trabajador y, por otro, el poder de dirección empresarial imprescindible para la buena marcha de la organización productiva, que es reflejo de los derechos constitucionales reconocidos en los arts. 33 y 38 CE y que, como se ha visto, en lo que ahora interesa se concreta en la previsión legal ex art. 20.3 TRLET que expresamente faculta al empresario a adoptar medidas de vigilancia y control para

verificar el cumplimiento por los trabajadores de sus obligaciones laborales (SSTC 186/2000, de 10 de julio, FJ 5; 170/2013, de 7 de octubre, FJ 3). Esta facultad general de control prevista en la ley legitima el control empresarial del cumplimiento por los trabajadores de sus tareas profesionales (STC 170/2013, de 7 de octubre; STEDH de 12 de enero de 2016, caso Barbulescu v.Rumania), sin perjuicio de que serán las circunstancias de cada caso las que finalmente determinen si dicha fiscalización llevada a cabo por la empresa ha generado o no la vulneración del derecho fundamental en juego".

A estos tratamientos se refiere el artículo 6, al incluir en el contenido mínimo obligatorio del acuerdo de trabajo a distancia, en su letra h), los h) medios de control empresarial de la actividad. Asimismo, el Anteproyecto dedica el CAPÍTULO IV a las "Facultades de organización, dirección y control empresarial en el trabajo a distancia", con el siguiente contenido:

Artículo 19. Protección de datos y seguridad de la información.

Las personas trabajadoras, en el desarrollo del trabajo a distancia, deberán cumplir las instrucciones que, en el marco de la legislación sobre protección de datos y seguridad de la información, haya establecido la empresa, previa información a la representación legal de las personas trabajadoras.

Artículo 20. Condiciones e instrucciones de uso y conservación de equipos o útiles informáticos.

Las personas trabajadoras deberán cumplir las condiciones e instrucciones de uso y conservación establecidas en la empresa en relación con los equipos o útiles informáticos, dentro de los términos que, en su caso, se establezcan en la negociación colectiva.

Artículo 21. Facultades de control empresarial.

La empresa podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por la persona trabajadora de sus obligaciones y deberes laborales, incluida la utilización de medios telemáticos, guardando en su adopción y aplicación la consideración debida a su dignidad y teniendo en cuenta, en su caso, la capacidad real de los trabajadores con discapacidad.

Ahora bien, esto no implica que en el ámbito laboral quepa todo tratamiento de datos personales para el control por el empresario del cumplimiento de los deberes laborales del trabajador, puesto que habrá de observarse el principio de proporcionalidad. Respecto de la proporcionalidad, pese a ser un concepto jurídico indeterminado, la Sentencia del Tribunal

Constitucional 207/1996 determina que se trata de “una exigencia común y constante para la constitucionalidad de cualquier medida restrictiva de derechos fundamentales, entre ellas las que supongan una injerencia en los derechos a la integridad física y a la intimidad, y más en particular de las medidas restrictivas de derechos fundamentales adoptadas en el curso de un proceso penal viene determinada por la estricta observancia del principio de proporcionalidad.

En este sentido, hemos destacado que, para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres siguientes requisitos o condiciones: «si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto)”.

Por consiguiente, cualquier medida de control que se adopte debe superar este juicio de proporcionalidad, determinando si la medida es adecuada, necesaria y equilibrada, ya que en otro caso resulta desproporcionada y por ello contraria a la normativa de protección de datos.

En definitiva, el control laboral como causa legitimadora para el tratamiento de datos personales no implica, que quepa todo tratamiento de datos amparado en dicha finalidad, sino que dicho tratamiento deberá ser proporcional, cumpliendo igualmente con el resto de principios que se establecen en el artículo 5 del RGPD.

Con carácter general, esta Agencia ha venido manifestando que no cabe una monitorización del trabajador durante toda su jornada en el lugar de trabajo que supondría una medida intrusiva y probablemente desproporcionada en relación con la finalidad perseguida, sin ser una respuesta proporcionada ante riesgos potenciales o concretos.

En este sentido se pronunciaba, igualmente, el Grupo de Trabajo sobre protección de datos del artículo 29 en su Dictamen 2/2017 sobre el tratamiento de datos en el trabajo, adoptado el 8 de junio de 2017 (WP 249), “La rápida adopción de las nuevas tecnologías de la información en el lugar de trabajo, en términos de infraestructura, aplicaciones y dispositivos inteligentes, permite nuevos tipos de tratamiento de datos sistemáticos y potencialmente invasivos”, entre los que cita “las nuevas formas de tratamiento, como las relativas a los datos personales sobre el uso de servicios en línea y/o los datos de localización de un dispositivo inteligente son mucho menos visibles para los trabajadores que otros tipos más tradicionales” por lo que “Con las nuevas

tecnologías, la necesidad de transparencia se hace más evidente, ya que permiten la recogida y el tratamiento posterior de posiblemente grandes cantidades de datos personales de forma encubierta". Asimismo, directamente relacionado con el objeto del presente informe, señala que "cuando los trabajadores trabajan a distancia (desde su domicilio) o mientras viajan por motivos profesionales, puede llevarse a cabo un seguimiento de las actividades realizadas fuera del entorno físico de trabajo, que puede incluir el control del individuo en un contexto privado" y reitera la importancia de observar todos los principios de la normativa de protección de datos personales:

"Con anterioridad, el GT29 indicó en el dictamen 8/2001, que los empresarios deben tener en cuenta los principios fundamentales relativos a la protección de datos de la DPD a la hora de tratar los datos personales en el contexto laboral. El desarrollo de nuevas tecnologías y métodos de tratamiento no han modificado esta situación; de hecho, puede decirse que estos avances hacen que sea más importante que los empresarios respeten dichos principios. En este contexto, los empresarios deben:

- garantizar que los datos se tratan con fines específicos y legítimos que sean proporcionados y necesarios;

- tener en cuenta el principio de limitación de la finalidad y al mismo tiempo asegurarse de que los datos sean adecuados, pertinentes y no excesivos para la finalidad legítima;

- aplicar los principios de proporcionalidad y subsidiariedad, independientemente del fundamento jurídico aplicable;

- ser transparentes con los trabajadores sobre el uso y la finalidad de las tecnologías de control;

- permitir el ejercicio de los derechos del interesado, incluidos el derecho de acceso y, en su caso, la rectificación, supresión o bloqueo de datos personales;

- mantener la exactitud de los datos y no conservarlos más tiempo del necesario; y

- adoptar todas las medidas necesarias para proteger los datos contra el acceso no autorizado, así como garantizar que el personal conozca suficientemente las obligaciones en materia de protección de datos.

Asimismo, en cuanto a los riesgos, señala que "Las tecnologías modernas permiten que los trabajadores puedan ser objeto de seguimiento a lo largo del tiempo, en los lugares de trabajo y en sus hogares, a través de muchos dispositivos diferentes, como teléfonos inteligentes, ordenadores de mesa,

tabletas, vehículos y tecnología ponible" y que "Además, debido a las capacidades de estas tecnologías, es posible que los trabajadores no sepan qué datos personales se están tratando y para qué fines, aunque también es posible que ni siquiera conozcan la existencia de la propia tecnología de control".

IV

En otras ocasiones, el tratamiento de los datos personales de los trabajadores por el empleador vendrá determinado por el cumplimiento de obligaciones legales, siendo lícito al amparo de lo previsto en el artículo 6.1.c) del RGPD: el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento.

Este sería el caso de los tratamientos necesarios para cumplir con la obligación del empresario de garantizar la seguridad y la salud de los trabajadores a su servicio en todos los aspectos relacionados con el trabajo, de acuerdo con la Ley 31/1995, de 8 de noviembre, de prevención de Riesgos Laborales o de las obligaciones de garantizar la seguridad de los datos de carácter personal impuestas por el RGPD y la LOPDGDD.

El texto del Anteproyecto dedica la Sección 4.ª al "Derecho a la prevención de riesgos laborales":

> Artículo 14. Aplicación de la normativa preventiva en el trabajo a distancia.
>
> Las personas que trabajan a distancia tienen derecho a una adecuada protección en materia de seguridad y salud en el trabajo, de conformidad con lo establecido en la Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales, y su normativa de desarrollo.
>
> Artículo 15. Evaluación de riesgos y planificación de la actividad preventiva.
>
> 1. La evaluación de riesgos y la planificación de la actividad preventiva del trabajo a distancia deberán tener en cuenta los riesgos característicos de esta modalidad de trabajo, poniendo especial atención en los factores psicosociales, ergonómicos y organizativos. En particular, deberá tenerse en cuenta la distribución de la jornada, los tiempos de disponibilidad y la garantía de los descansos y desconexiones durante la jornada.
>
> En cualquier caso, la evaluación de riesgos únicamente debe alcanzar a la zona habilitada para la prestación de servicios, no extendiéndose esta obligación al resto de zonas de la vivienda o del lugar elegido para el desarrollo del trabajo a distancia.

2. La empresa deberá obtener toda la información acerca de los riesgos a los que está expuesta la persona que trabaja a distancia mediante una metodología que ofrezca confianza respecto de sus resultados, y prever las medidas de protección que resulten más adecuadas en cada caso.

Cuando la obtención de dicha información exigiera la visita por parte de quien tuviera competencias en materia preventiva al lugar en el que, conforme a lo recogido en el acuerdo al que se refiere el artículo 7 de esta norma, se desarrolla el trabajo a distancia, deberá emitirse informe escrito que justifique dicho extremo que se entregará a la persona trabajadora y a las delegadas y delegados de prevención.

La referida visita requerirá, en cualquier caso, el permiso de la persona trabajadora, de tratarse de su domicilio o del de una tercera persona física.

De no concederse dicho permiso, el desarrollo de la actividad preventiva por parte de la empresa podrá efectuarse en base a la determinación de los riesgos que derive de una autoevaluación a cumplimentar por la persona trabajadora, realizada conforme al modelo recogido en el anexo de esta norma.

A este respecto debe indicarse que, en materia de prevención de riesgos laborales, adaptada a las especificidades del trabajo a distancia, deben tenerse en cuenta no sólo las limitaciones dirigidas a garantizar la intimidad de la persona, a la que responden las cautelas del artículo 15, sino también las derivadas del derecho fundamental a la protección de la persona, especialmente los principios de limitación de la finalidad, exactitud y minimización de datos, de modo que en la visita al domicilio o, en su defecto en el modelo de autoevaluación (que no se ha acompañado a la consulta) únicamente se recojan los datos adecuados, pertinentes y estrictamente necesarios para el desarrollo de la actividad preventiva.

V

Asimismo, como supuesto de cumplimiento de obligaciones legales amparados por el artículo 6.1.c), se encontraría el tratamiento de los datos personales necesarios para el establecimiento del registro de jornada al que se refiere el artículo 13:

Artículo 13. Derecho al registro horario adecuado.

El sistema de registro horario que se regula en el artículo 34.9 del Estatuto de los Trabajadores, de conformidad con lo establecido en la negociación colectiva, deberá reflejar fielmente el tiempo que la persona trabajadora que realiza trabajo a distancia dedica a la actividad laboral, sin

perjuicio de la flexibilidad horaria, y deberá incluir, entre otros, el momento de inicio y finalización de la jornada.

A este respecto, hay que tener en cuenta que la obligación del empleador de establecer un registro de jornada, prevista en el artículo 34.9 del Estatuto de los Trabajadores, se impone con una finalidad específica, favorable al trabajador, tal y como se reitera en diversos apartados del Preámbulo del Real Decreto Ley 8/2019 (que ya de por sí lleva en su título "medidas urgentes de protección social y de lucha contra la precariedad laboral en la jornada de trabajo"):

"este real decreto-ley incluye también determinadas disposiciones dirigidas a establecer el registro de la jornada de trabajo, a los efectos de garantizar el cumplimiento de los límites en materia de jornada, de crear un marco de seguridad jurídica tanto para las personas trabajadoras como para las empresas y de posibilitar el control por parte de la Inspección de Trabajo y Seguridad Social."

[…]

"El capítulo III incluye reformas normativas dirigidas a regular el registro de jornada, como forma de combatir la precariedad laboral.

Las reglas sobre limitación de la jornada laboral son uno de los elementos que están en el origen del Derecho del Trabajo. Estas reglas se configuran como un elemento de protección de las personas trabajadoras y se aglutinan en torno al establecimiento legal de una jornada máxima de trabajo y su indisponibilidad para las partes del contrato de trabajo, al ser normas de derecho necesario.

La realización de un tiempo de trabajo superior a la jornada laboral legal o convencionalmente establecida incide de manera sustancial en la precarización del mercado de trabajo, al afectar a dos elementos esenciales de la relación laboral, el tiempo de trabajo, con relevante influencia en la vida personal de la persona trabajadora al dificultar la conciliación familiar, y el salario. Y también incide en las cotizaciones de Seguridad Social, mermadas al no cotizarse por el salario que correspondería a la jornada realizada."

Por tanto, atendiendo a la específica finalidad a la que atiende la obligación legal que impone el 34.9 ET, dicho registro debe diferenciarse de aquellos otros que hasta ahora venía imponiendo el empresario sobre la base de su poder de dirección y control del artículo 20.3 del ET y que era sobre el que se ha venido pronunciando la AEPD, siendo la base jurídica de su tratamiento el artículo 6.1.b): "el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte…".

Esto tiene especial incidencia como luego veremos en la aplicación de los principios de finalidad, minimización y proporcionalidad. Así como en el deber

de información, ya que si el mismo registro se va a usar para las dos finalidades, deberá informarse correctamente de las diferentes finalidades y las diferentes bases jurídicas.

En principio, de acuerdo con el citado artículo 34.9, tiene que ser mediante la negociación con los representantes de los trabajadores como se tienen que concretar los aspectos relativos a este registro (sistemas a utilizar, garantías, accesos, etc.). Solo en el caso de que así no se haga, será el empresario, previa consulta con los representantes legales el que organice y documente el registro de jornada. Aunque se trata de una cuestión de derecho laboral, tiene su trascendencia desde el punto de vista de la protección de datos, ya que el artículo 88 del RGPD prevé que se puedan establecer medidas específicas por convenio colectivo.

Lo que no puede entenderse es que la empresa pueda habilitar el sistema que estime más adecuado, ya que como se ha dicho reiteradamente por la AEPD, la existencia de una base de legitimación no exime de cumplir con los principios del artículo 5 del RGPD, y especialmente, además del de limitación de la finalidad citado anteriormente, con el de proporcionalidad y el de minimización, debiendo buscarse los medios que, atendida la concreta finalidad, sean lo menos intrusivos en la esfera íntima del afectado, lo que solo puede valorarse atendiendo al caso concreto. En este sentido, debe valorarse si el registro va a usarse a los solos efectos de lo previsto en el artículo 34.9 ET o si también se va a usar como medida de control por el empresario, persiguiendo ambas finalidades, atendiendo a las circunstancias concretas en que vaya a desarrollarse el trabajo a distancia.

VI

El artículo 5 del proyecto contempla, de manera análoga a lo previsto en el artículo 8 del Estatuto de los Trabajadores respecto de la copia básica del contrato de trabajo, la entrega a los representantes de los trabajadores de la copia de los acuerdos suscritos, señalando lo siguiente:

> 3. La empresa deberá entregar a la representación legal de las personas trabajadoras copia de todos los acuerdos de personas trabajadoras a distancia que se realicen y de sus actualizaciones, excluyendo aquellos datos 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.
>
> Esta copia se entregará por la empresa en plazo no superior a diez días desde su formalización, a la representación legales de las personas

trabajadoras, quienes la firmarán a efectos de acreditar que se ha producido la entrega.

Posteriormente, dicha copia se enviará a la oficina de empleo. Cuando no exista representación legal de las personas trabajadoras también deberá formalizarse copia básica y remitirse a la oficina de empleo.

A este respecto, dicha comunicación se encontraría legitimada, igualmente, en el cumplimiento de una obligación del empleador, correlativa al derecho de información de los representantes legales de los trabajadores reconocido en el artículo 64 del ET, si bien deben respetarse los límites derivados, no solo de la protección a la intimidad, sino también del derecho a la protección de datos, especialmente el principio de minimización, de modo que los datos facilitados deberán ser pertinentes, adecuados y limitados a lo necesario en relación con los fines para los que son tratados. Por ello, deberías, suprimirse, tal y como prevé el artículo 8.4 del RGPD, de la copia facilitadas los datos personales correspondientes al número del documento nacional de identidad o del número de identidad de extranjero, el domicilio, el estado civil, y cualquier otro que no resulte necesario para el ejercicio de la función de vigilancia y control que corresponde a la representación legal de los trabajadores.

Por tanto, se propone la siguiente redacción:

La empresa deberá entregar a la representación legal de las personas trabajadoras copia de todos los acuerdos de personas trabajadoras a distancia que se realicen y de sus actualizaciones, **excluyendo aquellos datos relativos al número del documento nacional de identidad o del número de identidad de extranjero, el domicilio, el estado civil y cualquier otro que no sean necesarios para el ejercicio de su función de vigilancia y control o 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.

VII

Asimismo, el tratamiento de datos personales podrá fundarse en un interés legítimo del empleador, siempre que frente al mismo no prevalezcan los derechos y libertades del trabajador, al amparo del artículo 6.1.f) del RGPD: el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que

sobre dichos 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.

Para estos casos, en el Dictamen del Grupo del 29 6/2014, de 9 de abril, sobre el concepto de interés legítimo del responsable del tratamiento (WP 217), se incorporan diversas directrices y orientaciones en orden a la concurrencia del "interés legítimo", así como los elementos de salvaguarda necesarios en atención al respeto y garantía de los derechos de los afectados por este tipo de tratamientos.

En el marco de dichas garantías, destaca la exigencia de la *"prueba de sopesamiento"* entre el interés legítimo del responsable del tratamiento o cualesquiera terceros a los que se comuniquen los datos y los intereses o los derechos fundamentales del interesado.

El análisis inherente a la *"prueba de sopesamiento"* requiere la consideración completa de una serie de factores, con el fin de garantizar que se tienen en cuenta debidamente los intereses y los derechos fundamentales de los afectados. Al mismo tiempo, se trata de una prueba modulable, que puede variar desde sencilla hasta compleja. Los factores que deben considerarse cuando se efectúe dicha prueba de sopesamiento comprenderán:

- La naturaleza y la fuente del interés legítimo, y si el tratamiento de datos es necesario para el ejercicio de un derecho fundamental, resulta de interés público o se beneficia del reconocimiento de la comunidad afectada;

- La repercusión para el interesado y sus expectativas razonables sobre qué sucederá con sus datos, así como la naturaleza de los datos y la manera en la que sean tramitados;

- Las garantías adicionales que podrían limitar un impacto indebido sobre el interesado, tales como la minimización de los datos, las tecnologías de protección de la intimidad, el aumento de la transparencia, el derecho general e incondicional de exclusión voluntaria y la portabilidad de los datos.

Como ejemplo de interés legítimo, el Considerando 49 señala que

> "Constituye un interés legítimo del responsable del tratamiento interesado el tratamiento de datos personales en la medida estrictamente necesaria y proporcionada para garantizar la seguridad de la red y de la información, es decir la capacidad de una red o de un sistema información de resistir, en un nivel determinado de confianza, a acontecimientos accidentales o acciones ilícitas o malintencionadas que

comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos personales conservados o transmitidos, y la seguridad de los servicios conexos ofrecidos por, o accesibles a través de, estos sistemas y redes, por parte de autoridades públicas, equipos de respuesta a emergencias informáticas (CERT), equipos de respuesta a incidentes de seguridad informática (CSIRT), proveedores de redes y servicios de comunicaciones electrónicas y proveedores de tecnologías y servicios de seguridad. En lo anterior cabría incluir, por ejemplo, impedir el acceso no autorizado a las redes de comunicaciones electrónicas y la distribución malintencionada de códigos, y frenar ataques de «denegación de servicio» y daños a los sistemas informáticos y de comunicaciones electrónicas".

Este supuesto es igualmente objeto de un análisis detallado en el Dictamen 2/2017 sobre el tratamiento de datos en el trabajo:

5.3 Operaciones de tratamiento derivadas de la vigilancia del uso de las TIC en el lugar de trabajo

Tradicionalmente, se consideraba que el control de las comunicaciones electrónicas en el lugar de trabajo (teléfono, navegación por Internet, correo
electrónico, mensajería instantánea, VoIP, etc.) era la principal amenaza para la privacidad de los trabajadores. En su Documento de trabajo relativo a las comunicaciones electrónicas en el lugar de trabajo de 2001, el GT29 formuló una serie de conclusiones en relación con el control del correo electrónico y la utilización de Internet. Si bien esas conclusiones siguen siendo válidas, es necesario tener en cuenta los avances tecnológicos que han permitido formas de control más nuevas, potencialmente más intrusivas y generalizadas. Estos avances incluyen, entre otros:

- herramientas de prevención de pérdida de datos (DLP), que controlan las comunicaciones salientes con el fin de detectar posibles violaciones de la seguridad de los datos;
- cortafuegos de próxima generación (NGFW) y sistemas de gestión unificada de amenazas (UTM), que pueden proporcionar una variedad de tecnologías de control, entre ellas la inspección profunda de paquetes, interceptación TLS, filtrado de sitios web, filtrado de contenido, informes sobre dispositivos, información de identidad de usuario y (como se describió anteriormente) prevención de pérdida de datos. Estas tecnologías también pueden utilizarse individualmente, dependiendo del empresario;

- aplicaciones y medidas de seguridad que impliquen registrar el acceso de los trabajadores a los sistemas del empresario;
- tecnología de detección electrónica (eDiscovery), es decir, cualquier proceso de búsqueda de datos electrónicos con el fin de utilizarlos como prueba;
- seguimiento del uso de la aplicación y el dispositivo a través de programas informáticos ocultos, ya sea en el ordenador o en la nube;
- uso en el lugar de trabajo de aplicaciones de oficina proporcionadas como servicio en la nube que, en teoría, permiten un registro muy detallado de las actividades de los trabajadores;
- control de los dispositivos personales (por ejemplo, ordenadores personales, teléfonos móviles, tabletas), que los trabajadores aportan para su trabajo, de acuerdo con una política de uso específico, como la de que el trabajador utilice su propio dispositivo, y tecnología de gestión de sistemas móviles, que permite la distribución de aplicaciones, datos y ajustes de configuración y parches para dispositivos móviles; y
- uso de dispositivos ponibles (por ejemplo, dispositivos de salud y estado físico).

Es posible que un empresario pueda aplicar una solución de control única, tal como un conjunto de paquetes de seguridad que le permita controlar todo el uso de las TIC en el lugar de trabajo, en vez de controlar solo el correo electrónico y/o el sitio web, como sucedía antes.
Las conclusiones adoptadas en el WP55 se aplicarían a cualquier sistema que permita este control.

[…]

Independientemente de la tecnología o de las capacidades que posea, la base jurídica del artículo 7, letra f), solo está disponible si el tratamiento cumple determinadas condiciones. En primer lugar, los empresarios que utilicen estos productos y aplicaciones deben tener en cuenta la proporcionalidad de las medidas que apliquen y, si es posible, adoptar medidas adicionales para mitigar o reducir la escala y el impacto del tratamiento de los datos. Como ejemplo de buena práctica, esta consideración podría llevarse a cabo a través de una EIPD antes de la introducción de cualquier tecnología de control. En segundo lugar, los empresarios deben aplicar y comunicar políticas de uso aceptables, junto con políticas de privacidad, que indiquen el uso permisible de la red y los equipos de la organización, y que detallen de manera rigurosa el tratamiento que se está llevando a cabo.

En algunos países, la formulación de una política de este tipo requeriría legalmente la aprobación de un comité de empresa o una representación similar de los trabajadores. En la práctica, el personal de mantenimiento informático suele elaborar estas políticas. Dado que su principal interés será sobre todo la seguridad y no la expectativa legítima de privacidad de los trabajadores, el GP29 recomienda que, en todos los casos, una muestra representativa de trabajadores participe en la evaluación de la necesidad del control, así como en la lógica y accesibilidad de la política.

Y en particular, en relación con el trabajo a distancia, indica lo siguiente:

5.4.1 OBSERVACIÓN DEL TRABAJO A DOMICILIO Y REMOTO

Cada vez es más común que los empresarios ofrezcan a los trabajadores la opción de trabajar a distancia, por ejemplo, desde casa y/o durante el traslado. De hecho, esto es un factor central que explica la poca diferenciación entre lugar de trabajo y hogar. En general, se trata de que el empresario entregue equipos o programas informáticos a los trabajadores que, una vez instalados en su hogar o en sus propios dispositivos, les permitan tener el mismo nivel de acceso a la red, los sistemas y los recursos que tendrían si estuvieran en el lugar de trabajo, en función de la aplicación.

Aunque el trabajo a distancia puede ser una evolución positiva, también presenta un tipo de riesgo adicional para el empresario. Por ejemplo, los trabajadores que tienen acceso remoto a la infraestructura del empresario no están sujetos a las medidas de seguridad física que existen en las instalaciones del empresario. Dicho claramente: sin la aplicación de las medidas técnicas adecuadas, el riesgo de acceso no autorizado aumenta y puede dar lugar a la pérdida o destrucción de información, incluidos los datos personales de trabajadores o clientes de los que pueda disponer el empresario.

Con el fin de mitigar este tipo de riesgo, los empresarios pueden pensar que existe una justificación para utilizar paquetes de programas informáticos (ya sea en las instalaciones o en la nube) que tengan la capacidad de, por ejemplo, registrar pulsaciones en el teclado y movimientos del ratón, capturas de pantalla (ya sea al azar o a intervalos determinados), registrar las aplicaciones utilizadas (y durante cuánto tiempo se utilizaron) y, en dispositivos compatibles, habilitar las cámaras web y recopilar secuencias de las mismas. Estas tecnologías están ampliamente disponibles,

> incluso por parte de terceros, como los proveedores de servicios en la nube.
> Sin embargo, el tratamiento que implican estas tecnologías es desproporcionado y es muy poco probable que el empresario tenga un fundamento jurídico en virtud del interés legítimo, por ejemplo, para registrar las pulsaciones en el teclado y los movimientos del ratón de un trabajador.
> La clave está en abordar el riesgo que supone el trabajo a domicilio y a distancia de forma proporcionada y no excesiva, sea cual fuere la opción que se ofrezca y la tecnología que se proponga, en particular si los límites entre el uso profesional y privado son fluidos

Por consiguiente, solo en los casos en que, como resultado de la prueba de sopesamiento, no prevalezcan los intereses y los derechos fundamentales de los trabajadores a distancia, podrá llevarse a cabo el tratamiento sobre la base jurídica del artículo 6.1.f) del RGPD.

VIII

Por otro lado, hay que tener en cuenta que los tratamientos de datos personales en el trabajo a distancia, especialmente en lo que se refiere a las medidas de control del trabajador, puede implicar el tratamiento de categorías especiales de datos, como podría ser en el supuesto de datos biométricos dirigidos a la identificación unívoca del trabajador, cuyo tratamiento queda prohibido por el artículo 9.1. del RGPD, salvo que concurra alguno de los supuestos contemplados en su apartado 2 que levanten la prohibición de dicho tratamiento, y que es presupuesto indispensable para, posteriormente, valorar la existencia de una base jurídica que legitime el tratamiento conforme al artículo 6 del RGPD.

A este respecto, debe recordarse el criterio restrictivo que viene manteniendo esta Agencia respecto al reconocimiento facial, recogido en el informe 31/2019 relativo al ámbito de la seguridad privada y en el informe 36/2020 relativo al uso de técnicas de reconocimiento facial en la realización de pruebas de evaluación online por las universidades.

El informe 36/2020 analizaba los tratamientos de datos biométricos mediante el empleo de técnicas de reconocimiento facial, concluyendo que los mismos implicaban un tratamiento de categorías especiales de datos a efectos del RGPD, con un razonamiento que resultaría igualmente aplicable en el caso de que el mismo pretendiera usarse como medida de control del trabajador:

> En el presente caso, versando la consulta sobre técnicas de reconocimiento facial dirigidas a acreditar la identidad del alumno, nos

encontraríamos ante el tratamiento de datos biométricos, tal y como los define el artículo 4.14 del RGPD:

«datos biométricos»: datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos;

No obstante, hay que adelantar que el RGPD no parece considerar a todo tratamiento de datos biométricos como tratamiento de categorías especiales de datos, ya que el artículo 9.1. se refiere a los "datos biométricos dirigidos a identificar de manera unívoca a una persona física", por lo que, de una interpretación conjunta de ambos preceptos parece dar a entender que los datos biométricos solo constituirían una categoría especial de datos en el caso de que se sometan a un tratamiento técnico específico dirigido a identificar de manera unívoca a una persona física. En este sentido, parece que igualmente se pronuncia el Considerando 51 al señalar que "El tratamiento de fotografías no debe considerarse sistemáticamente tratamiento de categorías especiales de datos personales, pues únicamente se encuentran comprendidas en la definición de datos biométricos cuando el hecho de ser tratadas con medios técnicos específicos permita la identificación o la autenticación unívocas de una persona física".

Con igual criterio, el Protocolo de enmienda al Convenio para la Protección de Individuos con respecto al procesamiento de datos personales, aprobada por el Comité de Ministros en su 128º período de sesiones en Elsinore el 18 de mayo de 2018 (Convenio 108+) incluye únicamente como categorías especiales de datos, en su artículo 6.1 a los datos biométricos dirigidos a la identificación unívoca de una persona ("biometric data uniquely identifying a person"), sin incluir la referencia a la autenticación.

Al objeto de aclarar las dudas interpretativas que surgen respecto a la consideración de los datos biométricos como categorías especiales de datos puede acudirse a la distinción entre identificación biométrica y verificación/autenticación biométrica que establecía el Grupo del Artículo 29 en su Dictamen 3/2012 sobre la evolución de las tecnologías biométricas:

Identificación biométrica: la identificación de un individuo por un sistema biométrico es normalmente el proceso de comparar sus datos biométricos (adquiridos en el momento de la identificación) con una serie

de plantillas biométricas almacenadas en una base de datos (es decir, un proceso de búsqueda de correspondencias uno-a-varios).

Verificación/autenticación biométrica: la verificación de un individuo por un sistema biométrico es normalmente el proceso de comparación entre sus datos biométricos (adquiridos en el momento de la verificación) con una única plantilla biométrica almacenada en un dispositivo (es decir, un proceso de búsqueda de correspondencias uno-a-uno).

Esta misma diferenciación se recoge en el Libro blanco sobre la inteligencia artificial de la Comisión Europea:

"En lo que se refiere al reconocimiento facial, por «identificación» se entiende que la plantilla de la imagen facial de una persona se compara con otras muchas plantillas almacenadas en una base de datos para averiguar si su imagen está almacenada en ella. La «autenticación» (o «verificación»), por su parte, se refiere habitualmente a la búsqueda de correspondencias entre dos plantillas concretas. Permite la comparación de dos plantillas biométricas que, en principio, se supone que pertenecen a la misma persona; así, las dos plantillas se comparan para determinar si la persona de las dos imágenes es la misma. Este procedimiento se emplea, por ejemplo, en las puertas de control automatizado de fronteras empleadas en los controles fronterizos de los aeropuertos".

Atendiendo a la citada distinción, puede interpretarse que, de acuerdo con el artículo 4 del RGPD, el concepto de dato biométrico incluiría ambos supuestos, tanto la identificación como la verificación/autenticación. Sin embargo, y con carácter general, los datos biométricos únicamente tendrán la consideración de categoría especial de datos en los supuestos en que se sometan a tratamiento técnico dirigido a la identificación biométrica (uno-a-varios) y no en el caso de verificación/autenticación biométrica (uno-a-uno).

No obstante, esta Agencia considera que se trata de una cuestión compleja, sometida a interpretación, respecto de la cual no se pueden extraer conclusiones generales, debiendo atenderse al caso concreto según los datos tratados, las técnicas empleadas para su tratamiento y la consiguiente injerencia en el derecho a la protección de datos, debiendo, en tanto en cuanto no se pronuncia al respecto el Comité Europeo de Protección de Datos o los órganos jurisdiccionales, adoptarse, en caso de duda, la interpretación más favorable para la protección de los derechos de los afectados.

En el presente caso, tal y como hemos señalado, la consultante no identifica las técnicas de tratamiento facial a la que se refiere la

consulta. No obstante, tal y como ha informado al Gabinete Jurídico la Unidad de Evaluación y Estudios Tecnológicos, son diferentes las técnicas que se están empleando en el momento actual:

"En el conjunto de consultas planteadas se establecen medidas para la identificación y control durante la prueba online que abarcan, desde las menos intrusivas a las más intrusivas:

- Acceso a la imagen y micrófono del alumno, incluyendo
  - Grabación de la imagen y sonido del alumno durante el examen
  - Visualización del alumno multicámara, desde distintas perspectivas.
  - Grabaciones del entorno personal del alumno previa a la prueba y/o durante la prueba.
- Acceso al sistema del alumno
  - Acceso a la pantalla del alumno
  - Control del sistema del alumno (al menos bloqueando la ejecución de aplicaciones distintas a las aplicaciones docentes).
  - Grabación de la interacción del alumno con el sistema
- Tratamiento de la información biométrica
  - Identificación mediante reconocimiento facial y, además, otros parámetros biométricos del alumno (como perfil de mecanografía).
  - Tratamiento de datos biométricos para perfilar actitudes, gestos, estados de ánimo o de ansiedad, etc".

Debiendo tenerse en cuenta que, tal y como se reconoce en la "Segunda Jornada Online para Compartición de Experiencias de Modelos de Evaluación" ya citada, las universidades están combinando diferentes sistemas para acreditar la identidad del alumno y evitar las posibles suplantaciones de identidad. Además, una de las características de los sistemas de e-proctoring existentes en el mercado es que garantizan la identificación del alumno mediante el reconocimiento facial, evitando la suplantación de su identidad, no solo en el momento inicial, sino a lo largo del desarrollo de toda la actividad, para lo cual se graba la misma y se van realizando diferentes capturas que se comparan con la información biométrica previamente almacenada en sus bases de datos. Asimismo, dichos sistemas incluyen, tal y como se ha indicado, el tratamiento de otro tipo de datos biométricos (como las pulsaciones en el teclado) y de datos no biométricos, como la grabación del entorno en el

que se encuentra el alumno, así como el acceso al micrófono para la grabación de sonidos.

Por tanto, atendiendo a las circunstancias concretas, que implican el tratamiento de diferentes tipos de datos biométricos y en los que el reconocimiento facial no se realiza en un momento determinado sino que se realiza de manera continuada, lo que puede implicar, asimismo, el tratamiento de los datos biométricos de un tercero para su comparación con los del alumno al objeto de identificar una posible suplantación, debe concluirse que los procesos de reconocimiento facial empleados para la realización de evaluaciones online implican el tratamiento de datos biométricos con la finalidad de identificar unívocamente a una persona física.

En este mismo sentido, cabe recordar que el Supervisor Europeo de Protección de Datos, en sus “Guidelines 3/2019 on processing of personal data through video devices" de 10 de julio de 2019 considera el empleo de videovigilancia con reconocimiento facial como categoría especial de datos del artículo 9 del RGPD:

76. The use of video surveillance including biometric recognition functionality installed by private entities for their own purposes (e.g. marketing, statistical, or even security) will, in most cases, require explicit consent of all data subjects (Article 9 (2) (a)), however another suitable exception in Article 9 could also be applicable.

Example: To improve its service a private company replaces passenger identification check points within an airport (luggage drop-off, boarding) with video surveillance systems that use facial recognition techniques to verify the identity of the passengers that have chosen to consent to such a procedure. Since the processing falls under Article 9, the passengers, who will have previously given their explicit and informed consent, will have to enlist themselves at for example an automatic terminal in order to create and register their facial template associated with their boarding pass and identity.

Por ello, esta Agencia comparte el criterio de la consultante, en el sentido de que los sistemas de reconocimiento facial objeto de la consulta implican el tratamiento de categoría especiales de datos.

En el presente caso, teniendo en cuenta que el consentimiento, en el ámbito de las relaciones laborales, no puede exceptuar la prohibición de tratamiento de categorías especiales de datos al no considerarse libre, tal y como se ha indicado ya en este informe, el tratamiento de datos biométricos

mediante el empleo de tecnologías de reconocimiento facial, debería ampararse en lo previsto en la letra b) del artículo 9.2 del RGPD:

> b) el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice el Derecho de la Unión de los Estados miembros o un convenio colectivo con arreglo al Derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado;

Considerando esta Agencia que el tratamiento de datos personales mediante el empleo de técnicas de reconocimiento facial es muy intrusivo para el trabajador, resulta imprescindible que, como señala el citado precepto, dicho tratamiento se encuentre autorizado por una norma con rango de ley, de acuerdo con el principio de reserva de ley consagrado en el artículo 53 nuestra Constitución, o en un convenio colectivo, estableciendo las reglas precisas que hagan previsible al interesado el uso de dichas técnicas y sus consecuencias y que se establezcan las garantías adecuadas de tipo técnico, organizativo y procedimental, que prevengan los riesgos de distinta probabilidad y gravedad y mitiguen sus efectos.

Además, dicha ley o convenio colectivo deberá respetar en todo caso el principio de proporcionalidad, en los términos que recuerda la Sentencia del Tribunal Constitucional 14/2003, de 28 de enero, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia, de modo que la existencia de otras medidas que permitan el control de los trabajadores con una menor intrusión en el derecho de los afectados, exigiría una especial justificación de la necesidad de optar por el reconocimiento facial respecto de dichas otras medidas.

IX

Por otro lado, aunque ya se ha vendido señalando a lo largo del presente informe, debe incidirse en la necesidad de garantizar la necesaria transparencia en el tratamiento de datos y el derecho a la información de los trabajadores y, en su caso, de sus representantes legales.

Determina el artículo 12 del RGPD en su apartado 1, lo siguiente:

> 1. El responsable del tratamiento tomará las medidas oportunas para facilitar al interesado toda información indicada en los artículos 13 y 14, así como cualquier comunicación con arreglo a los artículos 15 a 22 y 34 relativa al tratamiento, en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular cualquier

información dirigida específicamente a un niño. La información será facilitada por escrito o por otros medios, inclusive, si procede, por medios electrónicos. Cuando lo solicite el interesado, la información podrá facilitarse verbalmente siempre que se demuestre la identidad del interesado por otros medios.

El artículo 12 del RGPD regula de qué modo o manera se debe proporcionar la información, es decir, qué características o cualidades debe tener la información que se ofrece a los titulares de los datos que van a ser objeto de tratamiento, regulando el artículo 13 el cumplimiento del deber de información cuando los datos se obtienen del propio afectado y el artículo 14 cuando se obtienen de terceros.

Por su parte, la LOPDGDD en su artículo 11, bajo la rúbrica "Transparencia e información al afectado" establece la posibilidad de instaurar un sistema de información por capas, diferenciando una primera información básica y permitiendo la remisión a otro espacio informativo donde el interesado que lo desee pueda consultar con más amplitud todo lo relativo al tratamiento de sus datos personales.

X

Por otro lado, el RGPD ha supuesto un cambio sustancial en la forma de abordar la garantía del derecho fundamental a la protección de datos personales, que gira en torno al principio de responsabilidad proactiva o accountability de modo que es el responsable el que, a través de los instrumentos regulados en el propio RGPD como el análisis de riesgos o la evaluación de impacto en la protección de datos personales y asistido, en su caso, por el delegado de protección de datos, debe garantizar la protección de dicho derecho, documentando adecuadamente todas las decisiones que adopte.

Debe, por tanto, ser el responsable el que, tras un análisis detallado de la situación, en los términos que posteriormente se expondrán, deberá valorar y garantizar el cumplimiento de la normativa de protección de datos de carácter personal y de los principios que rigen la misma, debiendo hacerse especial referencia en el presente caso a los principios de "licitud, lealtad y transparencia" del artículo 5.1.a), el de "limitación de la finalidad" del artículo 5.1.b), el de "minimización" de los datos del art. 5.1.c) del RGPD, el de exactitud del artículo 5.1.d), el de "limitación del plazo de conservación" del artículo 5.1.e) el de "integridad y confidencialidad" del artículo 5.1.f) así como el ya citado de responsabilidad proactiva del artículo 5.2., teniendo especialmente en cuenta, en el presente caso, la protección de datos desde el diseño y por defecto a que se refiere el artículo 25 del RGPD:

> 1. Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados.
>
> 2. El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas.
>
> 3. Podrá utilizarse un mecanismo de certificación aprobado con arreglo al artículo 42 como elemento que acredite el cumplimiento de las obligaciones establecidas en los apartados 1 y 2 del presente artículo.

Para el adecuado cumplimiento de dicho principio, el RGPD contempla una serie de instrumentos que permiten a responsables y encargados valorar el riesgo que pueda implicar el tratamiento y adoptar las medidas que procedan.

En primer lugar, resulta necesario realizar el análisis de riesgos al que se refiere el artículo 24 del RGPD:

> 1. Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario.
> 2. Cuando sean proporcionadas en relación con las actividades de tratamiento, entre las medidas mencionadas en el apartado 1 se incluirá la aplicación, por parte del responsable del tratamiento, de las oportunas políticas de protección de datos.

> 3. La adhesión a códigos de conducta aprobados a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrán ser utilizados como elementos para demostrar el cumplimiento de las obligaciones por parte del responsable del tratamiento.

Cuando, en virtud de dicho análisis, "sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales", en los términos previstos en el artículo 35 del RGPD.

En los supuestos en que la Evaluación de Impacto relativa a la Protección de Datos muestre que el tratamiento sigue teniendo un alto riesgo para los derechos y libertades de los interesados aún tras aplicar las garantías, medidas de seguridad y mecanismos de protección razonables en cuanto a técnica disponible y costes de aplicación, el responsable del tratamiento deberá formular la consulta previa a la que se refiere el artículo 36 del RGPD:

> 1.El responsable consultará a la autoridad de control antes de proceder al tratamiento cuando una evaluación de impacto relativa a la protección de los datos en virtud del artículo 35 muestre que el tratamiento entrañaría un alto riesgo si el responsable no toma medidas para para mitigarlo.
>
> 2.Cuando la autoridad de control considere que el tratamiento previsto a que se refiere el apartado 1 podría infringir el presente Reglamento, en particular cuando el responsable no haya identificado o mitigado suficientemente el riesgo, la autoridad de control deberá, en un plazo de ocho semanas desde la solicitud de la consulta, asesorar por escrito al responsable, y en su caso al encargado, y podrá utilizar cualquiera de sus poderes mencionados en el artículo 58. Dicho plazo podrá prorrogarse seis semanas, en función de la complejidad del tratamiento previsto. La autoridad de control informará al responsable y, en su caso, al encargado de tal prórroga en el plazo de un mes a partir de la recepción de la solicitud de consulta, indicando los motivos de la dilación. Estos plazos podrán suspenderse hasta que la autoridad de control haya obtenido la información solicitada a los fines de la consulta.
>
> 3.Cuando consulte a la autoridad de control con arreglo al apartado 1, el responsable del tratamiento le facilitará la información siguiente:

a) en su caso, las responsabilidades respectivas del responsable, los corresponsables y los encargados implicados en el tratamiento, en particular en caso de tratamiento dentro de un grupo empresarial;

b) los fines y medios del tratamiento previsto;

c) las medidas y garantías establecidas para proteger los derechos y libertades de los interesados de conformidad con el presente Reglamento;

d) en su caso, los datos de contacto del delegado de protección de datos;

e) la evaluación de impacto relativa a la protección de datos establecida en el artículo 35, y

f) cualquier otra información que solicite la autoridad de control.

(…)"

En este contexto normativo se inscribe el artículo 28 de la LOPDGDD, cuando -bajo el título "Obligaciones generales del responsable y encargado del tratamiento", prevé que:

"1. Los responsables y encargados, teniendo en cuenta los elementos enumerados en los artículos 24 y 25 del Reglamento (UE) 2016/679, determinarán las medidas técnicas y organizativas apropiadas que deben aplicar a fin de garantizar y acreditar que el tratamiento es conforme con el citado reglamento, con la presente ley orgánica, sus normas de desarrollo y la legislación sectorial aplicable. En particular valorarán si procede la realización de la evaluación de impacto en la protección de datos y la consulta previa a que se refiere la Sección 3 del Capítulo IV del citado reglamento.

2. Para la adopción de las medidas a que se refiere el apartado anterior los responsables y encargados del tratamiento tendrán en cuenta, en particular, los mayores riesgos que podrían producirse en los siguientes supuestos:

a) Cuando el tratamiento pudiera generar situaciones de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico, moral o social significativo para los afectados.

b) Cuando el tratamiento pudiese privar a los afectados de sus derechos y libertades o pudiera impedirles el ejercicio del control sobre sus datos personales.

c) Cuando se produjese el tratamiento no meramente incidental o accesorio de las categorías especiales de datos a las que se refieren los

artículos 9 y 10 del Reglamento (UE) 2016/679 y 9 y 10 de esta ley orgánica o de los datos relacionados con la comisión de infracciones administrativas.

d) Cuando el tratamiento implicase una evaluación de aspectos personales de los afectados con el fin de crear o utilizar perfiles personales de los mismos, en particular mediante el análisis o la predicción de aspectos referidos a su rendimiento en el trabajo, su situación económica, su salud, sus preferencias o intereses personales, su fiabilidad o comportamiento, su solvencia financiera, su localización o sus movimientos.

e) Cuando se lleve a cabo el tratamiento de datos de grupos de afectados en situación de especial vulnerabilidad y, en particular, de menores de edad y personas con discapacidad.

f) Cuando se produzca un tratamiento masivo que implique a un gran número de afectados o conlleve la recogida de una gran cantidad de datos personales.

g) Cuando los datos personales fuesen a ser objeto de transferencia, con carácter habitual, a terceros Estados u organizaciones internacionales respecto de los que no se hubiese declarado un nivel adecuado de protección.

h) Cualesquiera otros que a juicio del responsable o del encargado pudieran tener relevancia y en particular aquellos previstos en códigos de conducta y estándares definidos por esquemas de certificación.”

Asimismo, deberán tenerse en cuenta las “Listas de tipos de tratamientos de datos que requieren evaluación de impacto relativa a protección de datos” y la “Lista orientativa de tipos de tratamientos que no requieren una evaluación de impacto relativa a la protección de datos” publicados por la Agencia Española de Protección de Datos al amparo de lo previsto en el artículo 35.5 del RGPD.

En este punto, hay que tener en cuenta que, en principio, la obligación de realizar una EIPD recaería sobre el responsable, circunstancia que, en principio ostentaría el empleador, sin perjuicio de que, de acuerdo con el Considerando 78 del RGPD, al “desarrollar, diseñar, seleccionar y usar aplicaciones, servicios y productos que están basados en el tratamiento de datos personales o que tratan datos personales para cumplir su función, ha de alentarse a los productores de los productos, servicios y aplicaciones a que tengan en cuenta el derecho a la protección de datos cuando desarrollan y diseñen estos productos, servicios y aplicaciones, y que se aseguren, con la

debida atención al estado de la técnica, de que los responsables y los encargados del tratamiento están en condiciones de cumplir sus obligaciones en materia de protección de datos".

Por otro lado, un papel fundamental dentro de este nuevo modelo de responsabilidad activa establecido en el Reglamento general de Protección de Datos lo desempeñará el delegado de protección de datos (DPD), que el Reglamento General regula en sus artículos 37 a 39, señalando este último precepto sus funciones:

Artículo 39 -Funciones del delegado de protección de datos-

1. El delegado de protección de datos tendrá como mínimo las siguientes funciones:

a) informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del presente Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros;

b) supervisar el cumplimiento de lo dispuesto en el presente Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes;

c) ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35;

d) cooperar con la autoridad de control;

e) actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36, y realizar consultas, en su caso, sobre cualquier otro asunto.

2. El delegado de protección de datos desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento."

La designación del delegado de protección de datos será obligatoria en los supuestos contemplados en el artículo 34 de la LOPDGDD.

Por consiguiente, para determinar las medidas y garantías adoptadas para garantizar que el tratamiento es conforme con la normativa de protección de datos personales, el responsable ha de tener en cuenta, como establece el artículo 24 del RGPD el ámbito, el contexto y los fines del tratamiento y los riesgos para los derechos y libertades de las personas físicas, y a partir del análisis de riesgos y la EIPD, deberá adoptar todas las medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el Reglamento, incluidas las correspondientes medidas de seguridad.

En cuanto a estas últimas, el artículo 32 del RGPD no establece una lista cerrada de medidas de seguridad que el responsable y el encargado hayan de adoptar, de manera que, adoptándolas, habrían cumplido con sus obligaciones en materia de seguridad, sino que en virtud del principio de responsabilidad proactiva, establece que "teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo", que en su caso incluya, entre otras:

"a) la seudonimización y el cifrado de datos personales;
b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;
c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;
d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento".

En consecuencia, corresponde al responsable del tratamiento y, en su caso, al encargado, asesorados, en su caso, por el DPD, determinar, dentro del marco de gestión del riesgo para los derechos y libertades establecido en el artículo 24, todas las medidas y garantías, incluidas las medidas de seguridad, necesarias para el tratamiento de datos personales que se pretende realizar, no correspondiendo a esta Agencia pronunciarse sobre las mismas, salvo en el supuesto excepcional de que resulte necesario formular una consulta previa cuando la EIPD muestre un riesgo alto para los derechos y libertades de las personas tras haber aplicado medidas para mitigarlo, y sin perjuicio de los poderes de investigación que corresponden a la misma.

XI

Como puede observarse, son muchos los aspectos derivados de la normativa de protección de datos que tienen incidencia y deben valorarse en el trabajo a distancia, algunos de los cuales son considerados parcialmente, directa o indirectamente, en el texto informado, que incluye, además, de los preceptos ya analizados en el presente informe, una cláusula genérica en su artículo 16.

> Artículo 16. Derecho a la intimidad y a la protección de datos.
>
> 1. La utilización de los medios telemáticos y el control de la prestación laboral mediante dispositivos automáticos garantizará adecuadamente el derecho a la intimidad y a la protección de datos, en los términos previstos en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, de acuerdo con los principios de idoneidad, necesidad y proporcionalidad de los medios utilizados.
>
> 2. La empresa no podrá exigir la instalación de programas o aplicaciones en dispositivos propiedad de la persona trabajadora, ni la utilización de estos dispositivos en el desarrollo del trabajo a distancia.
>
> 3. Las empresas deberán establecer criterios de utilización de los dispositivos digitales respetando en todo caso los estándares mínimos de protección de su intimidad de acuerdo con los usos sociales y los derechos reconocidos legal y constitucionalmente. En su elaboración deberá participar la representación de las personas trabajadoras.
>
> La negociación colectiva o, en su defecto, los acuerdos de empresa podrán especificar los términos dentro de los cuales las personas trabajadoras pueden hacer uso por motivos personales de los equipos informáticos puestos a su disposición por parte de la empresa para el desarrollo del trabajo a distancia, teniendo en cuenta los usos sociales de dichos medios y las particularidades del trabajo a distancia.

A este respecto, debe considerarse que el derecho a la protección de datos personales es un derecho fundamental reconocido en el artículo 18.4 de la Constitución, que es independiente del derecho a la intimidad recogido en el mismo precepto, de acuerdo con reiterada doctrina del Tribunal Constitucional.

En este sentido, la sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre de 2000 recuerda cómo “el Tribunal ya ha declarado que el art. 18.4 C.E. contiene, en los términos de la STC 254/1993, un instituto de

garantía de los derechos a la intimidad y al honor y del pleno disfrute de los restantes derechos de los ciudadanos que, además, es en sí mismo «un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la Constitución llama ´la informática»´, lo que se ha dado en llamar «libertad informática» (F.J. 6, reiterado luego en las SSTC 143/1994, F.J. 7, 11/1998, F.J. 4, 94/1998, F.J. 6, 202/1999, F.J. 2). La garantía de la vida privada de la persona y de su reputación poseen hoy una dimensión positiva que excede el ámbito propio del derecho fundamental a la intimidad (art. 18.1 C.E.), y que se traduce en un derecho de control sobre los datos relativos a la propia persona. La llamada «libertad informática» es así derecho a controlar el uso de los mismos datos insertos en un programa informático (habeas data) y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención (SSTC 11/1998, F.J. 5, 94/1998, F.J. 4)".

Para el Alto Tribunal, "la peculiaridad de este derecho fundamental a la protección de datos respecto de aquel derecho fundamental tan afín como es el de la intimidad radica, pues, en su distinta función, lo que apareja, por consiguiente, que también su objeto y contenido difieran. La función del derecho fundamental a la intimidad del art. 18.1 C.E. es la de proteger frente a cualquier invasión que pueda realizarse en aquel ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad (por todas STC 144/1999, de 22 de julio, F.J. 8). En cambio, el derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado […]".

También destaca cómo el objeto del derecho a la protección de datos es más amplio que el del derecho a la intimidad, partiendo de que "el derecho fundamental a la protección de datos amplía la garantía constitucional a aquellos de esos datos que sean relevantes para o tengan incidencia en el ejercicio de cualesquiera derechos de la persona, sean o no derechos constitucionales y sean o no relativos al honor, la ideología, la intimidad personal y familiar a cualquier otro bien constitucionalmente amparado […]. Por consiguiente, también alcanza a aquellos datos personales públicos, que por el hecho de serlo, de ser accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos. También por ello, el que los datos sean de carácter personal no significa que sólo tengan protección los relativos a la vida privada o íntima de la persona, sino que los datos amparados son todos aquellos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo".

Y por último, destaca otra diferencia fundamental del derecho a la protección de datos, derivada de su contenido, ya que a diferencia del derecho a la intimidad personal y familiar, que confiere a la persona el poder jurídico de imponer a terceros el deber de abstenerse de toda intromisión en la esfera íntima de la persona y la prohibición de hacer uso de lo así conocido "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.

Atendiendo a las distintas cuestiones planteadas en el presente informe, esta Agencia considera necesario que, de manera separada a las previsiones que contiene el artículo 16 del proyecto, referidas al derecho a la intimidad, se integre en el mismo un nuevo artículo relativo a la necesidad de garantizar el cumplimiento de la normativa de protección de datos personales, constituida, fundamentalmente, por el Reglamento (UE) 679/2016, con el siguiente contenido:

"1.- Los tratamientos de datos de carácter personal de las personas físicas se realizarán con estricta sujeción a lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

2.- El empleador, previo el análisis de los riesgos para los derechos y libertades de las personas físicas y, en su caso, de la evaluación de impacto en la protección de datos, está obligado a adoptar las medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar el cumplimiento de la normativa señalada en el apartado anterior.

3.- Mediante convenio colectivo se procurará establecer normas más específicas para garantizar la protección de los derechos y libertades en relación con el tratamiento de datos personales de los trabajadores en el trabajo a distancia, especialmente en lo que se refiere al tratamiento de categorías especiales de datos del artículo 9 del Reglamento (UE) 2016/679.