ACCIÓN SINDICAL Y LEY ORGÁNICA DE PROTECCIÓN DE DATOS

Aránzazu Escribano Clemente. Gabinete Jurídico Confederal CGT. Junio 2021.

ÍNDICE

1.-Introducción.

Lo primero que tenemos que tener presente a la hora de hablar de protección de datos es que ésta es un derecho fundamental recogido en el art. 18.4 de la Constitución Española y que, como tal, ha sido posteriormente desarrollado por distintas normativas: **LORTAD** 1992 (Ley Orgánica de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal), la **antigua LOPD** de 1999 (Ley Orgánica de Protección de Datos), el **RGPD** (Reglamento General de Protección de Datos, Reglamento (UE) 2016/679 del parlamento europeo y del consejo de 27 de abril de 2016) y la Ley que finalmente desarrolla este último (LOPD 3/2018 de 5 de diciembre, **LOPDGDD**). Recientemente, ha sido publicada la **Ley Orgánica 7/2021**, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.

2.- Antecedentes y conceptos básicos.

2.1. Antecedentes.

El Reglamento General de Protección de Datos (RGPD) entró en vigor en mayo de 2016, pero es aplicable desde el 25 de mayo de 2018, ya que se concedió un periodo transitorio de adaptación a los responsables y encargados de tratamiento para que fueran preparando y adoptando las medidas necesarias para estar en condiciones de cumplir con las previsiones contenidas en dicho Reglamento.

Estamos ante una norma directamente aplicable, aunque tiene su posterior desarrollo en la Ley 3/2018, de 5 de diciembre.

2.2. Conceptos básicos.

Antes de nada es conveniente tener claros una serie de conceptos claves para entender no sólo el nuevo RGPD, sino también la LOPD. Dichos conceptos son:

Datos de carácter personal: cualquier dato concerniente a personas físicas identificadas o identificables. Se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

Fichero: todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

Tratamiento de datos: Operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

Responsable del fichero o tratamiento: persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento

Encargado del tratamiento: persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.

Responsable de seguridad: persona o personas a las que el responsable del fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables.

Afectado o interesado: Persona física titular de los datos que sean objeto de tratamiento. Persona identificable: Toda persona cuya identidad pueda determinarse directa o indirectamente mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social.

Tercero: La persona física o jurídica, pública o privada, u órgano administrativo distinta del afectado o interesado, del responsable del tratamiento, del responsable del fichero, del encargado del tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable del tratamiento o del encargado del tratamiento.

Consentimiento del interesado: Toda manifestación de voluntad libre, inequívoca, específica e informada mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.

Sistema de tratamiento: Modo en que se organiza o utiliza un sistema de información. Atendiendo al sistema de tratamiento los sistemas de información podrán ser automatizados, no automatizados o parcialmente automatizados.

Copia de respaldo: Copia de los datos de un fichero automatizado en un soporte que posibilite su recuperación.

Ficheros temporales: Ficheros de trabajo creados por usuarios o procesos que son necesarios para un tratamiento ocasional o como paso intermedio durante la realización de un tratamiento.

Accesos autorizados: Autorizaciones concedidas a un usuario para la utilización de los diversos recursos. En su caso incluirán las autorizaciones o funciones que tenga atribuidas un usuario por delegación del responsable del fichero o tratamiento o del responsable de seguridad.

Transferencia internacional de datos: Tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo, bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español.

3. Obligaciones en materia de protección de datos.

Los sindicatos también tienen en sus manos una gran cantidad de datos, de afiliados, de proveedores, de empleados, por lo que también tienen que adaptarse a la normativa. Para el correcto manejo de esos datos es necesario llevar a cabo varias actuaciones:

1. Realizar un Registro de Actividades de tratamiento.
2. Firmar los contratos con terceros.
3. Firmar los contratos y demás comunicaciones informativas con los empleados.

4. Solicitar el consentimiento a los afiliados.

5. Incluir los textos legales en la página web.

6. Realizar un Análisis de riesgos.

7. Evaluación de impacto.

8. Notificar brechas de seguridad.

9. Nombrar un DPD.

3.1. Registro de actividades de tratamiento.

Lo primero que hay que tener en cuenta es qué tipo de datos se manejan en el sindicato y qué cantidad. Para dicho registro hay que incluir la siguiente información:

- Tipo de datos almacenados.
- Finalidad.
- Legitimados.
- **P**olítica de almacenamiento de esos datos.
- Si se realizan cesiones o transferencias internacionales.
- Medios a través de los que se realiza el tratamiento.

Este registro debe estar siempre actualizado.

3.2. Contratos con encargados de tratamiento.

Es necesario tener una lista de empresas o terceros externos con las que se tiene contacto y que maneja algunos o todos los datos personales que nos ceden para asegurar que también se cumple la normativa. Por ej.: gestoría, empresa informática… Para ello es necesario firmar con ellos un contrato de encargado de tratamiento en el que se establezcan obligaciones de estos para proteger los datos personales que se les cedan.

El contrato debe incluir, como mínimo:

- objeto, la duración, la naturaleza y la finalidad del tratamiento,
- tipo de datos personales,
- categorías de interesados, y
- obligaciones y derechos del responsable.

Se adjunta modelo anexo.

3.3. Acuerdo de confidencialidad con empleados.

Los empleados deben firmar un acuerdo de confidencialidad para evitar que la información que manejan sea revelada a personas no autorizadas. También debe cumplir con las medidas de seguridad establecidas para garantizar la protección de los datos personales.

3.4. Consentimiento de afiliados.

El sindicato debe tener el consentimiento expreso de los afiliados para poder tratar sus datos. Debe haber un formulario (virtual o en papel, según sea el modo de recabar los datos personales) solicitando el consentimiento para el tratamiento de los datos. En el se debe informar claramente de:

- datos del responsable del tratamiento (sindicato),
- finalidad concreta del tratamiento,
- tiempo que se conservarán,
- destinatarios, si los hay (si se ceden los datos a otras entidades o terceros),
- transferencias de datos internacionales si se realizan,
- derechos de los afectados y cómo se pueden exigir estos

• datos del Delegado de Protección de datos (si el sindicato debe contar con uno o así lo ha decidido).

3.5. Incluir los textos legales en la página web.

Si el sindicato tiene página web, debe incluir en esta los textos exigidos en la Ley de Protección de Datos y la Ley de Servicios de la Sociedad de la Información:

•- **Aviso Legal.** Es el documento donde se identifica al propietario de la página web. En el se debe incluir el nombre del propietario, CIF/NIF, dirección y email.

•- **Política de privacidad.** La **política de privacidad de una página web** es un documento legal en el que el titular de la web debe informar sus clientes y usuarios sobre los datos personales que se recopilan al navegar en el sitio, a través de que medios se recogen estos datos, se almacenan y sobre el tratamiento que se realizará de los mismos.

La política de Privacidad también debe recoge las medidas empleadas para garantizar la seguridad y el uso legal de los datos personales recogidos en la web.

De acuerdo al artículo 12 del RGPD, la política de privacidad de una web debe ser sencilla, concisa, transparente y comprensible, es decir, no debe estar redactada en términos ambiguos o demasiado técnicos.

Así mismo, la política de privacidad debe cumplir con una serie de principios:

•Principio de transparencia lealtad y licitud: Se necesita el consentimiento expreso del usuario para poder realizar el tratamiento de datos personales.

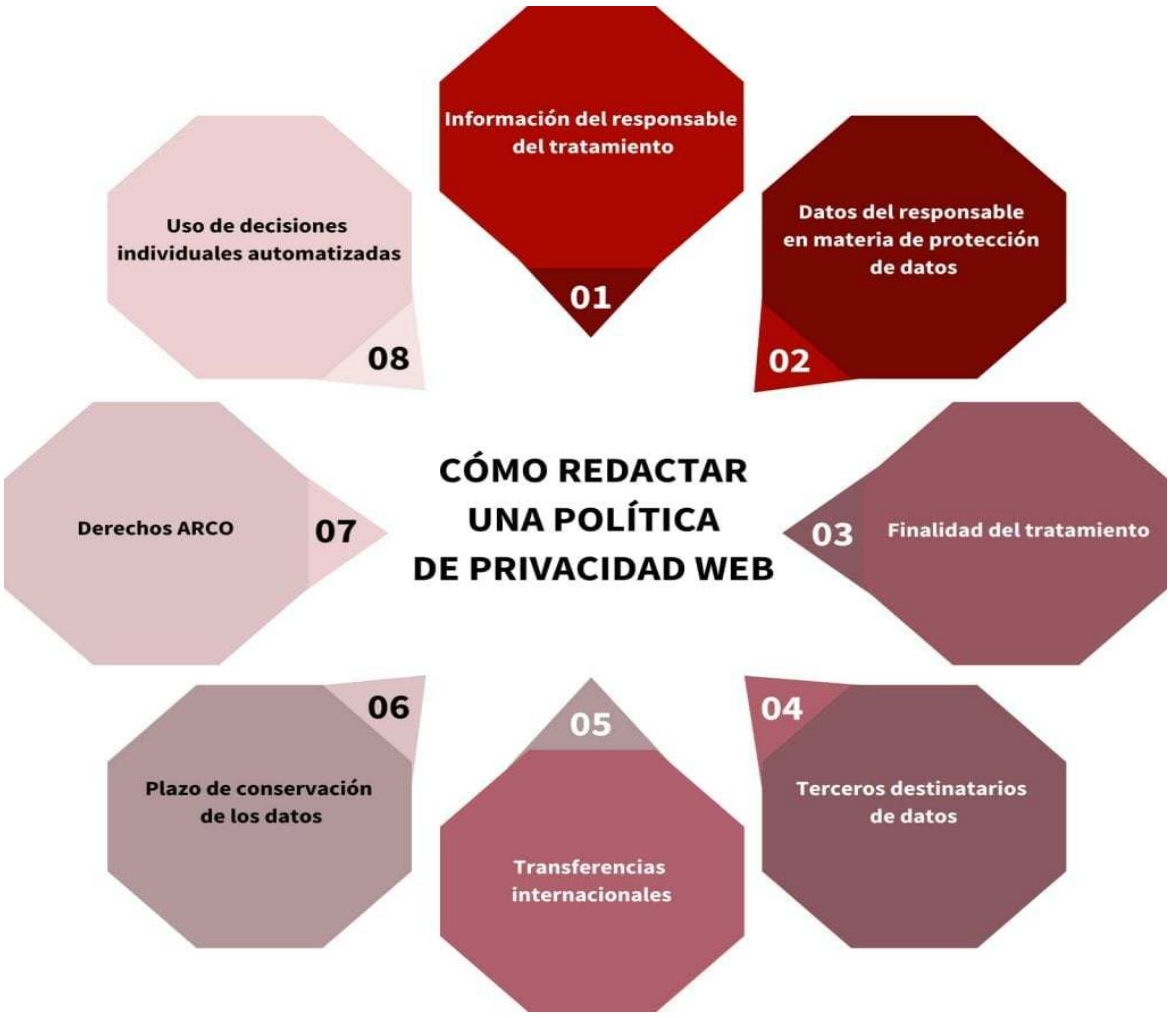
•Principio de minimización: Solo se recabarán los datos imprescindibles para poder llevar a cabo los servicios solicitados por el usuario.

•Principio de limitación del plazo: Los datos personales se destruirán una vez se haya cumplido la finalidad para que fueron recabados.

•Principio de confidencialidad e integridad: Se debe asegurar que se cumplen y toman todas las precauciones para que terceros no autorizados no puedan acceder a los datos.

Es importante que se tenga una versión extensa de la política de privacidad que incluya más información sobre el procesamiento de los datos. Se debe informar expresamente sobre:

- existencia de un tratamiento de los datos que se le están solicitando,
- finalidad,
- destinatario o destinatarios de aquella información,
- legitimación para el tratamiento,
- plazo de conservación de los datos,
- identidad y dirección del responsable del tratamiento de los datos y
- posibilidad de ejercer sus derechos y por qué vía.



•- **Política de cookies.** Las cookies son archivos de información enviados por un sitio web y almacenados en el navegador del usuario que visita ese sitio. Se utilizan para analizar las visitas a la página web o mostrar publicidad dinámica.

Por tanto, si la web del sindicato incluye algo de esto, se debe cumplir con la ley de cookies, que es la propia LSSI. En ese texto debe informarse sobre las cookies utilizadas en la página, su finalidad y duración.

Para cumplir con el RGPD, la política de cookies debe indicar:

•Qué tipos de cookies se establecen,

•Cuánto tiempo persisten en el navegador del usuario,

•Qué datos rastrean / las categorías de información personal recopilada

•Con qué finalidad (funcionalidad, rendimiento, estadísticas, marketing, etc.),

•Dónde se envían los datos y con quién se comparten,

•Cómo rechazar las cookies y cómo cambiar posteriormente el estado de las cookies.

¿Qué ocurre si no cumplo la política de cookies?

Dado que la legislación de la UE sobre cookies no es una ley, no establece sanciones específicas. En cambio, requiere que los gobiernos locales establezcan sus propias leyes y sanciones asociadas. Esto significa que las posibles sanciones que enfrentas por incumplimiento variarán según el lugar donde vivas.

Pero, en la mayoría de los casos, si no cumples, los reguladores locales probablemente tomarán una de las siguientes acciones:

•Solicitar información: antes de que tu regulador local comience a realizar solicitudes de cambios, es posible que te pida que proporciones información adicional. Esto puede implicar información específica sobre los tipos de cookies que utiliza tu sitio, enlaces a la sección de información de cookies o cualquier otra cosa que pueda ayudarlos a determinar si tu sitio cumple con los requisitos o si es necesario realizar más esfuerzos.

•Solicitud de cambios: si tu regulador local determina que tu sitio no cumple con los requisitos, es probable que te soliciten que realices alguna acción para

cumplir con los requisitos. Si aún no has agregado esa ventana emergente de consentimiento, ahora es el momento de hacerlo.

•Cumplimiento: esta es la solicitud de cambio no tan agradable. En este punto, el regulador local te dará acciones específicas que deben completarse dentro de un período de tiempo establecido. Si aún no has mencionado esos anuncios de Google en tu página de información de cookies, ahora es absolutamente necesario. Si no cumples, podrías enfrentar importantes sanciones.

•Multas: las pautas que involucran lo que califica para una multa varían de un país a otro, al igual que el importe máximo de la multa que puedes recibir. Para obtener detalles específicos, debes consultar a tu regulador local. O, mejor aún, asegúrate de que tu sitio sea compatible, para no tener que preocuparte por las multas.

COOKIE (Y PROVEEDOR)	**DURACIÓN**	**DESCRIPCIÓN**
__cfduid (notin.es)	Sesión	Publicidad
personalization_id (twitter.com)	Sesión	Twitter
Facebook	Publicidad, estadísticas mediciones	Coloca Cookies en el ordenador o dispositivo y recibe la información almacenada en ellas cuando utilizas o visitas v servicios prestados por otras empresas que utilizan los servicios de Facebook.
_ga (Google)	2 años	Se usa para distinguir a los usuarios.
_gid (Google)	24 horas	Se usa para distinguir a los usuarios.

_gat (Google)	1 minuto	Se usa para limitar el porcentaje de solicitudes. Si has implementado Google Analytics mediante Google Tag Manager, esta cookie se llamará _dc_gtm_<property-id>.
_gali (Google)	30s	Atribución de enlace mejorada.
_unam (SHARETHI	Persistente	Su finalidad es cuantificar el número de Usuarios que comparten un determinado contenido y cuántas páginas web son visitadas a raíz de esa acción.
WordPress	2 años	Utilizado para el correcto funcionamiento del gestor de contenido WordPress.

3.6. Análisis de riesgos.

El sindicato debe hacer un análisis en el que se valoren los riesgos derivados de los tratamientos que se realicen. En especial, se deben tener en cuenta las siguientes cuestiones:

- tipo de datos,
- naturaleza de los datos,
- medios de tratamiento,
- cesiones,
- transferencias internacionales y
- número de interesados afectados.

Tras estos análisis se deben implementar las medidas de seguridad adecuadas.

3.7. Evaluación de impacto.

Si el riesgo resulta especialmente alto se debe realizar una evaluación de impacto para minimizar las posibilidades de afectar a los derechos y libertades de los interesados e implementar las medidas de seguridad adecuadas.

¿Quiénes tienen que realizar una evaluación de impacto?

- Empresas que realicen una evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar.
- Entidades que realicen un tratamiento a gran escala de las categorías especiales de datos, o de los datos personales relativos a condenas e infracciones penales.
- Empresas que realicen una observación sistemática a gran escala de una zona de acceso público.

Los sindicatos realizan un tratamiento de categorías especiales de datos ya que manejan datos de afiliación sindical, que son datos sensibles, por tanto, tienen que hacer una Evaluación de Impacto.

3.8. Brechas de seguridad.

Es obligatorio notificar cualquier incidente de seguridad que se produzca a la Agencia Española de Protección de Datos y a los afectados. Sería importante que, para estos casos, el sindicato tenga previsto un plan de respuesta, ya que, además, el límite son 72 horas para notificar a las autoridades y dotarlas de información.

3.9. Delegado de protección de datos.

El sindicato debe designar a un profesional con la cualificación necesaria en esta materia para que **salvaguarde los procesos y políticas internas** del tratamiento de datos personales. Este profesional será el Delegado de Protección de Datos (DPD).

Además, para cumplir con el principio de información del RGPD, la designación del DPD y sus datos de contacto deben hacerse públicos y deberán ser comunicados a las autoridades de supervisión competentes.

El Delegado de Protección de Datos podrá ser tanto una persona en plantilla como una externa y el cargo podrá ser desempeñado también por una empresa que ofrezca el servicio.

CONSIDERACIONES

PRIMERA.-

1º.- La afiliación sindical se encuentra dentro de la actividad principal recogida en el art. 37 RGPD, en relación con el art. 9.

2º.- Nuestra actividad no está dentro de las recogidas en el art. 34 LOPDyGDG (colegios profesionales, centros docentes, entidades que traten datos a gran escala…).

3º- El RGPD tampoco define qué se entiende por tratamiento a gran escala, aunque el considerando 91 ofrece alguna orientación. De hecho, no es posible dar una cifra exacta, ya sea con relación a la cantidad de datos procesados o al número de personas afectadas, que pudiera aplicarse en todas las situaciones. No obstante, esto no excluye la posibilidad de que, con el tiempo (según el Grupo de Trabajo del artículo 29), se desarrolle un método estándar para identificar en términos más específicos o cuantitativos dicho concepto. En cualquier caso, el citado Grupo de Trabajo recomienda que se tengan en cuenta los siguientes factores, en particular, a la hora de determinar si el tratamiento se realiza a gran escala:

- el número de interesados afectados, bien como cifra concreta o como proporción de la población correspondiente;

- el volumen de datos o la variedad de elementos de datos que son objeto de tratamiento;

- la duración, o permanencia, de la actividad de tratamiento de datos;

- el alcance geográfico de la actividad de tratamiento. Como ejemplos de tratamiento a gran escala cabe citar:

- el tratamiento de datos de pacientes en el desarrollo normal de la actividad de un hospital;

- el tratamiento de datos de desplazamiento de las personas que utilizan el sistema de transporte público de una ciudad (p. ej. seguimiento a través de tarjetas de transporte);

- el tratamiento de datos de geolocalización en tiempo real de clientes de una cadena internacional de comida rápida con fines estadísticos por parte de un responsable del tratamiento especializado en la prestación de estos servicios;

- el tratamiento de datos de clientes en el desarrollo normal de la actividad de una compañía de seguros o de un banco;

- el tratamiento de datos personales para publicidad comportamental por un motor de búsqueda;

- el tratamiento de datos (contenido, tráfico, ubicación) por proveedores de servicios de telefonía o internet.

Como casos que no constituyen tratamiento a gran escala cabe señalar:

- el tratamiento de datos de pacientes por parte de un solo médico;

- el tratamiento de datos personales relativos a condenas e infracciones penales por parte de un abogado.

SEGUNDA.-

En atención a lo anterior, cabe concluir que, ya que no existe un criterio concreto para determinar qué consideramos "a gran escala", y teniendo en cuenta

que cada Sindicato tendrá un número distinto de datos, tendrán que ser ellos los que valoren esta circunstancia.

A juicio de esta letrada, cada Sindicato, acogiéndose a la **voluntariedad** y valorando lo ya mencionado, debería designar a un profesional con la cualificación necesaria en esta materia para que **salvaguarde los procesos y políticas internas** del tratamiento de datos personales. Este profesional será el Delegado de Protección de Datos (DPD).

Sin embargo, no creo que exista dicha obligación en el caso del Comité Confederal, ya que en este caso no se tratan datos "a gran escala" (ni siquiera se rellena ficha afiliativa propia), ni entramos dentro de los supuestos del art. 34 de la LOPDyGDG.

TERCERA.-

Cabría preguntarse si puede existir un único DPD para varios responsables, es decir, un DPD común.

En este caso podríamos concluir que sí ya que el artículo 37, apartado 2, del RGPD permite a un grupo empresarial designar un único delegado de protección de datos (DPD), siempre que este **"sea fácilmente accesible desde cada establecimiento".**

La noción de accesibilidad se refiere a las tareas del DPD como punto de contacto con respecto a los interesados y a la autoridad de control, pero también internamente dentro de la organización, teniendo en cuenta que una de esas tareas es "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".

Con el fin de garantizar que el DPD, ya sea interno o externo, sea accesible, es importante asegurarse de que sus datos de contacto están disponibles de conformidad con los requisitos del RGPD. El DPD, con ayuda de un equipo si fuese

necesario, debe estar en condiciones de comunicarse eficazmente con los interesados y cooperar con las correspondientes autoridades de control. Esto significa también que dicha comunicación debe tener lugar en el idioma o idiomas utilizados por las autoridades de control y los interesados afectados.

La disponibilidad de un DPD (ya sea físicamente en las mismas instalaciones como empleado, ya sea en línea o mediante otros medios seguros de comunicación) es fundamental para garantizar que los interesados puedan contactar con el DPD.

Sin embargo, considero que para mayor y mejor accesibilidad, sería mejor que, como ya he afirmado antes, cada Sindicato designe su propio DPD.

CONCLUSIONES SEGÚN CONSULTA AEPD:

- Cada Sindicato debería ver, en función de la cantidad de datos que manejan, la obligatoriedad o no de nombrar un DPD o no. Pero, como ni el Reglamento ni la Ley son claros a la hora de determinarlo, mi consejo es que nombren un DPD, aunque sea voluntariamente (solo los que manejen más datos).

- El nombramiento, si se hace, debe hacerse por Sindicato, ya que se trata de facilitar la accesibilidad.

- Como Confederal aconsejo el estudio de la necesidad del nombramiento, aunque en este caso no lo considero obligatorio porque no creo que entremos dentro de la categoría (no manejamos datos "a gran escala").

- Si hay nombramiento debe comunicarse a la AEPD (10 días), y esa persona puede ser o no el mismo que el Responsable del tratamiento de datos, siempre que cuente con conocimientos en Derecho y práctica en protección de datos.

3.10. Documento de seguridad. Modelo anexo.

Es necesario actualizar o elaborar un **Documento de Seguridad** (el documento que recoge las medidas de seguridad de índole técnica y organizativa acordes a la

normativa de seguridad vigente que será de obligado cumplimiento para el personal con acceso a los sistemas de información.).

¿Qué debe contener este Documento?:

1. **Identificación, servicios y ámbito de aplicación** del documento de seguridad.
2. **Los ficheros** que se tiene (clientes, proveedores, trabajadores, cámaras de seguridad, etc.) y su estructura, es decir, nombre del fichero, origen de los datos, forma de tratamiento de los datos (soporte papel o informático), tipos de datos que se recogen (nombre, apellidos, dirección postal, teléfono, dirección electrónica…), nivel de seguridad del fichero (básico, medio o alto) y la empresa encargada de gestionar el fichero si la hubiere (por ejemplo: la gestoría laboral es la encargada de gestionar el fichero de RRHH, en tanto y en cuanto, elabora las nóminas de los trabajadores).
3. Cuáles son las **medidas de seguridad** que se tiene para proteger esos ficheros, señalar, entre otras: armarios cerrados con llave, despachos cerrados con llave, destructoras de papel en los despachos que contiene documentación en soporte papel, contraseñas personales en los ordenadores con acceso a datos personales, caducidad de las contraseñas, cómo, dónde y cuándo se hacen las copias de seguridad, dónde se guardan las referidas copias de seguridad, con qué periodicidad se hacen, cuál es el procedimiento a seguir en caso de que se produzca una incidencia en la empresa respecto a datos personales, etc.
4. Relación de los **encargados del tratamiento**, es decir, de las empresas a las que se ha contratado la prestación de un servicio y en función de dicha prestación tienen acceso a datos personales. Por ejemplo: la gestoría laboral, gestoría fiscal, la empresa de mantenimiento informático, la empresa de prevención de riesgos laborales, etc.).
5. **Inventario** de: los soportes con acceso a datos personales dónde se realizan las copias de seguridad, de los equipos informáticos que tienen acceso a datos y de los programas informáticos.

6. **Lista del personal de la empresa (Sindicato) con acceso a datos y las funciones** de cada uno de ellos (a qué ficheros acceden y qué pueden acceder con los datos personales que tratan).

4. Acción sindical y derecho de los trabajadores/as a la protección de datos.

4.1. Consideraciones previas.

La jurisprudencia, tanto del Tribunal Supremo, como del Tribunal Constitucional (STC 281/2005), ha avanzado hacia el criterio de disponibilidad por la empresa de la correspondiente estructura informática de comunicación (cuentas de correo, internet, etc.). Esclarecedora es la STS de 14 de julio de 2016, según la cual el art. 8 LOLS no impone a la empresa la obligación de facilitar las comunicaciones electrónicas a las centrales sindicales, aunque sí ha fijado los criterios siguientes en relación con el derecho de estas a disponer de una cuenta corporativa de correo electrónico:

- Obligación empresarial de atender la demanda sindical si existe previsión legal o convencional.

- Existe dicha obligación empresarial si tales medios telemáticos existen y su uso sindical no supone la asunción de costes económicos y de gestión que el empleador no está obligado a afrontar.

- La empresa puede condicionar el uso sindical de los medios de comunicación propios si tal uso produce una perturbación de la actividad de la misma y de los objetivos de intercambio de información para los que fueron creados (riesgos de colapso de la red informática, virus informáticos, extensión desmesurada de documentos) o implica un incremento de costes económicos.

- Es la empresa la que debe asumir la carga de probar las perturbaciones o costes económicos que pueda suponerle el permitir a las secciones sindicales utilizar la comunicación electrónica de la empresa como mecanismo de comunicación e información con los trabajadores.

- En caso de conflicto entre el uso empresarial y el sindical debe primar el interés de la empresa por tratarse de una herramienta configurada para la producción.

- La empresa deberá ser neutral respecto a los criterios de acceso sindical al uso de las TIC, lo que se traduce en la "interdicción de la desigualdad no justificada por razón de la sindicación y del ejercicio de la libertad sindical, de manera que los parámetros técnicos han de ser iguales para los diferentes usuarios sindicales " (SAN 83/14, de 27 de mayo).

4.2. Potestad empresarial VS acción sindical.

Los convenios colectivos o los protocolos empresariales deben contemplar dos aspectos:

a.- El uso sindical de las TIC para la actividad sindical.

b.- El uso de los sindicatos y de los trabajadores para la comunicación de asuntos laborales o sindicales.

Sin embargo, la empresa puede imponer limitaciones o condiciones en el uso sindical de las TIC. Ej.: prohibición para fines particulares, control de acceso a internet, prohibición de algunas descargas, prohibición de algunas publicaciones, etc.

Además, el uso de las TIC tiene que estar relacionado con fines sindicales y de representación.

Hay dos cuestiones más polémicas en este asunto: 1ª solicitud del listado de correos corporativos de los trabajadores y 2ª envío masivo de correos a través de la red corporativa empresarial.

Respecto a la primera cuestión se ha manifestado la STS 14/07/2016 (rec 199/2015), según la cual es "incuestionable el legítimo interés de la sección sindical en disponer de acceso a la lista de correo electrónico de distribución conjunta de todos los empleados de la empresa, para facilitar de esta manera el más ágil y eficaz flujo de la información sindical a través de este mecanismo".

Respecto al envío masivo de correos, la jurisprudencia considera legítimo que la empresa condicione el envío al respeto de las normas de funcionamiento del correo electrónico corporativo, a los efectos de garantizar la seguridad y el buen funcionamiento de la red corporativa. Para el TS, ello "viene avalado por la referida doctrina constitucional cuando dice que resultaría lícito desde esa suprema perspectiva que la empresa predeterminase las condiciones de utilización para fines sindicales de las comunicaciones electrónicas, siempre que no las excluyera en términos absolutos, y que no teniendo fundamento el derecho en una carga empresarial expresamente prescrita en el ordenamiento, la utilización del instrumento empresarial no podrá ocasionar gravámenes adicionales para el empleador" (STS 24-3-2015, Rec. 118/2014). Sin embargo, fuera de las exigencias técnicas que la empresa puede imponer, por ejemplo, para el envío de correos masivos, queda vedado a la empresa la indagación sobre remitentes y destinatarios de la correspondencia electrónica o el control de las listas de correo corporativo empleadas por los sindicatos. Además, la prohibición empresarial a los trabajadores de uso del correo con fines personales no puede servir ni para impedir el uso del correo electrónico con la finalidad de comunicación entre representantes y representados, ni puede justificar la injerencia en la privacidad de las comunicaciones de contenidos sindicales.

Aspecto también delicado es el del impacto que el uso de los listados de correos corporativos puede tener en la información sobre afiliación sindical de los trabajadores. Es conveniente tener en cuenta que, conforme a la doctrina constitucional, se garantiza el derecho del sindicato a no revelar datos que afecten a la libertad ideológica de los trabajadores. Por ello, la empresa debe evitar la indagación al respecto, y, en todo caso, la información que le venga dada por el uso sindical de los correos no podría ser utilizada fuera del contexto de comunicación entre el sindicato y sus afiliados

Por otra parte, en la medida en que el uso de listados de correos corporativos individuales pueda dar publicidad a la afiliación sindical, el sindicato debe contar con la aprobación del trabajador, puesto que, para el TC, la afiliación a un sindicato es una opción ideológica individual del trabajador protegida por el art. 16 CE.

4.3. Derecho de los trabajadores a la protección de datos.

Esta cuestión ha sido objeto de mucha controversia en los últimos años, dado el choque producido entre el derecho a la libertad sindical y el derecho a la protección de datos personales de las personas físicas. Tal es así que la Agencia Española de Protección de Datos (AEPD) se ha pronunciado reconociendo que aunque pueda existir una intromisión en el derecho fundamental a la protección de datos éste no es absoluto, pudiendo ceder ante "intereses relevantes". Esto sucede por ejemplo con la libertad sindical (Resolución de la AEPD de 15 de marzo de 2018 en materia de tutela de derechos fundamentales en asunto relativos a envío de información sindical por correo electrónico a los trabajadores).

La AEPD diferencia entre dos escenarios:

1.Tratamiento de datos durante el proceso electoral: en este caso los empleados no pueden oponerse al tratamiento de sus datos personales siempre y cuando el sindicato trate sus datos ciñéndose al marco del propio proceso electoral.

2.Tratamiento de datos al margen del proceso electoral: en esta circunstancia los empleados podrán mostrar su oposición a los sindicatos para que no les envíen información sindical a través de la cuenta de e-mail si existen motivos legítimos relativos a una situación personal específica. Las organizaciones sindicales a su vez están obligadas a atender el ejercicio de ese derecho con los requisitos formales previsto en la normativa, resolviendo y contestando preceptivamente al solicitante.

5.- Representación unitaria y sindical de las personas trabajadoras.

5.1. Tratamiento de datos por parte de los/as representantes de las personas trabajadoras.

El cumplimiento de las obligaciones y el ejercicio de los derechos de los representantes de las personas trabajadoras permiten el tratamiento de datos personales de las personas trabajadoras sin el consentimiento de éstas.

No obstante, este tratamiento cuenta con una serie de límites:

1º- Sólo podrán ser objeto de tratamiento los datos necesarios para el ejercicio de esas funciones de representación.

2º- El empleador no debe ceder a los representantes más datos de los imprescindibles para realizar sus funciones (minimización de datos).

Ejemplo.

No es admisible el tratamiento de datos privados de la persona trabajadora, como el número de teléfono personal. Sí lo sería, en cambio, la identificación de las personas trabajadoras que ocupan cada puesto de trabajo con nombre y apellidos (**STS 572/2018 de 7 de febrero, Sala de lo Social**) y también la dirección de correo electrónico corporativo.

Ejemplo.

El derecho a la protección de datos es contrario a una petición masiva de datos sobre las personas trabajadoras cuando los sindicatos no acrediten una «necesidad debidamente justificada» y no se especifique la finalidad para la que se requieren tales datos (**Auto del TC 29/2008, de 28 enero**). Por tanto, se vulnera el derecho a la protección de datos cuando, en el marco de un despido colectivo, no sólo se comunica a los representantes el nombre, la antigüedad o la categoría de la persona trabajadora, sino otra información innecesaria, como el número de DNI o el domicilio.

Respecto del absentismo, la empresa deberá informar sobre las causas y consecuencias de las bajas por incapacidad temporal (IT), pero no de las patologías médicas concretas de las personas trabajadoras que, por otra parte, tampoco debería conocer la empresa.

Mención aparte merece el Covid. Se adjunta anexo resumen de la guía publicada por la AEPD.

3º- Los datos no podrán ser utilizados con finalidades distintas a las del ejercicio de las tareas representativas.
4º- Siempre que los representantes de las personas trabajadoras hagan uso de los medios proporcionados por la empresa para el ejercicio de sus funciones, se les considerarán aplicables las políticas de seguridad de la entidad, tanto para el trabajo en los locales de la entidad, como en situación de movilidad o teletrabajo. Al tratarse de funciones distintas de las que llevan a cabo como usuarios en la empresa, tendrían que recibir perfiles específicos para acceder a los sistemas de información para el ejercicio de su acción representativa y recibir la formación adecuada para su manejo.

Como responsables del tratamiento en el desarrollo de su acción representativa, deberán cumplir las medidas de seguridad aplicables y, en particular, en el caso de que se produzca una brecha de seguridad que afecte a los tratamientos de datos de carácter personal realizados en el desempeño de sus funciones, tendrán que cumplir con los requisitos relativos a la notificación de quiebras de seguridad a la autoridad de control y, dependiendo de su alcance, a los afectados. En cualquier caso, deberán comunicarlo de forma inmediata a la empresa en la que desempeñen sus funciones.
5º- Los convenios colectivos, en los términos previstos en el art. 64.9 del ET, podrían ser base jurídica para la lícita cesión de datos personales a los representantes de las personas trabajadoras (art. 88.1 RGPD).
6º- El tratamiento de datos requiere cumplir la obligación de informar a las personas trabajadoras.
7º- Los representantes deben respetar la confidencialidad de esos datos.

5.2. Publicación de datos personales en tablones de anuncios.

Como ya sabemos, el art. 81 del ET y la Ley Orgánica 11/1985, de 2 de agosto, de Libertad Sindical (LOLS), reconocen el derecho a disponer de un tablón de anuncios (on line o físico) para facilitar información sindical a los trabajadores. Cuando las publicaciones contienen datos personales su publicación comporta el acceso a datos por personas que no tienen esa legitimación, por tanto, hay que tener en cuenta una serie de aspectos:

■ Será responsable del tratamiento de datos en el tablón de anuncios y, por tanto, de las informaciones publicadas en el mismo, aquél órgano u organización que decida sobre su uso y finalidad y sitúe materialmente la información en él.

■ Debe considerarse el espacio físico o virtual concreto en el que se situará el tablón con la finalidad de que, en caso de contener información personal, ésta sólo resulte visible a los usuarios legitimados para consultarla.

Ej. No es razonable que un tablón del que se pueda obtener información sindical, se sitúe en una zona de acceso libre para clientes o proveedores.

■ Es fundamental que los tablones sindicales online se sitúen en las intranet de la empresa, nunca en Internet, salvo que únicamente resulten accesibles mediante usuario y contraseña (SAN 3578/2019, de 8 de junio, Sala de lo contencioso).

■ Debe tenerse muy en cuenta el principio de calidad desde el punto de vista de la proporcionalidad de los tratamientos y de la finalidad de los mismos.

■ Es recomendable considerar la posibilidad de que los tablones impidan el acceso a la información por terceros no autorizados, salvo que prevalezcan las libertades de expresión e información propias de la libertad sindical (SAN 3094/2014, de 12 de junio, Sala de lo Contencioso).

■ Sólo los usuarios legitimados deben tener acceso al tablón de anuncios.

5.3. Descuento de la cuota sindical.

El art. 9.1 del RGPD prohíbe el tratamiento de datos personales que revele la afiliación sindical, dato personal que se encuadra entre las categorías especiales. No obstante, el art. 9.2 del RGPD contiene excepciones respecto de esa prohibición.

Concretamente la recogida en su apartado d), dentro de las actividades legítimas del sindicato, y siempre con el consentimiento de la persona afiliada, el sindicato puede proceder a la comunicación del dato de afiliación a la empresa a efectos del descuento de la cuota sindical.

El tratamiento de datos sobre la afiliación sindical por el empleador es lícito «cuando sea 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» (art. 9.2.b del RGPD).

Por tanto, en este marco, el consentimiento es necesario para que el sindicato pida a la empresa el descuento de la cuota.

Una vez obtenido el consentimiento para ese tratamiento, las siguientes operaciones:

- que la empresa comunique al sindicato las personas trabajadoras a las que corresponden las cuotas que ingresa, así como los datos del pago y
- que la empresa informe al sindicato sobre las cuotas impagadas identificando a la persona trabajadora concreta, tienen su base jurídica en el cumplimiento de una obligación legal por el responsable.

El tratamiento de estos datos requiere la adopción de procedimientos para proteger información particularmente sensible:

a) Es recomendable disponer de procedimientos de captación del consentimiento como impresos o modelos de solicitud en los que la persona trabajadora autorice por escrito el tratamiento.

b) Debe limitarse el uso de estos datos a la finalidad para la que se han recabado (cobrar la cuota y transferir las cantidades a la organización sindical).

5.4. Comunicaciones por correo electrónico y/o envíos sindicales.

El envío de información sindical a través del correo electrónico implica un tratamiento de datos personales, pues una dirección electrónica es un dato personal. El Tribunal Constitucional ha señalado que el envío de este tipo de mensajes de correo electrónico constituye un derecho de los representantes amparado por el derecho fundamental de libertad sindical (**STC 281/2005**), de modo que los

representantes podrían utilizar la infraestructura de la empresa, que a su vez debería proporcionarles la dirección de correo electrónico de las personas trabajadoras. No obstante, deben darse ciertas condiciones, como que la empresa disponga del servicio de correo electrónico corporativo, que los envíos se realicen de modo proporcional y que no se perjudique el normal funcionamiento de la organización.

Cuando se den las circunstancias anteriores, existirá legitimación para que se produzca una comunicación de datos personales a los representantes.

Sin embargo, deben tenerse en cuenta las siguientes consideraciones:

1. Existen procedimientos automatizados que permiten satisfacer el derecho a la libertad sindical sin necesidad de realizar una cesión de datos personales.

Ejemplo.

La utilización de listas de distribución permite que el sindicato remita la información a una dirección corporativa del tipo listasindical@empresa.es, sin acceso a los datos. Además, puede incorporarse la información exigida por el RGPD en los pies de los correos y automatizar la supresión y la oposición a los tratamientos mediante las bajas en las listas a petición del usuario**.**

2. La comunicación de datos se limitará a los estrictamente necesarios.

Ejemplo.

En ningún caso se cederán datos como la dirección de cuentas privadas de la persona trabajadora, sólo la dirección de correo electrónico corporativa.

3. El dato se utilizará para la finalidad para la que fue comunicado.

4. El sindicato está obligado a cumplir con las previsiones del RGPD y de la LOPDGDD.

5. El sindicato debe respetar el derecho de oposición de los trabadores, salvo en el supuesto de elecciones sindicales, momento en el cual prevalece la libertad sindical respecto del derecho a la protección de datos.

La celebración de elecciones sindicales legitima las comunicaciones de los datos censales necesarios para permitir al sindicato remitir información electoral y participar en el proceso electoral.

5.5. Fichas afiliados/as.

Es importante que todas las fichas de afiliados/as incorporen una cláusula en la que se de expresamente el consentimiento para la utilización de los datos personales que se dan al rellenar dicha ficha.

Ejemplo:

Cláusula Reglamento 2016/679 de protección de datos. De conformidad con lo establecido en la normativa de Protección de Datos, le comunicamos que sus datos se incorporarán por un tiempo ilimitado a un fichero cuyo titular es el **Sindicato de XXXXXX de la Confederación General del Trabajo** (en adelante CGT XXX) con domicilio social en XXXX, para las siguientes finalidades: emisión de tarjetas de afiliación, emisión de recibos de la cuota sindical y gestión del cobro de la misma, envío de publicaciones e información que afecte a la actividad de CGT, elaboración de estadísticas y prestación de servicios. Si desempeña labores de representación colectiva, los datos serán tratados para la realización y seguimiento de las actividades sindicales amparadas en la legislación vigente.

Mediante la firma de esta solicitud, usted otorga **consentimiento expreso y escrito** para que CGT XXXX proceda a la cesión de sus datos a las siguientes entidades: **1)** al Secretariado Permanente del Comité Confederal de la CGT sito en la Calle Sagunto, 15 1º 28010 Madrid para las mismas finalidades apuntadas anteriormente; **2)** a la Confederación territorial de XXXXX de la CGT para la verificación de la vigencia de la afiliación y consiguiente prestación de servicios jurídicos; **3)** a la entidad bancaria para proceder al cobro de la cuota sindical; **4)** a la empresa que preste sus servicios informáticos para la realización de todas estas acciones. Puede ejercitar los **derechos de acceso, rectificación, cancelación, oposición, supresión o portabilidad de sus datos**, solicitándolo por escrito a CGT XXX en la dirección arriba indicada o en el email XXX Más información en XXXXX.

Guía anexo

5.7. Redes sociales.

Últimamente, está siendo objeto de debate hasta qué punto resulta de aplicación la normativa de protección de datos en la publicación de datos personales de terceros en redes sociales (Facebook, Instagram, etc.) por parte de particulares.

En este sentido, el artículo 2 del Reglamento General de Protección de Datos (RGPD), el cual establece su ámbito de aplicación material, indica expresamente que esta norma **no se aplica al tratamiento de datos personales efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas.** Esta excepción también se recoge en el considerando 18 del RGPD que establece que "*El presente Reglamento no se aplica al tratamiento de datos de carácter personal por una persona física en el curso de una actividad exclusivamente personal o doméstica y, por tanto,* ***sin conexión alguna con una actividad profesional o comercial***".

Precisamente, este considerando 18 recoge que "***Entre las actividades personales o domésticas cabe incluir*** *la correspondencia y la llevanza de un repertorio de direcciones, o* ***la actividad en las redes sociales*** *y la actividad en línea realizada en el contexto de las citadas actividades*".

Por lo tanto, de una primera lectura rápida, podría deducirse claramente que la publicación en redes sociales de imágenes y vídeos por un particular se encuentra fuera del ámbito de aplicación de la normativa de protección de datos, **siempre y cuando dicha publicación no tuviese conexión con una actividad profesional o comercial**.

Teniendo en cuenta lo indicado, el motivo del debate sería hasta qué punto la publicación por un particular de imágenes o vídeos en redes sociales se encuentra fuera del ámbito de aplicación de la normativa de protección de datos, por considerarse una actividad personal y doméstica, y cuándo dicha publicación excede de dicha esfera y sí le resulta de aplicación el RGPD.

En definitiva, ¿me puede sancionar la Agencia Española de Protección de Datos si publico en Facebook fotografías de mis amigos, familiares o conocidos sin su previo consentimiento?

Sobre los criterios a analizar a la hora de determinar **en qué circunstancias el tratamiento de datos personales en redes sociales excede el ámbito personal y doméstico** es importante destacar los siguientes documentos:

1. **Dictamen publicado por el Grupo de Trabajo del Artículo 29, que adoptó el 12 de junio de 2009, sobre las redes sociales en línea:**

El GT29 estima que, **con carácter general, en la mayor parte de las actividades realizadas por los usuarios de un servicio de redes sociales debe aplicarse lo que denomina "exención doméstica", en lugar de la normativa de protección de datos**.

Pero en el citado Dictamen se especifican **tres supuestos** en los que tales actividades no estarían cubiertas por la "exención doméstica".

1.**Cuando se utiliza el servicio de redes sociales como plataforma de colaboración para una asociación o una empresa.** Si un usuario actúa en nombre de una empresa o de una asociación o utiliza el servicio de la red social principalmente como una plataforma con fines comerciales, políticos o sociales, la exención no se aplica.

2.El GT29 expone que los prestadores de servicios de redes sociales deben garantizar la instauración de configuraciones por defecto gratuitas y que respeten la privacidad, restringiendo el acceso a los contactos seleccionados. En estas condiciones, **cuando el acceso a la información del perfil se amplía hasta más allá de los contactos seleccionados, como cuando se facilita el acceso al perfil a todos los miembros del servicio de redes sociales o cuando los datos son indexables por motores de búsqueda, el acceso se sale de la esfera personal o doméstica.** De igual manera, si un usuario toma una decisión informada de ampliar el acceso más allá de los "amigos" seleccionados, las responsabilidades inherentes a un responsable de datos se activan.

3.Aquellos supuestos en los que es preciso garantizar los derechos de terceros, particularmente **en relación con datos sensibles, como los que revelan el origen racial o étnico, opiniones políticas, creencias religiosas o filosóficas, la pertenencia a un sindicato o datos relativos a la salud o a la vida sexual**.

No obstante, se hace constar que, aun cuando se aplique la "exención doméstica", un usuario podría ser responsable de acuerdo con las disposiciones generales de la legislación civil o penal nacional en cuestión.

Centrándonos en las responsabilidades en materia de protección de datos, la AEPD indica que "***la difusión de datos sensibles*** *de una persona física (en contenidos tales como imágenes, audios o vídeos que permitan identificarla), publicados en diferentes servicios de internet sin consentimiento se considera una infracción de la normativa de protección de datos personales. La AEPD es competente para sancionar estas conductas con multas que, en los casos más graves, pueden alcanzar los 20.000.000 de euros o, tratándose de una empresa, una cuantía equivalente al 4% del volumen de negocio total anual global del ejercicio financiero anterior.*

Analizaremos la reclamación de forma prioritaria y, en su caso, ordenaremos la retirada del contenido al prestador del servicio o plataforma donde se esté difundiendo. Además, si hay indicios de delito, lo pondremos en conocimiento de la Fiscalía. En tales circunstancias, te informaremos de estos pasos. ***Si procede, la investigación continuará para tramitar un procedimiento sancionador contra las personas responsables de la difusión."***

¿Y si yo publico una fotografía de un tercero **sin su consentimiento** en redes sociales **sin contenido sensible pero accesible a todo el mundo**? ¿no estaríamos también fuera del ámbito personal y doméstico y la AEPD debería tener potestad para sancionar?

Está claro que afecta más a la privacidad de una persona las publicaciones realizadas en redes sociales con un contenido sexual y violento. No obstante, conforme al criterio manifestado por el GT29 en el Dictamen analizado, las publicaciones que sean accesibles a todo el mundo también excederían del ámbito personal y doméstico y, por lo tanto, les resultaría de aplicación la normativa de protección de datos, teniendo la AEPD potestad para sancionarlas, aunque entiendo que, de ser así, la AEPD no daría abasto a dar respuesta a estas reclamaciones y podría afectar al uso cotidiano que los ciudadanos hacen de las redes sociales.

En cualquier caso, por ahora, parece que el elemento fundamental que tiene en cuenta la AEPD para valorar que la publicación en redes sociales excede el ámbito personal y doméstico y que la conducta, por tanto, resulta sancionable por protección de datos es el carácter sensible de la publicación.

Para terminar, hacer mención al artículo 94 de la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), que regula el

derecho al olvido en redes sociales y servicios equivalentes. En concreto, este artículo establece lo siguiente:

1. Toda persona tiene derecho a que sean suprimidos, a su simple solicitud, los datos personales que hubiese facilitado para su publicación por servicios de redes sociales y servicios de la sociedad de la información equivalentes.
2. Toda persona tiene derecho a que sean suprimidos los datos personales que le conciernan y que hubiesen sido facilitados por terceros para su publicación por los servicios de redes sociales y servicios de la sociedad de la información equivalentes cuando fuesen inadecuados, inexactos, no pertinentes, no actualizados o excesivos o hubieren devenido como tales por el transcurso del tiempo, teniendo en cuenta los fines para los que se recogieron o trataron, el tiempo transcurrido y la naturaleza e interés público de la información.
Del mismo modo deberá procederse a la supresión de dichos datos cuando las circunstancias personales que en su caso invocase el afectado evidenciasen la prevalencia de sus derechos sobre el mantenimiento de los datos por el servicio.
Se exceptúan de lo dispuesto en este apartado los datos que hubiesen sido facilitados por personas físicas en el ejercicio de actividades personales o domésticas.

¿Quiere esto decir que no procedería, en la mayoría de los casos, el derecho al olvido en las redes sociales conforme a lo indicado en el apartado 2 del artículo 94 LOPDGDD? Teniendo en cuenta que, salvo los supuestos indicados, en la mayor parte de las actividades realizadas por los usuarios de un servicio de redes sociales debe aplicarse la excepción relativa al tratamiento de datos para fines personales o domésticos.

6.- Sanciones.

Con el RGPD se incrementan las exigencias en materia de Protección de Datos y también las sanciones en caso de incumplimiento, sanciones que se endurecen considerablemente, llegando a alcanzar los 20 millones de euros o el 4% de la facturación global anual.

Las infracciones se dividen en dos categorías:

- Menos graves: hasta 10 millones de euros o 2% de facturación global.
- Más graves: hasta 20 millones de euros o el 4% de la facturación.

El RGPD otorga una serie de facultades a las autoridades de control que podrán aplicar una serie de criterios de graduación a la hora de fijar la cuantía de la sanción: volumen de negocio, intencionalidad, reincidencia, perjuicios causados, si han resultado dañados también intereses de terceras personas, etc.

Se prevé también la posibilidad de que la sanción económica sea sustituida por un apercibimiento, con el fin de que el infractor adopte las medidas necesarias correctoras que se le indiquen.

Ejemplo de sanciones impuestas a sindicatos:

- No atender debidamente el ejercicio del derecho de rectificación o cancelación, para lo que tiene el plazo de 10 días.

- Acceso a datos personales por terceros no autorizados. El responsable del tratamiento deberá adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos.