LA PROTECCIÓN DE DATOS EN EL ÁMBITO SINDICAL

Aránzazu Escribano Clemente. Gabinete Jurídico Confederal CGT.

Octubre 2019.

ÍNDICE

4.- Derechos de los interesados.

a.- Derecho de acceso.

b.- Derecho de rectificación.

c.- Derecho de oposición.

d.- Derecho de cancelación.

e.- Derecho a la limitación del tratamiento.

f.- Derecho de supresión o derecho al olvido.

g.- Derecho de portabilidad.

5.- Acción sindical y derechos de los trabajadores a la protección de datos.

5.1. Consideraciones previas.

5.2. Potestad empresarial VS acción sindical.

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

5.4. Publicación de datos personales de trabajadores.

5.5. Acceso a datos por los Comités de Empresa.

5.6. Cesión de datos a Sindicatos.

6.- Sanciones.

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 (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) y la Ley que finalmente desarrolla este último (LOPD 3/2018 de 5 de diciembre).

2.- ANTECEDENTES, CONCEPTOS Y PRINCIPIOS BÁSICOS.

2.1. Antecedentes.

El nuevo 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.

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, de naturaleza pública o privada, u órgano administrativo que decida sobre la finalidad, contenido y uso del tratamiento.

Encargado del tratamiento: Persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que sólo, o conjuntamente con otros, 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 coordina 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 información: Conjunto de ficheros, tratamientos, programas, soportes, y en su caso, equipos empleados para el tratamiento de datos de carácter personal.

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

2.3. Principios básicos.

La mayor innovación que introduce el RGPD respecto de la LOPD la constituyen dos elementos generales, a saber:

1. ***Principio de responsabilidad proactiva:*** necesidad de que el responsable del tratamiento aplique las medidas técnicas y organizativas apropiadas que garanticen y demuestren que el tratamiento se ha hecho conforme con el RGPD. Se exige, pues, una actitud consciente, diligente y proactiva por parte de las organizaciones frente a los tratamientos de datos personales que lleven a cabo.

2. ***El enfoque de riesgo:*** las medidas que se tomen para garantizar el cumplimiento del RGPD deben tener en cuenta la naturaleza, el ámbito, el

contexto y los fines del tratamiento, así como el riesgo para los derechos y libertades de las personas. Así, algunas medidas solo se tomarán cuando exista un alto riesgo para los derechos y libertades, mientras que otras se modularán en función del nivel y del tipo de riesgo que se presente.

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.

- **Política 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.

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.** 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.

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.

3.10. Documento de seguridad.

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 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. Derechos de los interesados.

a. Derecho de acceso, derecho a obtener del Responsable del Tratamiento confirmación de si se están tratando o no datos personales que le conciernen y, en tal caso, derecho de acceso a los datos personales y a la siguiente información:

a) los fines del tratamiento;
b) las categorías de datos personales de que se trate;

c) los destinatarios o las categorías de destinatarios a los que se comunicaron o serán comunicados los datos personales, en particular destinatarios en terceros u organizaciones internacionales;

d) de ser posible, el plazo previsto de conservación de los datos personales o, de no ser posible, los criterios utilizados para determinar este plazo;

e) la existencia del derecho a solicitar del responsable la rectificación o supresión de datos personales o la limitación del tratamiento de datos personales relativos al interesado, o a oponerse a dicho tratamiento;

f) el derecho a presentar una reclamación ante una autoridad de control;

g) cuando los datos personales no se hayan obtenido del interesado, cualquier información disponible sobre su origen;

h) la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

b. Derecho de rectificación: posibilidad de que mediante su ejercicio ante el responsable que trata los datos personales, se modifiquen aquellos datos que sean inexactos o incompletos, debiendo en la solicitud de rectificación indicar qué datos desea que se modifiquen. A esta solicitud deberá acompañar la documentación justificativa correspondiente.

Cuando se ejercita este derecho deben contestar en el plazo máximo de 10 días hábiles. Si los datos hubieran sido comunicados a un tercero, el responsable deberá comunicarle los datos rectificados para que a su vez el tercero lo rectifique.

c. Derecho de oposición: el afectado se puede oponer a que no se realice el tratamiento de sus datos personales en los siguientes supuestos:

a) Cuando no siendo necesario el consentimiento para el tratamiento de los datos, exista un motivo legítimo y fundado referente a la concreta situación personal (salvo que una Ley establezca lo contrario).

b) Cuando existan tratamientos de datos personales cuya finalidad sea la realización de actividades de publicidad y prospección comercial.

c) Cuando el tratamiento tenga como fin la adopción de una decisión referida al afectado basada únicamente en un tratamiento automatizado de sus datos personales.

El plazo de respuesta ante el derecho de oposición es de 10 días hábiles.

d. Derecho de cancelación. Este derecho permite la cancelación de los datos personales que sean inadecuados o excesivos. Se conservarán bloqueados de manera que se impida su tratamiento, sin perjuicio de su puesta a disposición de las administraciones públicas, jueces y tribunales, para la atención de las

posibles responsabilidades que hayan surgido del tratamiento durante su plazo de prescripción.

Cumplido este plazo se procederá a la supresión de los mismos.

Cuando se solicite la cancelación de los datos personales, se deberá indicar a qué datos se refieren, aportando la documentación que justifique tal pretensión.

Deben contestar en el plazo máximo de 10 días hábiles. Si los datos hubieran sido comunicados a un tercero, el responsable deberá comunicarle los datos cancelados para que, a su vez, este tercero los cancele.

e. Derecho a la limitación del tratamiento, supon que, a petición del interesado, no se aplicarán a sus datos personales las operaciones de tratamiento que en cada caso corresponderían.

Este derecho se puede solicitar cuando:

- El interesado ha ejercido los derechos de rectificación u oposición y el responsable está en proceso de determinar si procede atender a la solicitud;

- El tratamiento es ilícito, lo que determinaría el borrado de los datos, pero el interesado se opone a ello;

- Los datos ya no son necesarios para el tratamiento, lo que también determinaría su borrado, pero el interesado solicita la limitación porque los necesita para la formulación, el ejercicio o la defensa de reclamaciones.

f. Derecho de supresión (derecho al olvido), "*el interesado tendrá derecho a obtener sin dilación indebida del Responsable del Tratamiento la supresión de los datos personales que le conciernan (...)*" cuando concurra alguna de las circunstancias siguientes:

a) Los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos.

b) El interesado retire el consentimiento en que se basa el tratamiento y no se base en otro fundamento jurídico.

c) El interesado se oponga al tratamiento (derecho de oposición).

d) Los datos personales se hayan tratado de forma ilícita.

e) Los datos personales deban suprimirse para el cumplimiento de una obligación legal que se aplique al Responsable del Tratamiento.

f) Los datos personales se hayan obtenido en relación con la oferta directa a niños de servicios de sociedad de la información.

El reglamento refuerza este derecho cuando estamos ante tratamientos en línea (internet). Por ello en el considerando 66 se indica que el Responsable del Tratamiento que haya hecho públicos datos personales está obligado a indicar a los responsables del tratamiento que estén tratando tales datos personales que supriman todo enlace a ellos, o las copias o réplicas de tales datos.

Existen una serie de excepciones a la supresión, que se darán cuando la necesidad del tratamiento resida en:

1. Ejercer el derecho a la libertad de expresión e información.

2. El cumplimiento de una obligación legal que se aplique al Responsable del Tratamiento.

3. Tratamiento para el cumplimiento de una misión realizada por interés público o en el ejercicio de los poderes públicos.

4. Razones de interés público en el ámbito de la salud pública.

5. Fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos.

6. La formulación, el ejercicio o la defensa de reclamaciones.

Por lo que se refiere a la eliminación de fotos y vídeos que han sido publicados en internet sin el consentimiento del afectado, puesto que ambos ostentan la consideración de datos personales, se puede ejercitar el derecho de cancelación de los mismos. Para ello hay que dirigirse, acreditando la identidad e indicando los enlaces donde aparecen los vídeos y fotos, ante quien los haya subido a la red, solicitando por tanto, el borrado de los mismos. Si no

responden o la respuesta es insatisfactoria, se puede interponer una reclamación de tutela de derecho ante la Agencia.

g. Derecho de portabilidad: implica que el interesado que haya proporcionado sus datos a un responsable que los esté tratando de modo automatizado podrá solicitar recuperar esos datos en un formato que le permita su traslado a otro responsable. Requisitos:

- El tratamiento debe estar basado en el consentimiento del interesado o cuando el mismo sea necesario para la ejecución de un contrato.

- Se debe estar realizando a través de medios automatizados.

- La transmisión de los datos se efectuará cuando sea técnicamente posible por los responsables.

- Que el ejercicio del derecho por parte del interesado no afecte o pueda afectar negativamente a los derechos y libertades de otros.

- No podrá por su propia naturaleza ejercerse en contra de responsables que traten datos personales en el ejercicio de sus funciones públicas.

- Y no debe aplicarse, cuando el tratamiento de los datos personales sea necesario para cumplir una obligación legal aplicable al responsable o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable.

Se establece la obligación para el responsable del tratamiento de proporcionar medios para que las solicitudes de ejercicio de derechos se presenten por medios electrónicos, en particular cuando los datos personales se hayan recabado a través de estos medios (Considerando 59).

5. Acción sindical y derecho de los trabajadores a la protección de datos.

5.1. 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 la 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).

5.2. 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 2ªenvío 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 con-

junta 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.

5.3. 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.

5.4. Publicación de datos personales de trabajadores.

Como ya sabemos, la LOLS reconoce 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.

■ 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.

5.5. Acceso a datos por los Comités de Empresa.

El Estatuto de los Trabajadores atribuye un amplio haz de facultades a los representantes sindicales y en particular al comité de empresa. En algunos casos el ejercicio de estas facultades puede comportar el acceso a datos. No obstante este acceso potencial a datos personales debe estar regido por el cumplimiento estricto de los principios de protección de datos.

■ Únicamente podrán cederse datos en aquellos casos en los que resulte estrictamente necesario para el cumplimiento de los deberes que el Estatuto de los Trabajadores establece para la empresa.

■ Los destinatarios de la información serán los previstos por la norma que habiliten para la cesión.

■ El comité de empresa o los representantes sindicales que acceden a información de los trabajadores están obligados a guardar secreto y al cumplimiento de los principios de la LOPD y de los específicamente previstos en las normas que les sean de aplicación.

5.6. Cesión de datos a sindicatos.

La cesión de datos más común a las organizaciones sindicales es la relativa al cobro de la cuota sindical en el pago de la nómina. El tratamiento de estos datos requiere la adopción de procedimientos por parte de la organización ya que se trata de proteger información particularmente sensible. Para ello hay que tener en cuenta lo visto anteriormente y, en concreto, las siguientes consideraciones:

- Tener un procedimiento adecuado de captación del consentimiento.

- Limitar el uso de los datos a la finalidad prevista.

- Se recabarán los datos estrictamente necesarios.

- El sindicato debe cumplir con todas las obligaciones vistas en los puntos anteriores como responsable de la información.

- Previsión del derecho de oposición salvo que haya elecciones sindicales.

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.