3 PROTECCIÓN DE DATOS

Hoy en día, es raro que al llegar a una empresa o solicitar un servicio no nos exijan la cumplimentación de un formulario. Dependiendo del fin del mismo, es posible que pidan datos más o menos sensibles (como, por ejemplo, qué religión profesamos o algún dato de nuestro historial médico). Al facilitar todos estos datos personales por cualquier medio damos lugar a que puedan caer en manos de personas no autorizadas que hagan un uso indebido de ellos.

3.1. Normativa sobre protección de datos

A diario, es frecuente que nos soliciten datos personales para hacar trámites en empresas y organismos públicos y privados (como cuando contratamos un nuevo proveedor de servicios de internet). En ese momento, nuestro nombre, apellidos y dirección, además de otros datos, pasan a formar parte de unos ficheros que son propiedad de la empresa que nos ha suministrado el servicio, pero su gestión debe estar en todo momento autorizada por la persona a la que realmente le pertenecen los datos.

La **Constitución española** ya contempla en su artículo **18.4** (relacionado con la protección de datos) que: "la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".

No obstante, es importante conocer la normativa que se aplica en materia de protección de datos de carácter personal. Para ello, hay que estar familiarizado con el **Reglamento General de Protección de Datos** (**RGPD**), de 25 de mayo de 2016 (con entrada en vigor el 25 de mayo de 2018). Este reglamento se aprobó en el Parlamento y en el Consejo Europeo con el fin de unificar la legislación en materia de protección de datos dentro de la Unión Europea, y desde su publicación en 2016 las empresas han tenido dos años para ir adaptándose a la nueva norma. En España, su cumplimiento está supervisado por la **Agencia Española de Protección de Datos**.

¡RECUERDA!

El objetivo del RGPD es **garantizar y proteger los derechos fundamentales** y la intimidad de las personas físicas en relación con sus datos personales.

Es importante conocer la normativa de protección de datos, tanto desde el punto de vista de técnicos en sistemas microinformáticos y redes, como también desde el de particulares, pues nuestros datos están almacenados en ficheros que deben adaptarse a esta ley.

3.2. Mecanismos de control de acceso a información personal almacenada

Las instalaciones donde se localizan los sistemas que contienen los ficheros de carácter personal (automatizados o no) deben tener una protección especial para asegurar la integridad, confidencialidad y disponibilidad de los datos. Especialmente si existe en nuestros sistemas, datos altamente sensibles y ubicado en un recinto al que acceda personal, tanto interno como externo, no involucrado en el tratamiento del mismo.

Para gestionar la seguridad de los edificios del sistema, podemos **definir el registro tanto de entrada como de salida** de aquellas personas que quieran acceder al mismo. Este se hará en la entrada, si es posible, por el personal de seguridad, el cual estará encargado de recoger distinta información de las personas ajenas a la empresa, como su documento nacional de identidad, la finalidad de su visita y la fecha y hora (tanto de entrada como de salida). Estos datos se transcriben por escrito, pero no se incorporan a fichero alguno a menos que se ocasione alguna incidencia mayor. Asimismo, se guardan por estrictas razones de seguridad durante una semana, pero al cabo de ese tiempo son eliminados mediante su destrucción física. Seguidamente, el responsable del registro concede el acceso mediante contacto telefónico.

Por otra parte, **cuando se trata de un nuevo empleado**, a este **se le suministra un código provisional**, junto con el nombre de su responsable. También se le facilita un documento con las medidas de seguridad para tener en cuenta.

Cuando se trata de entrar a salas con un acceso más restringido (salas de servidores o de seguridad), los controles pueden gestionarse mediante **claves**, **tarjetas identificativas o exámenes basados en algún rasgo físico del empleado**, de forma que quede inaccesible para cualquier persona no autorizada.

Debemos entender que, si alguna persona no autorizada accede a las salas en algún momento, este hecho debe quedar recogido en el registro correspondiente. Las consecuencias (de haberlas) serán responsabilidad de la persona encargada de la seguridad del sistema. Suele ser algo ocasional y, en cualquier caso, debe estar siempre justificado por razón del encargo, empleo o actividad.

Por otro lado, el personal a cargo de los ficheros tiene que asegurar en todo momento que la información almacenada en el sistema no pueda ser vista o tratada por personas no autorizadas. Una vez finalizada la jornada laboral, el responsable del servicio debe cerrar el archivador y verificar que ningún archivo no automatizado queda fuera del mismo.

Algo más común que el robo de información son los documentos olvidados en las impresoras. Para evitar que esto suceda, es recomendable que los usuarios retiren los papeles según van saliendo de la máquina y se aseguren de no dejarlos por medio. La supervisión de los impresos y la limpieza del material no informatizado de la oficina también es una tarea del responsable de la seguridad.

3.3. Datos personales. Tratamiento y mantenimiento de ficheros de datos

Datos personales

Según el artículo 4 del RGPD, los datos personales corresponden a toda la información referente a una persona física viva identificada o identificable.

La información referente a datos personales (nombre, DNI, sexo), circunstancias sociales y personales (estado civil, religioso), datos sanitarios (alergias, historial médico), datos profesionales (titulación académica) o datos comerciales o económicos (solvencia económica) son los datos que deben ser protegidos ante las autoridades.

El objetivo de la normativa es asegurar el método, la seguridad y el control que tienen las empresas de tratar los datos.

¡RECUERDA!

No todos los datos están protegidos por el RGPD: los personales sí, mientras que aquellos relativos a empresas o personas jurídicas no entran dentro de este ámbito.

Elementos personales del tratamiento

Los elementos que intervienen en el tratamiento de los datos son:

- **Afectado**: es la persona propietaria de los datos que se deben almacenar.
- **Responsable del fichero**: es la persona que decide el tratamiento y la finalidad de los archivos propiedad de la empresa.
- **Encargado del tratamiento**: es la persona responsable de todo el proceso de tratamiento de los datos. No tiene capacidad para decidir las razones del proceso, solo lo lleva a cabo.
- **Cesionario**: persona a la que se le ceden los datos del afectado.
- **Tercero**: persona con autorización del responsable para poder tratar los datos del afectado.

Tratamiento de los datos

CONCEPTO

El tratamiento de los datos es el **conjunto de las operaciones y procedimientos** para recoger, tratar, modificar y eliminar los datos suministrados por las personas, así como las cesiones que se hacen de ellos a terceros.

Los ficheros con material clasificado (investigaciones sobre acciones terroristas o delincuentes peligrosos) están sometidos a otras medidas más regladas y seguras.

Las personas cuyos datos sean facilitados a cualquier empresa para su tratamiento tienen los siguientes derechos:

- Los datos requieren el **consentimiento** de la persona afectada y este puede ser revocado mediante un procedimiento regulado.
- Cada individuo tiene derecho a solicitar el **acceso a los datos personales** (artículo 15). Además, en el RGPD se incorpora el derecho a recibir **información clara y comprensible** (artículos 12 a 14).
- Derecho a rectificar o eliminar los datos (derecho de **supresión**, artículo 17).
- Las personas afectadas pueden ser indemnizadas por el incumplimiento de la ley por parte del responsable o encargado del tratamiento.
- En el RGPD se incorpora la **necesidad de que exista una declaración del interesado o una acción positiva en la que se manifieste su conformidad** (no es válido el silencio o las casillas previamente marcadas).

¡RECUERDA!

En el RGPD se reconoce la necesidad de que el individuo realice una **acción positiva por la que muestre su conformidad**. Deja de ser válida, como prueba de consentimiento, una casilla ya marcada o la inacción del individuo.

En caso de las empresas que prestan el servicio y que necesitan de los datos personales de sus clientes, proveedores y trabajadores, existen varias formas para recogerlos:

- A través del **propio interesado**: rellenando una solicitud, escribiendo un correo electrónico o mediante una grabación telefónica.
- A través de una **cesión de datos** por parte de terceros.
- De **bancos públicos** de datos.

La RGPD **obliga a las empresas a informar al usuario a la hora de recabar los datos**. En dicha información previa anunciará que existe un fichero donde se almacenan todos los datos, así como la finalidad del mismo. Además, debe exponer el nombre de la persona responsable del tratamiento e informar de los derechos del afectado de cara al acceso, rectificación, cancelación y negación del uso de sus datos por parte de la empresa y sus correspondientes consecuencias a la hora no poder utilizar dichos datos.

Existen **algunos datos personales** (determinados por la normativa como datos especialmente sensibles) que requieren una **protección especial**, debido a su origen o a los valores que representan. Son aquellos que revelan la **ideología** del individuo, su **afiliación sindical**, su **religión** o sus **creencias**, y solo pueden solicitarse por escrito y con el consentimiento del usuario. Además, en la RGPD se incluyen como categorías especiales los datos genéticos y los datos biométricos.

Por otra parte, los datos que hacen referencia a la **salud personal**, la **raza** o la **vida sexual** solo podrán ser recopilados, tratados y cedidos cuando lo disponga la ley y por consentimiento del usuario.

Por último, la información relativa a las **infracciones penales y administrativas** solo puede almacenarse en los ficheros de tratamiento de las administraciones públicas competentes en el área.

Una vez vistos los datos personales a recoger, su posterior tratamiento, los datos más sensibles y los derechos del usuario, vamos a detallar la **conservación de estos datos**.

A este respecto, el responsable de los ficheros tiene un papel especial, ya que es el encargado de adoptar las medidas necesarias que asegurar la integridad y autenticidad de los mismos y de evitar que los datos se usen para otra finalidad distinta a aquella para la que fueron recogidos.

Nivel de protección de los datos

El **RGPD** llega con cambios importantes en relación con las medidas de seguridad de los datos. En él no encontramos ningún catálogo que nos indique las medidas para garantizar una adecuada seguridad.

BUSCA EN LA WEB

Puedes consultar la guía de la AEPD en el siguiente enlace:

https://bit.ly/3sXDclR

En su **artículo 32** expone:

"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**".

Como puede observarse, la norma actual se centra en los riesgos, pero no refiere de forma clara cómo garantizar una adecuada seguridad en función de los mismos. Por ello, la Agencia Española de Protección de Datos (AEPD) ha publicado una guía bastante completa con la que poder analizarlos. En ella se explica en profundidad la necesidad de realizar un análisis de los riesgos y de establecer medidas de control y seguridad para que se garanticen todos los derechos y libertades del individuo.

3.4. Legislación sobre los servicios de la sociedad de la información, comercio y correo electrónico

Desde su origen, internet es una **mina de interminables recursos** que se producen a diario en toda la red. Es tal la cantidad de datos producidos en un momento que existen verdaderas redes de traficantes de información.

Debido a la sensibilidad de los datos que nosotros mismos producimos de forma gratuita y con fines lúdicos (como cuando colgamos una foto nuestra en alguna red social) deben existir unas medidas de seguridad que velen por ellos para que no caigan en manos de terceros no autorizados.

Los riesgos aparecidos por la generalización del uso de internet han crecido, ya que la información se traslada de forma más rápida y llega a más lugares. Las administraciones no tienen tiempo de controlar y regir todo aquello que internet toca y, por tanto, algunas empresas aprovechan este vacío legal. Por ello, la seguridad en la red y en los propios sistemas se ha convertido en un aspecto de vital importancia.

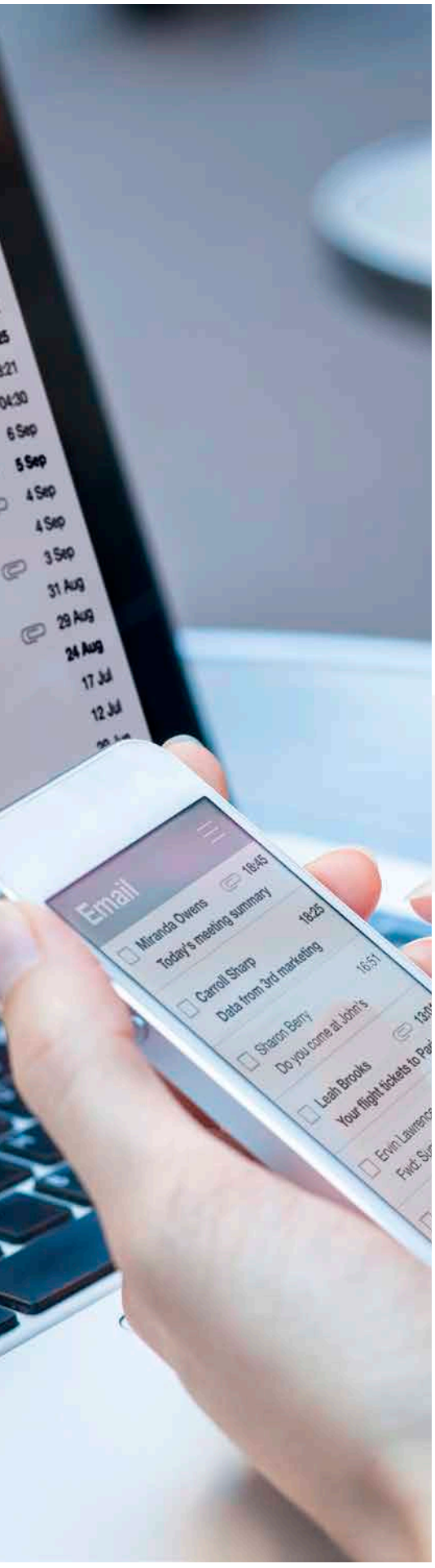
La regulación en la transmisión de los sistemas de información es un tema muy extenso, complejo y cada vez más difícil de regular debido al avance tan rápido de las tecno-

logías. Tanto es así que existe un organismo denominado **Comisión del Mercado de las Telecomunicaciones** (CMT) que establece las normas y los procedimientos a seguir por los mercados en relación con las comunicaciones electrónicas y los servicios audiovisuales.

En este contexto aparece la **ley 34/2002 de Servicios de la Sociedad de la Información y de Comercio Electrónico** (LSSICE), por la que se adaptan las transacciones comerciales de empresas o particulares a las nuevas formas surgidas con internet. Esta ley **regula el régimen jurídico** de los servicios de la sociedad de la información y la contratación por vía electrónica en las empresas que ofrecen estos servicios establecidos en España o en Estados miembros de la Unión Europea.

Algunos de los aspectos más importantes de esta ley son:

- Las **empresas** están **obligadas** o aportar información sobre el nombre, el domicilio, la dirección de correo electrónico, el número de identificación fiscal y el precio de los productos. Con que aparezca en la página web, la empresa ya estará cumpliendo con este requisito. Los datos del Registro Mercantil u otros registros de relativa importancia para los clientes como número de colegiado (abogado o médicos).
- **Exime de responsabilidad** a empresas que se dedican al alojamiento o almacenamiento de datos o enlaces a datos incluidos por clientes, pero únicamente si estas no tienen un conocimiento efectivo de la información que sus servidores contienen.
- En relación con los **contratos**, sus condiciones deben mostrarse antes de empezar con el procedimiento. La información debe visualizarse de forma gratuita, clara y fácilmente comprensible, lo que establece la validez de aquellos que por vía electrónica. Para demostrar jurídicamente que el contrato existe, basta con presentarlo en formato electrónico (como los billetes de avión o las entradas de cine compradas por internet).
- Los **alojamientos de la información** en servidores propios o contratados, el suministro de la información o la contratación de servicios mediante la vía electrónica son algunos de los servicios mencionados en dicha ley y que son facilitados por el proveedor del servicio de internet, portales o motores de búsqueda.
- Los **mecanismos de protección** que utiliza la empresa tienen que ser conocidos por el usuario en todo momento (programas antivirus, antiespías y *antispam*), así como las herramientas existentes para la restricción del acceso al sistema.
- En las comunicaciones realizadas de forma digital se deben **identificar** claramente los datos del anunciante, así como las condiciones y requisitos para adquirir el producto. Se hará también si se trata de algún tipo de oferta o publicidad.



3.5. Configuración de programas clientes de correo electrónico para el cumplimiento de normas sobre gestión de seguridad de la información

La empresa debe avisar al afectado de todo lo que conlleva la **cumplimentación** de cualquier **solicitud**. El reglamento promueve que se usen mecanismos de certificación (ya sean certificados, sellos o marcas).

Es frecuente que se realicen comunicaciones mediante el **correo electrónico**, a través del cual se informa al usuario del proceso de tratamiento de sus datos, los medios por los que puede oponerse a él y modificar o eliminar cualquier tipo de dato suministrado en algún momento. Normalmente, en la cláusula que acompaña al cuerpo de cualquier correo electrónico se indica la dirección postal donde pueden remitir dichas notificaciones de oposición y el nombre, junto con los datos del responsable del proceso. Como será necesario indicar esto en todos los correos que enviemos, podemos configurar nuestra herramienta introduciendo una firma con el mensaje de información al usuario desde el gestor de correos de la empresa (al cual se entra desde las opciones de configuración del apartado de mensajes).

3.6. Actualizaciones de seguridad del sistema

El **mantenimiento** y la **actualización** de los datos son tan importantes como la implantación, ya que un proceso de seguridad no actualizado es igualmente inseguro.

Los registros y listas con los afectados deben estar también al día, ya que cualquier individuo que ejerza sus derechos debe de quedar registrado en cuanto se le comunica.

Los afectados en el proceso de tratamiento pueden tener varios tipos de derechos:

- **Derecho de información**: derecho de la persona a saber quiénes tratan sus datos personales, con qué finalidad y de qué manera los tratan. Esta información se proporciona por **capas** o **niveles**: primero, se facilita una información básica y resumida; después, una adicional de forma detallada; y, por último, los datos que no han sido obtenidos directamente de nosotros.
- **Derecho de acceso**: derecho que tiene toda persona a obtener información sobre el tratamiento de sus datos personales. Esto incluye los tipos de datos personales

que se van a tratar y la finalidad de ese tratamiento, así como el plazo previsto durante el que van a conservarse los datos personales o los criterios utilizados para determinar este plazo.

- **Derecho de oposición**: derecho a oponerse a cualquier tratamiento en algunos supuestos.
- **Derecho de rectificación**: derecho que permite rectificar aquellos datos inexactos o incompletos.
- **Derecho de supresión**: derecho a eliminar los datos de carácter personal cuando concurran algunas circunstancias, como que ya no sean necesarios en relación con los fines para los que se recogieron.
- **Derecho a la limitación del tratamiento**: derecho a limitar los datos en algunos supuestos (como, por ejemplo, cuando se contradiga la exactitud de los datos personales mientras se verifica el hecho).
- **Derecho a la portabilidad**: derecho a que los datos personales se puedan recibir con un formato estructurado que permita transmitirlos a otro responsable cuando su tratamiento se realiza de forma automática. No obstante, hay algunos supuestos en los que este derecho no se aplica.

En caso de querer ejercer alguno de sus derechos como afectado, la persona debe contactar con el responsable del tratamiento de los mismos.

3.7. Legislación sobre licencias de uso de software

El 1 de julio del 2015 entró en vigor la reforma del Código Penal que afecta y endurece las penas sobre software legal y su indebido uso. Establece penas de prisión y el cese de la actividad para las empresas, ya que se considera falta grave el uso con fines comerciales de un software ilegal.

El objetivo de estas nuevas modificaciones es mejorar la protección de los derechos de la propiedad intelectual. Por mencionar un ejemplo, en el **artículo 197** se explica que:

"Será castigado con una pena de prisión de seis meses a dos años o multa de tres a dieciocho meses el que, sin estar debidamente autorizado, produzca, adquiera para su uso, importe o, de cualquier modo, facilite a terceros, con la intención de facilitar la comisión de alguno de los delitos a que se refieren los apartados 1 y 2 del artículo 197 o el artículo 197 bis:

a. Un programa informático, concebido o adaptado principalmente para cometer dichos delitos;

b. Una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información."

Además de hacer referencia a las empresas o particulares que utilizan programas sin su debida licencia, también menciona la reproducción, el plagio, la distribución y la facilitación del acceso a cualquier obra sin la autorización de los titulares de los derechos de la propiedad intelectual.
Por último, en estas modificaciones también se tipifican las sanciones contra estos delitos mencionados anteriormente.

3.8. Planes de entendimiento y de administración de seguridad

Como ya se ha mencionado, el hecho de poseer distintos datos puede ser un activo importante en la empresa. El correcto funcionamiento requiere la implementación de una serie de medidas que proporcionen un proceso seguro basado en la integridad, la confidencialidad y la disponibilidad.