NORMATIVAS DE CIBERSEGURIDAD

Unidad 3. Actividad 1

10 DE ABRIL DE 2023

CARLOS DÍAZ MONTES
ESPECIALIZACIÓN DE CIBERSEGURIDAD

Índice

Enunciado

La protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental protegido por el artículo 18.4 de la Constitución española. De esta manera, nuestra Constitución fue pionera en el reconocimiento del derecho fundamental a la protección de datos personales cuando dispuso 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». Se hacía así eco de los trabajos desarrollados desde finales de la década de 1960 en el Consejo de Europa y de las pocas disposiciones legales adoptadas en países de nuestro entorno.-

Informe de Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales

Título 1. Disposiciones generales.

- Objeto y ámbito de aplicación: Define el alcance de la ley, estableciendo que se aplica a los datos de carácter personal, así como a los derechos digitales reconocidos en la legislación.

- Principios de protección de datos: Establece los principios que deben regir el tratamiento de datos personales, como el principio de licitud, lealtad y transparencia en el tratamiento, el principio de minimización de datos, y el principio de exactitud y actualización de los datos.

- Legitimación para el tratamiento de datos: Define las bases legales que legitiman el tratamiento de datos personales, como el consentimiento del interesado, la ejecución de un contrato o el cumplimiento de obligaciones legales por parte del responsable del tratamiento.

- Derechos de los interesados: Enumera los derechos que asisten a las personas respecto al tratamiento de sus datos personales, como el derecho de acceso, rectificación, supresión, limitación del tratamiento, portabilidad de los datos, oposición y a no ser objeto de decisiones individuales automatizadas.

- Delegado de protección de datos: Establece la figura del Delegado de Protección de Datos (DPD) o Data Protection Officer (DPO), que es el responsable de velar por el cumplimiento de la normativa de protección de datos en una organización.

Título 2. Principios de protección de datos.

- Principio de licitud, lealtad y transparencia: Establece que el tratamiento de datos personales debe realizarse de manera lícita, leal y transparente para el interesado.

- Principio de limitación de la finalidad: Determina que los datos personales deben ser recogidos con fines específicos, explícitos y legítimos, y no pueden ser tratados de manera incompatible con dichos fines.

- Principio de minimización de datos: Señala que los datos personales deben ser adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.

- Principio de exactitud de los datos: Establece que los datos personales deben ser exactos y, si fuera necesario, actualizados, de manera que se garantice la adecuación de los mismos con respecto a los fines para los que fueron recogidos.

- Principio de limitación del plazo de conservación: Indica que los datos personales deben ser conservados de forma que se permita la identificación de los interesados durante el tiempo necesario para los fines del tratamiento.

- Principio de integridad y confidencialidad: Estipula que los datos personales deben ser tratados de tal manera que se garantice una seguridad adecuada, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental.

- Responsabilidad proactiva: Establece la obligación de los responsables del tratamiento de adoptar medidas técnicas y organizativas apropiadas para garantizar y demostrar que el tratamiento de datos personales se lleva a cabo de conformidad con la normativa aplicable.

Titulo 3. Derechos de las personas

- Transparencia e información al afectado: Cuando los datos personales sean obtenidos del afectado el responsable del tratamiento podrá dar cumplimiento al deber de información establecido en el artículo 13 del Reglamento (UE) 2016/679 facilitando al afectado la información básica a la que se refiere el apartado siguiente e indicándole una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información.

- Derecho de acceso: Las personas tienen derecho a obtener del responsable del tratamiento la confirmación de si se están tratando o no sus datos personales, así como a acceder a dichos datos y obtener información sobre el tratamiento realizado.

- Derecho de rectificación: Las personas tienen derecho a solicitar la rectificación de sus datos personales inexactos o incompletos sin demora indebida.

- Derecho de supresión (derecho al olvido): Las personas tienen derecho a solicitar la supresión de sus datos personales cuando estos ya no sean necesarios para los fines para los que fueron recogidos, entre otros motivos.

- Derecho de limitación del tratamiento: Las personas tienen derecho a solicitar la limitación del tratamiento de sus datos personales en ciertas circunstancias, como cuando impugnan la exactitud de los datos o el tratamiento es ilícito.

- Derecho a la portabilidad de los datos: Las personas tienen derecho a recibir sus datos personales en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento cuando sea técnicamente posible.

- Derecho de oposición: Las personas tienen derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular, al tratamiento de sus datos personales, salvo que existan motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, derechos y libertades del interesado.

Título 4. Disposiciones aplicables a tratamientos concretos.

- Tratamiento de datos en el ámbito laboral: Establece las condiciones para el tratamiento de datos personales de los trabajadores en el ámbito laboral, garantizando el respeto a su privacidad y derechos fundamentales.

- Tratamiento de datos en el ámbito de la videovigilancia: Regula el uso de sistemas de videovigilancia con el fin de proteger los derechos y libertades de las personas, estableciendo requisitos específicos para su instalación y uso.

- Tratamiento de datos en el ámbito de las relaciones entre operadores y clientes: Define las condiciones para el tratamiento de datos personales en el contexto de las relaciones entre operadores y clientes, asegurando el respeto a la privacidad y la protección de los derechos de los usuarios.

- Tratamiento de datos en el ámbito de las comunicaciones electrónicas: Regula el tratamiento de datos personales en el ámbito de las comunicaciones electrónicas, incluyendo aspectos como el consentimiento, la privacidad de las comunicaciones y la protección de la información de los usuarios.

- Tratamiento de datos en el ámbito de la salud: Establece las condiciones para el tratamiento de datos personales en el ámbito de la salud, garantizando la confidencialidad y seguridad de la información médica de los pacientes.

Título 5. Responsable y encargado del tratamiento.

- Responsabilidad del responsable del tratamiento: El responsable del tratamiento es la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento de datos personales

- Responsabilidad del encargado del tratamiento: El encargado del tratamiento es la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.

- Medidas de responsabilidad activa: Se establece la obligación tanto para el responsable como para el encargado del tratamiento de adoptar medidas de responsabilidad activa para garantizar el cumplimiento de la normativa de protección de datos.

- Registro de actividades de tratamiento: Se establece la obligación de llevar un registro de las actividades de tratamiento realizadas bajo su responsabilidad, que contenga información detallada sobre las operaciones de tratamiento realizadas y otras especificaciones requeridas por la ley.

- Encargado del tratamiento: El acceso por parte de un encargado de tratamiento a los datos personales que resulten necesarios para la prestación de un servicio al responsable no se considerará comunicación de datos siempre que se cumpla lo establecido en el Reglamento (UE) 2016/679, en la presente ley orgánica y en sus normas de desarrollo.

Título 6. Transferencias internacionales de datos.

- Requisitos para la transferencia internacional de datos: Este título establece que las transferencias internacionales de datos solo pueden realizarse si se cumplen ciertos requisitos específicos, como la existencia de una decisión de adecuación de la Comisión Europea respecto al país de destino, la aplicación de cláusulas tipo de protección de datos adoptadas por la Comisión, la existencia de garantías adecuadas a través de códigos de conducta o mecanismos de certificación, o la autorización de la autoridad de control competente.

- Cláusulas tipo de protección de datos: La ley contempla la posibilidad de utilizar cláusulas contractuales tipo adoptadas por la Comisión Europea para garantizar la protección de los datos personales transferidos fuera del EEE.

- Garantías adecuadas: Se reconocen otros mecanismos que puedan ofrecer garantías adecuadas para la protección de los datos personales transferidos, como códigos de conducta aprobados, certificaciones y sellos de protección de datos, así como mecanismos de cumplimiento vinculante y normas corporativas vinculantes.

- Transferencias internacionales basadas en decisiones de adecuación: Se menciona que la Comisión Europea puede adoptar decisiones de adecuación respecto a determinados países o territorios, estableciendo que proporcionan un nivel de protección adecuado para los datos personales transferidos desde la UE o el EEE hacia esos destinos.

- Autorización de la autoridad de control competente: En ausencia de una decisión de adecuación, cláusulas contractuales tipo u otros mecanismos reconocidos, las transferencias internacionales de datos pueden realizarse previa autorización de la autoridad de control competente en materia de protección de datos.

Título 7. Autoridades de protección de datos.

- Creación y funciones de las autoridades de protección de datos: Este título establece la creación de una autoridad de protección de datos en cada Estado miembro de la Unión Europea (UE), así como en cada comunidad autónoma en España.

- Independencia y recursos de las autoridades de protección de datos: Se establece la independencia de las autoridades de protección de datos para ejercer sus funciones de manera imparcial y sin interferencias.

- Cooperación entre autoridades de protección de datos: Se promueve la cooperación entre las autoridades de protección de datos de diferentes países, así como entre las autoridades de protección de datos y otras autoridades competentes, con el fin de garantizar una aplicación coherente y coordinada de la normativa de protección de datos en el ámbito de la Unión Europea.

- Funciones de la Agencia Española de Protección de Datos (AEPD): En el caso de España, se especifican las funciones de la Agencia Española de Protección de Datos (AEPD), la cual es la autoridad de protección de datos a nivel nacional.

Título 8. Procedimientos en caso de posible vulneración de la normativa de protección de datos.

- Notificación de violaciones de seguridad de datos: Este título establece la obligación de los responsables del tratamiento de datos de notificar a la autoridad de protección de datos competente las violaciones de seguridad de los datos personales en un plazo máximo de 72 horas después de haber tenido conocimiento de ellas, a menos que la violación no sea probable que suponga un riesgo para los derechos y libertades de las personas.

- Comunicación a los interesados sobre violaciones de seguridad de datos: Se establece la obligación de notificar a los interesados las violaciones de seguridad de los datos personales cuando estas supongan un alto riesgo para sus derechos y libertades, a menos que se hayan tomado medidas para mitigar el riesgo o la notificación requiera esfuerzos desproporcionados.

- Evaluación de impacto en la protección de datos: Se establece la obligación de llevar a cabo una evaluación de impacto en la protección de datos cuando el tratamiento de datos pueda suponer un alto riesgo para los derechos y libertades de las personas, especialmente cuando se utilicen nuevas tecnologías o se realicen tratamientos de datos a gran escala.

- Consulta previa: En determinados casos, se requiere que el responsable del tratamiento consulte a la autoridad de protección de datos antes de llevar a cabo un tratamiento de datos que pueda suponer un alto riesgo para los derechos y libertades de las personas, con el fin de obtener orientación sobre cómo llevar a cabo el tratamiento de manera conforme a la normativa de protección de datos.

- Cooperación con la autoridad de protección de datos: Se establece la obligación de cooperar con la autoridad de protección de datos durante la realización de investigaciones y la adopción de medidas correctivas en caso de posibles infracciones de la normativa de protección de datos.

Título 9. Régimen sancionador.

- Infracciones y sanciones: Se establecen tres niveles de infracciones, cada uno de los cuales conlleva diferentes sanciones:

a. Infracciones leves: Pueden ser sancionadas con multas de hasta 20 millones de euros o el 2% del volumen de negocio anual global del ejercicio financiero anterior, si este importe fuese superior.

b. Infracciones graves: Pueden ser sancionadas con multas de hasta 40 millones de euros o el 4% del volumen de negocio anual global del ejercicio financiero anterior, si este importe fuese superior.

c. Infracciones muy graves: Pueden ser sancionadas con multas de hasta 20 millones de euros o el 4% del volumen de negocio anual global del ejercicio financiero anterior, si este importe fuese superior.

- Criterios para la determinación de las sanciones: Se establecen una serie de criterios a tener en cuenta para la determinación de las sanciones, como la naturaleza, gravedad y duración de la infracción, el grado de responsabilidad del infractor, las medidas adoptadas para mitigar el daño causado, entre otros.

- Prescripción de las infracciones: Se establecen los plazos de prescripción para las infracciones, que varían en función de su gravedad: 2 años para las infracciones leves, 3 años para las infracciones graves y 4 años para las infracciones muy graves.

- Responsabilidad de las personas jurídicas: Se establece la responsabilidad de las personas jurídicas por las infracciones cometidas en su nombre o en su beneficio por sus representantes legales o empleados. Las sanciones pueden incluir multas, la prohibición temporal o definitiva de realizar tratamientos de datos, el cierre temporal de ficheros, entre otras.

- Procedimiento sancionador: Se establece el procedimiento para la imposición de sanciones, que incluye la instrucción del expediente sancionador, la audiencia al interesado, la resolución y notificación de la sanción, así como la interposición de recursos contra la misma.