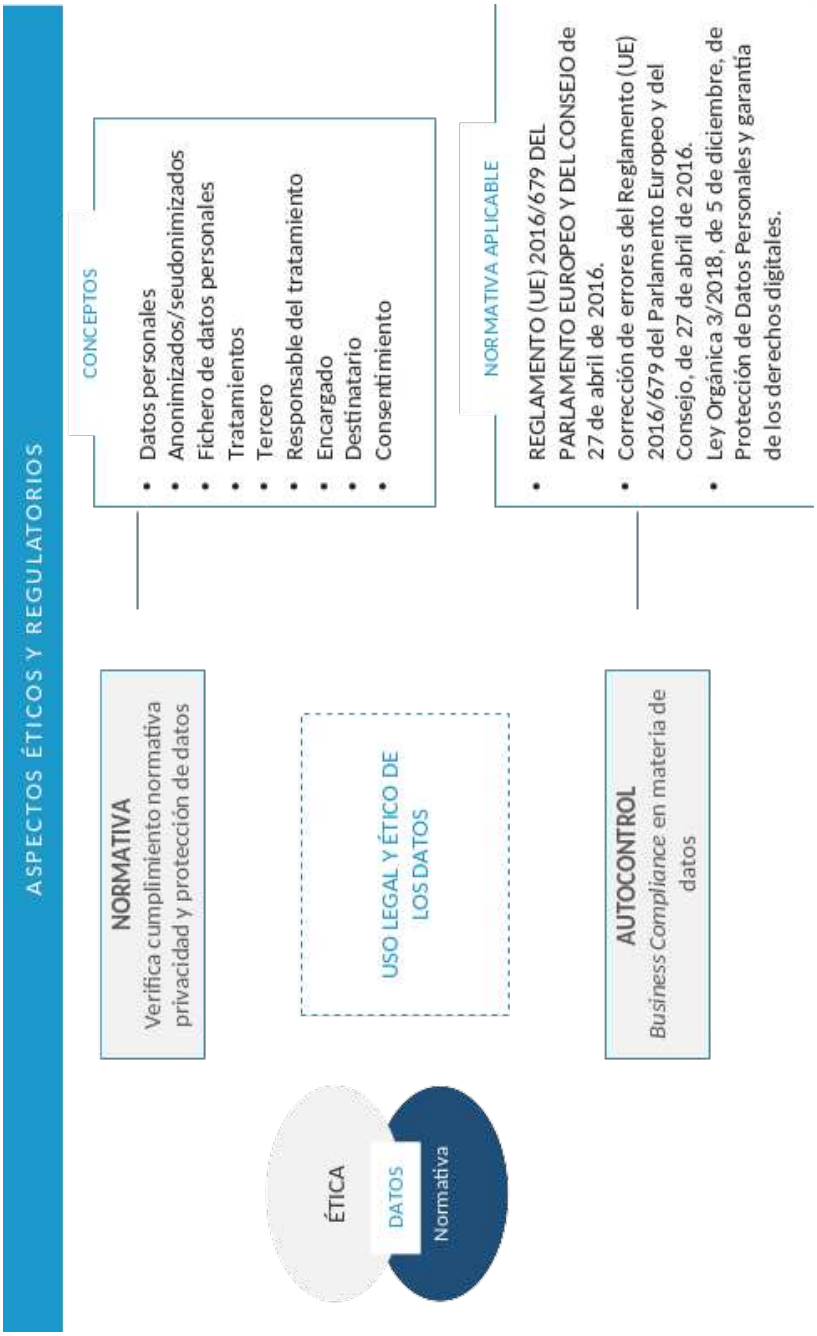
Estrategia y Gestión Empresarial Basada en Análisis de Datos

Tema 4. Aspectos éticos y regulatorios

Índice

Esquema



4.1. Introducción y objetivos

En este tema se trata de hacer una primera incursión en los **aspectos normativos y éticos** asociados al uso de los datos, identificando los límites y garantías que se han de tener presentes, así como la forma en la que la cultura de captura y uso de los datos debe irradiarse por todas las unidades de las organizaciones e identificando quienes son los responsables, en última instancia, de que se sigan los preceptos legales y ciertos códigos y protocolos éticos.

Se pretenden alcanzar los siguientes **objetivos**:

- Llevar a cabo una reflexión desde una perspectiva ética sobre la utilización de datos en las empresas.
- Conocer los principios legales de la protección de datos.
- Identificar la normativa aplicable.
- Reflexionar acerca de la privacidad de los ciudadanos y la utilización del *big data*.
- Reconocer la responsabilidad y el autocontrol normativo de las actividades empresariales.

4.2. La ética de los datos

El correcto uso de los datos nos lleva no solo a establecer una serie de protocolos con los que garantizar el cumplimiento de la ley (***business compliance***), sino también a tener en cuenta un buen número de dilemas morales y de códigos éticos y de buena conducta.

Junto a los retos que plantea la captura y el uso de los datos, desde el punto de vista ético, que serán analizados a lo largo de esta sección y la siguiente, no menos importante es el discernir quiénes han de ser los encargados de afrontar, delimitar y solucionar todos los dilemas éticos asociados a la captura, transferencia y uso de la información.

Nos referimos aquí a si esta tarea debe ser una competencia exclusiva de algún perfil profesional específico dentro de la empresa, por ejemplo, que sea el *chief digital officer* (en adelante, CDO) el responsable en última instancia de todos los aspectos legales y éticos asociados al uso de los datos y al análisis masivo de los mismos o si, por el contrario, en un mundo en el que todas las empresas aspiran a ser *data-driven*, en un intento de alcanzar los niveles de eficiencia necesarios para la supervivencia empresarial, la ética del dato debe ser una responsabilidad de toda la compañía que afecte de manera transversal a todos sus estamentos puesto que todos ellos, de una u otra forma, participan de la gestión basada en datos.

En este tema, tratamos de hacer al estudiante consciente de un buen número de **retos ético-sociales** a los que toda empresa *data-driven* ha de enfrentarse y en los que, de una u otra forma, han de participar las diferentes áreas funcionales de la empresa.

De la ética del dato a los retos éticos de la inteligencia artificial

Hasta hace relativamente poco tiempo, las cuestiones éticas, relativas al uso de los

datos, se centraban en hacer un uso adecuado de los mismos, lo que básicamente se resumía en solicitar de clientes, proveedores o personal, solo la información necesaria para el objetivo que pretendíamos asegurándonos de que estos habían entendido el objetivo con el que cedían el dato y las limitaciones y alcance de ese uso.

Como veremos a lo largo del tema, la normativa en este punto se ha convertido en muy estricta, lo que va a favorecer que, en ausencia de un adecuado código ético, sea la ley la que haga que las empresas hagan especial observancia de estas limitaciones de uso ante el temor de sanciones severas.

Sin embargo, todas las cuestiones éticas tradicionales, asociadas al uso de los datos, están quedando obsoletas debido a la integración de la inteligencia artificial (IA) con el *big data*.

Muchas empresas pertenecientes a sectores muy diversos se han dado cuenta de que almacenar y procesar datos no es costoso y que, además, el uso analítico, prescriptivo y comercial de estos datos es un **nicho de mercado**, cuya operativa puede añadirse como otra línea de negocio más. En otras palabras, un buen número de empresas están haciéndose conscientes de que un gran volumen de datos es otro elemento patrimonial más, susceptible de ser monetizado y darle nuevos usos.

Ejemplos tradicionales lo constituyen las empresas de telecomunicaciones, las financieras o las plataformas digitales, entre otras. Todo ello implica no solo el conocer a los clientes y proveedores, o el mejorar la gestión a través de la gestión basada en datos, sino que también nos lleva a la tentación de segmentar y discriminar a nuestros clientes para extraer el máximo excedente posible, o a nuestros empleados, siendo conscientes de que, en ocasiones, el uso que se puede hacer de esta información es perjudicial para el que la cedió y no estando completamente seguros de que el cesionario de los datos es plenamente consciente del uso que se puede derivar del mismo o de su cesión a terceros.

Además de todo esto, en este contexto de gestión basada en datos, la aparición de la inteligencia artificial nos lleva de manera directa al desafío de dilucidara quién ha de ser asignada la responsabilidad ética en estos contextos y si los algoritmos que esta utiliza son justos, responsables, transparentes y éticos, más si tenemos en cuenta que, en ocasiones, estos servicios son externalizados y gestionados por consultoras y empresas de gestión de datos especializadas.

En este contexto, ¿es el CDO el que ha de ser el garante de la creación y observancia del código ético de la empresa en materia de datos? En este punto y, aunque la respuesta podría matizarse en función de la complejidad de la organización de la que se trate, podemos convenir que, a pesar de que el papel del CDO es el de abordar todas las cuestiones relativas a la extracción de valor de los datos y de que esta se haga correctamente y con garantías, no es menos cierto que no tiene que estar al frente de todo el ciclo de vida del dato.

Los efectos y retos de esta gestión basada en datos son transversales a todas las unidades organizativas de la empresa, de forma que los aspectos éticos han de ser abordados de manera colegiada por los responsables de todas estas unidades.

En cualquier caso, con independencia de la forma de abordar y gestionar de manera éticamente responsable los datos y sus soportes de gestión, un **marco de gestión ética** de los datos debe garantizar al menos los siguientes elementos:

- La privacidad.
- La no discriminación.
- La responsabilidad sobre los mismos y la no diseminación.
- Evitar hacer un uso inadecuado en el entorno laboral.

Cultura y ética

Aunque las diferencias legislativas en estas cuestiones ya han quedado de

manifiesto, hay que hacer notar que las diferentes culturas no dan el mismo tratamiento a los problemas morales.

Esta inexistencia de un marco ético globalizado o estándar para las diferentes culturas provoca que todo lo referente a la ética del dato se complique aún más, especialmente en un entorno en el que un buen número de empresas, especialmente las más integradas en la economía digital, son empresas que operan en un mundo global.

Como ya advertíamos antes, la existencia de normativas transnacionales facilita cómo afrontar un buen número de dilemas éticos, ya que estas reflejan, en cierta medida, la intersección de diferentes culturas en la forma de afrontar y resolver este tipo de dilemas.

4.3. Un marco de ayuda a la toma de decisiones éticamente responsables

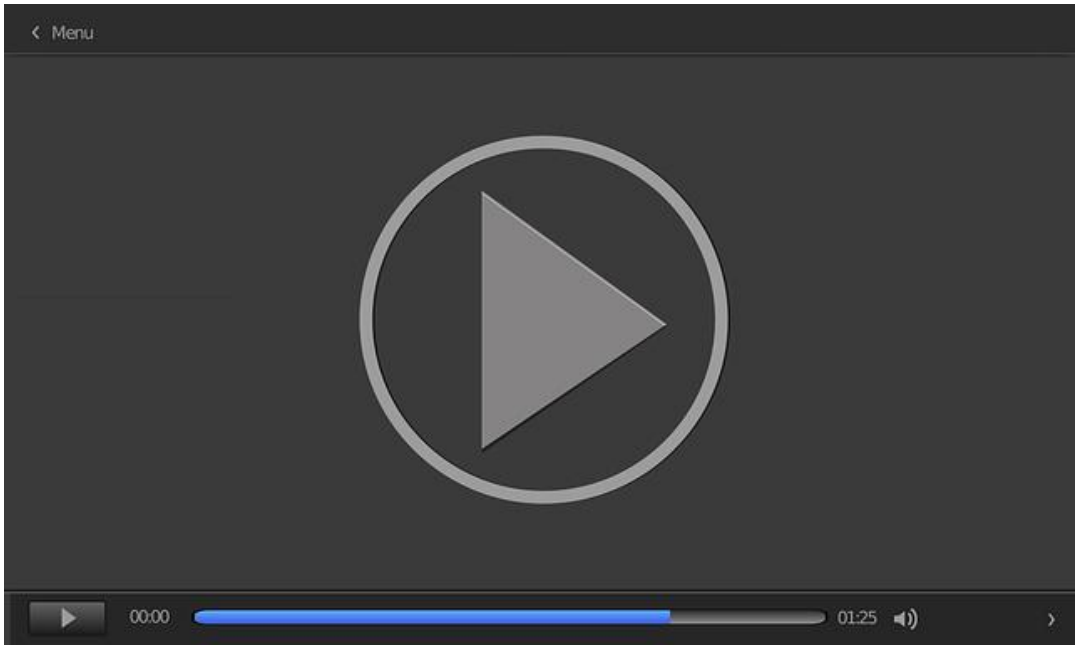
Se podrían plantear cientos de ejemplos en los que la cesión o el compartir datos nos plantearían no solo una serie de dilemas éticos, sino también su conveniencia para nuestra reputación o incluso si la petición de algún dato puede generar un efecto adverso por parte de clientes o proveedores.

Así, una empresa financiera está tentada de utilizar todo el historial financiero de que dispone para hacer *clusters* de clientes a los que asociar un cierto nivel de riesgo, en función del cual segmentar y realizar discriminación de precios en sus diferentes ofertas de financiación, u ofrecer de manera automática refinanciación y cambio de condiciones, cuando este cliente se separe de su centroide inicial para incorporarse a otro segmento de consumidores.

Compartir datos de velocidad o de salud con compañías aseguradoras, emitir mensajes que denoten que se conoce el tipo de consumo que ha hecho el cliente o determinada información de redes sociales puede resultar invasivo y en algunos casos plantear serios problemas éticos.

El desarrollo de métodos de decisión sobre ética de datos, basados en el riesgo en términos de reputación que estemos dispuestos a asumir en comparación a los beneficios asociados al mismo, requieren de una estrategia muy reflexionada, y quizás consensuada en diferentes estamentos de la organización.

4.4. Aspectos legales: conceptos previos



Accede al vídeo:

https://unir.cloud.panopto.eu/Panopto/Pages/Embed.aspx?id=11d6ab16-90fa-4ce6-91d4-b15d008027f8

El trabajar con datos requiere la observancia de ciertos preceptos legales que han de tenerse en cuenta y respetarse de manera integral por las diferentes unidades funcionales de la empresa, así como con carácter general por parte de la organización de manera global.

El hablar de estos temas es relativamente reciente, dado que, a diferencia de las obligaciones fiscales, mercantiles o de tipo laboral, esta legislación es mucho más reciente y, sobre todo, porque la falta de praxis en el trabajo con datos para muchas organizaciones hace que carezcan de una «cultura» de lo legalmente exigible en términos de las obligaciones, derechos y límites en lo relativo a la captura y uso de los datos.

Por ello, dedicaremos esta sección y la siguiente a repasar de manera somera ciertos aspectos regulatorios y la normativa aplicable, comenzando para ello con una breve clasificación acerca de los **tipos de datos** con los que las empresas e instituciones trabajan en su día a día, los tipos de ficheros y los responsables legales de la gestión de estos.

Tipos de datos

Datos de carácter personal y datos anonimizados

Los datos de carácter personal son todos aquellos datos e informaciones que puedan ser asociados a una persona física viva, ya sea directa o indirectamente, lo que la transforma en identificable. Frente a estos, los datos adquieren el carácter de datos anonimizados si han sido transformados de forma que la persona no se pueda identificar, y esta transformación tiene carácter irreversible.

Datos personales y datos seudonimizados

Por el contrario, tanto aquellos datos que se asocian de manera inequívoca a una persona y permiten identificarla (*person-related data*) como aquellos que, en compañía de otros, permiten de manera indirecta identificar a una persona (datos seudonimizados), sí tendrán el carácter de datos personales.

Fichero de datos personales

Los ficheros son los conjuntos de datos organizados que contienen datos de carácter personal, con independencia de la forma de almacenamiento, organización o acceso.

Tratamiento

El artículo 4 del apartado 2 del Reglamento General de Protección de Datos define el tratamiento como toda aquella operación que se realice sobre un fichero de datos personales, ya se trate de la captura, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización,

comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

Agentes

Para concluir con esta tipología o digresión terminológica, centrémonos ahora en las partes (agentes) que intervienen en este proceso:

Tercero

La persona física o jurídica, autoridad pública, servicio o cualquier otro organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable o del encargado del tratamiento.

Responsable del tratamiento

La persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que solo o conjuntamente con otros determine los fines y los medios del tratamiento de datos personales.

Encargado de tratamiento

Persona física o jurídica, autoridad, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento.

Destinatario

Se define como la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que reciba comunicación de datos, se trate o no de un tercero.

Finalmente, el denominado **consentimiento del interesado** hace referencia a toda manifestación mediante la cual el interesado consienta el tratamiento de sus datos personales.

4.5. Normativa aplicable

España, la **Constitución española de 1978** fue pionera en la protección de datos personales al reconocer su protección en su **artículo 18.4** que dispone 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».

Durante años, la aplicación de la **normativa europea** (Directiva 95/46/CE) dio soporte legal a todo lo relativo a la protección general de datos. Sin embargo, esta normativa había quedado obsoleta con la aparición de los avances en el campo de las tecnologías de la información.

En un mundo en el que los datos personales se han transformado en un activo y recurso fundamental de la sociedad de la información, surge la necesidad de:

- Incorporar los nuevos conceptos y elementos tales como el análisis masivo de datos o la inteligencia artificial.
- Regular los riesgos y oportunidades que nos ofrecen las redes para poder ejercer nuestros derechos fundamentales también en la realidad digital
- Armonizar legislaciones para atender las nuevas circunstancias marcadas por los flujos transfronterizos de datos personales.

Todo esto provocó la necesidad de adaptar la normativa al nuevo entorno. Fruto de este esfuerzo legislativo es la implantación del **Reglamento Europeo de Protección de Datos de 25 de mayo de 2018** (en adelante, RGPD).

La nueva normativa europea en vigor desde el 25 de mayo de 2018 fue aprobada en 2016 (Reglamento UE 2016/679 del Parlamento Europeo y del Consejo de27 de abril de 2016) y entra en la regulación de la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos

derogando la Directiva 95/46/CE (Reglamento General de Protección de Datos), que entró en vigor en mayo de 2016, pero con un período transitorio de dos años.

En general, el RGPD mantiene, reformula y desarrolla los **principios sobre protección de datos** ya incorporados en normativas anteriores. Los más importantes son:

- Prohibición salvo autorización: este principio significa que a priori se prohíbe cualquier procesamiento de datos personales a no ser que esté permitido.

- Limitación de la finalidad o principio de pertinencia: las empresas u organismos solo podrán recopilar y editar datos con unos objetivos específicos. Para ello, al empezar a recogerlos deben formularse los objetivos y documentarse el uso futuro de los datos. Los datos que se han recopilado para un fin no pueden ser usados para otro. Si se pretende cambiar la finalidad se necesita una justificación por separado y solo se permiten las modificaciones posteriores de los objetivos bajo determinadas circunstancias.

- Minimización de datos: el principio de la minimización de datos exige que las empresas recopilen la menor cantidad de datos posible. Esto choca con el llamado data enrichment. Así, no se puede recopilar más de lo requerido para conseguir el objetivo previsto con la obtención de datos.

- Transparencia: el tratamiento de los datos debe ser comprensible para los interesados, con avisos explícitos de privacidad, y comunicar bajo petición cuáles son los datos existentes y cómo se van a utilizar.

- Confidencialidad: las empresas tienen la obligación de proteger los datos personales de sus clientes de forma técnica y organizativa, ya sea del tratamiento o modificación no autorizados, del robo o de la destrucción de dichos datos y con la obligación de aplicar medidas técnicas de protección.

- Principio del derecho al olvido: los datos serán conservados durante un tiempo no superior al necesario para los fines para los que fueron recogidos.

Obligación de realizar un registro de actividades del tratamiento

En el RGPD se establece como primera obligación del empresario la elaboración de un registro de actividades del tratamiento en el que debe indicarse:

- Datos que se recogen.
- Finalidad.
- Medidas de seguridad.
- Nivel de seguridad.
- Tipo de fichero (manual, mixto o automatizado).
- Si estos datos van a ser cedidos o transferidos fuera del espacio económico europeo.

El objetivo es que el ciudadano pueda conocer de la forma más exacta posible qué se está realizando con sus datos de carácter personal y cómo y dónde puede ejercer sus derechos.

En clave nacional, la aprobación de **la Ley Orgánica 3/2018 de 5 de diciembre** supone la adaptación de la normativa española al Reglamento Europeo de Protección de Datos.

4.6. Business compliance en materia de datos

Como ya hemos advertido, el *compliance* o sistema de garantía de cumplimiento normativo que evite o minimice el riesgo de incurrir en sanciones o responsabilidades civiles o penales es especialmente importante en materia de datos, debido al elevado grado de desconocimiento sobre la materia y a la falta de una alfabetización o cultura del dato en los diferentes estratos de la empresa.

E l *compliance* consiste en el establecimiento de un conjunto de procedimientos adoptados por las empresas para **identificar los riesgos operativos y legales** derivados de las actividades de la empresa y establece un sistema de buenas prácticas y obligaciones que han de conocerse y seguirse en las organizaciones para minimizar estos riesgos.

El desarrollo de una **estrategia** de *business compliance* requiere identificar y clasificar los riesgos legales en los que se puede incurrir con la operativa de la empresa y, a partir de este conocimiento, establecer una serie de protocolos de gestión, detección y reacción, que permitan prevenir el riesgo de incumplimiento.

El modelo de protección de datos contemplado en el RGPD y en la Ley Orgánica recoge similitudes con las técnicas de *compliance*, ya que convierte el modelo de gestión y protección de los datos personales en un modelo de autogestión proactivo, en el que la empresa ha de preservar la norma e inscribir ficheros ante la autoridad de control.

Es decir, el responsable, como máximo garante del cumplimiento normativo del modelo de protección de datos, tiene que asegurar el cumplimiento y acreditar de qué forma su modelo de protección se acomoda al marco legal.

Ideas clave

La forma básica de demostrar esta adecuación lo constituye el llamado Registro de Actividades de Tratamiento, al que se añaden el análisis de riesgo y las evaluaciones de impacto asociadas a los tratamientos de datos.

La normativa completa este **sistema de garantías de cumplimiento** normativo con configuración de los sistemas de información de denuncias internas y por la promoción de códigos de conducta o estándares de actuación en materia de promoción de datos, que han de ser aprobados por la Agencia Española de Protección de Datos o por la autoridad autonómica competente en materia de protección de datos, e incluso contempla la configuración de mecanismos de certificación que acrediten el cumplimiento.

Finalmente, la normativa establece una figura: el llamado **delegado de protección de datos**, con cometido parecido al del *compliance officer* que actúa como órgano de supervisión y de respuesta ante reclamaciones, pero con estatuto legal reconocido.

El CDO, como principal responsable del diseño de la estrategia de gestión basada en datos, ha de jugar un papel protagonista en establecer una cierta pedagogía o cultura del uso responsable (ético y legal del dato), más aún cuando muchas de estas actuaciones ligadas al uso de los datos están gestionados por algoritmos que para muchas unidades de la empresa son una especie de caja negra.

En esos casos, se ha de establecer protocolos que garanticen que los modelos no generen resultados éticamente reprobables ni discriminatorios, para lo cual establecer un protocolo ético que deben respetar nuestros modelos y la experimentación (el entrenamiento con datos reales, pero sin ponerlos en práctica) para comprobar que se cumple con esos parámetros del protocolo acotados. Esto podría hacerse proporcionándoles una muestra real, pero sin llevar el resultado a producción.

Ideas clave

4.7. Referencias bibliográficas

Constitución Española. *Boletín Oficial del Estado*, núm. 311, de 29 de diciembre de 1978.

España. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. *Boletín Oficial del Estado*, núm. 294, de 6 de diciembre de 2018.

Unión Europea. Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respeta al tratamiento de datos personales y a la libre circulación de estos datos [Disposición derogada]. *DOCE*, núm. 281, de 23 de noviembre de 1995.

Unión Europea. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). *Diario Oficial de la Unión Europea,* L119/1, 4 de mayo de 2016.

Sobre la normativa en materia de protección de datos

España. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. *Boletín Oficial del Estado*, núm. 294, de 6 de diciembre de 2018. Recuperado de https://www.boe.es/buscar/pdf/2018/BOE-A-2018-16673-consolidado.pdf

Normativa básica sobre protección de datos y garantías de derechos.

Agencia Española de Protección de Datos

Agencia Española de Protección de Datos. Página web oficial.

https://www.aepd.es/guias-y-herramientas/herramientas/facilita-rgpd

La Agencia Española de Protección de Datos dispone de una herramienta gratuita para ayudar a las empresas a cumplir con la protección de datos.

1. ¿Cuál de las siguientes situaciones constituye un dilema ético asociado a la gestión de datos?

A. Utilizar el historial de uso de la tarjeta de fidelización para segmentar a nuestros clientes y realizar prácticas de discriminación de precios.

B. Usar la información clínica de un cliente para establecer primas de seguros médicos.

C. Utilizar la información e historial de accidentes de los miembros de un hogar para la oferta de diferentes tipos de seguros.

D. Todas las anteriores son correctas.

2. En un mundo globalizado:

A. La multiculturalidad ha de ser tenida en cuenta para encontrar un marco ético compatible con las diversas culturas.

B. Hay que adaptar los protocolos éticos a la ética imperante en los países más avanzados.

C. Los dilemas éticos son resueltos de diferente forma en las diferentes culturas.

D. A y C son correctas.

3. El *business compliance*:

A. Es especialmente importante en empresas *data-driven* dada la responsabilidad que la ley ha dado a la empresa en todo lo relativo a protección de datos.

B. Ha de reducir el número de litigios.

C. Disminuye la probabilidad de incurrir en conductas sancionables.

D. Todas las anteriores son correctas.

4. El registro de las actividades del tratamiento:

A. Es obligación de la administración.

B. Debe incluir los datos que se recogen.

C. Debe incorporar si los datos van a ser cedidos fuera del espacio europeo.

D. La B y la C son correctas.

5. La nueva disponibilidad de datos permite desde el punto de vista comercial:

A. Explotar a los clientes.

B. Discriminar precios.

C. Aumentar las posibilidades de realizar segmentaciones cada vez más precisas.

D. Ninguna de las anteriores es correcta.

6. No es un principio de la protección de datos:

A. Principio de pertinencia.

B. Principio de maximización de la cantidad de información.

C. Principio de transparencia.

D. Todas las anteriores son correctas.

7. La disponibilidad de mayor cantidad de información permite:

A. Llevar a cabo una gestión empresarial *data-driven*.

B. Mejorar la información sobre clientes.

C. Detectar desviaciones respecto a los objetivos e identificar su origen.

D. Todas las anteriores son correctas.

8. El responsable del tratamiento:

A. Determina los medios y fines del tratamiento.

B. Recibe la comunicación de datos.

C. Trata datos por encargo del responsable del tratamiento.

D. Ninguna de las anteriores es correcta.

9. Una operación sobre un fichero de datos personales se denomina:

A. Captura.

B. Tratamiento.

C. Registro.

D. Extracción.

10. Un fichero de datos personales:

A. Es un conjunto de datos que contiene datos de personas o empresas pero que no pueden ser identificados.

B. Es un conjunto de datos que contiene datos de personas que se asocian a una persona física.

C. Es un conjunto de datos personales organizados de personas físicas o jurídicas.

D. Ninguna de las anteriores es correcta.