CIFF
Centro Internacional
de Formación Financiera

CIFF Trustees:

Santander

Universidad de Alcalá

Aspectos legales y éticos del Big Data

Pedro Bennasar Cabrera

MASTER EN BUSINESS ANALYTICS & BIG DATA
2014 – 2015

PRIVACIDAD

BIG DATA. INFORME GRUPO DE TRABAJO ART. 29

Statement of the WP29 on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU

"The Working Party acknowledges that the challenges of big data might require innovative thinking on how some of these and other key data protection principles are applied in practice. However, at this stage, it has no reason to believe that ***the EU data protection principles****, as they are currently enshrined in Directive 95/46/EC,* ***are*** *no longer* ***valid and appropriate for the development of big data, subject to further improvements to make them more effective in practice****. It also needs to be clear that* ***the rules and principles are applicable to all processing operations, starting with collection in order to ensure a high level of data protectio****n. "*

.

Contexto histórico y Contexto actual

1. Origen histórico de la legislación de privacidad/LOPD:

Contrapeso a la informática para salvaguardar privacidad de los individuos. Poder de disposición y control sobre datos

Legislación en continua evolución como así lo hace la tecnología que motiva su existencia (p.e. derecho al olvido)

2. Contexto histórico normativo actual:

normativas preventivas de control y gestión como **respuesta** del legislador ante la **crisis**.

Cumplimiento normativo. Gobierno corporativa.

LOPD (sobretodo reglamento) es relativamente precursora.

Reglamento europeo de Protección de datos como plasmación en el ámbito lopd de esta corriente preventiva. Privacy by design y accountability

4. Contexto tecnológico actual confluencia de tecnologias (Big Data, IdC, Cloud, redes sociales, etc)

Dimensiones de la privacidad

Dimensión del individuo

Afecta personas. clientes, proveedores (autónomos) y trabajadores dotándoles sobretodo con el otorgamiento de una serie de derechos de un poder de disposición y control sobre sus datos.

No afecta a personas jurídicas ni a los datos profesionales.

Dimensión del que recoge los datos

Le otorga fundamentalmente obligaciones

Esquema

- Concepto derecho a la privacidad
- Concepto dato de carácter personal
- Obligaciones legales de los que recogen datos
- Derechos de los titulares de los datos
- Métodos de evaluación de impacto en la protección de datos (AEPD)
- Anonimización de los datos

Concepto derecho a la privacidad

"Título I. De los derechos y deberes fundamentales

Capítulo segundo. Derechos y libertades

Sección 1.ª De los derechos fundamentales y de las libertades públicas

Artículo 18 Constitución Española 1978

1. *Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.*
2. *El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.*
3. *Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.*
4. ***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.***

Concepto derecho a la privacidad II

"18.4. CE ***1978*** ***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."*

privacidad vs intimidad. Es más amplio que intimidad.

Derecho fundamental a la protección de datos" (también "Privacidad" "libertad informática"). **Derecho fundamental autónomo**

Espacio y tiempo han desaparecido como salvaguardas de la privacidad por causa de las TIC.

Conjuntos de datos aislados que unidos permiten una evaluación de la personalidad

Derecho fundamental autónomo que se concreta en un **poder de disposición y de control sobre los datos personales por parte de los individuos.** (STC292/**2000**).

Derecho en constante evolución paralela a las TIC (ejemplo derecho al olvido: derecho cancelación **2014**)

Dato de carácter personal (I)

EVOLUCIÓN DEL CONCEPTO EN LA NORMATIVA

DIRECTIVA EUROPEA 95/46.

«datos personales»: toda información sobre una persona física identificada o identificable

(el «interesado»); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social;

LOPD 1999.-

Datos de carácter personal: cualquier información concerniente a personas físicas identificadas o identificables**.**

Dato de carácter personal (II)

CONCEPTO

REGLAMENTO LOPD 2007.-

Datos de carácter personal: Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables.

REGLAMENTO EUROPEO 2015-2016?.-

«**interesado**»: ***toda persona física identificada o que pueda ser identificada*, directa o indirectamente**, **por medios que puedan ser utilizados razonable por el responsable del tratamiento o por cualquier otra persona física o jurídica**, **en particular mediante un número de identificación, datos de localización, identificador en línea o uno o varios elementos específicos de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;**

«**datos personales**»: toda información relativa a un interesado

Dato de carácter personal (III)

DATOS ESPECIALMENTE PROTEGIDOS (articulo 7 LOPD)

ideología, religión o creencias (derecho a no revelarlo).

consentimiento expreso y por escrito del afectado podrán tratarse datos que revelen la **ideología, afiliación sindical, religión y creencias**. Se exceptúan los ficheros mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos relativos a sus asociados o miembros, sin perjuicio de que la cesión de dichos datos precisará siempre el previo consentimiento del afectado.

origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente.

Prohibidos los ficheros creados con la **finalidad exclusiva** de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual.

Los datos de carácter personal relativos a la comisión de **infracciones penales o administrativas** sólo podrán ser incluidos en ficheros de las Administraciones públicas competentes en los supuestos previstos en las respectivas normas reguladoras.

Excepciones en motivos sanitarios o interés vital del interesado.

Dato de carácter personal (IV)

NIVELES DE SEGURIDAD EN FUNCIÓN DE LOS DATOS

1. BASICO

Todos los ficheros o tratamientos de datos de carácter personal deberán adoptar las medidas de seguridad calificadas de nivel básico.

2. MEDIO

Deberán implantarse, **además de las medidas de seguridad de nivel básico, las medidas de nivel medio**, en los siguientes ficheros o tratamientos de datos de carácter personal:

a) Los relativos a la comisión de **infracciones administrativas o penales**.

b) Aquellos cuyo funcionamiento se rija por el **artículo 29 de la Ley Orgánica 15/1999, de 13 de diciembre. (información sobre solvencia patrimonial y credito)**

Dato de carácter personal (V)

NIVELES DE SEGURIDAD EN FUNCIÓN DE LOS DATOS

2. MEDIO (cont)

c) Aquellos de los que sean responsables **Administraciones tributarias y se relacionen con el ejercicio de sus potestades tributarias.**

d) Aquéllos de los que sean **responsables las entidades financieras para finalidades relacionadas con la prestación de servicios financieros.**

e) Aquéllos de los que sean responsables las **Entidades Gestoras y Servicios Comunes de la Seguridad Social y se relacionen con el ejercicio de sus competencias**. De igual modo, aquellos de los que sean responsables las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social.

f) **Aquéllos que contengan un conjunto de datos de carácter personal que ofrezcan una definición de las características o de la personalidad de los ciudadanos y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos**.

Dato de carácter personal (VI)

3. ALTO

Además de las medidas de nivel básico y medio, las medidas de nivel alto se aplicarán en los siguientes ficheros o tratamientos de datos de carácter personal:

a) Los que se refieran a datos de **ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual.**

b) Los que contengan o se refieran a **datos recabados para fines policiales sin consentimiento de las personas afectadas.**

c) Aquéllos que contengan datos derivados de **actos de violencia de género**.

D) A los ficheros de los que sean. **responsables los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones electrónicas respecto a los datos de tráfico y a los datos de localización, se aplicarán, además de las medidas de seguridad de nivel básico y medio, la medida de seguridad de nivel alto contenida en el artículo 103 de este reglamento (registro de accesos)**

No obstante en caso de ficheros o tratamientos de datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual bastará la implantación de las medidas de seguridad de nivel **básico** en determinados casos.

Obligaciones legales de los que recaban datos (I)

RESPONSABLE DEL TRATAMIENTO Y/O DEL FICHERO

1. **Inscripción** en la AEPD de los **ficheros**
2. **Calidad de los datos** (Articulo 4 LOPD)
   - adecuados, pertinentes y no excesivos (minimización).
   - prohibición finalidades incompatibles (limitación de la finalidad).
   - exactos puestos al día.
   - cancelación.
3. **Información** (articulo 5 LOPD)

Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:

a) **De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.**

b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.

c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.

d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.

e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

Cuando el responsable del tratamiento no esté establecido en el territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, deberá designar, salvo que tales medios se utilicen con fines de trámite, un representante en España, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento.

Obligaciones legales de los que recaban datos (II)

RESPONSABLE DEL TRATAMIENTO Y/O DEL FICHERO

4. Consentimiento (artículos 6 y 7, 8) interés legitimo

5. Deber de secreto profesional (articulo 10 LOPD).

6. Salidas de datos

- encargado de tratamiento (proveedores. articulo 12 LODP)
- cesiones de datos (información consentimiento. artículos 11 y 27 LOPD)
- transferencia internacional (Autorizaciones Director AEPD, Binding Corporate Rules, etc) artículos 33 Y 34 LOPD).

7 atender derechos ARCO (artículos 14 a 18 LOPD)

Obligaciones legales de los que recaban datos (IV)

RESPONSABLE DEL TRATAMIENTO Y/O DEL FICHERO

8. Aplicación medidas seguridad.- implementación y plasmación en documento de seguridad.

Tratamiento (automatizado).-

- responsable de seguridad
- personal
- incidencias
- control de acceso
- identificación y autenticación
- gestión de soportes
- copias de respaldo y recuperación
- auditorias de seguridad
- telecomunicaciones

Obligaciones legales de los que recaban datos (V)

RESPONSABLE DEL TRATAMIENTO Y/O DEL FICHERO

8. **Aplicación medidas seguridad.- (Cont)**

Tratamiento (no automatizado).-

- criterios de archivo
- almacenamiento
- custodia de soportes
- copia o reproducción
- traslado de documentación
- dispositivos almacenamiento
- control de acceso

ENCARGADO DEL TRATAMIENTO.-

obligaciones del encargado (secreto, medidas de seguridad, cadena de encargo).

GUÍA PARA CLIENTES QUE CONTRATEN CLOUD COMPUTING

Los **puntos más relevantes** a destacar de la **Guia**:

1. **Responsabilidad**.- El cliente que contrata servicios de *cloud computing* sigue siendo responsable del tratamiento de los datos personales. Aunque los contrate con una gran compañía multinacional la responsabilidad no se desplaza al prestador del servicio, ni siquiera incorporando una cláusula en el contrato con esta finalidad. **Firmar contrato de encargo igualmente.**

2. **Subcontratistas-** Debe solicitar y obtener información sobre si intervienen o no terceras empresas (subcontratistas) en la prestación de servicios de *cloud computing*.

3. Localización de datos

Tiene importancia porque las **garantías exigibles adicionales (además las previstas en caso de comunicación y encargo del tratamiento**) para su protección son distintas según los países en que se encuentren.

- países del **Espacio Económico Europeo** ofrecen garantías suficientes y no se considera legalmente que exista una transferencia internacional de datos. El Espacio Económico Europeo está constituido por los países de la Unión Europea e Islandia, Liechtenstein y Noruega**.**
- si los datos están localizados en **países que no pertenecen al Espacio Económico Europeo** habría una transferencia internacional de datos, en cuyo caso, y dependiendo del país en que se encuentren, deberán proporcionarse garantías jurídicas adecuadas.

CLOUD COMPUTING III

- Se considera una garantía adecuada que el **país de destino ofrezca un nivel de protección equivalente al del Espacio Económico Europeo** y así se haya acordado por la Agencia Española de Protección de Datos o por Decisión de la Comisión Europea. En ese caso será suficiente con hacer constar la transferencia en la notificación del fichero realizada a la Agencia Española de Protección de Datos para su inscripción en el Registro General de Protección de Datos.

- Las proporcionadas por las **empresas ubicadas en los Estados Unidos que hayan suscrito los principios de Puerto Seguro**. Al igual que en el caso anterior será suficiente con hacer constar la transferencia en la notificación del fichero a la Agencia Española de Protección de Datos.

- En otro caso, la **transferencia internacional de datos necesitará autorización del Director de la Agencia Española de Protección de Datos**, que podrá otorgarse en caso de que el exportador de datos aporte garantías adecuadas.

Portabilidad

significa que el **proveedor ha de obligarse, cuando pueda resolverse el contrato o a la terminación del servicio, a entregar toda la información al cliente en el formato que se acuerde**, de forma que éste pueda almacenarla en sus propios sistemas o bien optar porque se traslade a los de un nuevo proveedor en un formato que permita su utilización, en el plazo más breve posible, con total garantía de la integridad de la información y sin incurrir en costes adicionales

Derechos de los titulares de los datos

- Derechos **ARCO** (incluye denominado “derecho al olvido”)

- Derecho de **indemnización**.

- **Tutela de la Agencia** en relación con ejercicio de los derechos

- **Consulta en la Agencia** de los ficheros inscritos.

- **Impugnación de valoraciones**

CONCEPTO

Una Evaluación de Impacto en la Protección de Datos Personales (EIPD) **es un análisis de los riesgos que un producto o servicio puede entrañar para la protección de datos de los afectados y,** como consecuencia de ese análisis, **la gestión de dichos riesgos mediante la adopción de las medidas necesarias para eliminarlos o mitigarlos.**

Las evaluaciones de impacto en la protección de datos personales:

- forman **parte esencial** de **una nueva generación de herramientas y metodologías** que buscan una **aproximación proactiva a los retos de implantar garantías** que salvaguarden el derecho fundamental a la protección de datos
- se constituyen en un **elemento destacado de la Privacidad desde el Diseño**.

Igualmente, cada vez se abre paso con más fuerza la idea de que los responsables de tratamientos de datos personales **han de ser capaces de demostrar** su compromiso con los derechos de los ciudadanos y el cumplimiento de sus obligaciones legales (**accountability**).

CONSTITUCIÓN DEL EQUIPO DE TRABAJO Y DEFINICIÓN DE SUS TÉRMINOS DE REFERENCIA

- equipo o grupo de trabajo interdisciplinar.

- compromiso de la **alta dirección** de la organización.

No existen reglas fijas sobre quién debería participar en el grupo o liderarlo, pues dependerá mucho de la organización de que se trate, su tamaño, estructura y cultura particular, así como del proyecto que se vaya a evaluar.

- En cualquier caso, la Guia ofrece unas directrices sobre **quiénes no podrían faltar en el mismo**:

representante –con capacidad de decisión– del proyecto sometido a evaluación

delegado de protección de datos o la persona que ejerza esta responsabilidad (o el asesor externo al que se le haya confiado esta misión)

responsable de seguridad y representantes cualificados del departamento TIC y de las áreas de negocio o departamentos a los que más afecte el proyecto dentro de la organización.

FASES EIPD

1. Análisis de necesidad.- Valoración de la conveniencia de llevar a cabo o no una Evaluación de Impacto en la Protección de Datos Personales.

2. Descripción del proyecto y de los flujos de información.- Análisis en profundidad del proyecto **obteniendo el detalle de las categorías de datos que se tratan, los usuarios de los mismos, los flujos de información y las tecnologías utilizadas.**

3. Identificación de los riesgos.- Análisis de los posibles riesgos para la protección de datos de los afectados y valoración de la probabilidad de que sucedan y del daño que causarían si se materializaran.

4. Gestión de los riesgos identificados.- Determinación de los controles y las medidas que han de adoptarse para eliminar, mitigar, transferir o aceptar los riesgos detectados.

5. Análisis de cumplimiento normativo.- Verificación de que el producto o servicio que se está desarrollando cumple con los requerimientos legales, generales o sectoriales, en materia de protección de datos.

6. Informe final.- Relación detallada de los riesgos identificados y de las recomendaciones y propuestas para eliminarlos o mitigarlos. Su destinatario principal es la dirección de la organización.

7. Implantación de las recomendaciones.- Decisión sobre las recomendaciones del informe final y las acciones que deben llevarse a cabo. Asignación de los recursos necesarios para su ejecución y del responsable de implantarlas.

8.. Revisión y realimentación.- Análisis del resultado final para comprobar la efectividad de la EIPD y verificar si se han creado nuevos riesgos o se han detectado otros que habían pasado desapercibidos. Estos resultados se utilizan para realimentar la evaluación de impacto y actualizarla cuando sea necesario

Consulta con las partes afectadas.- Para una correcta identificación de los riesgos, es imprescindible llevar a cabo, a lo largo de todo el proyecto y en los momentos apropiados, consultas con todas aquellas partes que vayan a resultar afectadas por el mismo, tanto internas como externas a la organización.

FASE 1. ANÁLISIS DE LA NECESIDAD DE LA EVALUACIÓN.

En relación con las situaciones en las que sería aconsejable llevar a cabo una evaluación de impacto, esta es la relación indicativa de algunas de ellas incluidas en la Guía por la AEPD:

– Cuando se enriquezca la información existente sobre las personas mediante la recogida de nuevas categorías de datos o se usen las existentes con nuevas finalidades o en formas que antes no se usaban, en particular, si los nuevos usos o finalidades son más intrusivos o inesperados para los afectados.

– Cuando se vaya a llevar a cabo un tratamiento destinado a evaluar o predecir aspectos personales relevantes de los afectados6, su comportamiento, su encuadramiento en perfiles determinados (para cualquier finalidad), encaminado a tomar medidas que produzcan efectos jurídicos que los atañen o los afectan significativamente y, en particular, cuando establezcan diferencias de trato o trato discriminatorio o que puedan afectar a su dignidad o su integridad personal .

– **Cuando se traten grandes volúmenes de datos personales a través de tecnologías como la de datos masivos (Big data), internet de las cosas (Internet of Things) o el desarrollo y la construcción de ciudades inteligentes (smart cities).**

– Cuando se vayan a utilizar tecnologías que se consideran especialmente invasivas con la privacidad como la videovigilancia a gran escala, la utilización de aeronaves no tripuladas (drones), la vigilancia electrónica, la minería de datos, la biometría, las técnicas genéticas, la geolocalización, o la utilización de etiquetas de radiofrecuencia o RFID (especisi forman parte de la llamada internet de las cosas) o cualesquiera otras que puedan desarrollarse en el futuro.

– Cuando el tratamiento afecte a un número elevado de personas o, alternativa o adicionalmente, se produzca la acumulación de gran cantidad de datos respecto de los interesados.

– Cuando se cedan o comuniquen los datos personales a terceros y, en particular, siempre que se pongan en marcha nuevas iniciativas que supongan compartir datos personales con terceros que antes no tenían acceso a ellos, ya sea entregándolos, recibiéndolos o poniéndolos en común de cualquier forma.

– Cuando se vayan a transferir los datos a países que no forman parte del Espacio Económico Europeo (EEE) y que no hayan sido objeto de una declaración de adecuación por parte de la Comisión Europea o de la Agencia Española de Protección de Datos.

– Cuando se vayan a utilizar formas de contactar con las personas afectadas que se podrían considerar especialmente intrusivas.

– Cuando se vayan a utilizar datos personales no disociados o no anonimizados de forma irreversible con fines estadísticos, históricos o de investigación científica.

– Cuando la recogida tenga como finalidad el tratamiento sistemático y masivo de datos especialmente protegidos.

FASE 2. DESCRIPCIÓN DEL PROYECTO Y DE LOS FLUJOS DE DATOS PERSONALES

La Guía indica Algunos apartados básicos que deberían abordarse y documentarse en esta fase son los siguientes:

—Un resumen del proyecto con sus **principales características, incluyendo una descripción de su necesidad u oportunidad para la organización.**

—**Identificación de aquellos aspectos** del proyecto especialmente relevantes para la privacidad de las personas y que sean **susceptibles de generar más riesgos o de dificultar el cumplimiento normativo**.

—Una descripción detallada de:

a. Los **medios de tratamiento y de las tecnologías** que se utilizarán y, en particular, de aquellas que introduzcan mayores riesgos para la privacidad.

b. Las **categorías de datos personales** que se van a tratar, finalidades para las que se usarán cada una de ellas, necesidad de su utilización y colectivos afectados.

c. **Quién accederá a cada categoría de datos personales** y los motivos y justificaciones para ello.

d. **Los flujos de información**: recogida, circulación dentro de la organización, cesiones fuera de la misma y recepciones de datos personales procedentes de otras organizaciones.

—Si resulta necesario, incluir información y diagramas adicionales para ilustrar aspectos como el **control de acceso o la conservación o destrucción de los datos personales.**

FASE 3. IDENTIFICACIÓN Y EVALUACIÓN DE RIESGOS PARA LA PROTECCIÓN DE DATOS

En este momento **comienza específicamente la evaluación** de impacto que el proyecto tendrá en la protección de datos personales, a través del análisis de toda la documentación generada y, en particular:

- **seguimiento del ciclo de vida de los datos personales**
- **sus usos previstos**
- **las finalidades para las que se tratarán**
- **las tecnologías utilizadas**
- **la identificación de los usuarios que accederán a ella**

Todo ello para conocer los riesgos, reales y percibidos, existentes para la privacidad.

FASE 4. GESTIÓN DE LOS RIESGOS IDENTIFICADOS

Es difícil detallar a priori un inventario completo de las posibles medidas que se pueden o deben adoptar para eliminar, mitigar o transferir los riesgos para la privacidad detectados en una EIPD puesto que dependen, en gran medida, de la naturaleza de los mismos y de cada proyecto específico.

Ejemplo: puede ser la existencia de transferencias internacionales, necesidad y conveniencia de tratar datos especialmente protegidos, etc.

Cada proyecto tendrá sus propios riesgos (derivados de necesidad cumplir obligaciones legales)

FASE 5. ANÁLISIS DE CUMPLIMIENTO NORMATIVO

Uno de los aspectos decisivos en toda Evaluación de Impacto en la Protección de Datos (EIPD) es el relativo a la **verificación de la conformidad del proyecto con las distintas regulaciones** que pueden contener elementos relativos a la privacidad y a la protección de datos que le sean de aplicación.

Ello **incluye la legislación básica de protección de datos personales** y, en concreto:

la Ley **Orgánica de Protección de Datos y su Reglamento de Desarrollo**.

Pero, **dependiendo del sector en el que opere la organización** o del proyecto concreto, también pueden existir **obligaciones adicionales** como, por ejemplo, la legislación sanitaria, de telecomunicaciones o de servicios de sociedad de la información o, en la propia LOPD, lo que se refiere a los ficheros de las Fuerzas y Cuerpos de Seguridad, a la prestación de servicios de solvencia patrimonial y crédito, o los tratamientos con fines de publicidad y prospección comercial

FASE 6. REDACCIÓN, PUBLICACIÓN E INTEGRACIÓN DEL INFORME FINAL

Apartados debe incluir:

—Identificación clara del proyecto, la persona o personas responsables de la EIPD y sus datos de contacto, la fecha de realización del informe y número de versión del mismo.

—Resumen del informe con los resultados esenciales escrito con claridad y concisión.

—Introducción y descripción general del proceso de evaluación para aquellos lectores que no estén familiarizados con esta técnica.

—Resultado del análisis de necesidad de la evaluación y su justificación.

—Descripción general del proyecto con el nivel de detalle necesario (se pueden incluir como anexos los documentos relevantes del proyecto que se juzguen oportunos).

—Descripción detallada de los flujos de datos personales.

—Riesgos identificados.

—Identificación de partes interesadas o a las que afecta el proyecto, tanto internas como externas a la organización, y resultados de las consultas llevadas a cabo con las mismas.

- Análisis de cumplimiento normativo y, en particular, detalle de posibles deficiencias detectadas y propuestas para su solución.

—Recomendaciones del equipo responsable de la EIPD y enumeración de las medidas adoptadas o que deben adoptarse en el diseño del proyecto para eliminar o evitar, mitigar, transferir o aceptar los riesgos para la privacidad incluidas las de carácter organizativo.

FASE 7. IMPLANTACIÓN DE LAS RECOMENDACIONES

El **informe final del equipo de la EIPD debe ser remitido a la alta dirección** de la organización para que tome las decisiones necesarias en relación con las recomendaciones realizadas y las medidas sugeridas.

Esta remisión tiene **dos motivos**:

1) la **dirección defina y tome las decisiones necesarias para poner en marcha los cambios o mejoras** que hubieran de ser introducidas en el proceso tomando como base las sugerencias realizadas en el informe.

2) **debe establecer la persona o unidad responsable** de coordinar que se implanten las medidas recomendadas y, para que su labor resulte eficaz, investirla de la necesaria autoridad para realizar su trabajo, **y comunicar a la dirección los avances y dificultades que encuentre en el mismo.**

Como **las medidas a adoptar pueden ser de muy diversos tipos (organizativas, tecnológicas, contractuales, etc**.) no existe un método que indique cómo han de ser llevadas a cabo, y cada organización debe decidir cuál es el que mejor se adapta a su cultura y estructuras de gestión.

Otro aspecto importante es el referente a aquellas **medidas que deben ser adoptadas por un proveedor externo**. En estos casos, aparte de las posibles modificaciones contractuales que pudieran resultar necesarias, también habría que prever los **mecanismos de control y supervisión** que se deben definir y adoptar para garantizar que estos terceros realmente implantan las medidas acordadas.

FASE 8. REVISIÓN DE LOS RESULTADOS Y REALIMENTACIÓN DE LA EVALUACIÓN DE IMPACTO

Una vez que se han obtenido los resultados de la EIPD y se han implantado las medidas correctoras y de mejora adoptadas por la alta dirección de la organización llega el momento de la revisión y comprobación de su implantación real y de su eficacia.

Es necesario, pues, examinar el proyecto una vez operativo para verificar que los riesgos detectados se han abordado correctamente y que no existen otros nuevos que en su momento pasaron desapercibidos o que han surgido posteriormente, lo que llevaría aparejada una nueva iteración de las fases de la EIPD.

Por ello, **una evaluación de impacto**, aunque tiene una importancia y un protagonismo especial en las fases iniciales de un proyecto, **es un proceso que acompaña al sistema de información, producto o servicio durante todo su ciclo de vida**.

Y, por supuesto, la **modificación del mismo o la incorporación de nuevas funcionalidades** deberán llevar consigo la necesidad de revisar la EIPD con un alcance mayor o menor en función de la profundidad y magnitud de los cambios introducidos.

Así, el esquema clásico de **la Rueda o Ciclo de Deming** (planificar, implantar, verificar y actuar) también **deberá ser observado en la realización y desarrollo de las EIPD.**

Anonimización de datos I

CONCEPTO.-

ANONIMIZACIÓN es el **resultado de un tratamiento de los datos personales realizado para evitar de forma irreversible su identificación**.

los datos anonimizados serían, por tanto, datos anónimos que antes hacían referencia a una persona identificable, pero que ahora ya no admiten identificación

En este proceso, los responsables del tratamiento deben considerar distintos aspectos y valorar todos los medios que puedan utilizarse «razonablemente» para la identificación de los datos (ya sea por el responsable del tratamiento o por terceros).

VALOR POTENCIAL DE LA ANONIMIZACIÓN.- como estrategia para permitir a las personas y la sociedad en su conjunto beneficiarse de los «**datos abiertos**» al mismo tiempo que se mitigan los riesgos para los interesados.

DIFICULTAD.- los estudios de caso y las publicaciones científicas muestran la dificultad de crear un conjunto de datos verdaderamente anónimo conservando, sin embargo, toda la información subyacente requerida para la tarea.

.

Anonimización de datos II

Tratamientos posteriores.- debe cumplir la prueba de compatibilidad con arreglo a las directrices formuladas por el Grupo de Trabajo en su Dictamen 03/2013 **sobre la limitación del fin.**

En particular, esto significa que es necesario llevar a cabo una **evaluación** sustantiva a la luz de las circunstancias relevantes, atendiendo especialmente a los siguientes **factores clave**:

a) la **relación entre los fines para los que se recogieron** los datos personales y los **fines de su tratamiento posterior**;

b) el **contexto** en el que se recogieron los datos personales **y las expectativas razonables de los interesados en cuanto a su uso ulterior**;

c) la **naturaleza de los datos personales y el impacto del tratamiento ulterior en los interesados**;

d) las **salvaguardas adoptadas por el responsable del tratamiento para garantizar un tratamiento correcto e impedir cualquier tipo de efecto negativo indebido en los interesados**.

Anonimización de datos III

Tan solo si el responsable del tratamiento **agrega los datos a un nivel** en el que los **eventos individuales dejan de ser identificables**, el **conjunto de datos** resultantes puede calificarse de **anónimo**.

EJEMPLO: si una **organización recoge datos sobre los desplazamientos de personas, los patrones de viaje individuales a nivel de evento seguirían considerándose datos personales para cualquier parte mientras el responsable del tratamiento** (o cualquier otra parte) **siga teniendo acceso a los datos originales** no tratados, aun en el caso de que se hayan eliminado los identificadores directos del conjunto entregado a terceros. Por el contrario, **si el responsable del tratamiento borra los datos no tratados y entrega únicamente estadísticas agregadas a terceros a un nivel general** (por ejemplo, «los lunes, en el trayecto X, hay un 160 % más de pasajeros que los martes»), entonces estaríamos hablando de datos anónimos.

Anonimización de datos IV

Una solución **de anonimización eficaz** impide:

1) a todos singularizar a una persona en un conjunto de datos

2) vincular dos registros en un conjunto de datos (o dos registros pertenecientes a conjuntos diferentes)

3) e inferir cualquier tipo de información a partir de dicho conjunto.

En definitiva, como norma general, **no basta con eliminar los elementos que pueden servir para identificar directamente** a una persona para garantizar que ya no se puede identificar al interesado.

Con frecuencia habrá que tomar medidas adicionales para evitar dicha identificación, las cuales dependerán una vez más del contexto y de los fines del tratamiento de que van a ser objeto los datos.

Anonimización de datos V

ANONIMIZACIÓN vs REIDENTIFICACIÓN

Los responsables del tratamiento deben ser conscientes de que un conjunto de datos anonimizado puede entrañar todavía riesgos residuales para los interesados.

CARACTERISTICAS

- Pueden considerarse **varias técnicas de anonimización**, sin que la legislación europea contenga **ninguna norma prescriptiva**.

- **importancia a los elementos contextuales**: debe considerarse «el conjunto de los medios que puedan ser razonablemente utilizados» para la identificación por parte del responsable del tratamiento o de un tercero, prestando especial atención a lo que se entiende, en el estado actual de la técnica, como «medios que puedan ser razonablemente utilizados» (dado el incremento de la potencia de los ordenadores y de las herramientas disponibles).
- La anonimización **lleva implícito un factor de riesgo** que ha de tenerse en cuenta al evaluar la validez de las técnicas de anonimización, incluidos los posibles usos de los datos «anonimizados» mediante estas, además de considerarse asimismo la gravedad y probabilidad del riesgo.

Anonimización de datos VI

EJEMPLO:

Debido a su naturaleza única, los perfiles de **datos genéticos** constituyen un **ejemplo** de datos personales que están en **riesgo** de ser identificados **si tan solo se utiliza la técnica de eliminación de la identidad del donante**.

Diversos estudios científicos ya han demostrado que, al combinar los recursos genéticos disponibles para el público (p. ej., registros genealógicos, obituarios y resultados de consultas en motores de búsqueda) y los metadatos sobre donantes de ADN (fecha de donación, edad o lugar de residencia), se puede revelar la identidad de determinadas personas aunque el ADN se haya donado de forma «anónima».

Anonimización de datos VII

RIESGOS DE LA ANONIMIZACIÓN

los **tres riesgos clave de la anonimización**:

- ***Singularización***: la **posibilidad** de **extraer** de un **conjunto de datos algunos registros** (o todos los registros) **que identifican a una persona**.

- ***Vinculabilidad***: la **capacidad de vincular como mínimo dos registros de un único interesado o de un grupo de interesados**, ya sea en la **misma base de datos** o en **dos bases de datos distintas**. **Si el atacante puede determinar** (p. ej., mediante un análisis de correlación) **que dos registros están asignados al mismo grupo de personas pero no puede singularizar a las personas** en este grupo, entonces la técnica es **resistente a la singularización, pero no a la vinculabilidad.**

- ***Inferencia***: la posibilidad de **deducir** con una probabilidad significativa el **valor de un atributo a partir de los valores de un conjunto de otros atributos.**

Anonimización de datos VIII

PRÁCTICAS Y TÉCNICAS DE ANONIMIZACIÓN

A) ALEATORIZACIÓN

La **aleatorización** es una familia de técnicas que **modifican la veracidad de los datos** a fin de eliminar el estrecho vínculo existente entre los mismos y la persona. Si los datos se hacen lo suficientemente ambiguos, no podrán remitir a una persona concreta.

Anonimización de datos IX

TIPOS DE ALEATORIZACIÓN

1. Adición de ruido

Consiste en **modificar los atributos del conjunto de datos para que sean menos exactos**, conservando no obstante su distribución general.

Ejemplo, aunque la altura de una persona se mida originalmente hasta el centímetro más próximo, el conjunto de datos anonimizado puede contener valores con una exactitud de ± 10 cm.

adición de ruido debe combinarse con otras técnicas de anonimización, como la eliminación de atributos obvios y de cuasi identificadores.

:

Anonimización de datos X

Ejemplo: Defectos de la adición de ruido

Un experimento de **reidentificación** muy famoso es el que se llevó a cabo con la **base de datos de clientes del proveedor de contenidos de vídeo Netflix.** Los investigadores analizaron las propiedades geométricas de esta base de datos, que está formada por más de 100 millones de valoraciones de unas 18 000 películas en una escala de 1 a 5 por parte de 500 000 usuarios. La empresa hizo pública esta base de datos tras anonimizarla con arreglo a sus directrices internas sobre privacidad. En concreto, eliminó todo tipo de información que pudiera identificar al cliente, excepto las valoraciones y las fechas. Se añadió ruido a las valoraciones mejorándolas o empeorándolas ligeramente.

A pesar de ello, se descubrió que se podía identificar de manera unívoca el 99 % de los registros de usuarios en el conjunto de datos usando 8 valoraciones y fechas con errores de 14 días a modo de criterio de selección. Aun rebajando los criterios de selección a 2 valoraciones y un error de 3 días, se podía identificar al 68 % de los usuarios13.

Anonimización de datos XI

TIPOS DE ALEATORIZACIÓN

2. Permutación

consiste en mezclar los valores de los atributos en una tabla para que algunos de ellos puedan vincularse artificialmente a distintos interesados. .

El siguiente ejemplo muestra que, si se permutan los atributos aleatoriamente, no se puede garantizar la intimidad si existen vínculos lógicos entre atributos diferentes. Tras realizar el intento de anonimización, resulta sencillo deducir los ingresos de cada persona en función de su trabajo y año de nacimiento. Por ejemplo, tras examinar los datos, se puede afirmar que el Director Ejecutivo que aparece en la tabla muy probablemente nació en 1957 y disfruta del salario más alto, mientras que el desempleado nació en 1964 y tiene los menores ingresos.

Año	Sexo	Cargo	Ingresos (permutados)
1957	M	Ingeniero	70k
1957	M	Director Ejecutivo	5k
1957	M	Desempleado	43k
1964	M	Ingeniero	100k
1964	M	Gerente	45k

Anonimización de datos XII

TIPOS DE ALEATORIZACIÓN

3. Privacidad diferencial

la **inserción de ruido** en la privacidad diferencial, por el contrario, puede usarse cuando el **responsable del tratamiento de datos genera vistas anonimizadas** de un conjunto de datos, al mismo tiempo que conserva una copia de los datos originales. Estas vistas anonimizadas normalmente se **generan mediante un subconjunto de consultas de un determinado tercero. Este subconjunto contiene algo de ruido aleatorio que se añade de manera deliberada con posterioridad**

Sin embargo, conviene aclarar que las técnicas de privacidad diferencial no modifican los datos originales. Por lo tanto, mientras se conserven los datos originales, el responsable del tratamiento es capaz de identificar a las personas a partir de los resultados de las consultas de privacidad diferencial mediante el conjunto de los medios que pueden ser razonablemente utilizados. Estos resultados también deben considerarse como datos personales.

Anonimización de datos XIII

PRÁCTICAS Y TÉCNICAS DE ANONIMIZACIÓN

B) GENERALIZACIÓN

La generalización es la segunda familia de técnicas de anonimización.

Este enfoque **generaliza o diluye los atributos de los interesados modificando las respectivas escalas u órdenes de magnitud** (por ejemplo, sustituyendo una ciudad por una región, o una semana por un mes).

Anonimización de datos XIV

TIPOS DE GENERALIZACIÓN

1 . Agregación y anonimato k.

Las técnicas de agregación y anonimato k tienen el objetivo de impedir que un interesado sea singularizado cuando se le agrupa junto con, al menos, un número k de personas. Para lograrlo, los valores de los atributos se generalizan hasta el punto de que todas las personas acaban compartiendo el mismo valor.

Por **ejemplo**, al reducir la granularidad de un lugar (de ciudad a región), muchos interesados compartirán esos valores. Las fechas de nacimiento pueden generalizarse en períodos de tiempo, o bien agruparse por mes o año. Otros atributos numéricos (p. ej., salario, peso, altura y dosis de medicina), pueden generalizarse por intervalos de valores (p. ej.: salario, entre 20 000 y 30 000 euros). Estos métodos son aplicables cuando la correlación de valores puntuales de atributos puede crear cuasi identificadores.

Anonimización de datos XVI

TIPOS DE GENERALIZACIÓN

2. Diversidad l, proximidad t

La diversidad l extiende el anonimato k para garantizar que ya no se puedan realizar ataques por inferencia deterministas. Para ello, se asegura de que en cada clase de equivalencia, todos los atributos tienen al menos *l valores diferentes.* .

Anonimización de datos XVII

SEUDOANONIMIZACIÓN

La seudonimización **consiste en la sustitución de un atributo (normalmente un atributo único) por otro en un registro.**

Por consiguiente, sigue existiendo una alta probabilidad de identificar a la persona física de manera indirecta; en otras palabras, el uso exclusivo de la seudonimización no garantiza un conjunto de datos anónimo.

seudonimización, para aclarar algunos errores e ideas falsas: **la seudonimización no es un método de anonimización;** simplemente, **reduce la vinculabilidad** de un conjunto de datos **con la identidad original del interesado** y es, en consecuencia, una medida de seguridad útil.

Los datos seudonimizados no constituyen información anonimizada, ya que permiten singularizar a los interesados y vincularlos entre conjuntos de datos diferentes.

La probabilidad de que el seudoanonimato admita la identificabilidad es muy alta; por ello, entra dentro del ámbito de aplicación del régimen jurídico de la protección de datos.

Anonimización de datos XVIII

TÉCNICAS DE SEUDOANONIMIZACIÓN

Las técnicas de seudonimización **más utilizadas** son las siguientes:

- Cifrado con clave secreta
- Función hash
- Función con clave almacenada
- Cifrado determinista o función hash con clave con borrado de clave:
- Descomposición en tokens

Anonimización de datos XIX

Ejemplos seudoanonimización

Redes sociales

Se ha demostrado que es posible extraer información sensible de personas concretas a partir de los gráficos de redes sociales, a pesar de las técnicas de seudonimización que se aplican a estos datos. El proveedor de una red social pensaba equivocadamente que la seudonimización era una estrategia sólida para evitar la identificación, de modo que vendió datos de usuarios a otras empresas para que estas pudieran utilizarlos con fines publicitarios y de comercialización. El proveedor remplazó los nombres reales por seudónimos, pero esta medida es claramente insuficiente para anonimizar los perfiles de los usuarios, ya que las relaciones entre las distintas personas son únicas y pueden utilizarse como identificadores.

Localizaciones

Investigadores del MIT20 analizaron recientemente un conjunto de datos seudonimizados formado por coordenadas de movilidad espacio-temporales de 1,5 millones de personas a lo largo de un período de 15 meses en un territorio con un radio de 100 km. Este análisis les permitió singularizar al 95 % de la población mediante cuatro puntos espaciales, y a más del 50 % de los interesados con apenas dos puntos espaciales (uno de esos puntos es conocido: normalmente se trata del domicilio o la oficina), con un margen muy estrecho para la protección de la privacidad, aun teniendo en cuenta que las identidades de las personas se habían seudonimizado reemplazando sus atributos verdaderos [...] por otras etiquetas.

Anonimización de datos XX

TABLA FORTALEZAS Y DEBILIDADES

La tabla contenida en el informe del Grupo art. 29 ofrece un resumen de las fortalezas y debilidades de estas técnicas con relación a los tres requisitos básicos:

	Existe riesgo de singularización?	¿Existe riesgo de vinculabilidad?	¿Existe riesgo de inferencia?
Seudonimización	Sí	Sí	Sí
Adición de ruido	Sí	Puede que no	Puede que no
Sustitución	Sí	Sí	Puede que no
Agregación y anonimato k	No	Sí	Sí
Diversidad l	No	Sí	Puede que no
Privacidad diferencial	Puede que no	Puede que no	Puede que no
Hash/Tokens	Sí	Sí	Puede que no

CONCLUSIONES ANONIMIZACIÓN

- La **solución óptima** debería adoptarse **CASO A CASO**.

- EQUIPO **MULTIDISCIPLINAR (ej. Dato genético)**

- **Una solución** (es decir, un proceso de anonimización integral) **que cumpla estos tres criterios tendrá la solidez necesaria** para impedir que la identificación de los datos se lleve a cabo mediante los medios más probables y razonables que pudiera emplear el responsable del tratamiento o cualquier tercero.

- **Siempre** que una posible solución no **cumpla con alguno de los criterios, habrá que evaluar exhaustivamente los riesgos de identificación**.

.

INFRACCIONES (I)

infracciones muy graves

a) La **recogida** de datos en forma **engañosa o fraudulenta**.

b) **Tratar o ceder los datos de carácter personal a los que se refieren los apartados 2, 3 y 5 del art. 7** (datos especialmente protegidos) **de esta Ley salvo en los supuestos en que la misma lo autoriza o violentar la prohibición contenida en el apartado 4 del art. 7** (ficheros exclusivamente de datos protegidos).

c) **No cesar en el tratamiento ilícito de datos de carácter personal cuando existiese un previo requerimiento** del Director de la Agencia Española de Protección de Datos para ello.

d) **La transferencia internacional de datos de carácter personal con destino a países que no proporcionen un nivel de protección equiparable** sin autorización del Director de la Agencia Española de Protección de Datos salvo en los supuestos en los que conforme a esta Ley y sus disposiciones de desarrollo dicha autorización no resulta necesaria.

INFRACCIONES (II)

infracciones graves

a) Proceder *a la creación de ficheros de titularidad pública o iniciar la recogida de datos de carácter personal para los mismos, sin autorización de disposición general, publicada en el "Boletín Oficial del Estado" o diario oficial correspondiente.*

b) Tratar datos de carácter personal sin recabar el consentimiento de las personas afectadas, cuando el mismo sea necesario conforme a lo dispuesto en esta Ley y sus disposiciones de desarrollo.

c) Tratar datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en el artículo 4 de la presente Ley y las disposiciones que lo desarrollan, salvo cuando sea constitutivo de infracción muy grave.

d) La vulneración del deber de guardar secreto acerca del tratamiento de los datos de carácter personal al que se refiere el artículo 10 de la presente Ley.

e) El impedimento o la obstaculización del ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

f) El incumplimiento del deber de información al afectado acerca del tratamiento de sus datos de carácter personal cuando los datos no hayan sido recabados del propio interesado.

g) El incumplimiento de los restantes deberes de notificación o requerimiento al afectado impuestos por esta Ley y sus disposiciones de desarrollo.

h) Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen.

i) No atender los requerimientos o apercibimientos de la Agencia Española de Protección de Datos o no proporcionar a aquélla cuantos documentos e informaciones sean solicitados por la misma.

j) La obstrucción al ejercicio de la función inspectora.

k) La comunicación o cesión de los datos de carácter personal sin contar con legitimación para ello en los términos previstos en esta Ley y sus disposiciones reglamentarias de desarrollo, salvo que la misma sea constitutiva de i

INFRACCIONES (III)

Infracciones leves

a) No remitir a la Agencia Española de Protección de Datos las notificaciones previstas en esta Ley o en sus disposiciones de desarrollo.

b) No solicitar la inscripción del fichero de datos de carácter personal en el Registro General de Protección de Datos.

c) El incumplimiento del deber de información al afectado acerca del tratamiento de sus datos de carácter personal cuando los datos sean recabados del propio interesado.

d) La transmisión de los datos a un encargado del tratamiento sin dar cumplimiento a los deberes formales establecidos en el art. 12 de esta Ley.

SANCIONES (I)

TIPOS DE SANCIONES

Las infracciones leves serán sancionadas con multa de 900 a 40.000 euros.

Las infracciones graves serán sancionadas con multa de 40.001 a 300.000 euros.

Las infracciones muy graves serán sancionadas con multa de 300.001 a 600.000 euros.

*La **cuantía de las sanciones se graduará atendiendo** a los siguientes criterios:*

a) El carácter continuado de la infracción.

b) El volumen de los tratamientos efectuados.

c) La vinculación de la actividad del infractor con la realización de tratamientos de datos de carácter personal.

d) El volumen de negocio o actividad del infractor.

e) Los beneficios obtenidos como consecuencia de la comisión de la infracción.

f) El grado de intencionalidad.

g) La reincidencia por comisión de infracciones de la misma naturaleza.

h) La naturaleza de los perjuicios causados a las personas interesadas o a terceras personas.

i) La acreditación de que con anterioridad a los hechos constitutivos de infracción la entidad imputada tenía implantados procedimientos adecuados de actuación en la recogida y tratamiento de los datos de carácter personal, siendo la infracción consecuencia de una anomalía en el funcionamiento de dichos procedimientos no debida a una falta de diligencia exigible al infractor.

j) Cualquier otra circunstancia que sea relevante para determinar el grado de antijuridicidad y de culpabilidad presentes en la concreta actuación infractora.

SANCIONES (II)

CRITERIOS

El órgano sancionador establecerá la cuantía de la sanción aplicando la escala relativa a la clase de infracciones que preceda inmediatamente en gravedad *a aquella en que se integra la considerada en el caso de que se trate,* ***en los siguientes supuestos:***

a) Cuando se aprecie una cualificada disminución de la culpabilidad del imputado o de la antijuridicidad del hecho como consecuencia de la concurrencia significativa de varios de los criterios enunciados en el apartado 4 de este artículo.

b) Cuando la entidad infractora haya regularizado la situación irregular de forma diligente.

c) Cuando pueda apreciarse que la conducta del afectado ha podido inducir a la comisión de la infracción.

d) Cuando el infractor haya reconocido espontáneamente su culpabilidad.

e) Cuando se haya producido un proceso de fusión por absorción y la infracción fuese anterior a dicho proceso, no siendo imputable a la entidad absorbente.

Excepcionalmente el órgano sancionador podrá, previa audiencia de los interesados y atendida la naturaleza de los hechos y la concurrencia significativa de los criterios establecidos en el apartado anterior, no acordar la apertura del procedimiento sancionador y, en su lugar, apercibir al sujeto responsable a fin de que, en el plazo que el órgano sancionador determine, acredite la adopción de las medidas correctoras que en cada caso resultasen pertinentes, siempre que concurran los siguientes presupuestos:

a) Que los hechos fuesen constitutivos de infracción leve o grave conforme a lo dispuesto en esta Ley.

b) Que el infractor no hubiese sido sancionado o apercibido con anterioridad.Si el apercibimiento no fuera atendido en el plazo que el órgano sancionador hubiera determinado procederá la apertura del correspondiente procedimiento sancionador por dicho incumplimiento.

CÓDIGO PENAL (I)

Del descubrimiento y revelación de secretos

Artículo 197

1. El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.
2. Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.
3. El que por cualquier medio o procedimiento y vulnerando las medidas de seguridad establecidas para impedirlo, acceda sin autorización a datos o programas informáticos contenidos en un sistema informático o en parte del mismo o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años.

Cuando de acuerdo con lo establecido en el artículo 31 bis una persona jurídica sea responsable de los delitos comprendidos en este artículo, se le impondrá la pena de multa de seis meses a dos años. Atendidas las reglas establecidas en el artículo 66 bis, los jueces y tribunales podrán asimismo imponer las penas recogidas en las letras b) a g) del apartado 7 del artículo 33.

4. Se impondrá la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores.

CÓDIGO PENAL (II)

Será castigado con las penas de prisión de uno a tres años y multa de doce a veinticuatro meses, el que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realizare la conducta descrita en el párrafo anterior.

5. Si los hechos descritos en los apartados 1 y 2 de este artículo se realizan por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros, se impondrá la pena de prisión de tres a cinco años, y si se difunden, ceden o revelan los datos reservados, se impondrá la pena en su mitad superior.
6. Igualmente, cuando los hechos descritos en los apartados anteriores afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere un menor de edad o un incapaz, se impondrán las penas previstas en su mitad superior.
7. Si los hechos se realizan con fines lucrativos, se impondrán las penas respectivamente previstas en los apartados 1 al 4 de este artículo en su mitad superior. Si además afectan a datos de los mencionados en el apartado anterior, la pena a imponer será la de prisión de cuatro a siete años.
8. Si los hechos descritos en los apartados anteriores se cometiesen en el seno de una organización o grupo criminales, se aplicarán respectivamente las penas superiores en grado.

CÓDIGO PENAL (III)

Artículo 198

La autoridad o funcionario público que, fuera de los casos permitidos por la Ley, sin mediar causa legal por delito, y prevaliéndose de su cargo, realizare cualquiera de las conductas descritas en el artículo anterior, será castigado con las penas respectivamente previstas en el mismo, en su mitad superior y, además, con la de inhabilitación absoluta por tiempo de seis a doce años.

Artículo 199

1. El que revelare secretos ajenos, de los que tenga conocimiento por razón de su oficio o sus relaciones laborales, será castigado con la pena de prisión de uno a tres años y multa de seis a doce meses.
2. El profesional que, con incumplimiento de su obligación de sigilo o reserva, divulgue los secretos de otra persona, será castigado con la pena de prisión de uno a cuatro años, multa de doce a veinticuatro meses e inhabilitación especial para dicha profesión por tiempo de dos a seis años.

CONCLUSIONES PRIVACIDAD BIG DATA:

- =Poder de disposición y control de los datos por parte de los individuos
- Dimensión individual (derechos)
- Dimensión responsable (obligacional)
- **Realización EIPD (privacy by design y accountability)**
- **Equipos multidisciplinares**
- **Anonimización**

ASPECTOS ÉTICOS

Aspectos éticos I

¿Qué puede hacer el Big Data?

Ámbitos de actuación

- Lo que es técnicamente posible
- Lo que querría hacer la empresa
- Lo que es legalmente posible
- Lo que es éticamente posible

Aspectos éticos II

Algunas empresas están desarrollando un enfoque respecto al Big Data que no se refiere únicamente a las capacidades de la analítica o al cumplimiento de la legislación de protección de datos, pero también examina el Big Data en un contexto más amplio y esencialmente ético.

De forma que no sólo cabe preguntarse “¿podemos hacer esto con los datos?", es decir, cumplimos los requisitos normativos, sino también “¿*d*eberíamos hacer esto con los datos? ", es decir ¿que es lo que los clientes esperan o deben esperar?

Aspectos éticos III

Es significativo que **estos marcos se han desarrollado** no por los autoridades, sino **por las mismas empresas**, como una respuesta a la situación en la que se encuentran en el entorno del Big Data.

Estos enfoques se derivan de la preocupación por la propia **relación entre la empresa y sus clientes**.

Sin embargo, es de destacar que **muchos aspectos de estos marcos**, tanto de las empresas como de marcos propuestos **plasman principios y requisitos clave de la protección de datos .**

Aspectos éticos IV

"**TRUST ADVANTAGE**" :

Concepto acuñado por The Boston Consulting Group.

La **organización más confiable** para los clientes **accederá a**, al menos, **cinco a diez veces más datos** que la que dé menos confianza .

Esto, a su vez, dará lugar a mejores recomendaciones online, focalización más precisa , más rápido desarrollo de nuevos productos y servicios, y otros beneficios tangibles a los consumidores . Esta es la ventaja de la confianza .

También ser una **ventaja competitiva para una organización el ser visto como responsable y custodio confiable de datos de sus clientes.**

Aspectos éticos V

IAF Big Data Ethics Initiative

Se hace referencia, por su interés, a este proyecto de The Information Accuontability Foundation (IAF)‘que trabaja en un futuro código ético para procesos de Big data para aquellas organizaciones que se adhieran a él.

La Agencia Española de Protección de Datos y otras Agencias han participado en el mismo.

Aspectos éticos VI

IAF Big Data Ethics Initiative

El UEF **separa el big data analytics en dos fases: "Discovery" and "Application."**

"Building on prior work, the UEF separated big data analytics into two phases, "Discovery" and "Application."

Generally, Discovery is where new insights, which go beyond experience and intuition, and come instead from correlations among data sets, are aggregated. Application is where these insights are put into effect and where individuals may be particularly affected in these insights are employed in an individually unique manner. ***The Application phase is more often individually impactful, while risks related to false insights are more of a concern in the Discovery phase.*** *Organizations should assess the risks and benefits of analysing data as part of both phases."*

Aspectos éticos VII

IAF Big Data Ethics Initiative

Hay cuatro momentos en el Big Data Analitics en el que tiene sentido aplicar Marco de Evaluación :

1) Concept

Before any real analytics takes place, organizations should brain storm the reasons for using all the intended data sets, new data created, chances for new insights, usefulness of those insights, and possibilities of further application. The results of this process should be presented to decision makers for a determination on whether to proceed to the actual Discovery phase.

2) Discovery

The research to generate new insights takes place during the Discovery phase. It is during this phase that data is aggregated, formatted, enhanced, or created. While this process will vary based on sector and industry, at some organizations, pre-analysis will take place at the concept phase.

The Assessment Framework may include similar questions during both the Concept and Discovery phases. It is unnecessary to repeat questions during both phases. Rather, the assessment should be customized for different sectors and industry practices.

Aspectos éticos VIII

IAF Big Data Ethics Initiative

Hay cuatro momentos el Big Data Analytics en el que Marco de Evaluación tiene sentido:

3) Application

Between the completion of the Discovery phase and the commencement of the Application phase, a decision to move forward or not is made. Beyond the objectives or interests of the organization, the organization must determine whether the analytics will create real benefits and who will receive those benefits; whether the insights will be sustainable once analytics commences; whether improvements in analytics are significant enough to justify more robust big data analytics; and whether the application is respectful and fair. Much of this evaluation may have taken place at the Concept and Discovery phases, and if that reasoning is still relevant, it does not need to be repeated. Key questions should not be ignored, and the decision maker is responsible for the integrity of the process.

4) Review

In order to assure controls are working, ongoing reviews are required. An ethical review should take place when routine reviews of new applications of data are scheduled. The level of the ethical review should be proportional to the constant evolution of the programs. New data sets may have been introduced, or processing shortcuts may have been developed.

Aspectos éticos IX

IAF Big Data Ethics Initiative

El UEF también establece cinco valores clave que actúan como una brújula para una revisión ética:

1) Beneficious

Both the discovery and application phases require an organization to define the benefits that will be created by the analytics and **should identify the parties that gain tangible value from the effort**. The act of big data analytics **may create risks for** some **individuals and benefits for others** or society as a whole.

2) Progresive

Because bringing large and diverse data sets together and looking for hidden insights or correlations may create some risks for individuals, the value from big data analytics should be materially better than not using big data analytics.

Organizations should not create the risks associated with big data analytics if there are other processes that will accomplish the same objectives with fewer risks

IAF Big Data Ethics Initiative

El UEF también establece cinco valores clave para actuar como una brújula para la revisión ética

3) Sustainable

All algorithms have an effective half-life – a period in which they effectively predict future behaviour. Some are very long, others are relatively short. Models used in the mortgage securitization market to assign risk to sub-prime mortgages in the first decade of this century are examples of data scientists not understanding how the models themselves would influence the behaviour of various market players.

Big data analysts should understand this concept and articulate their best understanding of how long an insight might endure once it is reflected in application.

For example, an early application of big data analytics led to a significant reduction in fraud when the discovery phase produced new insights showing a significant portion of identity fraud was not identity theft but rather came from synthetic or manufactured identities. Later insights showed that the fraudsters changed the makeup of those fake identities as organizations improved their processes to catch them. As a result, the predicative algorithms were continually refined to sustain their effectiveness in detecting and preventing fraud.

Aspectos éticos XI

IAF Big Data Ethics Initiative

El UEF también establece cinco valores clave para actuar como una brújula para la revisión ética

4) Respectful

Respectful **relates directly to the context in which the data originated and to the contractual or notice related restrictions on how the data might be applied.**

- The United States Consumer Privacy Bill of Rights speaks to data being used within context;
- **European law discusses processing not incompatible to its defined purpose; and**
- Canadian law allows for implied consent for evolving uses of data.

Organizations using big data analytics should understand and respect the interests of all the stakeholders involved in, or affected by, the application. Anything less would be disrespectful.

Aspectos éticos XII

El UEF también establece cinco valores clave para actuar como una brújula para la revisión ética

5) Fairness

Fairness relates to the insights and applications that are a product of big data, while respectful speaks to the conditions related to, and the processing of, the data. In lending and employment, United States law prohibits discrimination based on gender, race, genetics or age. Yet, big data processes can predict all of those characteristics without actually looking for fields labelled gender, race or age. The same can be said about genotypes, particularly those related to physical characteristics. Section 5 of the United States Federal Trade Commission Act prohibits unfair practices in commerce that are harmful to individuals not outweighed by countervailing benefits. **European guidance on application of the data protection directive continually references fairness as a component of determining whether a use of data is incompatible or a legal basis to process is appropriate. Big data analytics, while meeting the needs of the organization that is conducting or sponsoring the processing, must be fair to the individuals to whom the data pertains.**

The analysis of fairness needs to look not only at protecting against unseemly or risky actions but also at enhancing beneficial opportunities. Human rights speak to shared benefits of technology and broader opportunities related to employment, health and safety. Interfering with such opportunities is also a fairness issue.

In conducting this fairness assessment, organizations should take steps to balance individual interests with integrity.

Aspectos éticos XIII

Ejemplo 1: AIMA

Han desarrollado un conjunto de valores con las siglas TACT, que significa Transparency, Added value, Control and Trust..

- Transparencia

significa decirle a los clientes qué datos son siendo recopilada , cómo se recopila y cómo se está utilizado.

- Valor añadido

significa hacer que los clientes conscientes de que recibirán recompensas por su participación.

- Control

Se refiere a dar a los clientes el control sobre los datos que proporcionan y lo que les permite compartir y optar.

-Confianza

significa dar clientes la confianza de que los datos sólo se utilizarán en la forma descrita por Aimia

Aspectos éticos XIV

Ejemplo 2: IBM

have been developing **an ethical framework** for big data analytics. They say that big data has "widened the gap between what is possible and what is legally allowed".

Their ethical framework takes account of:

- the context in which the data will be collected and used;
- whether people will have a choice in giving their data;
- whether the amount of data and what will be done with it is reasonable in terms of the application;
- the reliability of the data;
- **who owns the insights to be gained from the data;**
- **whether the application is fair and equitable; the consequences of processing.**
- people's access to the data; and accountability for mistakes and **unintended consequences.**

Aspectos éticos XV

CONCLUSIONES

- Conveniencia de incorporar un análisis ético mas allá del cumplimiento normativo.
- ¿Análisis ético junto/incorporado dentro del EIPD?
  - Adopción estándares (p.e. UEF)
- “Trust advantage”
- Dificultad: las diferencias de lo que es ético entre países
- mantener actualizado el análisis ético

Otros aspectos legales

- **Información como activo**

  (p.e. due diligence de compraventa de empresas: valoración usuarios. Datos personales en el centro del negocio)

- **Big Data como activo**.

  Propiedad intelectual (Bases de datos, secreto industrial o empresarial know how empresarial).

- **Derecho de la Competencia desleal**
- **Derecho de la competencia**
- **Responsabilidad**
- **Ley consumidores y usuarios y comercio electrónico**

CONTACTO

Pedro Bennasar Cabrera

pedro.bennasar@tc-abogados.com

Teléfono: (+34) 91 310 66 60 (+34) 670 647 153

LinkedIn

https://www.linkedin.com/pub/pedro-bennasar/12/bb7/17a

@BennasarP

CIFF

Centro Internacional
de Formación Financiera

CIFF Trustees:

Santander

Universidad de Alcalá