Protección de datos

"[…] en el momento en que tienen nuestra dirección, estado civil, edad, ingresos, marca del coche, compras, hábitos de bebida e impuestos, ya nos han cazado: somos una unidad demográfica de una persona" (Negroponte, 2003)

El principal objetivo de este tema es ofrecer un acercamiento al marco legal de la protección de datos personales en Europa, con un especial interés en lo que respecta a España.

Como objetivos de aprendizaje, destacamos el sintetizar los elementos fundamentales de la protección de datos, y argumentar el texto legal aplicable ante casos reales.

Advirtamos en este momento que los presentes apuntes no pretenden en ningún momento sustituir la consulta de la legislación, sino simplemente servir de apoyo docente. Es preciso dejar claro que se simplifica la misma para poder dar cuenta de ella en el tiempo reservado por los planes docentes, por lo que para concretar el conocimiento de cara a su ejecución práctica, se hace imprescindible acudir al texto legal. Para que los apuntes actuales sirvan de hoja de ruta, cuando se cite un derecho concreto, se indicará cual es el artículo de la norma concreta donde este puede ser consultado de forma entera y no resumida.

El eje que vertebrará estos apuntes será el Reglamento Europeo de Protección de Datos, así como su reflejo en la legislación española, nuestra Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, en adelante Ley 3/2018, aunque obviamente no serán las únicas normas aludidas.

Introducción

Cuando abordamos el tema de la protección de datos personales, debemos tener en cuenta que tratamos de la protección de un derecho constitucional fundamental, que ya en 1978 se recogía en nuestra Constitución.

Artículo 18 C.E.

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.

Debemos ser conscientes de que se trata de un asunto que genera mucha confusión: además de considerarlo derecho fundamental, escuchamos que se identifica con muchos otros términos: privacidad, intimidad, secreto, derecho fundamental, ley… vemos como las palabras "protección de datos" nos hace pensar en muchas cosas.

Quizá la respuesta estribe en que se trata de un poco de todo. Hablamos de un derecho fundamental, de una disciplina jurídica, de Ley Orgánica… de todo a la vez. Aunque para nosotros va a ser, de forma principal, casi sinónimo de "ley". De la ley que deben aplicar y conocer al menos en sus partes fundamentales todos los profesionales de la información que de algún modo trabajen con datos de carácter personal. Y, para ayudar a centrar el asunto, descubramos ya cual es el texto legal por excelencia de este tema: el Reglamento Europeo de Protección de Datos (Diario Oficial de la Unión Europea, 2016)[1], y fijémonos en particular en los artículos 2º y 3º, donde se delimita el ámbito del Reglamento (idéntico a lo que nos dice el artículo 1º de la Ley 3/2018 (BOE, 2018), en adelante omitiremos estas similitudes en aras de una lectura más ligera. Si no se indica lo contrario, en todo momento los artículos y considerandos citados son referencias del Reglamento)

Descubrimos que se aplica al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero, aunque con una larga serie de excepciones. Así, vemos que no se aplica en el ejercicio de una actividad no comprendida en el ámbito de aplicación del Derecho de la Unión; cuando se trate del tratamiento efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas o cuando se trata de un tratamiento realizado por las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención.

Vemos que se aplica el Reglamento a las personas físicas, pero no se regula el tratamiento de datos personales relativos a personas jurídicas y en particular a empresas constituidas como personas jurídicas, incluido el nombre y la forma de la persona jurídica y sus datos de contacto. (Considerando 14)

Concretamente, el ámbito del Reglamento será el tratamiento de datos personales en el contexto de las actividades de un establecimiento del responsable[2] o del encargado en la Unión, independientemente de que el tratamiento tenga lugar en la Unión o no. Se aplica sobre aquellos interesados que estén en la Unión por parte de un responsable o encargado no establecido en la Unión, cuando las actividades de tratamiento estén relacionadas con la oferta de bienes o servicios, el control de su comportamiento, si este tiene lugar en la Unión.

[1] Como va a ser esta norma empleada de forma exhaustiva, omitiremos incluso su cita. Así, si hablamos de artículos o considerandos, lo hacemos en todo momento en alusión al Reglamento Europeo de Protección de Datos, si no se indica otra cosa. Omitimos, salvo citas textuales donde se referencie así, las siglas anglosajonas GDPR que aluden al mismo.

[2] En breve, veremos las definiciones de las figuras principales: responsable del tratamiento, encargado del tratamiento y delegado de datos.

Vemos que aparecen ya palabras que necesitan ser definidas: por ejemplo, el responsable o encargado del tratamiento. En unas pocas páginas, podremos encontrarlas en este mismo tema.

La protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental, como avanzábamos pero que además queda refrendado por el Reglamento en su primer considerando. Y aún más, se indica expresamente que el tratamiento de datos personales debe estar concebido para servir a la humanidad. Pero se añade un matiz que nos dará mucho juego: el derecho a la protección de los datos personales no es un derecho absoluto sino que debe considerarse en relación con su función en la sociedad y mantener el equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad. (Considerando 4). Esto ya lo anticipaba (Davara Rodríguez, 1998) una década antes del texto literal del Reglamento.

El Reglamento no se aplica a cuestiones de protección de los derechos y las libertades fundamentales o la libre circulación de datos personales relacionadas con actividades excluidas del ámbito del Derecho de la Unión, como las actividades relativas a la seguridad nacional. Tampoco se aplica al tratamiento de datos de carácter personal por los Estados miembros en el ejercicio de las actividades relacionadas con la política exterior y de seguridad común de la Unión (considerando 16). De igual modo, tampoco se aplica al tratamiento de datos de carácter personal por una persona física en el curso de una actividad exclusivamente personal o doméstica (como la correspondencia, una agenda personal o la actividad en las redes sociales). Si se aplica a los responsables o encargados del tratamiento que proporcionen los medios para tratar datos personales relacionados con tales actividades personales o domésticas (considerando 18).

Debemos tener claro que el derecho no es un conjunto de disciplinas autoexcluyentes. Muchas veces se solapan entre sí, como en este caso, por ejemplo, sucede con las normas que rigen la libertad de expresión e información, incluida la expresión periodística, académica, artística o literaria, y el derecho a la protección de los datos personales. A este respecto el tratamiento de datos personales está sujeto a excepciones o exenciones si así se requiere para conciliar el derecho a la protección de los datos personales con otros derechos (Considerando 153)

El problema que surge al regular cualquier derecho fundamental es que debe hacerse sin poner en peligro otros derechos fundamentales. Sin embargo, el que dos derechos no entren en colisión es prácticamente utópico (De Miguel Molina & Oltra Gutiérrez, 2007). En la protección de datos, normalmente se entrará en colisión con otros dos derechos fundamentales:

- el derecho a la información,
- la libertad de expresión.

Además, la colisión con las normas de transparencia resulta evidente. ¿Qué hacer entonces? Los Tribunales aplican en este caso el principio de proporcionalidad, pues habrá que ver en cada caso concreto qué derecho prevalece. El derecho a la información no es un derecho absoluto, como tampoco lo es la libertad de expresión, y normalmente los Jueces y Magistrados siempre se volcarán más hacia la intimidad del individuo que hacia los otros

derechos. Otra cosa será que haya razones de interés general que aconsejen otra medida. Sin pretender generalizar, lo cierto es que tanto el Tribunal Constitucional como el Supremo resuelven normalmente que el derecho a la intimidad prevalece frente al derecho a la información.

Tratamiento vs libertad de expresión
¿Cuál debe primar? No hay una receta única. El Reglamento, nos dice que deben conciliarse ambos, generando exenciones o excepciones. (Artículo 85) Curiosamente, otro artículo 85, este el de la Ley 3/2018 nos dice expresamente que "Todos tienen derecho a la libertad de expresión en Internet".

La rápida evolución tecnológica y la globalización han planteado nuevos retos para la protección de los datos personales desde la anterior normativa. Se ha incrementado la magnitud de la recogida y del intercambio de datos personales permitiendo las TIC que empresas privadas y autoridades públicas utilicen datos personales en una escala sin precedentes a la hora de realizar sus actividades. Datos que muchas veces salen directamente de los usuarios en una difusión voluntaria (redes sociales, por ejemplo). No hace falta que recordemos que en nuestra sociedad los datos personales son potencialmente generadores de lo mejor y de lo peor: mientras vemos como la Inteligencia Artificial apoyada en grandes bases de datos médicos comienza a aplicarse en plenitud a la medicina, en paralelo nos enteramos de cómo en China se es capaz de identificar a 200 personas por minuto, estudiar su comportamiento pasado presente y predeciblemente futuro y otorgar así carnets de buenos ciudadanos. En este mundo donde la intimidad parece haberse dado la vuelta como un calcetín y que se nutre de "likes" y retuits, es importante generar confianza que permita a la economía digital desarrollarse en todo el mercado interior europeo. Las personas físicas deben tener el control de sus propios datos personales. Hay que reforzar la seguridad jurídica y práctica para las personas físicas, los operadores económicos y las autoridades públicas. (Considerandos 6 y 7) En busca de esa seguridad, y de los derechos de los ciudadanos, hay que minimizar las diferencias en las normas de los países de la Unión, pues pueden constituir un obstáculo al ejercicio de las actividades económicas a nivel de la Unión (Considerando 9).

Un elemento de mucho interés aparece cuando el Reglamento se destapa con una indicación que nos afecta de forma importante como tecnólogos: se dice expresamente que la protección de las personas físicas debe ser tecnológicamente neutra y no debe depender de las técnicas utilizadas. Esto implica que en materia de selección de elementos software y hardware debemos mantener "posturas agnósticas", que sirvan al fin con independencia del medio.

No hay que olvidar tampoco algo que ya heredamos de atrás, de normas anteriores (como por ejemplo la Ley Orgánica de Protección de Datos de 1999, (BOE, 1999)): la protección de las personas físicas debe aplicarse al tratamiento automatizado de datos personales, así como a su tratamiento manual, cuando los datos personales figuren en un fichero o estén destinados a ser incluidos en él.

Esto es: una carpeta de gomas con fichas de clientes… es un fichero a proteger.

Pero a pesar de eso, hay una pequeña indicación que puede evitarnos mucho trabajo técnico, que por su importancia no debemos olvidar: los ficheros o conjuntos de ficheros, así como sus portadas, que no estén estructurados con arreglo a criterios específicos, no deben entrar en el ámbito de aplicación del presente Reglamento. (Considerando 15)

Por otra parte, no podemos dejar de subrayar que no es, ni con mucho, la única legislación a tener en cuenta a la hora de tratar con datos. A este respecto, resulta interesante la consulta del texto de García Mirete (García Mirete, 2014). Por ejemplo, cuando hablamos de uso de datos en comunicaciones electrónicas, debemos referenciar a la LSSI. (BOE, 2002). No debemos olvidar tampoco que las leyes son interpretadas por los jueces y muchas veces debemos prestar especial atención a estas interpretaciones[3].

Para cerrar este apartado de introducción, vamos a intentar eliminar algunas confusiones típicas.

La primera de ellas es la que viene cuando se confunden palabras como datos, información e informática. Un dato es difícil que por sí solo pueda tener incidencia grave en la llamada privacidad (Davara Rodríguez, 1998): mientras el dato no resuelva una consulta determinada, no dé respuesta a una pregunta o solución a un problema, puede ser un antecedente pero poco más. La información es esa pared que construimos con datos, y eso ya es un soporte firme. Si sometemos la información a tratamiento (tratamiento que suele ser informático, por lo complejo que resulta hacer manualmente acciones con grandes cantidades de datos), ya tenemos un resultado útil para un fin determinado. Y potencialmente peligroso, según sea ese fin. Con la informática se ofrecen múltiples posibilidades de almacenamiento y tratamiento de la información, y de recuperación de la misma, de formas tan variadas e invisibles para el ciudadano que puede llegar a producir verdadera presión y control social. El cruce de datos entre bases de datos, con su implícito tratamiento automático provoca en ocasiones la pérdida de control del titular de los datos, que no es ni más ni menos que la persona a quien estos datos describen.

Pero aún queda otro punto de confusión: ¿todos los datos personales son iguales? ¿Tienen la misma importancia? ¿Qué padezcamos una enfermedad degenerativa y se haga público ente las compañías aseguradoras tiene el mismo valor que el dato de nuestro número de teléfono o el nombre de nuestro padre? ¿Y si el dato lo hemos revelado en un blog, o si procede de un listado público? Aunque ahondaremos en este asunto más adelante, vale la pena emplear un

[3] Ejemplos hay muchos. Citemos dos, por no hacer esto muy largo.
La STC 202/1999, 8 de noviembre. Recurso de amparo contra las Sentencias de la Sala de lo Social del Tribunal Superior de Justicia de Cataluña y del Juzgado de lo Social nº 2 de Barcelona que deniegan la cancelación de los datos médicos del recurrente los cuales se encontraban en un fichero informático sobre "absentismo con baja médica" de la entidad crediticia donde este trabajaba. Se trata de: Vulneración de derecho a la intimidad, negativa a la cancelación de datos, quiebra de la garantía de la confidencialidad de los mismos e inexistencia de responsable de fichero. Se otorga el amparo.
Un último ejemplo. Obsérvese que intencionalmente he escogido sentencias antiguas, anteriores a la propia LOPD, para que puedan ser comparados sus efectos con las normas que hoy nos rigen. Sentencia T.S.J. de Andalucía de 6 de octubre de 1995: Los Ayuntamientos están excluidos de la obligación de facilitar los datos obrantes en el padrón a efectos de embargos y otras diligencias ejecutorias, de forma que deben suministrar datos a los servicios estadísticos estatales a los solos efectos de elaborar estadísticas.

gráfico en este momento para establecer, a modo de capas, la mayor o menor incidencia en nuestra vida de los distintos tipos de datos.

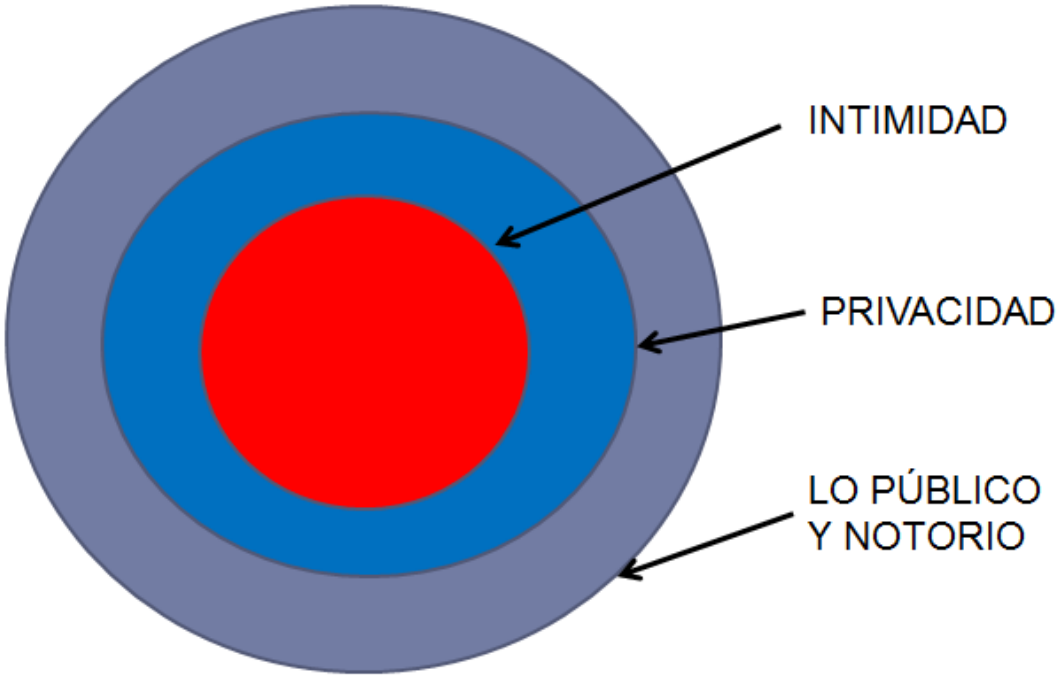


Ilustración 1. De lo íntimo a lo público. Elaboración propia.

Hemos visto de forma muy general que es esto de la protección de datos, que protege. Y parece que es una cosa nueva, que surge con las TIC. Pero en realidad es algo que siempre, de alguna manera ha estado aquí. Vamos a verlo.

Un poco de historia

En la antigua Grecia nada parecido a la protección de datos existía. Es en Roma cuando aparece el derecho de propiedad del yo. Se habla de un hombre exterior, y otro interior.

El tiempo pasa, y en la Edad Media aparece San Agustín hablando del hombre como portador de valores y Santo Tomás de Aquino considerando la intimidad como un bien sagrado. Lo privado existe, pero se resume y recae sobre el "pater familias". Sigue avanzando la historia y en la Edad Moderna, con "La razón" y sus filósofos, aparece una nueva vuelta de tuerca. Locke, y su concepto de la "libertad negativa" reconocen al individuo una esfera íntima. Rousseau añade la intimidad desde el ámbito de la persona. Y con estas vueltas llegamos al siglo XX, donde empieza a jugar la baza un nuevo participante, la informática, y al XXI, donde parece haberse quedado con toda la partida.

Hoy en día, sabemos que los datos son propiedad del titular, del ciudadano. La información sacia las ansias de poder de muchos, pues poder es información. La intimidad ahora sube de nivel, no solo es ocultamiento, reserva, sino la capacidad de decidir en la esfera íntima.

Vemos como la privacidad, la intimidad de las personas, es algo que nos ha preocupado siempre a los seres humanos. Incluso en las casas romanas donde vivía la no-élite, donde se hacinaban las familias, las personas buscaban sus lugares para la intimidad, sus secretos particulares que no deseaban que se hicieran públicos. Pero, entonces lo que preocupaba era el rumor. Hoy, es la red de redes. Hay un pequeño matiz en ello. La informática ha supuesto una herramienta importante para todo, bien y mal. Para quebrar esa intimidad también. Es lógico que crecieran las normas al respecto.

En España, por hacer una vista rápida a nuestra particular historia del derecho, podríamos viajar en el pasado hasta la ley de 11 de enero 1541 donde el emperador Carlos I dota de inviolabilidad a las cartas. Algo que se extiende ya en un momento tan tardío como la Constitución de 1869 a la inviolabilidad de domicilio y por primera vez, al secreto de la correspondencia y efectos personales.

En el siglo XX, la única referencia previa a nuestra Constitución actual la encontramos en el Fuero de los Españoles de 17 julio de 1945. En su Título preliminar aparece un principio fundamental: el respecto a la dignidad y libertad humanas. Y llegamos al marco actual, con el año 1978 donde la Constitución se promulga, y tras la Constitución, aparecen unas cuantas leyes, que van marcando el camino:

- LO 1/1982, de5 de mayo, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen
- 16/1985 de Patrimonio histórico español
- 13/1986 de Fomento y coordinación general de la investigación científica y técnica
- Otras: 12/1989 Reguladora de la función estadística pública

Por supuesto, aparece la LORTAD, Ley Orgánica de Regulación del Tratamiento Automatizado de los Datos de carácter personal en el 92, ley precedente y casi madre de la LOPD, Ley Orgánica de Protección de Datos de carácter personal, del 99, y a nuestra actual Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Pero por el camino van surgiendo algunas leyes que matizan algunos aspectos. Por ejemplo:

- Ley 34/2002 de 11 de julio de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI).
- Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información.
- Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones. (Ley ad hoc para la lucha contra el terrorismo y crimen organizado)
- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.

Podríamos hacer mucho, mucho más largo este listado. Pero por definir concretamente nuestro marco, dejemos claro lo esencial, partiendo de esa piedra basal que es el Artículo 18 de la Constitución:

> *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.*

Con este parco punto de partida, apareció en su momento, condicionado por el protocolo de Schengen, "Espacio de Libertad, Seguridad y Justicia") (Goizueta Vértiz, González Murua, & Pariente, 2013) nuestra extinta LORTAD, Ley Orgánica 5/1992, de 29 de octubre. Ley que fue modificada mediante Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la LORTAD y reglamentada con el Real Decreto 994/1999, de 11 de junio, Reglamento de Medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal. Esto es: poco a poco el legislador va construyendo el edificio legal.

Y cuando parecía terminado, una Directiva Comunitaria (95/46/CE de 24/octubre/95) exigía la extensión a ficheros manuales. Eso provocó el nacimiento de la LOPD, Ley Orgánica 15/1999, de 13 de diciembre, y posteriormente del Real Decreto 1720/2007, de 21 de diciembre, Reglamento de desarrollo de la Ley Orgánica 15/1999. Ley que ya ha quedado obsoleta, por la necesaria entrada en vigor del Reglamento Europeo de Protección de Datos, que nos ha traído hasta la actual Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Podemos ver un hilo temporal en la siguiente imagen.

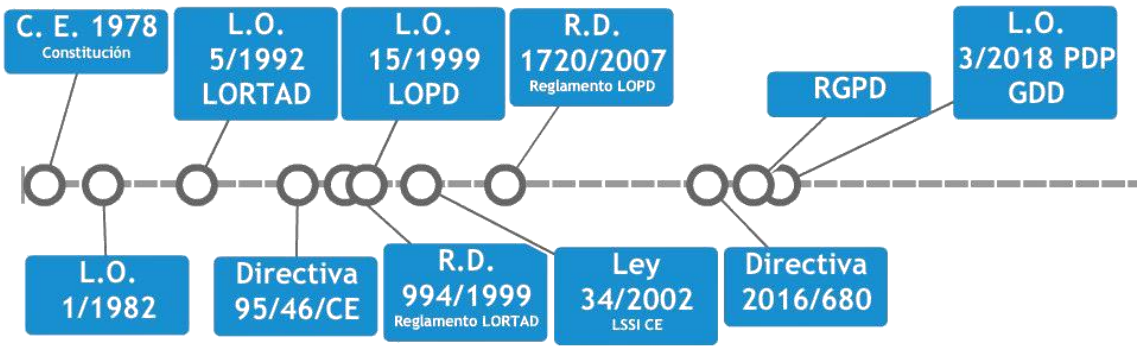


Ilustración 2. Legislación principal sobre protección de datos que afecta a España (elaboración propia)

¿Y qué ocurría en "El mundo", fuera de nuestras fronteras?

En los ordenamientos de ámbito anglosajón se le hadado en llamar "privacy", aquí españolizado como "privacidad" (Davara Rodríguez, 1998). No es exactamente lo mismo, pero atendiendo a la segunda acepción del diccionario de la RAE ("Ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión), podemos establecer para nuestro trabajo una cierta identidad. (Real Academia Española, 2017). Cabe indicar que, si rastreamos textos del otro lado del charco escritos en inglés con el término "privacy" podemos observar algunas diferencias, que no es momento de relacionar.

¿Cuándo se cifra el origen de la privacidad en el mundo anglosajón?

Parece haber una coincidencia generalizada en indicar que fueron Samuel D. Warren y Louis D. Brandeis (Warren & Brandeis, 1890) quienes en su "Derecho a la privacidad" fundamentaron en el principio de inviolabilidad a la persona los límites jurídicas a la intromisión en la vida de las mismas. Garriga (Garriga Domínguez, 2010) indica que poco después de su aplicación se empieza a usar por un tribunal de Nueva York empleando la expresión acuñada (*the right to privacy*), que a partir de ese momento se multiplicaría en resoluciones judiciales (aunque también se usará con el curioso nombre de "Derecho a ser dejado en paz").

En Estados Unidos (seguimos a Garriga en este punto) William Prosser publica en 1960 un ensayo usando las líneas maestras de Warren y Brandeis, sentando las posibles violaciones del derecho a la intimidad en la sociedad moderna. En el año siguiente, 1961, la idea salta el charco y se suceden en el Reino Unido diversos proyectos de ley para la creación de un derecho autónomo a la intimidad. Aparecen los estudios de Frosini, Alan F. Westin y en nuestro país de Pérez Luño, que divulgan a lo largo de los dos continentes estas ideas. (Garriga Domínguez, 2010). Conviene precisar, ya que hemos mencionado diferencias entre ambos conceptos, que mientras en Europa se habla de protección de datos, en Estados Unidos se habla de privacidad sin abordar propiamente cuál es el objeto de protección y qué medios técnicos pueden contribuir a proteger los datos.

Sin ceñirnos al ámbito anglosajón, ya en 1948 el derecho a la intimidad es recogido en el artículo 12 de la Declaración de los derechos humanos, y muy poco después, se refleja en el artículo 8 del Convenio de Roma, en 1950.

En mayo de 1967, en la Conferencia de Juristas Nórdicos, se aconseja la protección de la vida privada mediante instrumentos específicos y más adecuados a las nuevas formas de injerencia. Nace en Europa el espíritu de la protección de datos. Esto da paso a la creación de una Comisión consultiva del Consejo de Europa, para estudiar las tecnologías de la información y su influencia sobre los derechos de la persona, que a su vez emite la Resolución 68/509/CE de la Asamblea del Consejo de Europa, sobre "los derechos humanos y los nuevos logros científicos y técnicos ".

En un ámbito superior, en la ONU, mientras tanto, el 19 de diciembre de 1968 aparece la Resolución 2450 (XXIII), donde se establece la necesidad de fijar límites a las aplicaciones de la electrónica, que culmina en 1983 con un informe relativo a los principios respecto a la utilización de los ficheros informatizados de carácter personal.

El mundo sigue girando y en 1970, el 23 enero, surge la resolución 428 de la Asamblea Consultiva del Consejo de Europa: "Intimidad como un objeto de obligada protección frente a la intromisión de la tecnología de la información". Esto da paso a que en 1973 surja la resolución (22) de 26 de septiembre: "Protección de la vida privada de las personas físicas frente al sector privado" y en 1974(29) lo mismo, sobre el sector público. Pueden verse unas interesantes reflexiones sobre las resoluciones 1973(22) y 1974(29) en el texto de Davara referenciado en bibliografía (Davara Rodríguez, 1998). Es el momento en que empiezan a inspirarse algunos estados, como el alemán, para aprobar leyes como la de Hesse, de 1970, que busca proteger el derecho de la personalidad restringiendo la utilización de datos

personales que pudieran afectar a los ciudadanos por parte de la administración. Muy pronto, en 1974, se promulga la primera Privacy Act de los Estados Unidos de Norteamérica. Es en esta etapa cuando se introduce la idea de la protección efectiva a las personas frente al uso informatizado de los datos. Una tercera etapa viene marcada por la internacionalización de la protección del derecho fundamental a la autodeterminación informativa. (Garriga Domínguez, 2010)

En 1980, el 28 de septiembre, el Consejo de Ministros del Consejo de Europa da luz al convenio para la protección de las personas respecto al tratamiento automatizado de datos de carácter personal. Es el Convenio 108 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal del Consejo de Europa (publicado en 1981). Aquí se intenta armonizar el principio de libre circulación internacional de datos personales con la defensa de derechos y libertades de las personas, pero además se complementan los principios relativos a la calidad de los datos.

En ese mismo 1980 aparece la recomendación de la OCDE sobre circulación internacional de datos personales y la protección de la intimidad, centrada en personas físicas y donde surgen los que más tarde serían considerados los principios básicos de la protección de datos.

En este resumen a vuelapluma hemos dejado de mencionar sentencias interesantes, como la que desarrolla el "principio de consentimiento", o el "derecho de autodeterminación", procedentes del Tribunal Constitucional Alemán, de 1983, que inspiraron la ley alemana de 1990 y que desde entonces se expandió por el resto del continente.

La evolución que implica pasar de la privacidad como derecho de exclusión de los demás del ámbito privado a una configuración como libertad negativa frente a la información abusiva de nuestros días, ha supuesto un paso de gigante: hoy se concibe como una libertad positiva, la libertad de ejercer un derecho de control sobre los datos referidos a la propia persona que ya han salido de la esfera de la intimidad para convertirse en elemento de un archivo electrónico privado o público.

Ya en el año 1978 James Martin explicaba como en la sociedad de las telecomunicaciones los seres humanos podemos sentirnos como esos osos polares que llevan incorporado un radiotransmisor en miniatura permite que sus pasos sean registrados y enviados a un satélite. Los grandes bancos de datos de las administraciones públicas y grandes corporaciones que aparecen en esas fechas hicieron posible una vigilancia real de la vida cotidiana, permitiendo imputar a un individuo ciertas pautas de comportamiento, comunes a grupos censados y que distinguimos del resto de la población global. (Garriga Domínguez, 2010)

Esto da paso a lo que Frosini (Frosini, 1982) ha denominado la libertad informática: el derecho a autotutela de la propia identidad informática, esto es, la que resulta de la recogida, de la confrontación de los datos personales insertos en un sistema informático. El respeto a la intimidad se extiende hoy a una esfera amplia de la vida privada. No solo se trata de informes íntimos sino también algunos comportamientos personales, elementos distintos de la personalidad, opiniones religiosas y políticas… datos llamados sensibles para distinguirlos de los que están a disposición del público. Pensemos que lo que en un principio resultaba poco

llamativo, la obtención de información cruzando datos, creando perfiles, se ha convertido prácticamente en uno de los ejes de la legislación actual.

Puede observarse que el interés jurídico, centrado positivamente primitivamente sobre el problema de la tutela de la intimidad personal, ha variado su significación hacia su entendimiento como un derecho subjetivo, desplazamiento provocado por la profusión de empleo de archivos magnéticos y bancos de datos personales.

Se trata ya de libertad de controlar el uso de los propios datos personales insertos en un programa informático: es el Habeas Data, correspondiente al Habeas Corpus del respeto debido a la integridad y libertad de la persona y por tanto abre el derecho de acceso de los bancos de datos; el derecho de control de su actividad: el derecho de rectificación; el derecho de secreto por datos sensibles; el derecho a dar autorización para su difusión… es, en sí, una última etapa, donde nos preocupa la incidencia de Internet y los avances científicos, como el desciframiento del mapa genético.

Pero volvamos al principio: nos preguntábamos ¿es un Derecho fundamental, una disciplina jurídica? Tratemos de responder a éstas preguntas.

¿Es un derecho fundamental? El Tribunal Constitucional (sentencia TC 292/2000) dice que sí.

¿Es una disciplina jurídica? Abundantes textos (véase la bibliografía) lo interpretan como una disciplina jurídica que busca proteger la intimidad y demás derechos fundamentales de las personas físicas frente al riesgo que supone la recopilación y el uso indiscriminado de sus datos personales, de forma que abarca todo tipo de tratamiento (independientemente de que se realice de manera manual o informatizada) y marca la necesidad de desarrollar normas que, limitando el uso de los datos personales, garanticen el honor y la intimidad personal y familiar de los ciudadanos.

Con un sí rotundo a ambas preguntas, seguimos adelante.

Marco legal básico

El eje en que nos vamos a mover en el tema actual es doble: el Reglamento Europeo de Protección de Datos (RPGD en adelante) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (3/2018 en adelante). Un eje doble, pero que veremos que en realidad es convergente, pues la ley 3/2018 está repleta de alusiones al RGPD, que en algún caso matiza y en otros complementa.

A lo largo del resto del tema haremos alusión casi en exclusiva a estas dos normas. Pero cabe indicar que no son las únicas de interés, así que al menos trataremos de enumerar las de más interés (incluyendo también normativa técnica) y dar consejos para una eficaz consulta y actualización.

El mejor de los consejos es acudir a la zona de códigos del Boletín Oficial del Estado (BOE, 2019). En esta zona de descarga podemos encontrar, entre otros, los códigos relativos a la Protección de Datos de Carácter Personal y al Derecho al Olvido, que pronto veremos cómo nos es de mucho interés.

Para cada uno de los códigos podemos tener una descarga, en formatos pdf o epub, y siempre actualizada, de toda la legislación relevante: desde las leyes principales a las resoluciones e instrucciones de la Agencia Española de Protección de Datos, a los fragmentos de otras leyes que deben ser tenidos en cuenta por cualquier implicado en estos asuntos. Además, podemos acceder de forma alternativa al texto consolidado y a las versiones anteriores de las normas, lo que en algún momento puede ser de mucho interés, sobre todo en tareas de auditoría y consultoría.

Ilustración 3. Zona de descarga de códigos en la web del Boletín Oficial del Estado. Elaboración propia.

Se trata de documentos muy grandes, del orden de las quinientas y mil páginas cada uno de ellos, pero precisamente por su completitud (y actualización) son de sumo interés.

De entre las normas nacionales de interés, destacan (todo localizable a través de la web del BOE):

- Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público.
- Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen.
- Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información. Este RD es de alta importancia, no solo porque en todo momento se establece la necesaria relación entre la Agencia Española de Protección de Datos y los responsables de la seguridad, sino por su Disposición adicional tercera (Notificación de violaciones de seguridad de los datos personales a través de la plataforma común prevista en este real decreto-ley) que indica que la plataforma común para la notificación de incidentes prevista en este real decreto-ley podrá ser empleada para la notificación de vulneraciones de la seguridad de datos personales según el Reglamento (UE) 2016/679 (RGPD), en los términos que acuerden la Agencia Española de Protección de Datos y los órganos que gestionen dicha plataforma.

- Circular 1/2019, de 7 de marzo, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales relativos a opiniones políticas y envío de propaganda electoral por medios electrónicos o sistemas de mensajería por parte de partidos políticos, federaciones, coaliciones y agrupaciones de electores al amparo del artículo 58 bis de la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General.

No hay que descartar la normativa autonómica, y en concreto, lo emanado por las agencias autonómicas de protección de datos. A este respecto es de interés la ley vasca de Protección de Datos (LEY 2/2004, de 25 de febrero, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos). De cara a enfocar el Título X de la 3/2018, cosa que haremos más adelante en este tema, puede ser de interés consultar la Ley 10/2017, de 27 de junio, de las voluntades digitales y de modificación de los libros segundo y cuarto del Código civil de Cataluña.

Al respecto de la legislación europea, consideremos que no solo el RGPD es el único reglamento a considerar emanado de la unión. Entre otros reglamentos (y directivas y recomendaciones) de interés figuran (todo ello localizable desde el buscador legal del derecho de la UE, EUR-lex (EUR-Lex, 2019)):

- Reglamento (UE) n ° 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 , relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (éste es llamado comúnmente el reglamento EIDAS)
- Reglamento (UE) nº 611/2013 de la Comisión de 24 de junio de 2013 relativo a las medidas aplicables a la notificación de casos de violación de datos personales en el marco de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo sobre la privacidad y las comunicaciones electrónicas
- Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos.
- Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo de 25 de noviembre de 2015 sobre servicios de pago en el mercado interior.
- Dictamen 02/2013 sobre las aplicaciones de los dispositivos inteligentes, de mucho interés para quienes trabajen con apps para móviles, por ejemplo.
- Directrices sobre el consentimiento en el sentido del Reglamento (UE) 2016/679 adoptadas el 10 de abril de 2018
- Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del Reglamento (UE) 2016/679. Adoptadas el 4 de octubre de 2017
- Directrices sobre la notificación de las violaciones de la seguridad de los datos personales de acuerdo con el Reglamento 2016/679. Adoptadas el 6 de febrero de 2018.

- Comunicación de la Comisión al Parlamento Europeo y al Consejo "Mayor protección, nuevas oportunidades: Orientaciones de la Comisión sobre la aplicación directa del Reglamento general de protección de datos a partir del 25 de mayo de 2018"
- Resumen del Dictamen sobre la propuesta de Directiva relativa a determinados aspectos de los contratos de suministro de contenidos digitales (2017/C 200/07)
- Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas (e-privacy).

Entramos ahora en otro campo de mucho interés para el profesional, casi podríamos arriesgarnos a decir que superior al mero conocimiento legal: las normas (UNE, ISO, etc.) de carácter técnico que son o pueden ser de interés en distintos momentos del trabajo del profesional informático. Intentaremos categorizarlas por trabajos, destacando así las normas más importantes para:

- Realizar análisis de riesgos
    - ISO/IEC 29187-1:2013. Information technology - Identification of privacy protection requirements pertaining to learning, education and training (LET) - Part 1: Framework and reference model
    - ISO/IEC TR 29110-5-2-1:2016. Systems and software engineering - Lifecycle profiles for Very Small Entities (VSEs) - Part 5-2-1: Organizational management guidelines
    - ISO/IEC TR 29110-5-6-1:2015. Systems and software engineering - Lifecycle profiles for Very Small Entities (VSEs) - Part 5-6-1: Systems engineering - Management and engineering guide: Generic profile group: Entry profile
    - ISO/IEC TR 29110-5-6-2:2014. Systems and software engineering - Lifecycle profiles for Very Small Entities (VSEs) - Part 5-6-2: Systems engineering - Management and engineering guide: Generic profile group: Basic profile
    - ISO/IEC 29100:2011. Information technology - Security techniques - Privacy framework
- Actuaciones al descubrir una brecha de seguridad
    - UNE 71505-1:2013. Tecnologías de la Información (TI). Sistema de Gestión de Evidencias Electrónicas (SGEE). Parte 1: Vocabulario y principios generales.
    - UNE 71505-2:2013. Tecnologías de la Información (TI). Sistema de Gestión de Evidencias Electrónicas (SGEE). Parte 2: Buenas prácticas en la gestión de las evidencias electrónicas.
    - UNE 71505-3:2013. Tecnologías de la Información (TI). Sistema de Gestión de Evidencias Electrónicas (SGEE). Parte 3: Formatos y mecanismos técnicos.
    - ISO/IEC 29100:2011. Information technology - Security techniques - Privacy framework (sí, otra vez)

    - ISO/IEC 29147:2018. Information technology - Security techniques - Vulnerability disclosure
- Destrucción de material sensible
    - UNE-EN 15713:2010. Destrucción segura del material confidencial. Código de buenas prácticas.
- De forma general
    - UNE-EN ISO/IEC 27001:2017. Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos. (ISO/IEC 27001:2013 incluyendo Cor 1:2014 y Cor 2:2015)
        - ISO/IEC 27001:2013. Information technology — Security techniques — Information security management systems — Requirements
        - ISO/IEC 27001:2013/Cor 1:2014
        - ISO/IEC 27001:2013/Cor 2:2015
    - ISO/IEC 27013:2015. Information technology — Security techniques — Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1
    - ISO/IEC 27009:2016. Information technology — Security techniques — Sector-specific application of ISO/IEC 27001 — Requirements
    - ISO/IEC TR 27023:2015. Information technology — Security techniques — Mapping the revised editions of ISO/IEC 27001 and ISO/IEC 27002

Guías de interés de la Agencia Española de Protección de Datos y otras entidades. (Todas estas guías están disponibles en la web de la agencia o de la institución que se indique, y si en algún momento una de ellas desaparece se debe a la necesaria actualización del material. Se recomienda su búsqueda en la web de la agencia, el título indicado es el que se emplea literalmente en las guías, para facilitar su localización)

- Para el profesional, atendiendo a su figura:
    - Directrices para la elaboración de contratos entre responsables y encargados del tratamiento.
    - Guía del responsable de ficheros.
    - Guía del Reglamento General de Protección de Datos para responsables de tratamiento.
- Para el profesional, atendiendo a labores concretas:
    - Guía sobre el uso de cookies
    - Guía práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD.
    - Orientaciones sobre protección de datos en la reutilización de la información del sector público.
    - Guía de seguridad de datos.
    - Guía para la gestión y notificación de brechas de seguridad.
    - Guía para el cumplimiento del deber de informar.
    - Guía práctica para las evaluaciones de impacto en la protección de los datos sujetas al RGPD.

        - Existe en la Agencia Catalana de Protección de Datos una guía de mucho interés al respecto con nombre similar: Guía práctica de Evaluación de impacto relativa a la protección de datos.
        - También en otra agencia, la francesa, el CNIL, hay un material muy interesante: no solo guías, sino un software que puede ejecutarse al vuelo, que apoya al profesional en este trabajo, disponible en español (Comisión Nacional de Informática y de las Libertades, 2019).
    - Listado de cumplimiento normativo (una de las mejores herramientas, un gran "checklist" que ningún profesional puede permitirse el lujo de ignorar)
- Para elementos muy específicos, pero delicados:
    - Fingerprint o huella digital del dispositivo.
    - Guía para clientes que contraten servicios de Cloud Computing.
    - Protección de datos y administración local.
    - Protección de datos y prevención de delitos.
    - De la Agencia Catalana de Protección de Datos hay que destacar sus Pautas de protección de datos para los centros educativos (Agencia Catalana de Protección de Datos, 2018).
    - Sobre el blockchain, el CNIL tiene un documento de mucho interés: Solutions for a responsable use of the blockchain in the context of personal data.
- También existen guías orientadas a los ciudadanos. Destacamos la Guía para el ciudadano. En este sentido hay que destacar el esfuerzo de divulgación que hace la Agencia manteniendo el programa semanal en Radio Nacional de España "Protegemos tu privacidad" (RNE, 2019).

De la mucha bibliografía existente, se puede destacar un pequeño gran libro de Delgado y Puyol: La Implantación del Nuevo Reglamento General de Protección de Datos de la Unión Europea (Delgado Carravilla & Puyol Montero, 2018).

Dejamos de lado comentar sentencias de interés, por exceder del propósito del presente tema.

Figuras profesionales y actores a considerar

Son muchos los actores posibles en la gestión y protección de los datos personales. En este apartado nos centraremos en los tres más relevantes, con un amplio despliegue legal rodeándolos. Hablamos del Encargado del tratamiento, del responsable del tratamiento y del delegado de protección de datos.

Empecemos con unas breves definiciones para cada una de éstas figuras:

Responsable del tratamiento o «responsable»: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros;

Encargado del tratamiento o «encargado»: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento;

Delegado de protección de datos (DPD o DPO, según se empleen sus siglas en español o en inglés): Especialista en materia de protección de datos, que ocupará un lugar junto a las figuras del responsable y encargado del tratamiento. Esta figura aparece en la legislación a raíz del Reglamento europeo de Protección de Datos, mientras que las otras dos tienen ya su pequeña historia detrás. Es el encargado del tratamiento de las obligaciones legales en la materia de protección de datos de la organización que le contrate, y será el garante del cumplimiento del RGPD. Asesorará pues a la organización, se asegurará de que se cumple con las obligaciones en protección de datos y actuará de interlocutor con la Agencia Española de Protección de Datos y con todo ciudadano que quiera ejercer sus derechos ante la organización.

Responsable del tratamiento (Artículo 24)

Tras la definición, perfilemos su rol.

> Considerando naturaleza, ámbito, contexto, fines del tratamiento y riesgos, el responsable del tratamiento aplicará, revisará y actualizará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el Reglamento. La adhesión a códigos de conducta o a un mecanismo de certificación podrán ser utilizados como elementos para demostrar el cumplimiento de las obligaciones por parte del responsable del tratamiento.

Dado que nos movemos en un ámbito de actuación europeo, debe determinarse si es evidente que el responsable (o el encargado) actúa en ese ámbito. La mera accesibilidad del sitio web del responsable o encargado o de un intermediario en la Unión, de una dirección de correo electrónico u otros datos de contacto, o el uso de una lengua generalmente utilizada en el tercer país donde resida el responsable del tratamiento, son indicadores, pero no bastan para determinar dicha intención. Se pueden considerar factores, como el uso de una lengua o una moneda utilizada generalmente en uno o varios estados miembros, o la mención de clientes o usuarios que residen en la Unión (Considerando 23).

Una figura relacionada es la de **corresponsable del tratamiento** (Artículo 26). Ésta se da cuando dos o más responsables determinan conjuntamente los objetivos y los medios del tratamiento. Si es el caso, se debe determinar de modo transparente y de mutuo acuerdo sus responsabilidades respectivas, y los aspectos esenciales de ese acuerdo, se pondrán a disposición de los interesados.

Otra figura digna de mención es la de los **representantes de responsables o encargados no establecidos en la Unión** (Artículo 27). Debe designarse por escrito un representante en la Unión, pero esto puede obviarse si el tratamiento es ocasional, no incluye manejo a gran escala de categorías especiales de datos y es improbable que entrañe un riesgo para los derechos y libertades de las personas físicas o a las autoridades u organismos públicos. En todo caso, ésta designación se entenderá sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable o encargado.

Encargado del tratamiento (Artículo 28, 29)

Al igual que con el responsable del tratamiento, debemos perfilar su rol.

El responsable del tratamiento, elegirá a un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiadas. El encargado del tratamiento a su vez no recurrirá a otro encargado sin la autorización previa por escrito, específica o general, del responsable.

El tratamiento por el encargado se regirá por un contrato que vincule al encargado respecto del responsable y establezca el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable.

Este contrato estipulará:

- que el encargado tratará los datos personales únicamente siguiendo instrucciones documentadas del responsable (incluyendo transferencias a un tercer país);
- garantizará que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad;
- asistirá al responsable, teniendo cuenta la naturaleza del tratamiento, a través de medidas técnicas y organizativas apropiadas, siempre que sea posible, para que este pueda cumplir con su obligación de responder a las solicitudes;
- a elección del responsable, suprimirá o devolverá todos los datos personales una vez finalice la prestación de los servicios de tratamiento, y suprimirá las copias existentes a menos que se requiera la conservación de los datos personales;
- pondrá a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas, permitiendo y contribuyendo a la realización de auditorías.

Sobre éste contrato, la autoridad de control podrá adoptar cláusulas contractuales tipo. Constará por escrito (p.e. de forma electrónica). Si un encargado del tratamiento infringe el Reglamento al determinar los fines y medios del tratamiento, será considerado responsable del tratamiento con respecto a dicho tratamiento.

La adhesión del encargado del tratamiento a un código de conducta o a un mecanismo de certificación podrá utilizarse como elemento para demostrar la existencia de las garantías suficientes.

Propuesto: Localiza cláusulas contractuales tipo en la web de la Agencia Española de Protección de Datos (Agencia Española de Protección de Datos, 2018)

Hay que destacar que tanto responsable como encargado del tratamiento y sus representantes cooperarán con la autoridad de control que lo solicite en el desempeño de sus funciones. (Artículo 31)

Delegado de protección de datos (Artículo 37, 38)

Ya hemos dicho que se trata de las más recientes de las figuras (aunque en la legislación alemana ya existía). Su perfil debe ser el de un especialista en derecho de protección de datos,

con unas funciones que le hacen parecer una suerte de defensor del pueblo de los datos. Estas serían, básicamente (Artículo 39):

- Informar y asesorar a los responsables y encargados del tratamiento de datos personales (y a sus empleados) de las obligaciones que tienen, derivadas tanto de la legislación.
- Supervisar el cumplimiento de la legislación y de la política interna de protección de datos de una Administración Pública o empresa.
- Cuando se le solicite, asesorar sobre la evaluación de impacto de un tratamiento de datos personales (sobre este interesante elemento volveremos), cuando entrañe un alto riesgo para los derechos y libertades de las personas físicas, y supervisar luego su aplicación.
- Cooperar con las "autoridades de control" (esto es, con las Agencias de Protección de Datos)
- Servir de ventanilla o punto de contacto de las autoridades de control para cualquier consulta sobre el tratamiento de datos personales.

Así como el tratamiento de datos conlleva siempre la existencia de un encargado y un responsable, con los DPD no siempre los encontraremos. Solo hacen falta cuando el tratamiento lo lleve a cabo una autoridad u organismo público (excepto tribunales), o cuando las operaciones de tratamiento en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala, o si estas consisten en el tratamiento a gran escala de categorías especiales de datos personales y de datos relativos a condenas e infracciones penales.

En resumen: hace falta un delgado si se trata de un tratamiento desde la administración pública, cuando se trabaja con datos de un elevado número de personas, o cuando se trabaja con un elevado número de datos especiales.

¿Qué características debe cumplir un delegado de protección de datos? El nivel de conocimientos especializados necesario se debe determinar en función de las operaciones de tratamiento de datos que se lleven a cabo y de la protección exigida para los datos personales tratados por el responsable o el encargado. (Considerando 97). Desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.

Podrá formar parte de la plantilla del responsable o del encargado del tratamiento o desempeñar sus funciones en el marco de un contrato de servicios. En todo caso, tendrá una relación fluida con responsable y encargado del tratamiento, quienes garantizarán que el delegado de protección de datos participe de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales. Le facilitarán los recursos necesarios para el desempeño sus funciones y el acceso a los datos personales y a las operaciones de tratamiento, y para el mantenimiento de sus conocimientos especializados, garantizando que no recibe ninguna instrucción en lo que respecta al desempeño de sus funciones. Rendirá cuentas directamente al más alto nivel jerárquico del responsable o encargado.

Recordemos que ejerce de “ventanilla” con respecto a los interesados en lo que respecta a todas las cuestiones relativas al tratamiento de sus datos personales y al ejercicio de sus derechos.

Está obligado a mantener el secreto, aunque podrá desempeñar otras funciones y cometidos (que no deben dar lugar a conflicto de intereses).

Artículos de máximo interés para entender la figura del Delegado de Protección de Datos:

Artículo 34 Ley 3/2018. Designación de un delegado de protección de datos.

Artículo 35 Ley 3/2018. Cualificación del delegado de protección de datos.

Artículo 36 Ley 3/2018. Posición del delegado de protección de datos.

Artículo 37 Ley 3/2018. Intervención del delegado de protección de datos en caso de reclamación ante las autoridades de protección de datos.

RGPD Artículo 37. Designación del delegado de protección de datos.

RGPD Artículo 38. Posición del delegado de protección de datos.

RGPD Artículo 39. Funciones del delegado de protección de datos.

Definiciones. Principios de la ley

Conviene antes de entrar en definiciones que centremos que es lo que se espera del tratamiento de datos. Entra en juego una palabra, “calidad”, que puede traernos imágenes muy distintas. Para un espectador ajeno a la ley, puede que su primera impresión de la calidad de los datos sea que estos deben ser cuanto más completos y exhaustivos mejor. Pero ese espectador estaría muy equivocado.

Por calidad de los datos se ha considerado tradicionalmente el cumplimiento de una serie de características:

- Pertinencia: los datos personales deben estar relacionados con el fin perseguido, por lo que deben ser adecuados y no excesivos.
- Finalidad: solo se pueden recoger y tratar los datos que sean adecuados con el ámbito y finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.
- Veracidad y exactitud: Los datos deben ser exactos y puestos al día de forma que respondan con veracidad a la situación del interesado: deben ser datos actualizados y también ser veraces.
- Lealtad: Los datos personales deben ser recogidos sin engaños o falsedades por parte de quien los solicita.
- Seguridad: Deben adoptarse las medidas necesarias para garantizar la seguridad de los datos personales evitando alteración, pérdida, tratamiento o acceso no autorizados.

Si nos vamos al artículo 5 del reglamento, nos encontramos con los principios establecidos por la ley, que veremos que viene a ser un eco de esto que anticipábamos. Así, en el citado artículo nos encontramos con las siguientes exigencias:

- Licitud, lealtad y transparencia;
- Limitación de la finalidad: recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines;
- Minimización de datos: ;adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados
- Exactitud: exactos y actualizados
- Integridad y confidencialidad: se garantiza una seguridad adecuada de los datos personales

Debemos añadir, y esto es importante y un cambio de enfoque fundamental, que el responsable del tratamiento será responsable del cumplimiento y capaz de demostrarlo («responsabilidad proactiva»).

Ampliemos los términos que pueden ser más confusos.

La **"licitud del tratamiento"** (véase el artículo 6). El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones: o bien el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos, o bien el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales; o es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento; o es necesario para proteger intereses vitales del interesado o de otra persona física; o es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento; o es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.

Cuando el tratamiento para otro fin distinto de aquel para el que se recogieron los datos personales no esté basado en el consentimiento del interesado o en el Derecho de la Unión o de los Estados miembros, el responsable del tratamiento tendrá en cuenta, entre otros, cualquier relación entre los fines para los cuales se hayan recogido los datos personales y los fines del tratamiento ulterior previsto; el contexto en que se hayan recogido los datos personales, en particular por lo que respecta a la relación entre los interesados y el responsable del tratamiento; la naturaleza de los datos personales, sobre todo si pertenecen a categorías especiales de datos personales; las posibles consecuencias para los interesados del tratamiento ulterior previsto; y la existencia de garantías adecuadas, que podrán incluir el cifrado o la seudonimización[4].

[4] Entenderemos por seudonimización aquel procedimiento mediante el cual se reemplazan campos de información personal dentro de un registro de datos por uno o más identificadores artificiales (pseudónimos) consiguiendo así que cada registro sea menos identificable pero igualmente apto para su procesamiento. El Reglamento lo ofrece como alternativa a la anonimización (consideremos que esta es

Hablemos ahora de la **exactitud de los datos**. Cuando hablamos de datos exactos (y, si fuera necesario, actualizados) hay que ligar el concepto al fin en que se trata. Un dato desactualizado de una dirección puede ser inexacto para mandar una comunicación, pero no a fines históricos, por ejemplo. Es responsabilidad del responsable mantener la exactitud, para lo que ha de incorporar todas las medidas razonables para que se supriman o rectifiquen sin dilación, la inexactitud de los datos personales, excepto si vienen así directamente del afectado o han sido obtenidos de un mediador o intermediario que es quien asumirá las responsabilidades que pudieran derivarse en el supuesto de comunicación al responsable de datos que no se correspondan con los facilitados por el afectado. De igual manera, tampoco sería responsabilidad suya si han sido obtenidos de otro responsable en virtud del ejercicio por el afectado del derecho a la portabilidad o si han sido obtenidos de un registro público. Estos principios fundamentales podemos seguirlos en los artículos 4 y 11 de la ley 3/2018 y en el artículo 12 del RGPD y el apartado 5.1.d)

Sobre estos dos puntos, ligándolos muchas veces, figura la **transparencia**. El responsable del tratamiento tomará las medidas oportunas para facilitar al interesado toda información (indicada en los artículos 13 y 14) en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular cualquier información dirigida específicamente a un niño. La información será facilitada por escrito o por otros medios, inclusive, si procede, por medios electrónicos. Cuando lo solicite el interesado, la información podrá facilitarse verbalmente siempre que se demuestre la identidad del interesado por otros medios. La información facilitada, como toda comunicación serán a título gratuito. Cuando las solicitudes sean manifiestamente infundadas o excesivas, especialmente debido a su carácter repetitivo, el responsable del tratamiento podrá cobrar un canon razonable o negarse a actuar respecto de la solicitud. Este principio fundamental podemos seguirlo de nuevo en los artículos 4 y 11 de la ley 3/2018 y en el artículo 12 del RGPD y los apartados 5.1.d). y 5.1.f)

Es un interés legítimo de los usuarios la necesidad de saber si un sistema información es capaz de resistir, en un nivel determinado de confianza, a acontecimientos accidentales o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos personales conservados o transmitidos, y la seguridad de los servicios conexos ofrecidos por, o accesibles a través de, estos sistemas y redes, por parte de autoridades públicas, equipos de respuesta a emergencias informáticas (CERT), equipos de respuesta a incidentes de seguridad informática (CSIRT), proveedores de redes y servicios de comunicaciones electrónicas y proveedores de tecnologías y servicios de seguridad. Un ejemplo sería el tratar de impedir el acceso no autorizado a las redes de comunicaciones electrónicas y la distribución malintencionada de códigos, y frenar ataques de «denegación de servicio» y daños a los sistemas informáticos y de comunicaciones electrónicas. (Considerando 49).

---

un proceso irreversible, y los datos personales dejan de ser identificables, con la ventaja de evitar el derecho al olvido realizando un borrado completo, con lo que podemos seguir generando métricas clave para el negocio). Una posible seudonimización es el cifrado, que no se puede revertir sin la clave de descifrado). En este caso, esa clave, debe guardarse por separado de los datos seudonimizados. Hay que subrayar que los datos seudonimizados siguen siendo datos personales (considerando 26), amparados por el Reglamento General de Protección de Datos. La definición oficial del término, procedente del reglamento, aparece en el apartado “Definiciones”, de este mismo tema.

En todo momento, recordemos el sumatorio:

ADECUADOS + PERTINENTES + NO EXCESIVOS = CALIDAD

Definiciones

Una vez sentados los principios, pasemos a las definiciones. En el artículo 4 del Reglamento Europeo se nos da una serie de definiciones que conformarán los ladrillos con los que construyamos las ideas de este tema. Directamente de allí, tan solo introduciendo alguna nota aclaratoria, traemos éstas. Cabe hacer una apreciación: las definiciones parecen mostrarse como las cerezas de una cesta, de las que al coger una te llevas prendidas varias más. Esto podemos verlo claramente en la primera de ellas, "datos personales", donde para definir el término al tiempo se define que es una persona física identificable y, por enumeración, un identificador. Así, se habla de:

Datos personales: toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;

Debemos tener en cuenta que un dato, en sí, no es bueno ni malo, ni señala ni deja de señalar. Suele ser la unión entre datos lo que nos preocupa, aunque a veces también lo hacen datos sueltos. Un ejemplo: obviamente no es lo mismo decir 65, que "Hermógenes Finisterre Brodovín tiene 65 años". Un ejemplo más amplio en la tabla siguiente:

Datos aislados no afectados	Datos afectados
1979	Alberto Martínez Pujol
46071	http:\\www.pepemaiquez.net
95%	158.153.205.26
Barcelona	C\ Pato Cojo, 23, pta. 18
Amarillo	jacinto.quincoces@gmail.com

Tabla 1. Datos aislados afectados y no afectados. Elaboración propia.

Tratamiento: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, 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;

Conviene en este punto recordar la división por tiempos, por momentos, del tratamiento, que sugería (Davara Rodríguez, 1998):

1. Recogida
2. Tratamiento en si (cruce, relación…)
3. Utilización y en su caso comunicación (cesión)

Limitación del tratamiento: el marcado de los datos de carácter personal conservados con el fin de limitar su tratamiento en el futuro;

Un ejemplo extremo de limitación del tratamiento pueden ser las listas Robinson

Estas listas son elaboradas con todas las garantías legales por la Federación Española de Comercio electrónico y Marketing Directo, de manera que elaboran unas listas de posibles clientes en función de sus preferencias a la hora de recibir publicidad u otro tipo de promociones. Las empresas adheridas a la federación tienen acceso a ellas y las personas inscritas la posibilidad de solicitar la cancelación y supresión de sus datos en todo momento.

Es una buena posibilidad, al igual que el censo promocional pero más personalizado, de realizar envíos publicitarios de manera legal, pues en internet proliferan diversas bases de datos totalmente ilegales que pueden plantear problemas a las organizaciones poco cautelosas.

Para apuntarse en la lista, basta con acceder a la URL: https://www.listarobinson.es/

Elaboración de perfiles: toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física;

Seudonimización: corresponde al tratamiento de datos personales realizado de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable;

Fichero: todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica;

Ojo: según esta definición, un fichero convencional con los datos de los clientes escritos a mano en fichas ordenadas alfabéticamente es precisamente eso, un fichero. Con todo lo que supone.

Destinatario: la persona física o jurídica, autoridad pública, servicio u otro organismo al que se comuniquen datos personales, se trate o no de un tercero. No obstante, no se considerarán destinatarios las autoridades públicas que puedan recibir datos personales en el marco de una investigación concreta de conformidad con el Derecho de la Unión o de los Estados miembros; el tratamiento de tales datos por dichas autoridades públicas será conforme con las normas en materia de protección de datos aplicables a los fines del tratamiento;

Tercero: persona física o jurídica, autoridad pública, servicio u organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o del encargado;

Consentimiento del interesado: toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen;

Violación de la seguridad de los datos personales: toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos;

Datos genéticos: datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona;

¿Qué serían los datos genéticos? Se trataría de los datos personales relacionados con características genéticas, heredadas o adquiridas, de una persona física, provenientes del análisis de una muestra biológica de la persona física en cuestión, en particular a través de un análisis cromosómico, un análisis del ácido desoxirribonucleico (ADN) o del ácido ribonucleico (ARN), o del análisis de cualquier otro elemento que permita obtener información equivalente. (Considerando 34)

Datos biométricos: datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos;

Datos relativos a la salud: datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud;

Sobre los datos relativos a la salud, deben incluir todos los datos relativos al estado de salud del interesado que dan información sobre su estado de salud física o mental pasado, presente o futuro. Se incluye la información sobre la persona física recogida con ocasión de su inscripción a efectos de asistencia sanitaria, o con ocasión de la prestación de tal asistencia; todo número, símbolo o dato asignado a una persona física que la identifique de manera unívoca a efectos sanitarios; la información obtenida de pruebas o exámenes de una parte del cuerpo o de una sustancia corporal, incluida la procedente de datos genéticos y muestras biológicas, y cualquier información relativa, a título de ejemplo, a una enfermedad, una discapacidad, el riesgo de padecer enfermedades, el historial médico, el tratamiento clínico o el estado fisiológico o biomédico del interesado, independientemente de su fuente, por ejemplo un médico u otro profesional sanitario, un hospital, un dispositivo médico, o una prueba diagnóstica in vitro. (Considerando 35)

Como puede entenderse, hay datos genéticos y datos biométricos que encajarían en esta misma categoría.

Es de interés la Directiva 2011/24/UE del Parlamento Europeo y del Consejo, de 9 de marzo de 2011, relativa a la aplicación de los derechos de los pacientes en la asistencia sanitaria transfronteriza (DO L 88 de 4.4.2011, p. 45).

Establecimiento principal: en lo que se refiere a un responsable del tratamiento con establecimientos en más de un Estado miembro, el lugar de su administración central en la Unión, salvo que las decisiones sobre los fines y los medios del tratamiento se tomen en otro establecimiento del responsable en la Unión y este último establecimiento tenga el poder de hacer aplicar tales decisiones, en cuyo caso el establecimiento que haya adoptado tales decisiones se considerará establecimiento principal. En lo que se refiere a un encargado del tratamiento con establecimientos en más de un Estado miembro, el lugar de su administración central en la Unión o, si careciera de esta, el establecimiento del encargado en la Unión en el que se realicen las principales actividades de tratamiento en el contexto de las actividades de un establecimiento del encargado en la medida en que el encargado esté sujeto a obligaciones específicas con arreglo al presente Reglamento;

Representante: persona física o jurídica establecida en la Unión que, habiendo sido designada por escrito por el responsable o el encargado del tratamiento con arreglo al artículo 27 del Reglamento, represente al responsable o al encargado en lo que respecta a sus respectivas obligaciones en virtud del presente Reglamento;

Empresa: persona física o jurídica dedicada a una actividad económica, independientemente de su forma jurídica, incluidas las sociedades o asociaciones que desempeñen regularmente una actividad económica;

Grupo empresarial: grupo constituido por una empresa que ejerce el control y sus empresas controladas;

Normas corporativas vinculantes: las políticas de protección de datos personales asumidas por un responsable o encargado del tratamiento establecido en el territorio de un Estado miembro para transferencias o un conjunto de transferencias de datos personales a un responsable o encargado en uno o más países terceros, dentro de un grupo empresarial o una unión de empresas dedicadas a una actividad económica conjunta;

Autoridad de control: la autoridad pública independiente establecida por un Estado miembro;

Autoridad de control interesada: la autoridad de control a la que afecta el tratamiento de datos personales debido a que el responsable o el encargado del tratamiento está establecido en el territorio del Estado miembro de esa autoridad de control; o los interesados que residen en el Estado miembro de esa autoridad de control se ven sustancialmente afectados o es probable que se vean sustancialmente afectados por el tratamiento, ose ha presentado una reclamación ante esa autoridad de control;

Tratamiento transfronterizo :el tratamiento de datos personales realizado en el contexto de las actividades de establecimientos en más de un Estado miembro de un responsable o un encargado del tratamiento en la Unión, si el responsable o el encargado está establecido en más de un Estado miembro; o el tratamiento de datos personales realizado en el contexto de las actividades de un único establecimiento de un responsable o un encargado del tratamiento

en la Unión, pero que afecta sustancialmente o es probable que afecte sustancialmente a interesados en más de un Estado miembro;

Objeción pertinente y motivada: la objeción a una propuesta de decisión sobre la existencia o no de infracción del presente Reglamento, o sobre la conformidad con el presente Reglamento de acciones previstas en relación con el responsable o el encargado del tratamiento, que demuestre claramente la importancia de los riesgos que entraña el proyecto de decisión para los derechos y libertades fundamentales de los interesados y, en su caso, para la libre circulación de datos personales dentro de la Unión;

Servicio de la sociedad de la información: todo servicio conforme a la definición del artículo 1, apartado 1, letra b), de la Directiva (UE) 2015/1535 del Parlamento Europeo y del Consejo[5]; esto es: todo servicio prestado normalmente a cambio de una remuneración, a distancia, por vía electrónica y a petición individual de un destinatario de servicios. A efectos de la presente definición, se entenderá por:

i) «a distancia», un servicio prestado sin que las partes estén presentes simultáneamente,
ii) «por vía electrónica», un servicio enviado desde la fuente y recibido por el destinatario mediante equipos electrónicos de tratamiento (incluida la compresión digital) y de almacenamiento de datos y que se transmite, canaliza y recibe enteramente por hilos, radio, medios ópticos o cualquier otro medio electromagnético,
iii) «a petición individual de un destinatario de servicios», un servicio prestado mediante transmisión de datos a petición individual;

Organización internacional: una organización internacional y sus entes subordinados de Derecho internacional público o cualquier otro organismo creado mediante un acuerdo entre dos o más países o en virtud de tal acuerdo.

Son muchos términos, algunos muy similares en concepto a lo que podemos entender de ellos en el ejercicio de la profesión informática, pero otros dotados de características que los hacen diferentes a lo intuitivo de los mismos, al considerarlos en el marco legal.

Otras definiciones de sumo interés:

Cesión o comunicación de datos: Toda revelación de datos realizada a una persona distinta del interesado. (Por ejemplo, con fines publicitarios o entre empresas ubicadas en diferentes países).

Fuentes accesibles al público: Aquellos ficheros cuya consulta puede ser realizada por cualquier persona, no impedida por una norma limitativa, o sin más exigencia que, en su caso, el abono de una contraprestación. Tienen la consideración de fuentes de acceso público, exclusivamente, el censo promocional[6], los repertorios telefónicos en los términos previstos

[5] En nuestra legislación nacional, es conveniente consultar la Ley de Servicios de la Sociedad de la Información y Comercio Electrónico.
[6] No hay que confundir el censo promocional (disponible para el público) con el electoral ni con el padrón municipal (datos reservados, sólo con fines estadísticos). El censo promocional

por su normativa específica y las listas de personas pertenecientes a grupos de profesionales (siempre que hayan prestado su consentimiento) que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público, los Diarios y Boletines oficiales y los medios de comunicación.

Derechos

¿Qué derechos tiene el ciudadano? ¿Que indica la ley? Nuestros usuarios, clientes, nuestros vecinos, nosotros, vemos como nuestros datos son recogidos y posteriormente tratados. Y con ellos vamos nosotros. El proceso recuerda a algunos esas leyendas que nos hablan de aborígenes que se negaban a ser fotografiados pues así, se les robaba el alma. Bien, es posible que el alma no nos la roben, pero lo que si nos pueden hurtar es todo rastro de privacidad.

Sobre qué debemos hacer, un resumen nos lo da el RGPD en su considerando 59, donde leemos que se deben facilitar, incluyendo los mecanismos necesarios para ello, el acceso a los datos personales y su rectificación o supresión, así como el ejercicio del derecho de oposición. Además en el mismo considerando se indica el plazo máximo de un mes para atender a las peticiones a los interesados... o justificar por qué no las atiende. Vamos a hablar de estos derechos, y de otros con no menos importancia. Empecemos con el derecho de acceso, para ir desgranando el resto en sucesivos epígrafes.

Los derechos de los ciudadanos se han actualizado e incrementado. El derecho al olvido, la portabilidad… han venido para quedarse. Si queremos conocer la norma, debemos acudir a los artículos 12 a 18 de la 3/2018 y los 15 a 22 del RGPD.

Se trata de derechos que pueden ejercerse directamente o por medio de representante, pero siempre el interesadodebeserinformadosobrelosmediosasudisposiciónparaejercerlos. Se hace cargo de las solicitudes el responsable, o el encargado del tratamiento por cuenta del responsable. En general, con leves excepciones, su ejercicio es gratuito y la carga de la pruebadelarespuestaalejerciciodelosderechoscorrespondealresponsable.

Para desarrollarlos emplearemos unas fichas con este formato:

Nombre del derecho	Artículos de las normas
Breve descripción	
Consideraciones	

Derecho de acceso del interesado:

Acceso	13 3/2018; 15 RGPD

El interesado tendrá derecho a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen y, en tal caso, derecho de acceso a los

sólo incluiría nombre, apellidos y dirección. Además, en cuanto a los medios de comunicación nótese en cualquier periódico que, así como la lista de fallecidos incluye nombre y apellidos, la lista de nacimientos es una nota simple con el nombre de los niños (sin apellido).

datos personales y a la siguiente información: los fines del tratamiento; las categorías de datos personales de que se trate; los destinatarios o las categorías de destinatarios a los que se comunicaron o serán comunicados los datos personales, en particular destinatarios en terceros u organizaciones internacionales; de ser posible, el plazo previsto de conservación de los datos personales o, de no ser posible, los criterios utilizados para determinar este plazo; la existencia del derecho a solicitar del responsable la rectificación o supresión de datos personales o la limitación del tratamiento de datos personales relativos al interesado, o a oponerse a dicho tratamiento; el derecho a presentar una reclamación ante una autoridad de control; cuando los datos personales no se hayan obtenido del interesado, cualquier información disponible sobre su origen y la existencia de decisiones automatizadas, incluida la elaboración de perfiles.

Cuando el responsable trate una gran cantidad de datos del afectado y éste ejercite su derecho sin especificar a qué datos se refiere, el responsable podrá solicitarle mayor concreción.

El derecho se entenderá otorgado si el responsable facilitara al afectado un sistema de acceso remoto, directo y seguro a los datos que garantice, de modo permanente, el acceso a su totalidad. La comunicación al afectado del modo en que podrá acceder a dicho sistema bastará para tener por atendida la solicitud.

Se podrá considerar repetitivo el ejercicio del derecho de acceso en más de una ocasión durante el plazo de seis meses, a menos que exista causa legítima para ello, en cuyo caso el responsable podrá cobrar un canon o negarse a actuar.

Si el interesado elige un medio distinto al que se le ofrece con un coste desproporcionado, el será quien deba asumir el exceso de costes. En este caso no se podrán alegar dilaciones indebidas.

Hay que considerar que este derecho no debe afectar negativamente a los derechos y libertades de terceros, incluidos los secretos comerciales o la propiedad intelectual y, en particular, los derechos de propiedad intelectual que protegen programas informáticos. (Considerando 63)

Derecho de rectificación:

Rectificación	14 3/2018; 16 RGPD

El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la rectificación de los datos personales inexactos que le conciernan. Teniendo en cuenta los fines del tratamiento, el interesado tendrá derecho a que se completen los datos personales que sean incompletos, inclusive mediante una declaración adicional.

Deberá indicar a qué datos se refiere y la corrección a realizar.

Deberá acompañar documentación justificativa de la inexactitud o del carácter incompleto de los datos.

Derecho de supresión, llamado también derecho al olvido:

Garriga lo define como cancelación de datos personales que ya no sean necesarios para la realización del propósito concreto que motivó su recogida y tratamiento. (Garriga Domínguez, 2010)

Supresión (Olvido)	15 3/2018; 17 RGPD

El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando concurra alguna de las circunstancias siguientes: los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo; el interesado retire el consentimiento en que se basa el tratamiento de conformidad; el interesado se oponga al tratamiento y no prevalezcan otros motivos; los datos personales hayan sido tratados ilícitamente; los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento; los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información mencionados en el artículo 8, apartado 1. (menores)

Cuando haya hecho públicos los datos personales y esté obligado a suprimir dichos datos, el responsable del tratamiento, teniendo en cuenta la tecnología disponible y el coste de su aplicación, adoptará medidas razonables, incluidas medidas técnicas, con miras a informar a los responsables que estén tratando los datos personales de la solicitud del interesado de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos.

Cuando la supresión derive del ejercicio del derecho de oposición, el responsable podrá conservar los datos con el fin de impedir tratamientos futuros para fines de mercadotecnia directa.

Se abunda indicando que es particularmente pertinente cuando el consentimiento se dio siendo niño, por no tener la plenitud de la conciencia sobre los riesgos que implica el tratamiento. En concreto señala la necesidad de suprimir esos datos personales en internet. Es una ampliación de derechos preexistentes, de forma que se refuerza al respecto de los datos publicados en internet, de tal modo que el responsable del tratamiento que haya hecho públicos datos personales esté obligado a indicar a los responsables del tratamiento que estén tratando tales datos personales que supriman todo enlace a ellos, o las copias o réplicas de tales datos, algo que hay que hacer considerando posibles cambios en la tecnología.

Obviamente hay excepciones, entre las que destacan las que indican que son necesarios para el cumplimiento de una obligación legal, para el cumplimiento de una misión realizada en interés público (incluido el ámbito de la salud), con fines de archivo, investigación científica o histórica o estadísticos. De igual modo se hace la excepción pertinente para cuando es precisa la conservación de cara al ejercicio o defensa de reclamaciones.

El precedente claro lo tenemos que buscar en la actividad del tribunal europeo en defensa de los ciudadanos, algo que podemos particularizar en la sentencia de 13 de mayo de 2014de la Gran Sala del Tribunal de Justicia en el caso del ciudadano español M.C. frente a Google, donde, en sus declaraciones finales, podemos leer que

(…) el gestor de un motor de búsqueda está obligado a eliminar de la lista de resultados obtenida tras una búsqueda efectuada a partir del nombre de una persona vínculos a páginas web, publicadas por terceros y que contienen información relativa a esta persona, también en el supuesto de que este nombre o esta información no se borren previa o simultáneamente de estas páginas web, y, en su caso, aunque la publicación en dichas páginas sea en sí misma lícita (Google Spain SL y Google Inc. contra Agencia Española de Protección de Datos (AEPD) y Mario Costeja González, 2014)

Pregunta: ¿Cómo afectaría esto a una hemeroteca virtual histórica, como por ejemplo la Biblioteca Virtual de Prensa Histórica? (Secretaría de Estado de Cultura)

Véase la noticia El Constitucional extiende el derecho al olvido a las hemerotecas digitales (Rincón, 2018)

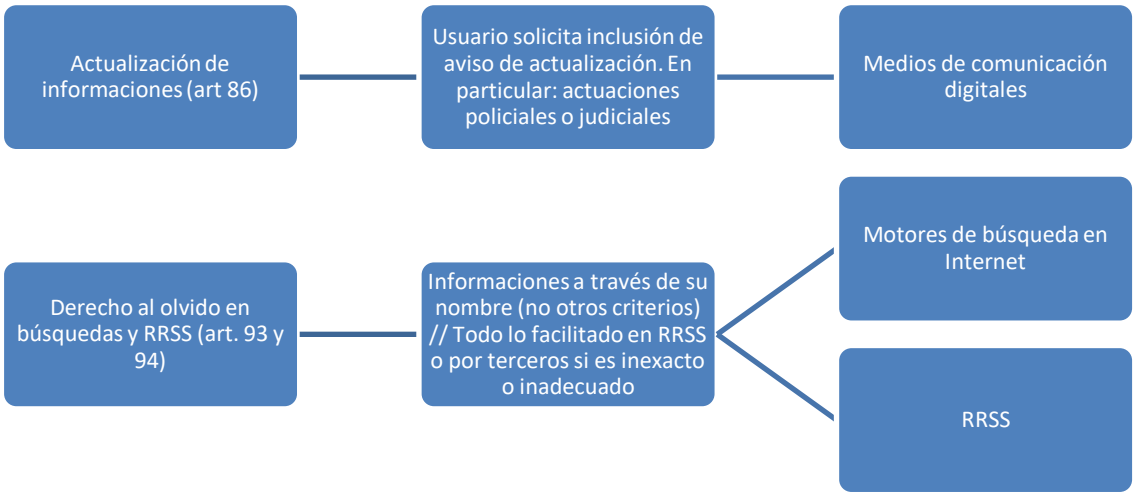


Ilustración 4. Actualización de informaciones y derecho al olvido. Elaboración propia.

Derecho a la limitación del tratamiento:

Limitación del tratamiento	16 3/2018; 18 RGPD

El interesado tendrá derecho a obtener del responsable del tratamiento la limitación del tratamiento de los datos cuando se cumpla alguna de las condiciones siguientes: el interesado impugne la exactitud de los datos personales, durante un plazo que permita al responsable verificar la exactitud de los mismos; el tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso; el responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones; el interesado se haya opuesto al tratamiento, mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado.

Debe constar claramente en los sistemas de información del responsable.

Siguiendo el reglamento, deben incluirse entre los métodos para limitar el tratamiento de datos personales el de trasladar temporalmente los datos seleccionados a otro sistema de

tratamiento, impedir el acceso de usuarios a los datos personales seleccionados o retirar temporalmente los datos publicados de un sitio internet.

Destaca la alusión a los ficheros automatizados donde la limitación del tratamiento debe realizarse por medios técnicos, de forma que los datos personales no sean objeto de operaciones de tratamiento ulterior ni puedan modificarse. (Considerando 67)

¿Cuándo puede ejercerse este derecho?

- Cuando se impugne la exactitud de los datos personales, durante el plazo en que el responsable pueda verificar su exactitud;
- cuando el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso;
- cuando el responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones.

El interesado será informado por el responsable antes del levantamiento de dicha limitación.

Además, el responsable del tratamiento debe comunicar cualquier rectificación o supresión de datos personales o limitación del tratamiento a cada uno de los destinatarios a los que se hayan comunicado los datos personales, salvo que sea imposible o exija un esfuerzo desproporcionado. (Artículo 19)

Derecho a la portabilidad:

Portabilidad	17 3/2018; 20 RGPD

El interesado tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado, cuando: el tratamiento esté basado en el consentimiento o en un contrato y el tratamiento se efectúe por medios automatizados.

El interesado tendrá derecho a que los datos personales se transmitan directamente de responsable a responsable cuando sea técnicamente posible.

Es un derecho que puede ser muy útil al cambiar de compañía de suministros (teléfono, por ejemplo) o de trabajo. Por ejemplo, al cambiar de compañía de teléfonos, el interesado solo ha de pedir la portabilidad, siendo la compañía que recibe esa petición la encargada de los trámites de baja de la línea anterior.

No se aplicará al tratamiento necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.

Derecho de oposición

Oposición	18 3/2018; 21 y 22 RGPD

El interesado tendrá derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular, a que datos personales que le conciernan sean objeto de un tratamiento incluido la elaboración de perfiles sobre la base de dichas disposiciones. El

responsable del tratamiento dejará de tratar los datos personales, salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones. Cuando el tratamiento de datos personales tenga por objeto la mercadotecnia directa, el interesado tendrá derecho a oponerse en todo momento al tratamiento de los datos personales que le conciernan, incluida la elaboración de perfiles en la medida en que esté relacionada con la citada mercadotecnia.

Cuando los datos personales se traten con fines de investigación científica o histórica o fines estadísticos, el interesado tendrá derecho, por motivos relacionados con su situación particular, a oponerse al tratamiento de datos personales que le conciernan, salvo que sea necesario para el cumplimiento de una misión realizada por razones de interés público.

Todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar.

Decisiones individuales automatizadas (elaboración de perfiles):

Hablamos ahora de un derecho que no suele ser incluido en los listados, pero que entendemos tiene mucho interés para el informático (recogido en el artículo 22 del RGPD), el que tiene el usuario a no ser objeto de una decisión que evalúe aspectos personales, y que se ésta base únicamente en el tratamiento automatizado y produzca efectos jurídicos o afecte significativamente al interesado (por ejemplo, la denegación automática de un crédito sin intervención humana). Se trata de evaluar (o no hacerlo) aspectos personales relativos a una persona física, para analizar o predecir aspectos relacionados con el rendimiento en el trabajo, la situación económica, la salud, las preferencias o intereses personales, la fiabilidad o el comportamiento, la situación o los movimientos del interesado... (Véase por ejemplo la película-documental Siclo de Michael Moore (Moore , 2007)[7]). Por otra parte, si se permiten las decisiones basadas en tal tratamiento, incluida la elaboración de perfiles, si lo autoriza expresamente el Derecho de la Unión o de los Estados miembros, por ejemplo para el control y prevención del fraude y la evasión fiscal, y para garantizar la seguridad y la fiabilidad de un servicio prestado, o cuando es necesario para la conclusión o ejecución de un contrato entre el interesado y un responsable del tratamiento, o en los casos en los que el interesado haya dado su consentimiento explícito. Las garantías de ese tratamiento de cualquier forma, debe ceñirse a las garantías apropiadas (dar información específica al interesado; derecho a obtener intervención humana; derecho a expresar su punto de vista; derecho a recibir una explicación de la decisión tomada y a impugnar la decisión). En todo caso no debe afectar a un menor.

El responsable del tratamiento debe utilizar procedimientos matemáticos o estadísticos adecuados para la elaboración de perfiles, aplicar medidas técnicas y organizativas apropiadas para garantizar la corrección de inexactitudes y reducción del riesgo de error, impidiendo efectos discriminatorios en las personas físicas por motivos de raza u origen étnico, opiniones políticas, religión o creencias, afiliación sindical, condición genética o estado de salud u

[7] Se trata de una visión muy crítica sobre el sistema de salud de Estados Unidos, en concreto sobre las compañías sanitarias privadas frente a un sistema de salud público como los que disfrutamos en algunos países europeos.

orientación sexual. Las decisiones automatizadas y la elaboración de perfiles sobre la base de categorías particulares de datos personales únicamente deben permitirse en condiciones específicas. (Considerando 71)

¿Qué limitaciones tienen estos derechos?

Hemos visto un conjunto muy importante de derechos, pero estos no significan una barra libre para que los usuarios los ejerzan a modo de castigo hacia las organizaciones. Hemos visto como se alude a pago de un canon cuando las peticiones son repetitivas, por ejemplo. Pero hay más limitaciones, que pueden encontrarse en el RGPD, en su artículo 23 y en su considerando 19. Los Estados miembros pueden encomendar a las autoridades competentes, (Véase la Directiva (UE) 2016/680) (Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, 2016) funciones que no se lleven a cabo necesariamente con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o ejecución de sanciones penales, incluida la protección frente a las amenazas a la seguridad pública y su prevención, indicándose expresamente que los Estados miembros puedan, en condiciones específicas, limitar conforme a Derecho determinadas obligaciones y derechos siempre que dicha limitación sea una medida necesaria y proporcionada en una sociedad democrática para proteger intereses específicos importantes.

Esto implica que deben respetarse en lo esencial los derechos y libertades fundamentales, a pesar de las excepciones que deben ser siempre "medidas necesarias y proporcionadas".

Sobre los intereses específicos importantes se destacan la prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales; intereses económicos o financieros importantes de la Unión o de un Estado miembro, inclusive en los ámbitos fiscal, presupuestario y monetario, la sanidad pública y la seguridad social; la protección de la independencia judicial; la prevención, la investigación, la detección y el enjuiciamiento de infracciones de normas deontológicas en las profesiones reguladas; la protección del interesado o de los derechos y libertades de otros.

Planteamiento abierto: si nos fijamos, al incluirse la prevención de infracciones penales ¿se autorizan expresamente las aplicaciones de “pre-crimen”, que permiten anticipar sobre que zonas o que individuos hay que reforzar la vigilancia?

Artículos de máximo interés para entender los derechos:

Artículo 12 Ley 3/2018. Disposiciones generales sobre ejercicio de los derechos.

Artículo 13 Ley 3/2018. Derecho de acceso.

Artículo 14 Ley 3/2018. Derecho de rectificación.

Artículo 15 Ley 3/2018. Derecho de supresión.

Artículo 16 Ley 3/2018. Derecho a la limitación del tratamiento.

Artículo 17 Ley 3/2018. Derecho a la portabilidad.

Artículo 18 Ley 3/2018. Derecho de oposición.

RGPD. Artículo 15. Derecho de acceso del interesado.

RGPD. Artículo 16. Derecho de rectificación.

RGPD. Artículo 17. Derecho de supresión («el derecho al olvido»).

RGPD. Artículo 18. Derecho a la limitación del tratamiento.

RGPD. Artículo 19. Obligación de notificación relativa a la rectificación o supresión de datos personales o la limitación del tratamiento.

RGPD. Artículo 20. Derecho a la portabilidad de los datos.

RGPD. Artículo 21. Derecho de oposición.

RGPD. Artículo 22. Decisiones individuales automatizadas, incluida la elaboración de perfiles.

Las autoridades de control: la Agencia Española de Protección de Datos (AEPD) y agencias autonómicas

Es de sumo interés conocer a los "vigilantes de la ley". En España, hablamos al respecto de la AEPD y las agencias autonómicas (en Francia de la *CNIL, Comisión Nacional de Informática y de las Libertades*, en Italia de la *Garante per la protezione dei dati personali*). No son entidades de nueva creación, ya llevan muchos lustros entre nosotros, pero algunos cambios han sufrido. Para dejar claro el marco en el que se mueven, tendríamos que recurrir en la ley 3/2018 a sus artículos 44 a 62 y a sus disposiciones adicional vigésima y transitoria primera y en el RGPD, en sus artículos 51 a 67.

De hecho, el Estatuto Jurídico actual sigue en vigor de forma un tanto provisional, ya que la ley indica que seguirá vigente en lo que no se oponga a lo establecido en la Ley Orgánica. De igual modo se indica que la nueva regulación relativa al Adjunto de la Presidencia de la Agencia y al Consejo Consultivo de la Agencia no se aplicará hasta que no expire el mandato del Director de la Agencia a la entrada en vigor de la Ley Orgánica.

¿Y en qué debe ocuparse la AEPD? (Funciones de la AEPD)

- Investigación (en caso de vulneración de la normativa y mediante auditorías preventivas). Administraciones públicas y particulares están obligados a proporcionar informes, antecedentes y justificantes.
- Regulación: Dictando disposiciones que fijen los criterios de actuación: Circulares que son de obligatorio cumplimiento una vez publicadas en el BOE.
- Acción exterior: funciones relacionadas con la acción exterior del Estado en materia de protección de datos. Ídem a las comunidades autónomas, a través de las autoridades autonómicas.

La confusión puede venir de la coexistencia en un mismo territorio de varias autoridades de control. Se suceden preguntas como ¿si se da una violación de la ley en alguna materia

que sea competencia autonómica, puede la AEPD requerir a las agencias autonómicas? La respuesta es elemental: sí. Sobre éstas, dejemos claro que su ámbito de actuación queda limitado a los ficheros de titularidad pública declarados por las Administraciones autonómicas y locales de sus respectivas comunidades autónomas.

Empecemos dejando claro que es la AEPD: se trata de un ente de Derecho Público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones Públicas en el ejercicio de sus funciones (lo que no quiere decir que sea totalmente independiente pues está sometida al Tribunal de Cuentas). Su finalidad principal es la de velar por el cumplimiento de la legislación sobre protección de datos personales y controlar su aplicación.

Y recordemos que es la española. Pensemos que se puede dar el caso de un ciudadano español que tenga un problema con una empresa francesa. O un ciudadano italiano con un problema con una empresa española ¿Qué sucede? ¿Qué agencia atiende? ¿A qué autoridad debemos considerar como la principal?

El hecho de que una autoridad de control pueda o no actuar como autoridad principal, según se traten asuntos locales o cuando afecta a interesados de ese único Estado miembro, provoca la necesaria coordinación entre autoridades de control que debe informar sin dilación y decidir si debe emplearse el «mecanismo de ventanilla única[8]», o si lo debe tratar localmente la autoridad de control que le haya informado. (Considerando 127)

Recordemos que en apartado de definiciones, decíamos que **Autoridad de control** es la autoridad pública independiente establecida por un Estado miembro con arreglo a lo dispuesto en el artículo 51 del Reglamento. Conviene que sepamos ahora que dice ese artículo 51.

Cada Estado miembro establecerá que sea responsabilidad de una o varias autoridades de control el supervisar la aplicación del Reglamento, para proteger los derechos y las libertades fundamentales de las personas físicas en lo que respecta al tratamiento y de facilitar la libre circulación de datos personales en la Unión. Esas autoridades de control cooperarán entre sí. Es posible que existan varias autoridades de control en un Estado miembro; una de ellas será la que represente a dichas autoridades en el Comité (el Comité es un organismo independiente de la Unión con personalidad jurídica, compuesto por el director de una autoridad de control de cada Estado miembro y el Supervisor Europeo de Protección de Datos, o por sus respectivos representantes)

Una vez claro qué es esto de una autoridad de control, vamos a ver unos cuantos aspectos de interés. Empecemos por su composición: ¿Quiénes son los miembros de la autoridad de control? (Artículo 53)

[8] Sirve para que los responsables que hagan tratamientos que afecten significativamente a ciudadanos en varios Estados de la UE tengan una única Autoridad de protección de datos como interlocutora. Esto no supone que los ciudadanos tengan que relacionarse con varias Autoridades o con Autoridades distintas de la del Estado donde residan. Siempre pueden plantear sus reclamaciones o denuncias ante su propia Autoridad nacional.

Los miembros de las autoridades de control deben ser nombrados mediante un procedimiento transparente, dejando que cada país de la Unión decida si lo serán por su Parlamento, Gobierno, Jefe de Estado, o un organismo independiente encargado del nombramiento. En todo caso, cada miembro poseerá la titulación, experiencia y aptitudes, en el ámbito de la protección de datos personales, necesarios para el cumplimiento de sus funciones y el ejercicio de sus poderes. Será destituido antes de su fin de mandato únicamente en caso de conducta irregular grave o si deja de cumplir las condiciones exigidas en el desempeño de sus funciones. Cada Estado miembro de la Unión establecerá al respecto de sus miembros (Artículo 54)

- las cualificaciones y condiciones de idoneidad necesarias para ser nombrado miembro;
- las normas y los procedimientos para el nombramiento miembros de cada autoridad de control;
- la duración del mandato del miembro o los miembros de cada autoridad de control, no inferior a cuatro años, salvo el primer nombramiento posterior al 24 de mayo de 2016;
- el carácter renovable o no del mandato del miembro o los miembros de cada autoridad de control y, en su caso, el número de veces que podrá renovarse;
- las condiciones, prohibiciones relativas a acciones, ocupaciones y prestaciones incompatibles con el cargo durante el mandato y después del mismo, y las normas que rigen el cese en el empleo.

La autoridad de control que tenemos en España es la Agencia Española de Protección de Datos, que definíamos como un Ente de Derecho Público, que actúa con plena independencia de las Administraciones Públicas en el ejercicio de sus funciones. Entra por tanto en la categoría de "Administraciones independientes" excluidas de la LOFAGE (Ley 6/1997, de 14 de abril, de Organización y Funcionamiento de la Administración General del Estado).

Decíamos que su finalidad principal es velar por el cumplimiento de la legislación sobre protección de datos personales y controlar su aplicación. Para el cumplimiento de esta misión, la Agencia realiza campañas de divulgación para una mejor defensa de los derechos de los ciudadanos. La AEPD lleva a cabo sus potestades de investigación fundamentalmente a instancias de los ciudadanos, aunque también está facultada para actuar de oficio

La AEPD, creada en 1993, es el organismo público encargado de velar por el cumplimiento de la Ley Orgánica de Protección de Datos de Carácter Personal en España. Tiene su sede en Madrid y su ámbito de actuación se extiende al conjunto de España.

Recordemos que las agencias de protección de datos de carácter autonómico (Cataluña y País Vasco) tienen un ámbito de actuación limitado a los ficheros de titularidad pública declarados por las Administraciones autonómicas y locales de sus respectivas comunidades autónomas.

Los miembros y el personal de cada autoridad de control estarán sujetos al deber de secreto profesional, tanto durante su mandato como después del mismo.

Hay que destacar (artículo 55) que las autoridades de control no serán competentes para controlar las operaciones de tratamiento efectuadas por los tribunales en el ejercicio de su función judicial.

La autoridad de control incluye en sus competencias (Artículo 56): tratar las reclamaciones presentadas o infracciones del Reglamento, y, si está en la sede del establecimiento principal o

del único establecimiento del responsable o del encargado del tratamiento de la empresa que pretenda hacer un tratamiento transfronterizo de datos, actuar como autoridad de control principal.

Algunas de sus funciones: (*Artículo57)*

De cara al interesado:

- previa solicitud, facilitar información a cualquier interesado en relación con el ejercicio de sus derechos;
- tratar las reclamaciones presentadas e investigar, en la medida oportuna, el motivo de la reclamación e informar al reclamante sobre el curso y el resultado de la investigación en un plazo razonable;

De cara a la sociedad en general:

- controlar la aplicación del Reglamento y hacerlo aplicar;
- promover la sensibilización del público y su comprensión de los riesgos, normas, garantías y derechos en relación con el tratamiento. Con especial atención a los niños;
- asesorar al Parlamento, al Gobierno y a otras instituciones;
- hacer un seguimiento de cambios que sean de interés, el desarrollo de las tecnologías de la información y la comunicación y las prácticas comerciales;

De cara al responsable y al encargado del tratamiento:

- promover la sensibilización de los responsables y encargados del tratamiento acerca de sus obligaciones;
- elaborar y mantener una lista relativa al requisito de la evaluación de impacto relativa a la protección de datos;
- ofrecer asesoramiento sobre las operaciones de tratamiento ;
- alentar la elaboración de códigos de conducta ;
- fomentar la creación de mecanismos de certificación de la protección de datos y de sellos y marcas de protección de datos ;
- elaborar y publicar los criterios para la acreditación de organismos de supervisión de los códigos de conducta;
- efectuar la acreditación de organismos de supervisión de los códigos de conducta;
- autorizar las cláusulas contractuales y disposiciones

De cara a otras autoridades de control y función investigadora:

- cooperar con otras autoridades de control y prestar asistencia mutua;
- llevar a cabo investigaciones en particular basándose en información recibida de otra autoridad de control u otra autoridad pública;

Todas estas funciones deben ser gratuitas para el interesado y para el delegado de protección de datos, pero cuando sean manifiestamente infundadas o excesivas, se podrá establecer una tasa razonable basada en los costes administrativos o negarse a actuar respecto de la solicitud. La carga de demostrar el carácter manifiestamente infundado o excesivo de la solicitud recaerá en la autoridad de control.

Poderes de las agencias de control (artículo 58)

De cara al responsable y al encargado del tratamiento y, en su caso, al representante del responsable o del encargado, puede ordenarles que faciliten cualquier información que requiera para el desempeño de sus funciones, así como obtener del responsable y del

encargado del tratamiento el acceso a todos los datos personales y a toda la información necesaria para el ejercicio de sus funciones, notificando al responsable o al encargado del tratamiento las presuntas infracciones; para ello puede llevar a cabo investigaciones en forma de auditorías de protección de datos y llevar a cabo una revisión de las certificaciones expedidas.

Una vez se detecta algo sancionable, puede sancionar a todo responsable o encargado del tratamiento mediante una advertencia o con un apercibimiento y ordenar al responsable o encargado del tratamiento que atiendan las solicitudes de ejercicio de los derechos del interesado, ordenándoles que las operaciones de tratamiento se ajusten a las disposiciones del Reglamento, cuando proceda, de una determinada manera y dentro de un plazo especificado; además de ordenar al responsable del tratamiento que comunique al interesado las violaciones de la seguridad de los datos personales y ordenar la rectificación o supresión de datos personales o la limitación de tratamiento.

Puede imponer una limitación temporal o definitiva del tratamiento, incluida su prohibición, retirar una certificación, imponer una multa administrativa y ordenar la suspensión de los flujos de datos hacia un destinatario situado en un tercer país.

A nivel de asesoramiento e información, puede asesorar al responsable del tratamiento conforme al procedimiento de consulta previa, emitir, por iniciativa propia o previa solicitud, dictámenes destinados al Parlamento nacional, al Gobierno del Estado sobre cualquier asunto relacionado con la protección de los datos personales, emitir un dictamen y aprobar proyectos de códigos de conducta.

Es importante reseñar la vinculación de las autoridades de control con los códigos de conducta. A ello volveremos en este mismo tema.

Agencia Española de Protección de Datos

Aunque ya hemos presentado a la AEPD, vamos a hablar un poco de su estructura y funcionamiento. Empecemos viendo un organigrama de la Agencia Española de Protección de Datos:

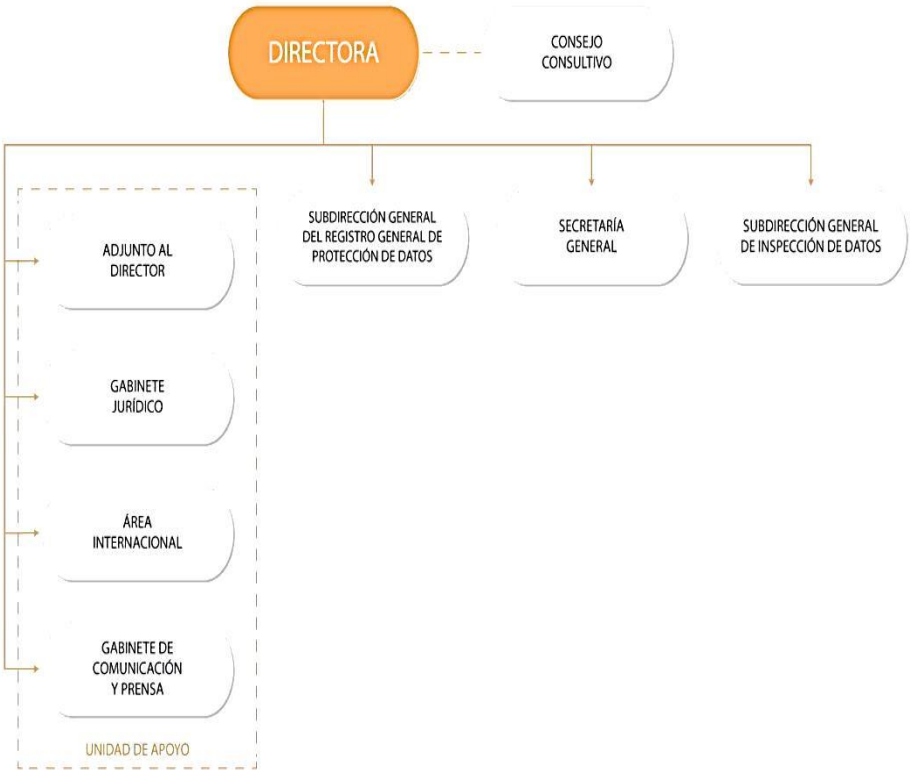


Ilustración 5. Organigrama de la AEPD. Fuente: (Agencia Española de Protección de Datos, 2018)

Vemos dos elementos muy singulares: el registro y la inspección de datos. Vamos a dedicarles unas líneas, así como a la figura de la directora.

El Registro General de Protección de Datos:

¿Qué papel tiene, en que se ocupa el Registro General? Sin ánimo exhaustivo, en esta parte de la AEPD:

- Se promocionan, registran y publican los códigos de conducta, tramitándolos y valorando las solicitudes de aprobación.
- Se elaboran los criterios para la acreditación de los organismos de supervisión de los códigos de conducta y se tramitan y valoran su acreditación y revocación.
- Se promoción los certificados, sellos y marcas en protección de datos. Se elaboran los criterios para la acreditación de los organismos de certificación y se realiza el control de las certificaciones expedidas y su revisión periódica.
- Se encargan de la elaboración y tramitación de cláusulas contractuales tipo de protección de datos para transferencias internacionales.
- Se tramitan y valoran las solicitudes de autorización de transferencias internacionales de datos, y gestión de las comunicaciones.
- Se tramitan y valoran las solicitudes de aprobación de normas corporativas vinculantes para transferencias internacionales de datos.
- Se elaboran y tramitan las cláusulas de encargados de tratamiento.
- Se elaboran materiales de ayuda a responsables y encargados en el cumplimiento de la normativa de protección de datos.
- Se atienden las consultas planteadas por responsables, encargados y delegados de protección. También se atienden las consultas presentadas por los ciudadanos sobre ejercicio de sus derechos y presentación de reclamaciones.

- Se hace cargo de las tares relativas a la transparencia exigidas a la Agencia.

Dentro de las campañas de sensibilización de protección de datos, destacan las orientadas a centros educativos y menores en particular, así como las orientadas a PYMES, las Administraciones Públicas y ONG´s.

Fijémonos de nuevo en los puntos de contacto entre AEPD y códigos de conducta.

La inspección de datos

De igual modo, sin ánimo de completitud, intentemos destacar sus principales funciones:

- Supervisión permanente del cumplimiento de la normativa en materia de protección de datos por parte de los responsables y encargados de los tratamientos, incluyendo la atención a los ciudadanos en el ejercicio de sus derechos de acceso, rectificación, oposición, supresión, oposición a decisiones automatizadas, limitación al tratamiento y portabilidad.
    - Para efectuar esta supervisión a su vez, se realiza el análisis de las reclamaciones por incidencias concretas, para determinar si las vulneraciones de la normativa se han producido por errores puntuales, o bien se deben a causas sistémicas, en cuyo caso, la Agencia procederá a investigar el origen del problema: esto es, el sistema de gestión de datos del responsable o encargado del tratamiento.
- Realización de investigaciones en forma de auditorías de protección de datos, manteniendo dialogo permanente con los Delegados de Protección de Datos, a efectos de resolver las reclamaciones que presenten los afectados.
- Comprobación del cumplimiento de los códigos de conducta.

Las actuaciones de inspección se orientan a esclarecer los hechos que presuntamente pudieran infringir la normativa en materia de protección de datos, la persona u órgano que pudiera resultar responsable y la repercusión de los mismos. Una de sus manifestaciones es el ejercicio de la potestad sancionadora.

Podrán examinar los soportes de información y equipos físicos, requerir la documentación de los programas y realizar auditorías.

Pero tiene otras labores, de entre las que destaca la necesaria cooperación con otras autoridades de control; el proponer imponer una limitación temporal o definitiva del tratamiento, incluida su prohibición; o proponer ordenar la suspensión de flujos de datos hacia un destinatario situado en un tercer país o hacia una organización internacional.

Director o Directora de la AEPD

El Director o Directora ostenta la representación de la Agencia y sus actos se consideran como actos propios de la Agencia. Sus resoluciones ponen fin a la vía administrativa y son recurribles ante la Sala de lo Contencioso de la Audiencia Nacional.

Su nombramiento lo efectúa el Gobierno mediante Real Decreto de entre quienes componen el Consejo Consultivo y a propuesta del Ministro de Justicia, con un mandato es de cuatro años. No puede recibir instrucciones de ningún poder o autoridad y actúa con pleno

sometimiento al Derecho. Ejerce sus funciones con dedicación exclusiva, plena independencia y total objetividad.

De sus funciones, destacamos:

- Dictar las resoluciones e instrucciones que requiera el ejercicio de las funciones de la Agencia.
- La coordinación con las autoridades autonómicas.
- La representación de la Agencia en el ámbito internacional.
- Funciones de gestión (adjudicar y formalizar los contratos; aprobar gastos y ordenar pagos,…).

El trabajo del profesional de la información.

Hablaremos en este apartado de las tareas que debe llevar a cabo el profesional, en algunos de los roles más destacados, centrándonos en la figura del encargado del tratamiento pero sin olvidar las del responsable o el delegado de datos…

Hay elementos que deben ser llevados a cabo con la máxima diligencia, como el registro de las actividades de tratamiento, la evaluación de impacto, la atención a los derechos de sus usuarios… vamos a ir desgranando los más importantes.

Subrayemos uno de los principales cambios: la actitud del profesional debe ser proactiva. No basta con cumplir la ley, hay que demostrar que se ha puesto todo lo posible por su parte por cumplirla.

¿Y que implica esta responsabilidad activa? Básicamente, que las empresas deben adoptar medidas que aseguren razonablemente que están en condiciones de cumplir con los principios, derechos y garantías, con una hoja de ruta prolija que incluiría[9]:

- Protección de datos desde el diseño
- Protección de datos por defecto
- Medidas de seguridad
- Mantenimiento de un registro de tratamientos
- Realización de evaluaciones de impacto sobre la protección de datos
- Nombramiento de un delegado de protección de datos
- Notificación de violaciones de la seguridad de los datos
- Promoción de códigos de conducta y esquemas de certificación.

Antes de empezar, el profesional debe plantearse una serie de preguntas cómo… ¿se pueden generar con el tratamiento situaciones de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño… ? ¿Se puede privar a los afectados de sus derechos y libertades? ¿Se trabaja con categorías especiales[10] de datos o datos relacionados con la comisión de infracciones administrativas? ¿Se crean perfiles? ¿Sobre economía, salud…? ¿Se trata de datos de grupos de afectados vulnerables[11]? ¿Se trata de un tratamiento

[9] Un paso excelente para no perderse es atender a las recomendaciones de la AEPD. Por ejemplo, seguir si "Listado de cumplimiento normativo" (AEPD, 2018)

[10] Datos genéticos, datos biométricos, datos relativos a la salud…

[11] Menores de edad y personas con discapacidad…

masivo? ¿Va a darse una transferencia, con carácter habitual, a terceros Estados u organizaciones internacionales sin un nivel adecuado de protección?.

Esto es… debe ponerse en el peor de los casos. Debe prever, y para ello, es muy recomendable que a priori, considere los códigos de conducta y estándares definidos.

Actuaciones del responsable y del encargado del tratamiento

Hay dos elementos de muy importante consideración: las medidas de responsabilidad activa y la evaluación de impacto. Podemos tener una relación completa en el artículo 28 de la ley 3/18 y en los 24 y 25 del RGPD

A modo de resumen, veamos cuales serían los tratamientos de mayor riesgo que conlleven considerar medidas y realizar evaluaciones de impacto. Debemos plantearnos...

¿Se pueden generar con el tratamiento situaciones de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico, moral o social significativo para los afectados?

¿Puede el tratamiento privar a los afectados de sus derechos y libertades o impedirles el control sobre sus datos personales?

¿Se trata de un tratamiento no meramente accesorio de las categorías especiales de datos o de datos relacionados con la comisión de infracciones administrativas?

¿Implica el tratamiento una evaluación de aspectos personales de los afectados con el fin de crear o utilizar perfiles personales de los mismos, en particular mediante el análisis o la predicción de aspectos referidos a su rendimiento en el trabajo, su situación económica, su salud, sus preferencias o intereses personales, su fiabilidad o comportamiento, su solvencia financiera, su localización o sus movimientos?

¿Se trata de datos de grupos de afectados en situación de especial vulnerabilidad, en particular, menores de edad y personas con discapacidad?

¿Se trata de un tratamiento masivo que implique a un gran número de afectados o la recogida de una gran cantidad de datos personales?

¿Van a ser los datos personales fuesen a ser objeto de transferencia, con carácter habitual, a terceros Estados u organizaciones internacionales respecto de los que no se hubiese declarado un nivel adecuado de protección?

Además de todo lo anterior, hay que considerar a juicio del responsable o del encargado otros factores con relevancia, sobre todo los previstos en códigos de conducta y estándares definidos.

Este punto será desarrollado en anexos.

Registro de actividades de tratamiento

Una de las tareas en las que el profesional debe poner más empeño, ya que se trata de algo que se produce en su día a día laboral, es el del registro de las actividades del tratamiento. En la ley 3/2018 podemos encontrar en su artículo 31 la regulación correspondiente, así como en el artículo 30 del RGPD.

Este registro puede organizarse mediante conjuntos estructurados de datos, y deberá especificar las actividades de tratamiento llevadas a cabo y las demás circunstancias que el RGPD establece. Todo cambio en el contenido de este registro debe comunicarse al DPD si lo hubiera. El inventario de las actividades de tratamiento debe ser público y accesible por medios electrónicos e incluir:

- el nombre y los datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable, y del delegado de protección de datos;
- los fines del tratamiento;
- una descripción de las categorías de interesados y de las categorías de datos personales;
- las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales;
- en su caso, las transferencias de datos personales a un tercer país o una organización internacional, incluida la identificación de dicho tercer país u organización internacional;
- si es posible, los plazos previstos para la supresión de las diferentes categorías de datos y una descripción general de las medidas técnicas y organizativas de seguridad.

Además, cada encargado llevará un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de un responsable que debe contener:

- Nombre y los datos de contacto del encargado o encargados y de cada responsable por cuenta del cual actúe el encargado, y, en su caso, del representante del responsable o del encargado, y del delegado de protección de datos;
- Categorías de tratamientos efectuados por cuenta de cada responsable;
- Si se dan, transferencias de datos personales a un tercer país;
- Cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad.

Estos registros, de encargado y responsable, constarán por escrito y se pondrá a disposición de la autoridad de control que lo solicite. Hay que indicar que no son aplicables a ninguna empresa ni organización que emplee a menos de 250 personas, a menos que el tratamiento que realice pueda entrañar un riesgo para los derechos y libertades de los interesados, no sea ocasional, o incluya categorías especiales de datos personales.

Con el Reglamento desaparece la obligación de notificar la inscripción de ficheros, tanto de responsables públicos o privados que existía en la LOPD, en el Registro de Ficheros de la AEPD, o registro de la autoridad autonómica competente, sin perjuicio de la obligación de implementar el Registro de Actividades de Tratamiento.

El registro de actividades de tratamiento sirve como primer elemento para valorar el compromiso del responsable y el encargado con los requisitos legales En él se reseñan tanto los ficheros que se emplean como las medidas de seguridad usadas.

Perfiles e información al afectado: transparencia.

Las capacidades de cálculo de los procesadores permiten jugar mucho con los datos y elaborar perfiles cada vez más complejos de nuestro comportamiento. A esto no es ciega la ley, que obliga a informar al afectado de la existencia de esos perfiles. Eso puede verse en la ley 3/2018 en su artículo 11 y en particular en el RGPD, en sus artículos 12, 13 y 14, con especial atención a los perfiles en su artículo 22.

Cabe distinguir dos posibilidades: que el interesado diera sus datos directamente o que no procedan de forma directa del mismo.

En todo caso, deben facilitarse: la identidad y los datos de contacto del responsable y, en su caso, de su representante; incluyendo una dirección electrónica u otro medio similar para que se puedan poner en contacto. Si hay DPD, también sus datos de contacto; los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento, así como los intereses legítimos del responsable o de un tercero para efectuarlo; los destinatarios o las categorías de destinatarios de los datos personales, y si se trata de datos no dados directamente por los afectados, las fuentes de las que proceden y, si se da el caso, informar de la intención del responsable de transferir datos personales a un tercer país u organización internacional.

Al afectado le debe quedar clara la posibilidad de ejercer sus derechos, de entre ellos, destaca el de no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar.

También hay que facilitar el plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo; la existencia de decisiones automatizas, incluida la elaboración de perfiles; y cuando el responsable del tratamiento proyecte el tratamiento ulterior de datos personales para un fin que no sea aquel para el que se recogieron, proporcionará al interesado, con anterioridad a dicho tratamiento, información sobre el mismo;

Es importante informar del derecho a solicitar al responsable del tratamiento el acceso, rectificación o supresión, limitación, oposición y portabilidad de los datos y el derecho a presentar una reclamación ante una autoridad de control.

Si el interesado es quien nos facilita sus datos, debemos indicar si la comunicación de los mismos es un requisito legal o contractual, o un requisito necesario para suscribir un contrato. Si los datos no vienen directamente del interesado, hay que añadir la fuente de la que proceden los datos personales y, en su caso, si proceden de fuentes de acceso público.

El plazo indicado es, a más tardar, en un mes desde la obtención de los datos personales, para comunicar si los datos van a emplearse para la comunicación con el interesado, y, si está previsto comunicarlos a otro destinatario, a más tardar en el momento en que los datos personales sean comunicados por primera vez. Pero esto no es aplicable si el interesado ya dispone de la información o comunicar esta supone un esfuerzo desproporcionado, sobre todo cuando se trate de tratamiento con fines de archivo en interés público (investigación científica, histórica o fines estadísticos); o bien si la obtención o comunicación esté expresamente establecida por el Derecho de la Unión o de los Estados miembros, o cuando los datos personales deban seguir teniendo carácter confidencial sobre la base de una obligación de secreto profesional regulada por el Derecho de la Unión o de los Estados miembros.

¿Y cómo se han de ofrecer esas informaciones? En un formato estructurado, de uso común, de lectura mecánica e interoperable[12]. El derecho del interesado a transmitir o recibir datos personales que lo conciernan no debe obligar al responsable a adoptar o mantener sistemas de tratamiento que sean técnicamente compatibles.

¿Y si se nos pide que suprimamos datos? Hay una consideración clave: Esto no debe implicar la supresión de los datos personales concernientes al interesado que este haya facilitado para la ejecución de un contrato, en la medida y durante el tiempo en que los datos personales sean necesarios para la ejecución de dicho contrato.

Artículos de máximo interés para entender los perfiles:

Artículo 11 Ley 3/2018. Transparencia e información al afectado.

RGPD. Artículo 12. Transparencia de la información, comunicación y modalidades de ejercicio de los derechos del interesado.

RGPD. Artículo 13. Información que deberá facilitarse cuando los datos personales se obtengan del interesado.

RGPD. Artículo 14. Información que deberá facilitarse cuando los datos personales no se hayan obtenido del interesado.

RGPD. Artículo 22. Decisiones individuales automatizadas, incluida la elaboración de perfiles.

Seguridad del tratamiento

El Reglamento obliga a que, considerando el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado apliquen medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo[13]. (Artículo 32)

[12] Por ello, desde los estados se alienta a los responsables a crear formatos interoperables que permitan la portabilidad de datos.

[13] Es muy difícil evaluar el riesgo. Pongamos dos ejemplos de ciberataques con robo de datos personales:

Estas medidas pasan por emplear:

- la seudonimización y el cifrado de datos personales;
- la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;
- la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;
- un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

Los riesgos que se marcan como más preocupantes serían la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

Buscamos evitar daños y perjuicios físicos, materiales o inmateriales, en particular en los casos en los que el tratamiento pueda dar lugar, por ejemplo, problemas de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación…

Cabe recordar en este punto que el Reglamento contempla la protección de datos desde el diseño y por defecto, en su artículo 25.

¿Y si se produce una violación de la seguridad de los datos personales? Este es uno de los momentos críticos para el profesional. Además de por indicarlo el sentido común, la norma advierte de la necesaria notificación, no solo al interesado (Artículo 34), sino también a la autoridad de control (Artículo 33), con unos plazos muy breves

¿Qué debe contener cada notificación? Antes de nada, precisemos que la AEPD ofrece un apoyo fantástico a este respecto, con su Guía para la gestión y notificación de brechas de seguridad (AEPD & INCIBE, 2017).

De cara a la autoridad de control, debe figurar:

1. la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados;
2. nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información;
3. descripción de las posibles consecuencias de la violación de la seguridad de los datos personales;
4. descripción de las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

Por una parte, un ataque de anonimous donde se llevaron más de 200GB de información de la base de datos de Stratfor Global, compañía especializada en seguridad, con información de sus clientes (nºs de tarjetas de crédito, direcciones y correos electrónicos). ¿Era previsible? Quizá por la visibilidad de la empresa ¿Qué sucedió con los datos? Lo importante aquí es la pregunta "que podría pasar". Y la respuesta es espeluznante. Frente a este caso de dimensiones casi globales, nos encontramos otros más de andar por casa, como aquel centro de salud que vio filtrados los datos de 1700 pacientes por medio del programa eMule en las redes P2P. Un alcance menor, con datos muy sensibles. ¿Cómo evitarlo?

De cara al interesado, si es previsible una violación de la seguridad, el responsable la comunicará al interesado sin dilación indebida, describiendo con lenguaje claro y sencillo, la naturaleza de la violación de la seguridad y las medidas a tomar. Esta comunicación no será necesaria si el responsable del tratamiento ha adoptado medidas de protección técnicas y organizativas apropiadas y los datos resultan ininteligibles (cifrado), o si se han tomado medidas ulteriores que garanticen que eliminen el riesgo; o si la comunicación supone un esfuerzo desproporcionado, en cuyo caso puede hacerse una comunicación pública. Destaquemos que las comunicaciones a los interesados deben realizarse tan pronto como sea razonablemente posible y en estrecha cooperación con la autoridad de control, siguiendo sus orientaciones o las de otras autoridades competentes, como las autoridades policiales.

Toda violación de la seguridad la documentará el responsable del tratamiento.

¿Y el secreto profesional?

Los Estados miembros podrán adoptar normas específicas para fijar los poderes de las autoridades de control en relación con los responsables o encargados sujetos a una obligación de secreto profesional, cuando sea necesario. Esas normas solo se aplicarán a los datos personales recibidos en ocasión de una actividad cubierta por la obligación de secreto. (Artículo 90)

Procurando un equilibrio entre lo técnicamente posible en cada momento, y los riesgos que entraña el tratamiento de datos, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización o la minimización de datos. **Solo deben ser objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento, lo que debe entenderse tanto en lo relativo a la extensión de su tratamiento, como a su plazo de conservación y a su accesibilidad. Esto es lo que entendemos por Protección de datos desde el diseño y por defecto** (Artículo 25)[14]

En los tratamientos que no requiere identificación de un interesado por el responsable, este no estará obligado a mantener, obtener o tratar información adicional con vistas a identificar al interesado con la única finalidad de cumplir el Reglamento. Si es capaz de demostrar que no está en condiciones de identificar al interesado, le informará de ser posible. (Artículo 11)

Un asunto espinoso para todo profesional es la confidencialidad, lo que muchas veces se confunde con el secreto profesional. En el caso de la protección de datos, además, las normas hablan expresamente de ella. Los artículos de interés son los mismos que para el consentimiento.

[14]Este principio de privacidad desde el diseño (art. 25.1), significa que en el diseño de aplicaciones que traten datos personales, se tiene que garantizar la privacidad de los mismos desde el principio. Esto implica, por ejemplo, que en materia de redes sociales, los perfiles de privacidad de los usuarios estarán por defecto cerrados a otros usuarios, debiendo ser el usuario quien los abra a otros.

La primer a pregunta sería ¿quién está sujeto al deber de confidencialidad? La respuesta es muy amplia: responsables y encargados del tratamiento, así como quienes intervengan en cualquier fase del mismo.

La segunda y más importante es ¿hasta cuándo se mantiene el deber de confidencialidad? Este deber, complementario al de secreto profesional cuando la relación profesional está en activo, se mantiene aunque hubiese finalizado la relación del obligado a guardar secreto con el responsable o encargado del tratamiento de los datos.

¿Cómo y cuándo se realiza una evaluación de impacto relativa a la protección de datos?

Sobre este punto hay unas directrices que detallan de forma concienzuda que hacer. Se trata de la WP 248 (Grupo "Protección de datos" del artículo 29, 2017). El punto fundamental a repasar en el RGPD es su artículo 35.

Los tratamientos de datos emplean técnicas cambiantes en el tiempo. A menudo, nos encontramos con problemas, con agujeros de seguridad, que resultan absolutamente inesperados. Otras, hay indicios que nos avisan de por dónde pueden venir los problemas.

Ya que es probable que las operaciones de tratamiento entrañen un alto riesgo para los derechos y libertades de las personas físicas, el responsable debe realizar una evaluación de impacto que evalúe el origen, la naturaleza, la particularidad y la gravedad de dicho riesgo.

El resultado de la evaluación debe tenerse en cuenta cuando se decidan las medidas adecuadas que deban tomarse con el fin de demostrar que el tratamiento de los datos personales es correcto (Considerando 84). Se realizará antes del tratamiento, con el asesoramiento del delegado de protección de datos, si lo hay.

Esta evaluación es imprescindible que se haga si se realiza una evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar; si se trata de tratamiento a gran escala de las categorías especiales de datos, o si se realiza una observación sistemática a gran escala de una zona de acceso público.

¿Qué operaciones son las que necesitan de una evaluación de impacto?¿Cuáles no? La autoridad de control (Agencia Española de Protección de Datos, 2018) tiene entre sus funciones informar de esto. Pero es tenemos una herramienta fabulosa en las directrices del Grupo 29 (Grupo "Protección de datos" del artículo 29, 2017).

En el documento de la Agencia (AEPD, 2017)nos encontramos con este gráfico que es muy clarificador al respecto del posible flujo de trabajo que un responsable debe seguir.

Ilustración 6 Hoja de ruta a seguir por un responsable del tratamiento. (AEPD, 2017)

La evaluación deberá incluir como mínimo:

1. una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive el interés legítimo perseguido por el responsable del tratamiento;
2. una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad;
3. una evaluación de los riesgos para los derechos y libertades de los interesados
4. las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales.

El cumplimiento de los códigos de conducta por los responsables o encargados correspondientes se tendrá debidamente en cuenta al evaluar las repercusiones de las operaciones de tratamiento, en particular a efectos de la evaluación de impacto relativa a la protección de datos.

Si es preciso el responsable examinará si el tratamiento es conforme con la evaluación de impacto relativa a la protección de datos, al menos cuando exista un cambio del riesgo que representen las operaciones de tratamiento (pensemos, por ejemplo, en un cambio de un algoritmo que revisa una base de datos de clientes, que al no estar previsto por la evaluación de impacto, deja al descubierto nuevos riesgos).

El responsable facilitará a la autoridad de control la evaluación de impacto relativa a la protección de datos e informará a la autoridad de control de las responsabilidades respectivas del responsable, los corresponsables y los encargados, así como de los fines y medios del tratamiento previsto y las medidas y garantías establecidas. Si lo hay, también facilitará los datos de contacto del delegado de protección de datos; además de cualquier otra información que solicite la autoridad de control. (Artículo 36)

Es de mucho interés la aplicación de la AEPD para realizar evaluaciones de impacto: https://gestiona.aepd.es/

¿Cómo debe actuar el profesional ante la transparencia?

Hemos hablado de la aparente incompatibilidad de algunas leyes. Hemos destacado ya como la protección de datos y la libertad de expresión parecen chocar, y algo avanzábamos sobre la transparencia. Obviamente, no podemos hacer transparente un pedazo de madera, no podemos revelar datos personales para decir que no tenemos secretos, sobre todo porque esos no serán nuestros secretos, sino los de los propietarios de los datos.

Ahora, rizamos el rizo: hemos de ser transparentes en nuestro trabajo. Hemos de hacer ver como impedimos que se vea lo que la ley impide ver. Este trabalenguas tiene respuesta en el artículo 12 del reglamento. Y es muy interesante por estar íntimamente ligado al punto que veremos a continuación, uno de los que despierta más preocupación entre los profesionales: el consentimiento.

El interesado debe conocer la existencia de la operación de tratamiento y sus fines. El responsable del tratamiento debe facilitar al interesado cuanta información complementaria sea necesaria para garantizar un tratamiento leal y transparente, considerando circunstancias y contexto. Debe así mismo informar al interesado de la existencia de la elaboración de perfiles y de las consecuencias de dicha elaboración. Si los datos personales se obtienen de los interesados, también se les debe informar de si están obligados a facilitarlos y de las consecuencias en caso de que no lo hicieran. Esta información puede transmitirse en combinación con unos iconos normalizados que ofrezcan, de forma fácilmente visible, inteligible y claramente legible, una adecuada visión de conjunto del tratamiento previsto. Los iconos que se presentan en formato electrónico deben ser legibles mecánicamente. (Considerando 60)

De mucho interés: el responsable debe tener en cuenta la necesidad de usar un lenguaje claro y sencillo, en particular cuando se dirija específicamente a un niño.

¿Debemos siempre dar la información que se nos pide de forma tangible o electrónica? No. No necesariamente ha de tener un formato electrónico o impreso, si la solicitud se hace de forma verbal, la respuesta puede darse de esta forma, siempre que esté suficientemente acreditada

la identidad del peticionario. Se puede solicitar que se facilite la información adicional necesaria para confirmar la identidad del interesado, lo que es lógico, para evitar darle información sobre los datos a quien no debería tenerla. Cuando el interesado presente la solicitud por medios electrónicos, la información se facilitará por medios electrónicos cuando sea posible, a menos que el interesado solicite que se facilite de otro modo. La información facilitada así como toda comunicación y cualquier actuación serán a título gratuito.

En cuanto a los plazos, en un mes debe darse cumplida respuesta y, si por razones de complejidad o de elevado número de solicitudes no es posible, se puede prorrogar otros dos meses, informando al interesado de dicha prórroga en el plazo de un mes a partir de la recepción de la solicitud, indicando los motivos de la dilación. Si no da curso a la solicitud y no informa de las razones de su no actuación, existe la posibilidad de presentar una reclamación ante una autoridad de control y de ejercitar acciones judiciales. Si las solicitudes son manifiestamente infundadas o excesivas (p.e. por su carácter repetitivo), el responsable del tratamiento podrá cobrar un canon razonable en función de los costes administrativos afrontados para facilitar la información o la comunicación o realizar la actuación solicitada, o negarse a actuar respecto de la solicitud. En todo caso, el responsable del tratamiento soportará la carga de demostrar el carácter manifiestamente infundado o excesivo de la solicitud.

El consentimiento

El consentimiento del afectado para el tratamiento de sus datos se modifica: se hace preciso que éste sea más claro. Por otra parte, hay singularidades con respecto al tratamiento de datos de menores que nos obliga a detenernos con algo más de detalle. En la ley 3/2918 tenemos que detenernos en los artículos 6, 9 y 10, para el consentimiento en general, y en particular en el 7 y en el 12.6 para lo que respecta a menores. En el RGPD debemos acudir a los artículos 4.11, 7 y 9 al que añadimos el 8 para hablar de menores.

Se nos plantean muchas preguntas. Por ejemplo: si tenemos una relación contractual con un cliente ¿debe supeditarse este contrato al consentimiento del tratamiento? La respuesta es NO. Si el afectado no consiente en el tratamiento para finalidades no relacionadas con el contrato, esto no debe condicionar la ejecución del mismo. Esto nos lleva a algo muy importante:

El consentimiento siempre debe prestarse a través de una declaración o una clara acción afirmativa y cuando sean varias las finalidades del tratamiento, debe otorgarse el consentimiento para cada una de ellas.

Por ejemplo, en un hospital privado no pueden negarnos la atención médica si no aceptamos el consentimiento para que nuestros datos sean empleados para mandarnos publicidad de su sección ortopédica.

Para las personas físicas debe quedar totalmente claro que se están recogiendo, utilizando, consultando o tratando de otra manera datos personales que les conciernen, así como la medida en que dichos datos son o serán tratados.

El principio de transparencia exige que toda información y comunicación relativa al tratamiento de dichos datos sea fácilmente accesible y fácil de entender, y que se utilice un lenguaje sencillo y claro, evidenciando tanto los riesgos, las normas, las salvaguardias y los derechos relativos al tratamiento de datos personales así como del modo de hacer valer sus derechos en relación con el tratamiento, como los fines específicos del tratamiento de los datos personales deben ser explícitos y legítimos, y deben determinarse en el momento de su recogida.

Aparece el término "inequívoco": esto quiere decir que se requiere que haya una declaración de los interesados o una acción positiva que indique el acuerdo del interesado.

Es importante subrayar que tiene que ser verificable, el responsable deberá ser capaz de demostrarlo.

Si se da en una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento se presentará de tal forma que se distinga claramente de los demás asuntos, de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo, dejando por sentado que no será vinculante ninguna parte de la declaración que constituya infracción del Reglamento.

El interesado tendrá derecho a retirar su consentimiento en cualquier momento. Será tan fácil retirar el consentimiento como darlo.

Al evaluar si el consentimiento se ha dado libremente, se tendrá en cuenta en la mayor medida posible el hecho de si, entre otras cosas, la ejecución de un contrato, incluida la prestación de un servicio, se supedita al consentimiento al tratamiento de datos personales que no son necesarios para la ejecución de dicho contrato.

Otro elemento de interés por su sensibilidad es el registro de datos relativos a condenas e infracciones penales, procedimientos y medidas de seguridad conexas. Además de lo que dicen los textos que manejamos, Ley y Reglamento, no olvidemos la norma específica (Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo)

En resumen, este tratamiento tan particular deberá realizarse conforme al artículo 10 del Reglamento y a lo establecido en el Sistema de registros administrativos de apoyo a la Administración de Justicia. Los tratamientos de los datos de naturaleza penal distintos a los anteriores sólo serán posibles cuando sean llevados a cabo por abogados y procuradores y tengan por objeto recoger la información facilitada por sus clientes para el ejercicio de sus funciones.

Cuando el tratamiento se lleva a cabo con el consentimiento del interesado, el responsable del tratamiento debe ser capaz de demostrar que aquel ha dado su consentimiento a la operación de tratamiento. En particular en el contexto de una declaración por escrito efectuada sobre

otro asunto, debe haber garantías de que el interesado es consciente del hecho de que da su consentimiento y de la medida en que lo hace. En todo caso ha de tratarse de una formulación inteligible y de fácil acceso que emplee un lenguaje claro y sencillo, y que no contenga cláusulas abusivas. Para que el consentimiento sea informado, el interesado debe conocer como mínimo la identidad del responsable del tratamiento y los fines del tratamiento a los cuales están destinados los datos personales. El consentimiento no debe considerarse libremente prestado cuando el interesado no goza de verdadera o libre elección o no puede denegar o retirar su consentimiento sin sufrir perjuicio alguno. (Considerando 42).

El consentimiento debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen, como una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal. Esto podría incluir marcar una casilla de un sitio web en internet, escoger parámetros técnicos para la utilización de servicios de la sociedad de la información, o cualquier otra declaración o conducta que indique claramente en este contexto que el interesado acepta la propuesta de tratamiento de sus datos personales.

El silencio, las casillas ya marcadas o la inacción no deben constituir consentimiento. El consentimiento debe darse para todas las actividades de tratamiento realizadas con el mismo o los mismos fines. Cuando el tratamiento tenga varios fines, debe darse el consentimiento para todos ellos. Si el consentimiento del interesado se ha de dar a raíz de una solicitud por medios electrónicos, la solicitud ha de ser clara, concisa y no perturbar innecesariamente el uso del servicio para el que se presta. (Considerando 42)[15].

Consentimiento y menores

La primera duda sería ¿Que es un menor? ¿A partir de que edades establecemos la frontera? La ley la establece en los 14 años, con las excepciones lógicas: aquellos supuestos en que la ley exija la asistencia de los titulares de la patria potestad o tutela; además, los titulares de la patria potestad podrán ejercitar en nombre y representación de estos menores los derechos de acceso, rectificación, cancelación, oposición u otros que pudieran corresponderles. Si miramos el RGPD, se nos indica, en relación con la oferta directa a niños de servicios de la sociedad de la información, que el tratamiento se considerará lícito a partir de los 16 años.

[15] No hace falta que aludamos a contraejemplos. El consentimiento es, probablemente, a fecha en que estas líneas son escritas, lo que peor parece haber sido entendido por los profesionales. Nada que extrañar, aunque si resulta cuando menos llamativo que muchas webs de ayuntamientos sigan sin actualizar sus avisos legales y políticas de privacidad y haciendo referencia no ya a la LOPD, omitiendo alusiones al Reglamento o a la ley 3/2018, sino incluso ¡a la LORTAD!, ley que fue derogada en el año 1999. Afortunadamente, admítaseme la ironía, ya no aluden a las "Leyes y ordenanzas nuevamente hechas por su Majestad para la gobernación de las Indias y buen tratamiento y conservación de los Indios".
No obstante, cabe señalar un ejemplo no solo de desconocimiento de la norma, sino incluso de mala praxis clarísima: en al menos dos importantes hospitales, gestionados por manos privadas, he constatado que el consentimiento se da de forma implícita al firmar el registro de entrada al servicio, con las casillas pre marcadas y aludiendo a que la no aceptación de alguna de las mismas implica cambios en el servicio y sobre todo en el pago ("En el caso de oponerse (…) será íntegramente de su cargo (…) el pago de los productos y/o servicios prestados").

El tema de los menores es lo suficientemente delicado como para que la ley los trate con detalle, como veremos en este mismo texto.

Ante cualquier duda, la recomendación inmediata es consultar las Directrices sobre el consentimiento en el sentido del Reglamento (UE) 2016/679. (GRUPO DE TRABAJO DE PROTECCIÓN DE LAS PERSONAS (Grupo de trabajo del artículo 29), 2018)

El Responsable del tratamiento ante la inexactitud de los datos.

La pregunta que ocupa al profesional que trabaja con datos cuando estos se demuestran no exactos es ¿Se me puede imputar algo por ello? La respuesta la traen los artículos 4 y 5 de la ley 3/2018 y los apartados d) y f) del artículo 5 del RGPD.

En resumen, no sería imputable cuando haya adoptado sin dilación las medidas razonables para su supresión o rectificación y siempre que los datos:

- Hubieran sido obtenidos por el responsable directamente del afectado o de un registro público o bien a través de un mediador o intermediario, en cuyo caso esté último asumirá la responsabilidad.
- Hubieran sido tratados por el responsable tras haberlos recibido de otro responsable, en virtud del ejercicio de portabilidad.

Los datos de los trabajadores. Tratamiento en el ámbito laboral (Artículo 88)

Una empresa no puede vivir sin gestionar los datos de sus trabajadores. Esto ha sido así desde tiempos inmemoriales, motivo por el que los distintos estados han creado a lo largo de las décadas sus propias normas al respecto. Eso, lo respeta el Reglamento indicando que podrán establecer normas más específicas para garantizar la protección de los derechos y libertades en relación con el tratamiento de datos personales de los trabajadores en el ámbito laboral, contemplando particularmente que deben incluirse medidas específicas para preservar la dignidad humana de los interesados así como sus intereses legítimos y sus derechos fundamentales, haciendo especial hincapié en la transparencia del tratamiento, la transferencia de los datos personales dentro de un grupo empresarial o de una unión de empresas dedicadas a una actividad económica conjunta y en los sistemas de supervisión en el lugar de trabajo.

¿Qué hacemos con el correo electrónico de los trabajadores? A priori, leer una cuenta de correo ajena, aunque sea de un trabajador, puede asemejarse al registro de una carta, escuchar las conversaciones telefónicas o abrir la taquilla del trabajador. Habrá que actuar por tanto con las mismas consideraciones, que suelen resumirse en obtener una orden judicial, a menos que el tipo de uso y las disposiciones contractuales permitan una opción menos costosa en tiempo. Podemos, eso sí, comprobar si se usa o no, durante cuánto tiempo… pero no ver el contenido, en líneas generales.

¿Y los resultados médicos? En las empresas se hacen revisiones anuales para saber si el trabajador es apto o no para el trabajo que debe desempeñar, pero esos resultados son datos muy sensibles, con una protección especial.

Por otra parte, también existen datos que deben guardarse un cierto tiempo, por lo que sobre ellos no se podrá realizar cancelación, pero si una limitación del uso.

Queda otro tipo de dato singular: los sistemas de videovigilancia. Las imágenes son en sí datos personales, por lo que las consideraciones a tomar deben incluir, además de las lógicas (no grabar conversaciones ni lugares como vestuarios o baños) todas las pertinentes de protección de datos.

Actuaciones del Delegado de protección de datos.

Esta nueva figura nos genera muchas dudas. La principal sería ¿qué organización tiene que contar con un Delegado? ¿Dónde encaja y cómo llega uno a ser Delegado de Protección de Datos (DPD)? La que puede ser más importante es ¿Que debe hacer si se da una reclamación? La ley 3/18 nos lo cuenta en sus artículos 34, 35, 36 y 37, y el RGPD en su artículo 37, 38 y 39.

¿Qué entidades deben contar con un DPD?

Entidad / campo	**Profesionales**	Deporte	Docencia
	Los colegios profesionales y sus consejos generales.	Las federaciones deportivas cuando traten datos de menores de edad.	Los centros docentes que ofrezcan enseñanzas en cualquiera de los niveles establecidos en la legislación reguladora del derecho a la educación, así como las Universidades públicas y privadas.
Entidad / campo	**Sanidad**		
	Los centros sanitarios legalmente obligados al mantenimiento de las historias clínicas de los pacientes. Se exceptúan los profesionales de la salud que, aun estando legalmente obligados al mantenimiento de las historias clínicas de los pacientes, ejerzan su actividad a título individual.		

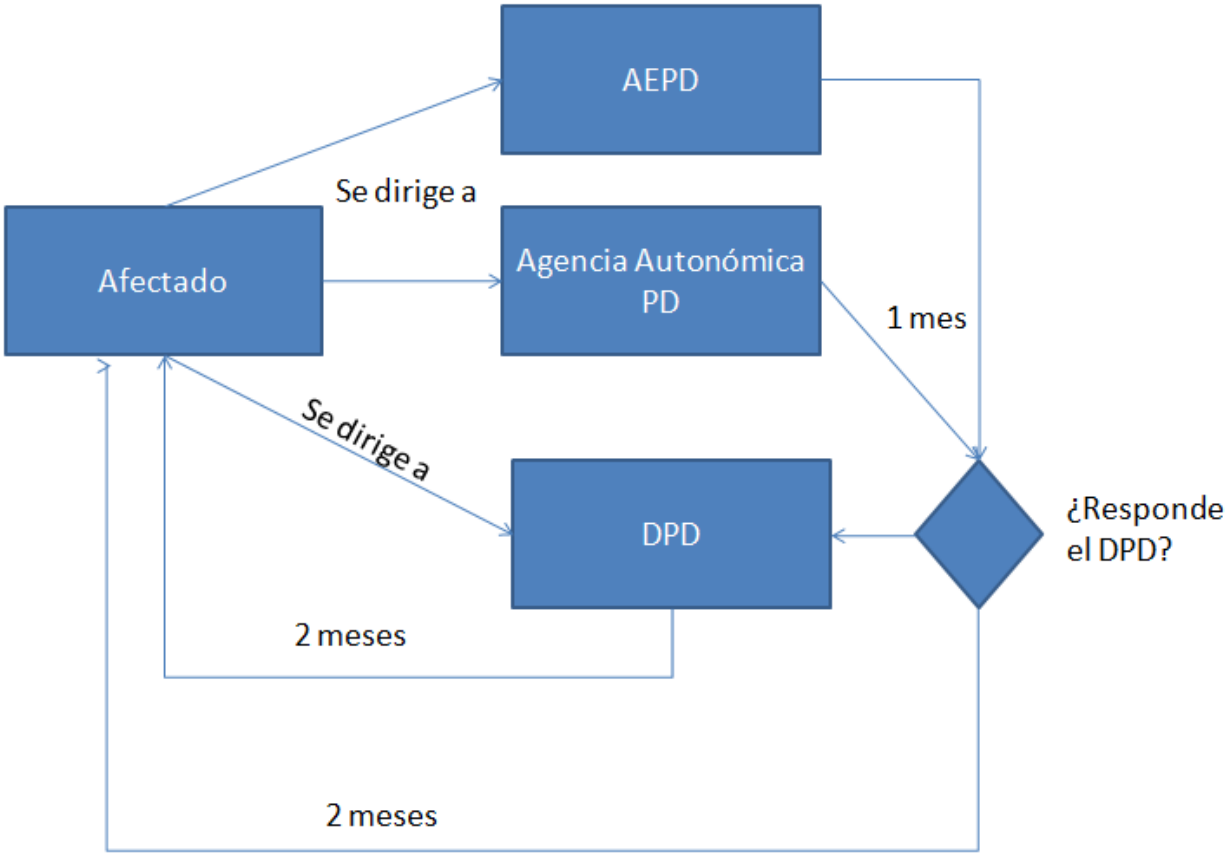
Entidad / campo	**Sector TIC**		
	Las entidades que exploten redes y presten servicios de comunicaciones electrónicas conforme a lo dispuesto en su legislación específica, cuando traten habitual y sistemáticamente datos personales a gran escala.	Los prestadores de servicios de la sociedad de la información cuando elaboren a gran escala perfiles de los usuarios del servicio.	Los operadores que desarrollen la actividad de juego a través de canales electrónicos, informáticos, telemáticos e interactivos, conforme a la normativa de regulación del juego.
Entidad / campo	**Economía, crédito**		
	Las entidades incluidas en el artículo 1 de la Ley 10/2014, de 26 de junio, de ordenación, supervisión y solvencia de entidades de crédito.	Los establecimientos financieros de crédito.	Las empresas de servicios de inversión, reguladas por la legislación del Mercado de Valores.
	Las entidades que tengan como uno de sus objetos la emisión de informes comerciales que puedan referirse a personas físicas.		
Entidad / campo	**Seguridad, aseguradoras**		
	Las entidades aseguradoras y reaseguradoras.	Las entidades responsables de ficheros comunes para la evaluación de la solvencia patrimonial y crédito o de los ficheros comunes para la gestión y prevención del fraude, incluyendo a los responsables de los ficheros regulados por	

		la legislación de prevención del blanqueo de capitales y de la financiación del terrorismo.	
Entidad / campo	**Grandes empresas, publicidad**		
	Los distribuidores y comercializadores de energía eléctrica y los distribuidores y comercializadores de gas natural.	Las entidades que desarrollen actividades de publicidad y prospección comercial, incluyendo las de investigación comercial y de mercados, cuando lleven a cabo tratamientos basados en las preferencias de los afectados o realicen actividades que impliquen la elaboración de perfiles de los mismos.	Las empresas de seguridad privada.

Una pregunta típica es si un DPD debe estar certificado por alguna entidad. Aún más: si puede no ser una persona "humana", física, y en su lugar ser una persona jurídica. No, no es obligatorio certificarse y no debe ser por obligación una persona física. Pero pasar por los procesos voluntarios de certificación (que consideran para ello la posesión de una titulación universitaria que acredite conocimientos especializados en el derecho, y la práctica en materia de protección de datos) es muy ventajoso.

Recordemos que el DPD será el interlocutor con la Agencia, y quien debe documentar y actuar ante vulneraciones relevantes de los derechos. Por ello no podrá ser despedido ni sancionado, salvo que incurra en dolo o negligencia grave, de otra manera impediríamos que actuara con plena independencia, evitando cualquier conflicto de intereses. De igual modo, no se le puede negar el acceso a los datos, sin que la confidencialidad pueda invocarse para ello.

Esta interlocución que señalábamos del DPD con la Agencia, y sus actuaciones ante una reclamación, podríamos resumirlo en la imagen siguiente:



Usando datos de otros. Usando datos en otras partes del globo.

Muchas veces, el profesional debe hacerse cargo de unos datos de los que no es el responsable del tratamiento, ni encargado, ni tan siquiera miembro de la empresa donde esos datos se gestionan. Pensemos en una pequeña gestoría que debe hacer los documentos destinados a la seguridad social de los trabajadores de sus empresas clientes. O pensemos en una agencia de viajes que intercambia los datos de sus clientes con la tienda de muebles que tiene enfrente, para lanzarles publicidad. O ricemos más el rizo, y consideremos que nuestra empresa tiene una sucursal en México y desde allí se nos pide una relación de los clientes locales.

A lo largo del presente epígrafe intentaremos desgranar los aspectos fundamentales de este tipo de situaciones, cada vez más corrientes.

Transferencias internacionales de datos

En este mundo cada vez más pequeño, es raro ceñirse a las propias fronteras a la hora de realizar negocios. Muchas veces se trata de países que no solo están en nuestro entorno, sino también en nuestro marco legal. Otras, se trata de terceros países con una legislación en temas de privacidad inferior la nuestra. Se hace preciso seguir a rajatabla la norma, en concreto los artículos 40 a 43 de la ley 3/2018 y los artículos 44 a 50 del RGPD.

Vemos como la existencia de flujos transfronterizos de datos personales es necesaria para el día a día de personas, negocios e instituciones. Sin embargo, a medida que se incrementan

estos flujos proporcionalmente crece la inquietud sobre la posible reducción o desaparición de la protección de nuestros datos de carácter personal.

Por ello, es precisa la evaluación del tercer país, considerando de qué forma en él se respeta el acceso a la justicia y como sus normas son o no homologables a la legislación europea. Hay que adoptar decisiones que, considerando la legislación vigente en el tercer país, se evalúe si ofrece un nivel adecuado de protección equivalente en lo esencial al ofrecido respecto a los datos personales que son objeto de tratamiento, con especial hincapié en la existencia de un control independiente de la protección de datos y en el establecimiento de mecanismos de cooperación con las autoridades de protección de datos.

Si no existe una decisión que deje clara la adecuación de la protección de los datos, el responsable o el encargado del tratamiento deben entonces por su cuenta tomar medidas para compensar la falta de protección de datos en el tercer país. Estas medidas pueden pasar por normas corporativas vinculantes, o por cláusulas tipo de protección de datos (p.e. las facilitadas por las autoridades de control). La AEPD y las agencias autonómicas prepararán cláusulas contractuales tipo para la realización de transferencias internacionales de pago, sometidas al dictamen del Comité Económico Europeo.

Si no hay una decisión de adecuación de la Comisión, la AEPD puede autorizar previamente transferencias internacionales de datos, con una duración máxima de seis meses cuando la transferencia pretenda fundamentarse en la aportación de garantías adecuadas con fundamento en cláusulas contractuales que no correspondan a las cláusulas tipo, o cuando la transferencia se funde en disposiciones incorporadas a acuerdos internacionales no normativos con otras autoridades u organismos públicos de terceros Estados, que incorporen derechos efectivos y exigibles para los afectados, incluidos los memorandos de entendimiento y se lleve a cabo por alguno de los responsables o encargados relacionados en el artículo 77.1

Con esas garantías se deben garantizar los derechos exigibles y la posibilidad de acceder a acciones legales efectivas, respetando no solo los principios generales relativos al tratamiento de los datos personales, sino también los principios de la protección de datos desde el diseño y por defecto.

No podemos olvidar que debe establecerse la posibilidad de mediar el consentimiento explícito del interesado, y al tiempo la posibilidad de realizar transferencias cuando así lo requieran razones importantes de interés público.

El deber de informar de una transferencia internacional a la AEPD o autoridad autonómica se da siempre que se trate de una transferencia sobre la base de su necesidad para fines relacionados con intereses legítimos imperiosos perseguidos por el responsable y no prevalezcan los derechos o intereses del interesado, y se den también los requisitos siguientes: que no sea repetitiva, que afecte sólo a un número limitado de interesados y que el responsable haya evaluado todas las circunstancias concurrentes. También se informará con carácter previo a los afectados de la transferencia y de los intereses legítimos imperiosos perseguidos, excepto si se realiza por las autoridades públicas en el ejercicio de sus poderes públicos.

Solo se podrán realizar transferencias internacionales de datos si el Responsable o Encargado del tratamiento pueden asegurar que el nivel de protección de datos está garantizado mediante:

- Decisión de adecuación tomada por la Comisión de la UE.

- Garantías adecuadas de protección de datos.

Siempre: contrato con el receptor de datos, especificando en el mismo las garantías adecuadas.

¿Qué debe tener en cuenta la Comisión al evaluar la adecuación del nivel de protección? A modo de esquema:

1. La existencia de un Estado de Derecho, con el respeto de los derechos humanos y las libertades fundamentales, y su legislación pertinente.

2. La existencia de autoridades de control independientes en el tercer país.

3. Los compromisos internacionales asumidos por el tercer país u organización internacional.

Cuando se determina que se tiene un adecuando nivel de protección, se debe establecer un mecanismo de revisión periódica, al menos cada cuatro años. Si se determina que ese tercer país u organización internacional, ya no garantiza un nivel de protección adecuado, se derogará, modificará o suspenderá, en la medida necesaria y sin efecto retroactivo la decisión.

La Comisión publicará en el Diario Oficial de la Unión Europea y en su página web una lista de terceros países, territorios y sectores específicos en un tercer país, y organizaciones internacionales respecto de los cuales haya decidido que se garantiza, o ya no, un nivel de protección adecuado.

El responsable o el encargado del tratamiento solo podrán transmitir datos personales a un tercer país u organización internacional si hubiera ofrecido garantías adecuadas. ¿Cuáles son las "garantías adecuadas"? ¿Cómo se contrastan? Esto puede hacerse mediante:

1. un instrumento jurídicamente vinculante

2. normas corporativas vinculantes

3. cláusulas tipo de protección de datos adoptadas por la Comisión

4. cláusulas tipo de protección de datos adoptadas por una autoridad de control y aprobadas por la Comisión

5. un código de conducta aprobado junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país

6. un mecanismo de certificación aprobado, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas.

Si existe autorización de la autoridad de control, las garantías adecuadas podrán ser aportadas mediante:

1. cláusulas contractuales entre el responsable o el encargado y el responsable, encargado o destinatario de los datos personales en el tercer país u organización internacional, o

2. disposiciones que se incorporen en acuerdos administrativos entre las autoridades u organismos públicos que incluyan derechos efectivos y exigibles para los interesados.

Pueden contemplarse una serie de excepciones para situaciones específicas (Artículo 47), de entre las que destacamos las siguientes:

1. el interesado haya dado explícitamente su consentimiento a la transferencia propuesta, tras haber sido informado de los posibles riesgos;

2. la transferencia sea necesaria para la ejecución de un contrato o para la ejecución de medidas precontractuales adoptadas a solicitud del interesado;

3. la transferencia sea necesaria por razones importantes de interés público;

4. la transferencia sea necesaria para la formulación, el ejercicio o la defensa de reclamaciones o para proteger sus intereses vitales cuando el interesado esté física o jurídicamente incapacitado para dar su consentimiento;

Pongamos un ejemplo, que en sí es toda una categoría: Estados Unidos. Estados Unidos obviamente no pertenece a la Unión Europea, pero nuestros continuos flujos comerciales obligan a que se llegue a un entendimiento en muchas cosas. En la privacidad, que es nuestro caso, se hizo el 26 de julio de 2000 al firmar un acuerdo denominado “puerto seguro” (safeharbour) por el que las empresas estadounidenses que cumplan unos requisitos básicos pasan a formar parte de una lista por el que se permite la cesión de datos a éstas. La información a este respecto puede consultarse en la web del Departamento de Comercio de Estados Unidos(The International Trade Administration, 2016).

El legislador obviamente es conocedor de que las grandes tecnológicas de Estados Unidos, al tiempo que nos suministran servicios, adquieren un conocimiento de nosotros mismos mayor que el que cada uno de nosotros pueda tener. Por ello pone salvaguardas legales, a sabiendas de que se intentarán saltar, porque la alternativa, cortar toda comunicación, es absolutamente impensable.

Los propietarios de webs deben dejar clara la finalidad de la misma: si es una página web privada para amigos o conocidos, o si no hay datos personales, no hay que hacer nada. Pero ¿y en el caso de una asociación? ¿Y si se trata de un club de escalada? Entonces estaremos sometidos a la regulación de la privacidad. Igual si somos autónomos, tendremos una serie de zonas sensibles en la web, como el formulario contacto, los datos de los clientes que deseen recibir nuestras novedades, el envío en sí de correos electrónicos, las “cookies” e incluso quien ha dado “me gusta” en nuestra página de Facebook.

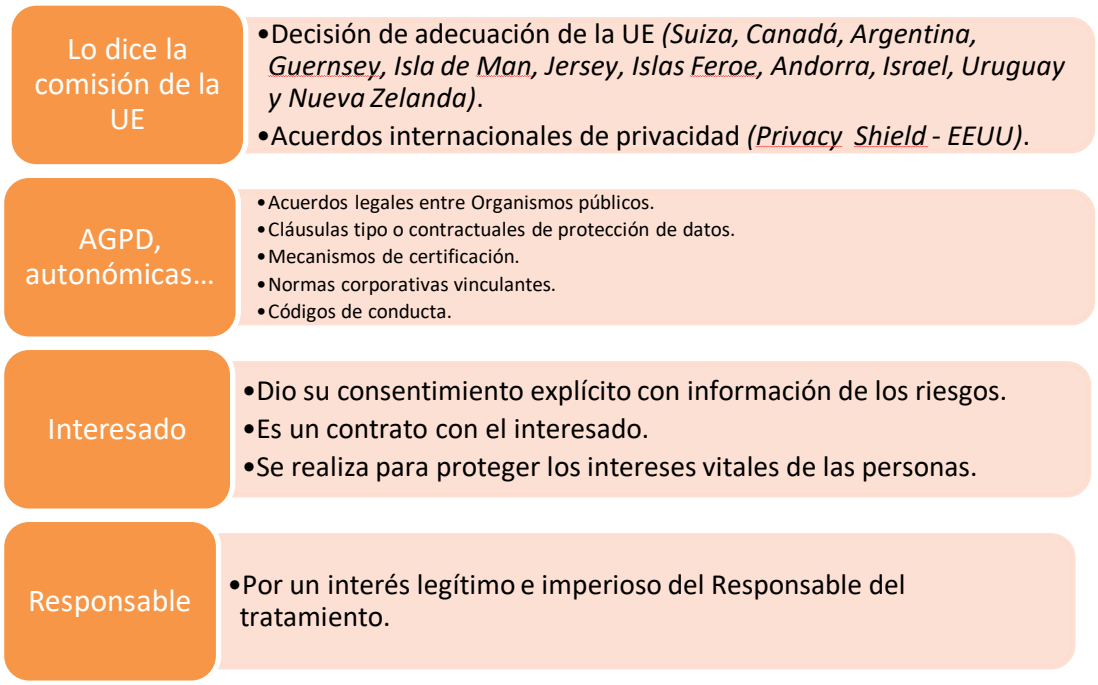


Ilustración 7 Licitud de las transferencias. Adaptación de (Delgado Carravilla & Puyol Montero, 2018)

¿Qué debe hacer el profesional?

Frente al interesado, debe:

- Informar la intención de realizar transferencias internacionales.
- Verificar la existencia o ausencia de una decisión de adecuación.
- Obtener garantías adecuadas y medios para obtener copia de ellas.

De cara al registro de actividades:

- Identificar las transferencias internacionales.
- Documentar la existencia de garantías apropiadas.

Artículos de máximo interés para entender las transferencias internacionales de datos.

Artículo 40 Ley 3/2018. Régimen de las transferencias internacionales de datos.

Artículo 41 Ley 3/2018. Supuestos de adopción por la Agencia Española de Protección de Datos.

Artículo 42 Ley 3/2018. Supuestos sometidos a autorización previa de las autoridades de protección de datos.

Artículo 43 Ley 3/2018. Supuestos sometidos a información previa a la autoridad de protección de datos competente.

RGPD. Artículo 44. Principio general de las transferencias.

RGPD. Artículo 45. Transferencias basadas en una decisión de adecuación.

RGPD. Artículo 46Transferencias mediante garantías adecuadas.

RGPD. Artículo 47 Normas corporativas vinculantes.

RGPD. Artículo 48Transferencias o comunicaciones no autorizadas por el Derecho de la Unión.

RGPD. Artículo 49 Excepciones para situaciones específicas.

RGPD. Artículo 50 Cooperación internacional en el ámbito de la protección de datos personales.

Cesión de datos y tratamiento por terceros

Si buscamos estas figuras en el Reglamento, haciendo una búsqueda rápida, veremos que no aparecen como tales. Sin embargo, en un contexto como el nuestro, y con el precedente de la LOPD de 1999, y el enorme trabajo desplegado al respecto desde largo tiempo atrás por la Agencia Española de Protección de Datos, conviene dedicar un tiempo al respecto, pues se trata de dos situaciones cotidianas que pueden sugerir confusión pues en ocasiones no quedan muy claras.

Cesión: Toda revelación de datos realizada a una persona distinta del interesado.

En la cesión de datos la organización a quien se le ceden los datos hará en tratamiento por sí misma, mientras que en el tratamiento por terceros, serán otros los que hagan el tratamiento para nosotros.

En la cesión, el responsable del fichero tiene obligación de informar a los afectados indicando la finalidad del fichero, la naturaleza de los datos y el nombre y dirección del cesionario. Suele incluirse una cláusula en la cual se establece que el afectado acepta la cesión de sus datos entre compañías del mismo grupo y/o sus agentes comerciales. No se considerará comunicación de datos el acceso de un tercero a la información cuando dicho acceso sea necesario para la prestación de un servicio a la empresa. La realización de tratamientos por cuenta de terceros tiene que estar regulada en un contrato que deberá constar preferentemente por escrito, y si no de alguna forma que permita acreditar su acuerdo y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, lo que implica que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas. Además debe figurar en el contrato toda aquella medida de seguridad que el encargado del tratamiento está obligado a implementar.

Por otra parte, en el tratamiento por cuenta de terceros (por ejemplo contratamos a una gestoría para que nos haga las gestiones frente a la seguridad social con datos de nuestros trabajadores, o a una empresa de marketing para que mande publicidad a nuestros clientes), es imprescindible regular este trasvase de datos a través de un contrato en el que el tercero que accede a la información se comprometa a garantizar el cumplimiento de la Ley en los mismos términos en que ésta obliga al titular de los datos.

En todo caso, supone un envío de datos de carácter personal a elementos ajenos a la empresa, esto es, una comunicación de datos personales, y por tanto lleva implícito que todas las partes implicadas en dicha comunicación tengan el deber de observar secreto sobre los citados datos. Y, parece obvio por lo visto hasta ahora, que al enviar datos a terceros o permitir el acceso a los mismos, estos solo podrán ser usados para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado.

Recordemos que hemos hablado del consentimiento. El consentimiento para la comunicación de los datos de carácter personal a un tercero será nulo cuando la información que se facilite al interesado no sea clara al explicar la finalidad a que se destinarán los datos cuya comunicación se autoriza, y/o el tipo de actividad que realiza aquel a quien se pretenden comunicar.

Recomendaciones: es más que conveniente estipular en el contrato de servicios con el cliente las condiciones y el objeto para el que van a ser recabados los datos de carácter personal así como la forma de ejercer los derechos sobre los mismos.

Singularidades a considerar por el profesional

En esta especie de cajón de sastre trataremos algunos temas con difícil clasificación en las anteriores categorías, pero que tienen gran interés para el profesional.

Las "cookies"

No solo se necesita recabar el consentimiento para el tratamiento de datos personales, sino que también existen casos, como la instalación de las cookies, donde es obligatorio.

Cuando sea técnicamente posible y eficaz, el consentimiento del destinatario para aceptar el tratamiento de los datos podrá facilitarse mediante el uso de los parámetros adecuados del navegador o de otras aplicaciones, siempre que aquél deba proceder a su configuración durante su instalación o actualización mediante una acción expresa a tal efecto.

En todo el responsable debe recordar que cuando la instalación y/o utilización de una cookie conlleve el tratamiento de datos personales, los responsables de tal tratamiento deberán asegurarse del cumplimiento de las exigencias adicionales establecidas por la normativa sobre protección de datos personales, en particular en relación con los datos especialmente protegidos. Además, es conveniente recordar la necesidad de adoptar cautelas adicionales en este ámbito en relación con los menores de edad.

"Cookies exceptuadas": aquellas que tienen por finalidad:

- Cookies de «entrada del usuario».
- Cookies de autenticación o identificación de usuario (únicamente de sesión).
- Cookies de seguridad del usuario.
- Cookies de sesión de reproductor multimedia.
- Cookies de sesión para equilibrar la carga.
- Cookies de personalización de la interfaz de usuario.
- Cookies de complemento (plug-in) para intercambiar contenidos sociales.

La información sobre las cookies facilitada en el momento de solicitar el consentimiento debe ser suficientemente completa para permitir a los usuarios entender la finalidad para las que se instalaron y conocer los usos que se les darán.

Si es necesario obtener el consentimiento para la instalación de las cookies por parte de usuarios ya registrados habrá que informarles de manera verificable sobre los cambios realizados en relación con el tratamiento de las cookies.

Contratación de servicios Cloud Computing

Es importante identificar qué proveedores de cloud están localizados dentro del Espacio Económico Europeo. Localización no sólo de la sede del proveedor, sino de sus recursos físicos. La contratación de servicios de cloud computing se realizará a través de un contrato de prestación de servicios que es imprescindible vincule el cumplimiento de la ley. Lamentablemente en la mayoría de los casos, lo que se ofrece por parte de los proveedores son contratos con cláusulas contractuales cerradas, sin opción para negociar sus términos.

El responsable debe decidir para qué datos personales contratará servicios de cloud computing y cuáles prefiere mantener en sus propios sistemas de información. Esta decisión es importante porque delimitará las finalidades para las que el proveedor de cloud puede tratar los datos. El responsable debe solicitar y obtener información sobre si intervienen o no terceras empresas (subcontratistas) en la prestación de servicios de cloud computing.

Para que el responsable pueda asegurarse de que las medidas de seguridad se cumplen, como cliente debe tener la opción de comprobar las medidas de seguridad, incluidos los registros que permiten conocer quién ha accedido a los datos de los que es responsable. El responsable, como cliente, debe ser informado diligentemente por el proveedor de cloud sobre las incidencias de seguridad que afecten a los datos de los que el propio cliente es responsable, así como de las medidas adoptadas para resolverlas o de las medidas que el cliente ha de tomar para evitar los daños que puedan producirse.

Normas de alto interés a considerar:

- Ley de Contratos del Sector Público. (RD Legislativo 3/2011, de 14 de noviembre).

- Ley 11/2007 de Acceso Electrónicos de los Ciudadanos a los Servicios Públicos, y RD 1671/2009 que desarrolla parcialmente esta ley.

- El Esquema Nacional de Seguridad (ENS) y el Esquema Nacional de Interoperabilidad (ENI) (Reales Decretos 3/2010 y 4/2010, de 8 de enero).

Sistemas de información de denuncias internas

Desarrollado en el artículo 24 de la ley 3/2018, se nos explica cómo se debe proceder con la información de posibles incumplimientos legales, éticos o de normativa interna, que pueda dar paso a sanciones o a denuncias ante la justicia.

¿Quién puede acceder a esos datos? Esos sistemas que pueden servir para poner en conocimiento de una entidad de Derecho privado, incluso anónimamente, la comisión de infracciones tendrán un acceso limitado por lo sensible de lo que albergan. Este acceso será

solo para los que desarrollen las funciones de control interno y de cumplimiento, los encargados del tratamiento designados para ello y a quienes resulte necesario para la adopción de medidas disciplinarias o para la tramitación de procedimientos judiciales. Solo en el caso de que se puedan adoptar medidas disciplinarias contra un trabajador, se permitirá al personal con funciones de gestión y control de recursos humanos.

Deberán tenerse en cuenta una serie de consideraciones, como que tanto empleados como terceros deberán ser informados acerca de la existencia de estos sistemas de información, la necesidad de adoptar medidas para preservar la identidad y garantizar la confidencialidad de los datos, especialmente del denunciante. Los datos deberán conservarse únicamente durante el tiempo imprescindible para decidir sobre la procedencia de iniciar una investigación.

Sobre la videovigilancia

La norma habla de ella de dos formas muy concretas: sobre los propios trabajadores (art. 89 3/2018) y en general (clientes...), en su art. 22. Se deja claro que solo se puede realizar en la vía pública cuando es imprescindible para preservar la seguridad, pero con una serie de condicionantes.

- Puede captarse una extensión superior cuando sea necesario para garantizar la seguridad de bienes o instalaciones estratégicos o de infraestructuras vinculadas al transporte, siempre que no suponga la captación de imágenes del interior de un domicilio privado.
- Salvo cuando deban ser conservados para acreditar la comisión de un delito, serán suprimidos en el plazo máximo de un mes desde su captación. Si se da el caso, las imágenes deberán ser puestas a disposición de la autoridad competente en un plazo máximo de setenta y dos horas desde que se tuviera conocimiento de la existencia de la grabación.
- El deber de información se entenderá cumplido mediante la colocación de un dispositivo informativo en lugar suficientemente visible identificando, al menos, la existencia del tratamiento, la identidad del responsable y la posibilidad de ejercitar los derechos previstos en los artículos 15 a 22 del Reglamento (UE) 2016/679.
- Queda excluido el tratamiento por una persona física de imágenes que solamente capten el interior de su propio domicilio (siempre que no lo haga una entidad de seguridad privada que hubiera sido contratada para la vigilancia de un domicilio y tuviese acceso a las imágenes).

Exclusión publicitaria

Las viejas conocidas "listas Robinson", cobran actualidad, con el art. 23 de la 3/2018. Hablamos ya de ellas al tratar de la limitación del tratamiento.

Al tratarse de una lista para no estar en ninguna lista, cabe preguntarse si es lícito ese tratamiento. Y si, se pueden crear sistemas de información en los que sólo se incluirán los datos imprescindibles para identificar a los afectados, de forma que se pueda eliminar la recepción de comunicaciones comerciales.

Debe comunicarse a la AEPD o agencias autonómicas su creación, carácter, modo de incorporarse al sistema y cómo hacer valer sus preferencias. La autoridad de control hará pública en su sede electrónica una relación de los sistemas y lo pondrá en conocimiento de las restantes autoridades de control para su publicación por todas ellas. Cuando un afectado

manifieste su deseo de que sus datos no sean tratados, éste deberá informarle de los sistemas de exclusión publicitaria existentes. Quienes pretendan realizar comunicaciones de mercadotecnia directa, deberán previamente consultar los sistemas de exclusión publicitaria que pudieran afectar a su actuación.

No será necesario realizar la consulta cuando el afectado hubiera prestado, su consentimiento para recibir la comunicación a quien pretenda realizarla.

Información crediticia

Las deudas, su reclamación... siempre han sido uno de los puntos más calientes de la normativa sobre protección de datos. El artículo 20 de la 3/2018 gira sobre este espinoso tema. ¿Cuándo se puede hacer un tratamiento de datos personales relativo al incumplimiento de las obligaciones de pago? Se han de dar las siguientes condiciones:

a) Que los datos hayan sido facilitados por el acreedor o por quien actúe por su cuenta o interés.

b) Que los datos se refieran a deudas ciertas, vencidas y exigibles, cuya existencia o cuantía no hubiese sido objeto de reclamación administrativa o judicial por el deudor o mediante un procedimiento alternativo de resolución de disputas vinculante entre las partes.

c) Que el acreedor haya informado al afectado en el contrato o en el momento de requerir el pago acerca de la posibilidad de inclusión en dichos sistemas, con indicación de aquéllos en los que participe. La entidad que mantenga el sistema de información crediticia con datos relativos al incumplimiento de obligaciones dinerarias, financieras o de crédito deberá notificar al afectado la inclusión de tales datos y le informará sobre la posibilidad de ejercitar los derechos establecidos.

d) Que los datos únicamente se mantengan en el sistema mientras persista el incumplimiento, con el límite máximo de cinco años desde la fecha de vencimiento de la obligación dineraria, financiera o de crédito.

e) Que los datos referidos a un deudor determinado solamente puedan ser consultados cuando quien consulte el sistema mantuviese una relación contractual con el afectado que implique el abono de una cuantía pecuniaria o este le hubiera solicitado la celebración de un contrato que suponga financiación, pago aplazado o facturación periódica, como sucede, entre otros supuestos, en los previstos en la legislación de contratos de crédito al consumo y de contratos de crédito inmobiliario.

f) Que, en el caso de que se denegase la solicitud de celebración del contrato, o éste no llegara a celebrarse, como consecuencia de la consulta efectuada, quien haya consultado el sistema informe al afectado del resultado de dicha consulta.

Empresarios autónomos, profesión liberal

El tejido empresarial que nos rodea está en gran medida compuesto de pequeñas empresas, aún más, micro empresas e incluso profesionales y trabajadores que con una licencia de autónomo se constituyen en empresa. Estas diminutas empresas no cuentan, obviamente, con informáticos en plantilla, pero si recurren al asesoramiento externo. Muchas veces nos

preguntarán ¿Qué pasa con los datos de mis clientes? Una visión de ello debe pasar por el artículo 19 de la ley 3/2018 y la definición de tratamiento lícito que se nos da en el 6.1.f) del RGPD

¿Qué es lo que pasa con los datos que conservan los profesionales liberales? A priori es lícito el tratamiento de datos, pues se entiende que el mismo es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento (el pequeño empresario) o por un tercero (un gestor), siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales. A la recíproca, la misma presunción sirve para el tratamiento de los datos relativos a los empresarios individuales y a los profesionales liberales, cuando se refieran a ellos únicamente en dicha condición y no se traten para entablar una relación con los mismos como personas físicas.

Obviamente, hablamos tan solo de los datos necesarios para su localización profesional.

Tratamientos de datos con peculiaridades

En este apartado vamos a ir un paso más allá. Hemos visto como existen una serie de datos que la legislación protege con celo. Vamos a ver cómo interpreta eso el Reglamento y la ley 3/2018, al tiempo que vemos que sucede con elementos peculiares, como los datos de los fallecidos o los de los niños. Algunos, como los datos relativos a condenas e infracciones penales (Artículo 10) ya son vistos en otras partes de éste tema.

Categorías especiales de datos personales

Hay una serie de tratamientos prohibidos: aquellos que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física. Es conveniente visitar el artículo 9 del RGPD en este punto.

Vemos que se trata de elementos que afectan a la intimidad más profunda del individuo. Aun así, hay una serie de excepciones. Estos datos se pueden tratar si se da alguna de las siguientes circunstancias:

1. Si el interesado dio su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados (si no hay una norma que lo impida);
2. Si el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social,
3. Si el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física, si no está capacitado, física o jurídicamente, para dar su consentimiento;
4. Si el tratamiento es efectuado, en el ámbito de sus actividades, por una fundación, una asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical.;
5. Si el tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicos;
6. Si el tratamiento es necesario para la formulación, el ejercicio o la defensa de

reclamaciones o para los tribunales;
7. Si el tratamiento es necesario por razones de un interés público esencial;
8. Si el tratamiento es necesario para fines de medicina preventiva o laboral;
9. Si el tratamiento es necesario por razones de interés público en el ámbito de la salud pública;
10. Si el tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos.

Los Estados miembros podrán mantener o introducir condiciones adicionales, inclusive limitaciones, con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud.

El tratamiento de categorías especiales de datos personales, sin el consentimiento del interesado, puede ser necesario por razones de interés público en el ámbito de la salud pública. «Salud pública» debe interpretarse como todos los elementos relacionados con la salud, concretamente el estado de salud, con inclusión de la morbilidad y la discapacidad, los determinantes que influyen en dicho estado de salud, las necesidades de asistencia sanitaria, los recursos asignados a la asistencia sanitaria, la puesta a disposición de asistencia sanitaria y el acceso universal a ella, así como los gastos y la financiación de la asistencia sanitaria, y las causas de mortalidad. Este tratamiento de datos relativos a la salud por razones de interés público no debe dar lugar a que terceros, como empresarios, compañías de seguros o entidades bancarias, traten los datos personales con otros fines. (Considerando 54)

Niños

Los niños merecen una protección específica, pues son menos conscientes de los riesgos, consecuencias, garantías y derechos concernientes al tratamiento de datos personales. Esto es de particular importancia cuando se trata del empleo de sus datos con fines de mercadotecnia o elaboración de perfiles de personalidad o de usuario. (Considerando 38) (Artículo 8 RGPD)

Si se hacen ofertas directas a niños, el tratamiento de los datos personales de un niño se considerará lícito cuando tenga como mínimo 16 años. Si el niño es menor, únicamente será lícito si el consentimiento lo dio o autorizó el titular de la patria potestad o tutela sobre el niño. El tope de 16 años podrá ser rebajado por los Estados miembros, pero de forma que nunca sea inferior a 13 años.

Consideremos que apenas existen servicios que permitan saber la edad de alguien. Esto es así por lo complicado de la validación al poder engañar con facilidad: dando el DNI del padre, o con acceso a las comprobaciones seguras de organismos públicos y organizaciones autorizadas al compartir ordenador con ellos. Para más información sobre niños, redes sociales y privacidad, se recomienda la consulta de (De Miguel Molina, Oltra Gutiérrez, & Sarabdeen, An exploratory study on the privacy of children's images in Spain's most widely used social network sites (Tuenti and Facebook), 2010). También de las Pautas de protección de datos para los centros educativos, publicadas por la Agencia Catalana de Protección de Datos (Agencia Catalana de Protección de Datos, 2018).

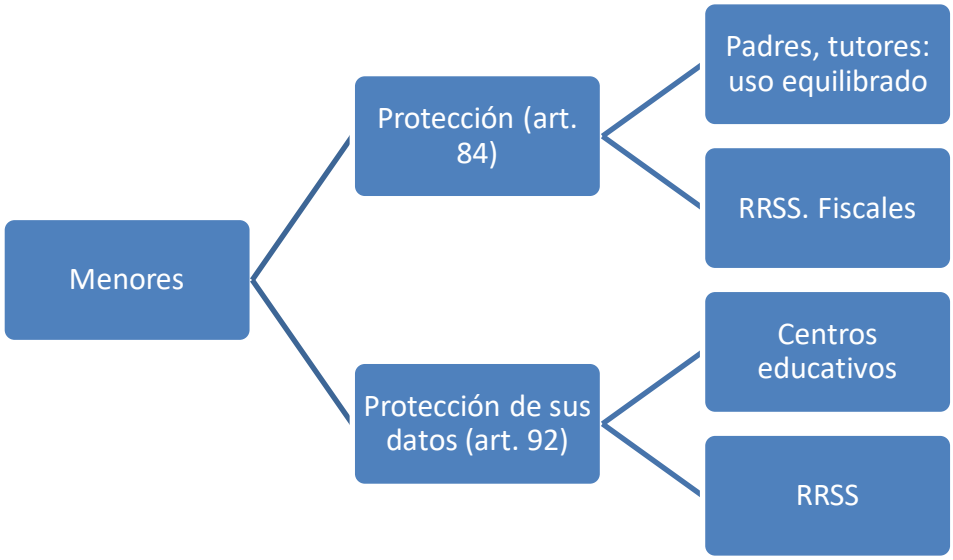


Ilustración 8 Título X y menores, elaboración propia

Condenas e infracciones penales

Sólo puede efectuarse bajo la supervisión de las autoridades públicas, con garantías adecuadas para los derechos y libertades de los interesados. (Artículo 10 RGPD)

En el caso de tener que enfrentarse a un supuesto de estas características, es imprescindible revisar la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo (Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, 2016)

Fallecidos

El Reglamento no se aplica a la protección de datos personales de personas fallecidas, aunque los estados miembros pueden establecer normas relativas al respecto. Hay que considerar la autorización para establecer el tratamiento ulterior de datos personales con fines de archivo y con fines de investigación histórica, incluyendo la investigación para fines genealógicos, y por causas graves, como por ejemplo, genocidio. (Considerandos 27, 158 y 160)

Según la ley 3/2018:

Se permite que las personas vinculadas al fallecido por razones familiares o de hecho o sus herederos puedan solicitar el acceso a los mismos, así como su rectificación o supresión, en su caso con sujeción a las instrucciones del fallecido.

No podrán acceder a los datos del causante, ni solicitar su rectificación o supresión, cuando la persona fallecida lo hubiese prohibido expresamente o así lo establezca una ley.

En caso de fallecimiento de menores y personas con discapacidad, estas facultades podrán ejercerse también por sus representantes legales o, en el marco de sus competencias, por el Ministerio Fiscal.

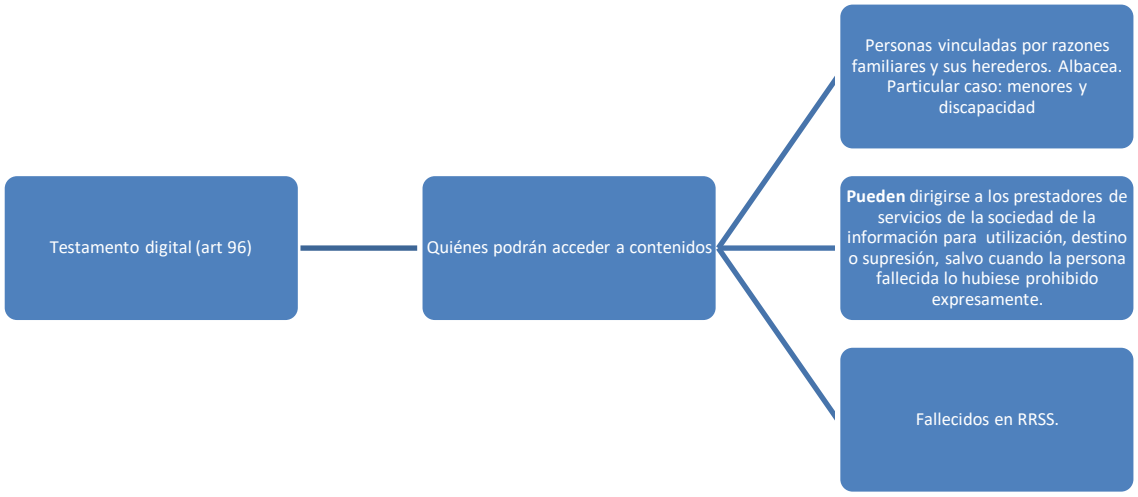


Ilustración 9 Título X y testamento digital. Elaboración propia

Tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos

Se deben establecer garantías de forma que se disponga de medidas técnicas y organizativas, en particular para garantizar el respeto del principio de minimización de los datos personales. Hablamos de elementos como la seudonimización. Cuando el ejercicio de los derechos derivados del tratamiento de datos personales con fines de investigación científica o histórica o estadísticos imposibiliten u obstaculicen gravemente el logro de los fines científicos, se podrán establecer excepciones. (Artículo 89)

El tratamiento de datos personales con fines de investigación científica debe interpretarse de manera, incluyendo el desarrollo tecnológico y la demostración, la investigación fundamental, la investigación aplicada y la investigación financiada por el sector privado. Entre los fines de investigación científica también se deben incluir los estudios realizados en interés público en el ámbito de la salud pública. (Considerando 159)

Por fines estadísticos se entiende cualquier operación de recogida y tratamiento de datos personales necesarios para encuestas estadísticas o para la producción de resultados

estadísticos. Estos resultados estadísticos pueden además utilizarse con diferentes fines, incluidos fines de investigación científica. El fin estadístico implica que el resultado del tratamiento con fines estadísticos no sean datos personales, sino datos agregados, y que este resultado o los datos personales no se utilicen para respaldar medidas o decisiones relativas a personas físicas concretas. (Considerando 162)

Protección de datos en iglesias y asociaciones religiosas

Ya sabemos de datos que implican una intimidad muy especial. De entre ellos, las creencias religiosas y las ideas políticas figuran entre los destacados. A este respecto, las iglesias, asociaciones o comunidades religiosas artículo estarán sujetas al control de una autoridad de control. Obviamente no se les puede impedir todo tratamiento, pues entonces su gestión del día a día sería imposible. (Artículo 91)

Tratamiento y acceso público de documentos oficiales

De nuevo nos encontramos con otro caso de derechos que se superponen. En este caso a privacidad enfrentamos transparente. ¿Cómo hacer público lo que es privado? ¿De qué modo un dato personal puede ser transparente? A este respecto el Reglamento indica que los datos personales de documentos oficiales en posesión de alguna autoridad pública o u organismo público o una entidad privada para la realización de una misión en interés público podrán ser comunicados por dicha autoridad, organismo o entidad a fin de conciliar el acceso del público a documentos oficiales con el derecho a la protección de los datos personales. (Artículo 86)

Se tiene en cuenta el principio de acceso del público a los documentos oficiales, que es algo de interés público. Se debe conciliar el acceso del público a documentos oficiales y la reutilización de la información del sector público con el derecho a la protección de los datos personales. Hay que prestar particular atención a aquellos documentos a los que no pueda accederse o cuyo acceso esté limitado en virtud de regímenes de acceso por motivos de protección de datos personales, y a partes de documentos accesibles que contengan datos personales cuya reutilización haya quedado establecida como incompatible con el Derecho relativo a la protección de las personas físicas con respecto al tratamiento de los datos personales. (Considerando 154)

Es interesante a este respecto la consulta de la Directiva 2003/98/CE del Parlamento Europeo y del Consejo, de 17 de noviembre de 2003, relativa a la reutilización de la información del sector público (DO L 345 de 31.12.2003, p. 90). (PARLAMENTO EUROPEO Y CONSEJO DE LA UNIÓN EUROPEA, 2003)

Otros datos especialmente protegidos

Existen datos que, por su naturaleza, son particularmente sensibles en relación con los derechos y las libertades fundamentales, pues el contexto de su tratamiento podría entrañar importantes riesgos: de entre ellos figuran los datos de carácter personal que revelen el origen racial o étnico. (Considerandos 51 y 51)

El tratamiento de fotografías no debe considerarse sistemáticamente tratamiento de categorías especiales de datos personales, únicamente se considerarían datos biométricos cuando el hecho de ser tratadas con medios técnicos específicos permita la identificación o la autenticación unívocas de una persona física.

Estos datos personales no deben ser tratados, a menos que se permita su tratamiento en situaciones específicas. Se deben establecer de forma explícita excepciones, entre otras cuando el interesado dé su consentimiento explícito o tratándose de necesidades específicas.

Otras excepciones: siempre que se den las garantías apropiadas, en interés público, en particular el tratamiento de datos personales en el ámbito de la legislación laboral, la legislación sobre protección social, incluidas las pensiones y con fines de seguridad, supervisión y alerta sanitaria, la prevención o control de enfermedades transmisibles y otras amenazas graves para la salud. También debe autorizarse a título excepcional cuando sea necesario para la formulación, el ejercicio o la defensa de reclamaciones.

Régimen sancionador

Una de las zonas más densas en la norma (título IX en la ley 3/2018, artículos 10 a 78 y artículos 83 y 84 del RGPD) es el de las sanciones. La primera pregunta sería ¿a quién se puede sancionar? a esto responde el artículo 70, que refiere a responsables y encargados de los tratamientos, y a sus representantes cuando se trata de entidades no establecidas en el territorio de la Unión Europea, y a las entidades de certificación y aquellas acreditadas de supervisión de los códigos de conducta. Deja fuera de este conjunto al DPD.

Hay una larga relación en la norma que nos permite clasificar infracciones y sanciones. A modo de resumen, indiquemos que ambas se clasifican en leves, graves y muy graves.

Tratemos de hacer un esquema de las infracciones y sanciones.

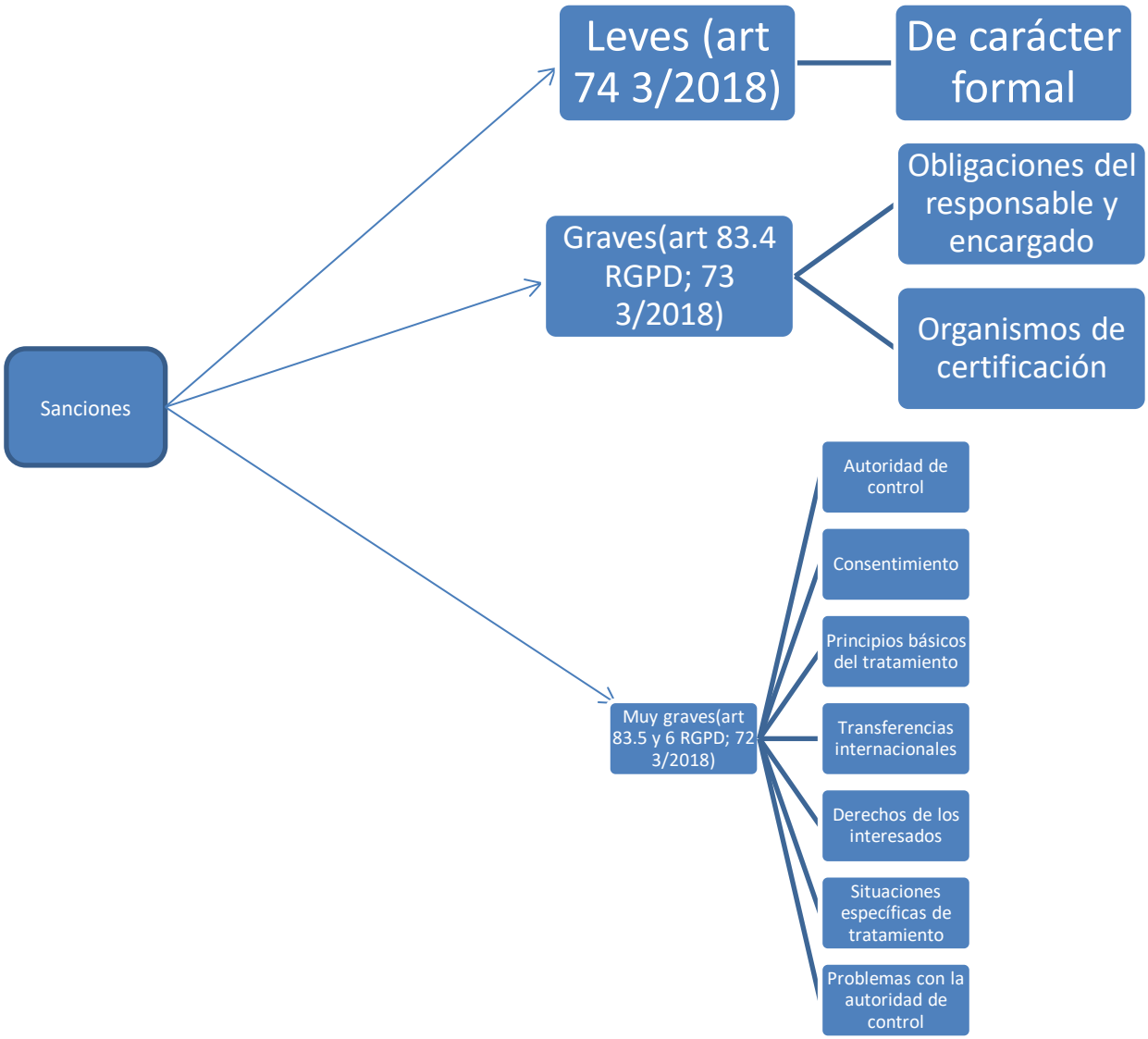


Ilustración 10 Sanciones. Elaboración propia

Al margen de la posibilidad de ejercer cualquier acción judicial o recurso administrativo, el interesado podrá presentar una reclamación ante una autoridad de control, la cual informará al reclamante sobre el curso y el resultado de la reclamación, sin olvidar informar sobre la posibilidad de acceder a la tutela judicial. Pueden ejercitarse acciones contra una autoridad de control ante los tribunales del Estado miembro en que esté establecida esta.

En el caso de una tutela judicial contra un responsable o encargado del tratamiento, esta se ejercita ante los tribunales del Estado miembro en el que el responsable o encargado tenga un establecimiento. Pero también podrán ejercitarse ante los tribunales del Estado miembro en que el interesado tenga su residencia habitual, a menos que el responsable o el encargado sea una autoridad pública de un Estado miembro que actúe en ejercicio de sus poderes públicos.

Todo aquel que sufra daños y perjuicios materiales por una infracción del Reglamento tendrá derecho a recibir del responsable o el encargado del tratamiento una indemnización.

¿Quién responde de los daños? Cualquier responsable que participe en la operación de tratamiento responderá de los daños y perjuicios causados en caso de que dicha operación no cumpla lo dispuesto por el presente Reglamento. Un encargado únicamente responderá de los daños y perjuicios causados por el tratamiento cuando no haya cumplido con las obligaciones del Reglamento dirigidas específicamente a él, o cuando haya actuado al margen o en contra de las instrucciones. Si demuestran que no son responsables del hecho que haya causado los daños, estarán exentos de responsabilidad. Si el daño es ocasionado por varios encargados o responsables, cada uno de ellos será responsabilizado, a fin de garantizar la indemnización. En estos casos, si un responsable o encargado del tratamiento paga una indemnización total por el perjuicio ocasionado, tendrá derecho a reclamar a los demás la parte de la indemnización correspondiente.

Cualquier infracción de este debe ser castigada con sanciones, incluidas multas administrativas, con carácter adicional a medidas adecuadas impuestas por la autoridad de control.

Si se trata de una infracción leve, o si la multa que probablemente se impusiera constituyese una carga desproporcionada para una persona física, en lugar de sanción mediante multa puede imponerse un apercibimiento. La imposición de sanciones, incluidas las multas administrativas, debe estar sujeta a garantías procesales suficientes. Los Estados miembros tienen la posibilidad de establecer normas en materia de sanciones penales por infracciones del Reglamento. No obstante, la imposición de sanciones penales por infracciones de dichas normas nacionales y de sanciones administrativas no debe entrañar la vulneración del principio *ne bis in ídem* ("No dos veces lo mismo").

Las autoridades de control garantizarán que las multas administrativas sean en cada caso efectivas, proporcionadas y disuasorias. Para determinar su cuantía se tendrá en cuenta (entre otros factores):

1. La naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento y el número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido;
2. La intencionalidad o negligencia en la infracción;
3. Medidas tomadas por el responsable o encargado del tratamiento para paliar los daños y perjuicios;
4. Infracciones anteriores cometidas;
5. Grado de cooperación con la autoridad de control con el fin de poner remedio y mitigar;
6. Las categorías de los datos de carácter personal afectados por la infracción;
7. Cómo la autoridad de control tuvo conocimiento (¿el responsable o el encargado notificaron la infracción?);
8. La adhesión a códigos de conducta.

Se produce un endurecimiento del régimen sancionador, las sanciones pueden llegar hasta los 20 millones de euros, o el 4% del volumen de negocio total anual global del ejercicio financiero anterior, lo que sea más alto. Para la cuantía de las multas administrativas, se aconseja consultar el Reglamento y la legislación nacional.

Derechos digitales. Título X

Uno de los elementos distintivos de la ley 3/2018 es su título X, donde se presentan una serie de derechos digitales. La ley expresa el deseo del legislador de alcanzar en una futura reforma de la Constitución una actualización de la misma a la era digital y, con ello, elevar a rango constitucional una nueva generación de derechos digitales.

Dado que la reforma es algo en apariencia lejano, aprovechando el gran tren de la ley de Protección de Datos, se suma un vagón específico que busca abordar el reconocimiento de un sistema de garantía de los derechos digitales que, como el resto de la ley, nace del mandato del apartado cuarto del artículo 18 de la Constitución Española. Hay que especificar que en algunos casos, ya han sido perfilados por la jurisprudencia ordinaria, constitucional y europea.

Veámoslos.

Ilustración 11 Derechos digitales. Elaboración propia.

1. Derecho a la neutralidad de Internet

Esto va ligado a la llamada Internet de dos velocidades. Pongamos un ejemplo: Si Paco desde su casa quiere ver un vídeo colgado en Vimeo sobre cómo hacer macramé a oscuras, un hobby con pocos seguidores y no patrocinado por nadie, y su padre don Francisco va a disfrutar del partido de la Final de la Copa entre el Pedernal F.C. y el Pedregal C.F., puede ver como su conexión va más lenta que la de su padre, porque una operadora ha establecido un canal de pago más rápido para visualizar el encuentro de balompié.

Lo que implica la neutralidad de la red se basa es que todos los paquetes de datos que viajan por Internet deben ser tratados de la misma forma independientemente de su contenido. "Los proveedores de servicios de Internet proporcionarán una oferta transparente de servicios sin discriminación por motivos técnicos o económicos".

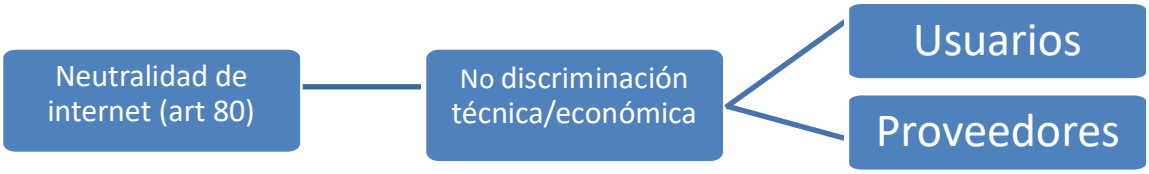


Ilustración 12 Neutralidad de internet. Elaboración propia.

2. Derecho de acceso universal a Internet

En virtud de esta ley, el Estado deberá garantizar "un acceso universal, asequible, de calidad y no discriminatorio para toda la población", de forma que "Todos tienen derecho a acceder a Internet independientemente de su condición personal, social, económica o geográfica", previniendo "acciones dirigidas a la formación y el acceso a las personas mayores" y atención a la población rural y personas que cuenten con necesidades especiales.

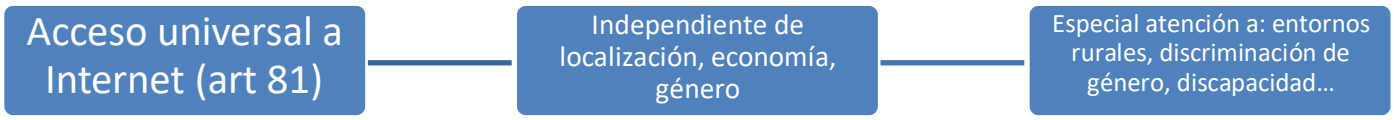


Ilustración 13 Derecho de acceso universal.

3. Derecho a la seguridad digital

Es una nueva vuelta de tuerca a un clásico, el derecho a la privacidad de las comunicaciones. Se subraya que "los proveedores de servicios de Internet informarán a los usuarios de sus derechos".

Ilustración 14 Seguridad digital. Elaboración propia.

4. Derecho a la educación digital

El modelo actual de educación se sujeta sobre competencias: lógico-matemática, social, lingüística… a éstas se añade la "competencia digital", que ya era desde 2014 en Educación Primaria una "competencia básica". Las comunidades autónomas deben considerar esta inclusión en todos los planes educativos, siendo este uso "seguro y respetuoso con la dignidad humana, los valores constitucionales, los derechos fundamentales y, particularmente con el respeto y la garantía de la intimidad personal y familiar y la protección de datos personales".

También afecta a las universidades, donde los alumnos de toda titulación deben saber manejar los medios digitales, y serán incluidas pruebas específicas al respecto en las oposiciones.

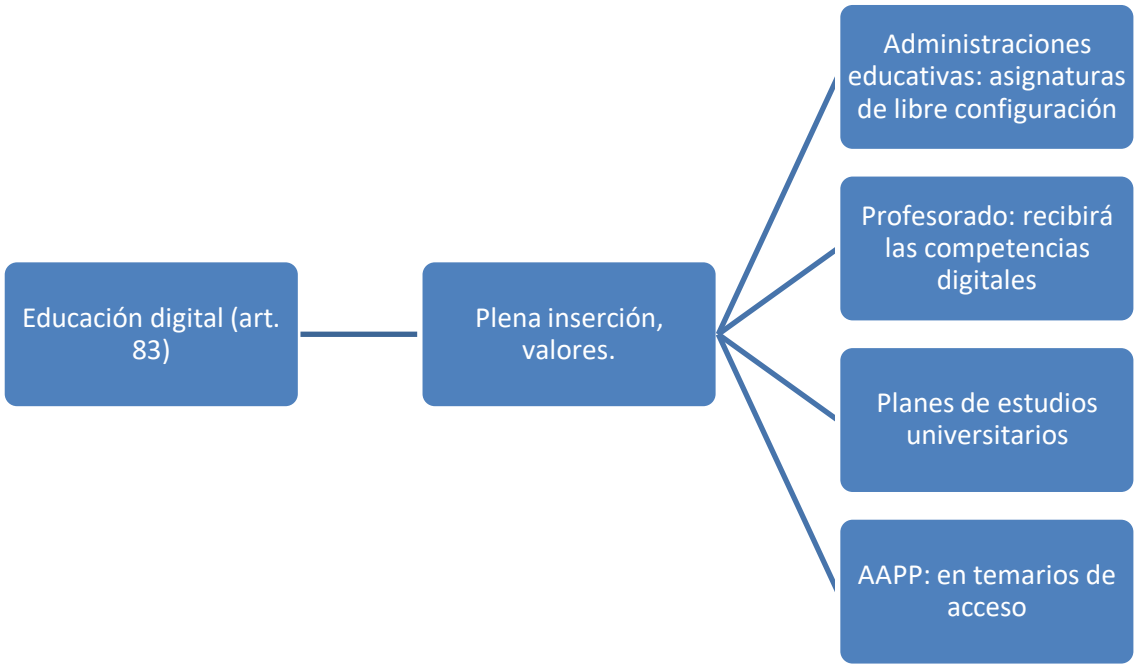


Ilustración 15 Educación digital. Elaboración propia.

5. Protección de los menores en Internet

Se carga en las obligaciones de padres y tutores que "los menores de edad hagan un uso equilibrado y responsable de los dispositivos digitales" para "garantizar el adecuado desarrollo de su personalidad y preservar su dignidad y sus derechos fundamentales". Si se diera una "intromisión ilegítima en sus derechos fundamentales" (recordemos recientes casos de abusos usando redes sociales), serán perseguidas por defecto por la Fiscalía.

Cualquiera que desarrolle actividades con menores de edad deberá contar con el consentimiento del menor o de sus representantes legales.

6. Derecho de rectificación en Internet

Aquí nos encontramos con un derecho ya recogido en una ley (se 1984, y por tanto nada adaptada al entorno digital) que ha sido vuelto a redactar para adaptarlo a la red, de forma que si se emiten datos inexactos o falsos en medios de comunicación, o, y esto es lo nuevo, en comentarios de redes sociales, se podrá ejercer el derecho de rectificación por vulneración del honor o la intimidad.

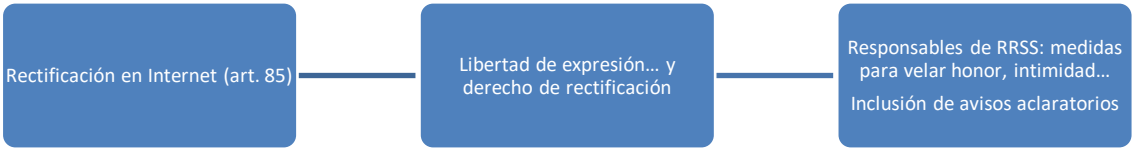


Ilustración 16. Rectificación. Elaboración propia.

7. Derecho a la actualización de informaciones en medios de comunicación digitales

Si una noticia publicada ha dejado de reflejar la situación actual de una persona "causándole un perjuicio" (por ejemplo con una sentencia que invalida otra anterior o con el pago de una cantidad adeudada) se puede "solicitar motivadamente de los medios de comunicación digitales la inclusión de un aviso de actualización suficientemente visible junto a las noticias que le conciernan".

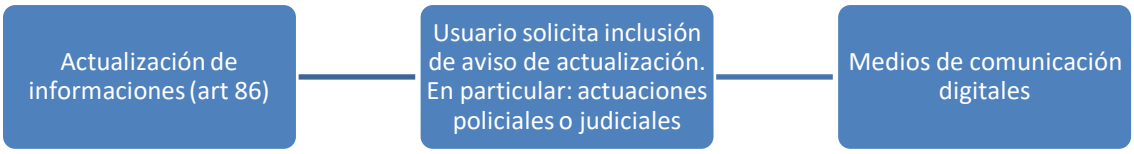


Ilustración 17 Actualización de informaciones. Elaboración propia.

8. Relativos a los trabajadores: derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral, derecho a la desconexión digital en el ámbito laboral, derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo, derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral y derechos digitales en la negociación colectiva.

Estamos ante una serie de derechos que tiene un nexo común: el trabajador.

8.1. Derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral.

En este caso se trata de la privacidad de los trabajadores, públicos y privados, en lo relativo al uso de los dispositivos electrónicos necesarios para el trabajo (teléfonos, portátiles, tabletas…) que les suministre su empleador. El empleador solo podrá acceder a ellos para "controlar el cumplimiento de las obligaciones laborales o estatutarias y de garantizar la integridad de dichos dispositivos". Para ello "deberán establecer criterios de utilización de los dispositivos digitales".

8.2 Derecho a la desconexión digital en el ámbito laboral.

No se podrán emplear herramientas digitales (mandar un WhatsApp, por ejemplo) para contactar con sus trabajadores fuera del horario laboral o durante sus períodos de descanso.

8.3 Derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo.

Se podrán instalar cámaras para el control de los trabajadores, pero solo se podrán instalar micrófonos cuando "resulten relevantes los riesgos para la seguridad de las instalaciones, bienes y personas derivados de la actividad que se desarrolle en el centro de trabajo" y en ningún caso en vestuarios, aseos, comedores o lugares destinados al esparcimiento de los trabajadores.

8.4 Derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral.

Se podrán usar sistemas de geolocalización para comprobar la ubicación de los trabajadores, siempre que se les informe a ellos y sus representantes "acerca de la existencia y características de estos dispositivos", y de sus derechos al respecto.

8.5 Derechos digitales en la negociación colectiva.

Los convenios colectivos podrán establecer "garantías adicionales de los derechos y libertades relacionados con el tratamiento de los datos personales de los trabajadores y la salvaguarda de derechos digitales en el ámbito laboral".

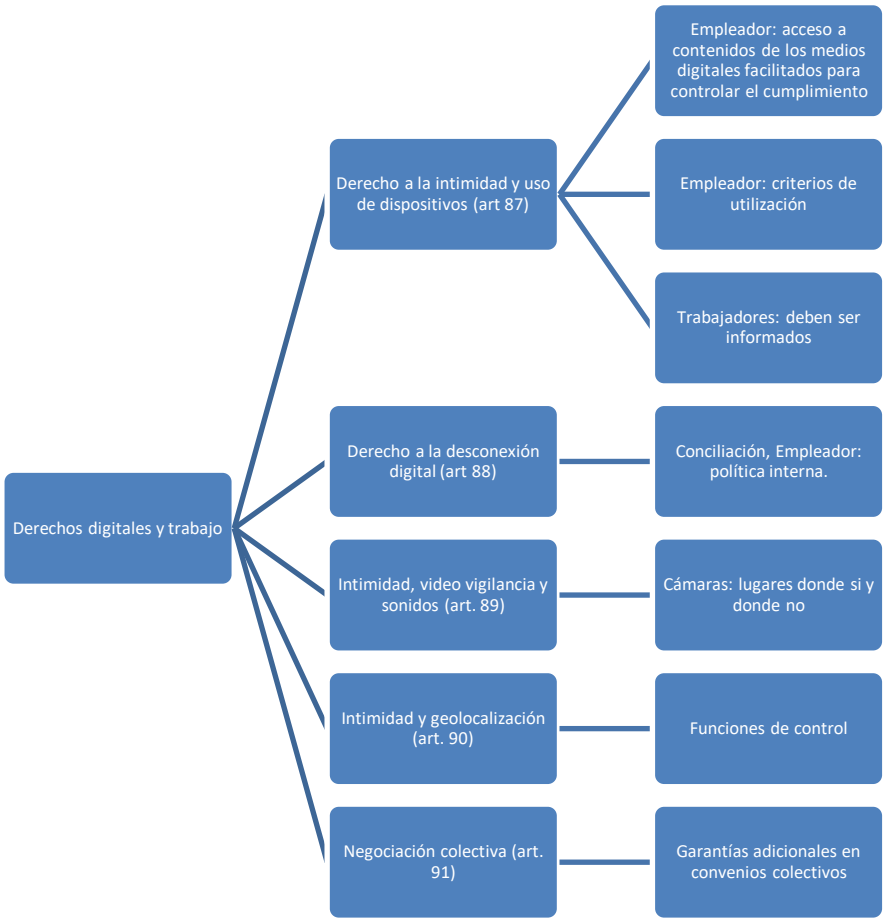


Ilustración 18 Derechos digitales y trabajo. Elaboración propia.

9. Derecho al olvido en búsquedas de Internet

El derecho al olvido aparece expresamente en la ley 3/2018 y en el RGPD. No obstante se reconoce su importancia incluyéndolo entre los llamados “derechos digitales”.

Por una parte se trata de impedir que los buscadores asocien información antigua a una persona, permitiendo ejercerlo cuando los datos que aparezcan sean "inadecuados, inexactos, no pertinentes, no actualizados o excesivos o hubieren devenido como tales por el transcurso del tiempo, teniendo en cuenta los fines para los que se recogieron o trataron, el tiempo transcurrido y la naturaleza e interés público de la información". Además de esto, que parece ser lo asumido clásicamente como derecho al olvido, aparece una variante en redes sociales y equivalentes: "toda persona tiene derecho a que sean suprimidos los datos personales que le

conciernan y que hubiesen sido facilitados por terceros para su publicación por los servicios de redes sociales" cuando estos sean "inadecuados, inexactos, no pertinentes, no actualizados o excesivos". Si además la subida de esos datos a las redes sociales se hubiera producido durante la minoría de edad del afectado, esta retirada deberá producirse "sin dilación".

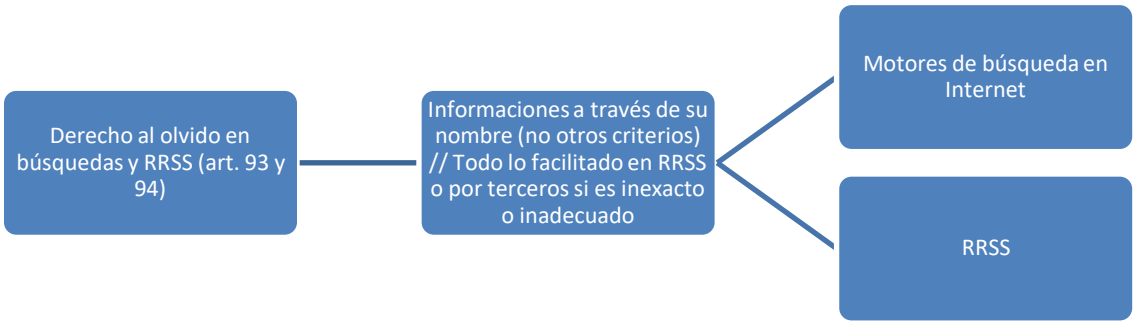


Ilustración 19 Derecho al olvido. Elaboración propia.

10. Derecho de portabilidad en servicios de redes sociales y servicios equivalentes

Es la portabilidad que conocíamos pero ampliada a las redes sociales.

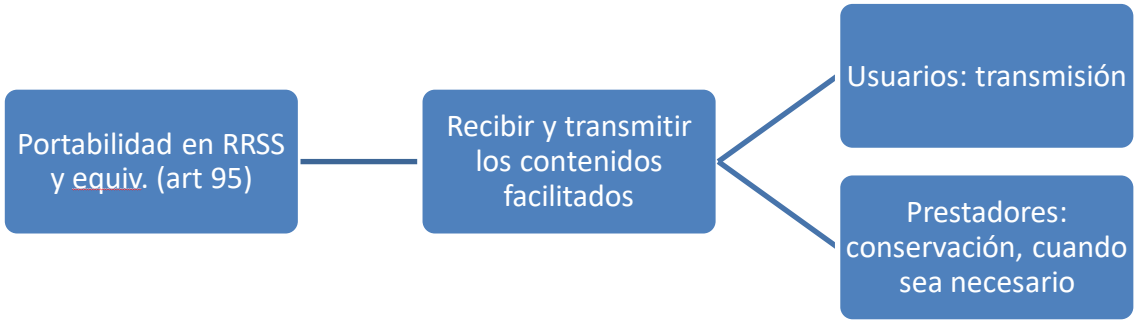


Ilustración 20 Portabilidad en redes sociales. Elaboración propia.

11. Derecho al testamento digital

Se trata del derecho a elaborar un testamento con instrucciones específicas para los perfiles de las redes sociales, contenidos en la nube, etc. Generó cierta polémica pues algunos notarios indican que no hacía falta modificar la norma para ello. Por otra parte, en la comunidad autónoma catalana esto ya se llevaba a cabo mediante una modificación de su Código Civil. Se concede a los familiares de un fallecido la posibilidad de tener acceso a los datos referentes a su vida digital si lo solicitan, y el difunto no dejara de forma expresa su idea en sentido contrario. De no ser así, podrán acceder "las personas vinculadas al fallecido por razones familiares", así como modificar o borrar los datos que contengan. También podrán decidir eliminar sus perfiles de redes sociales.

Políticas de impulso de los derechos digitales.

Por último, se trata de cubrir una serie de objetivos:

a) superar las brechas digitales y garantizar el acceso a Internet de colectivos vulnerables o con necesidades especiales y de entornos familiares y sociales económicamente desfavorecidos mediante, entre otras medidas, un bono social de acceso a Internet;

b) impulsar la existencia de espacios de conexión de acceso público; y

c) fomentar medidas educativas que promuevan la formación en competencias y habilidades digitales básicas a personas y colectivos en riesgo de exclusión digital y la capacidad de todas las personas para realizar un uso autónomo y responsable de Internet y de las tecnologías digitales.

También se promoverán las acciones de formación, difusión y concienciación necesarias para lograr que los menores de edad hagan un uso equilibrado y responsable de los dispositivos digitales y de las redes sociales y de los servicios de la sociedad de la información.

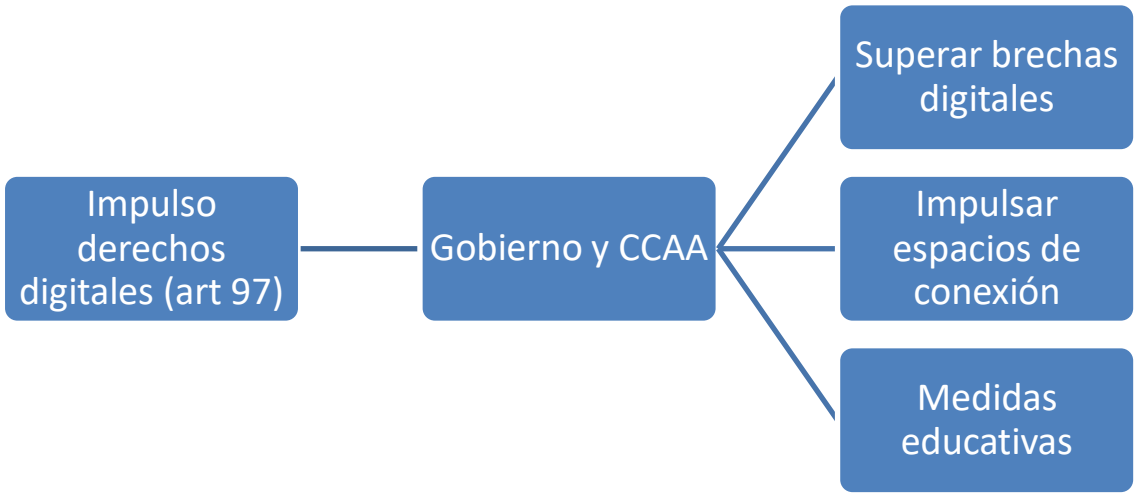


Ilustración 21 Impulso de los derechos digitales. Elaboración propia.

Breve aproximación ética al tratamiento de datos

No pensemos que por vivir en un momento de máxima eclosión tecnológica, estamos reinventando normas éticas y morales. Para muestra, vale con fijarnos en una frase ¡de un libro de 1939! que parece escrito para nosotros hoy mismo:

> *Una cosa es, por lo menos, clarísima: que las condiciones de todo orden, sociales, económicas, políticas, en que va a trabajar mañana son sumamente distintas de aquéllas en que trabajó hasta hoy.*

No se hable, pues, de la técnica como de la única cosa positiva, la única realidad inconmovible del hombre. Eso es una estupidez, y cuanto más cegados estén por ella los técnicos, más probable es que la técnica actual se venga al suelo y periclite.

Basta con que cambie un poco sustancialmente el perfil de bienestar que se cierne ante el hombre, que sufra una mutación de algún calibre la idea de la vida, de la cual, desde la cual y para la cual hace el hombre todo lo que hace, para que la técnica tradicional cruja, se descoyunte y tome otros rumbos.(Ortega y Gasset, 1968)

No, no hay nada nuevo bajo el sol. Pero hay elementos que producen interferencias con nuestra visión clásica, de siglos. Hobbes, en su Leviatán (Hobbes, 2003), establecía algo que había venido siendo aceptado por todos: el pacto de la ciudadanía con el estado por su seguridad. Ese padre estado ha cedido su contrato a compañías como Movistar, Google o Facebook, que gestionan, cuando no algo peor, nuestros datos y con ellos nuestra seguridad, tanto en la sociedad en red como fuera de ella. ¿Y cómo es ese contrato? ¿Quién debe vigilar las cláusulas? ¿Somos conscientes de que en muchas ocasiones regalamos nuestros datos a nuestros proveedores como Fausto vendía su alma al diablo?

Decíamos que no estábamos inventando nada. En efecto, ni tan siquiera desde el campo de la informática. Desde antes de la eclosión de internet el asunto ya preocupaba. Por ejemplo, desde la IEEE (Institute of Electrical and Electronics Engineers, una asociación tremendamente implicada en la ética de las TIC), en 1995 apareció el importante en tamaño y contenidos Ethics and Computing (Bowyer, 1995), donde la privacidad ocupa un espacio de mucho interés, y con una visión que podríamos llamar actual: partiendo de lo que él considera un precedente, las escuchas en líneas telefónicas[16] llega a lo que denomina "Efecto Gran Hermano", buscando la respuesta en ese momento únicamente en la tecnología, dado que la parca legislación estadounidense poca respuesta podía darle. En concreto, se centra en la encriptación, en la llave privada[17]. A este respecto, resulta interesante leer, por el contraste, la Sentencia del Tribunal Supremo, sala de lo penal, 1942/2016, donde se avalan las escuchas por medios tecnológicos, incluida la utilización de los teléfonos móviles como micrófonos ambientales (Recurso de casación por infracción de preceptos constitucionales e infracción de Ley, 2016) . Sobre los estudios técnicos, destacamos (Landau, y otros, 1994) y (Barlow , 1993). Sobre el espionaje sistemático del estado, (Oltra Gutiérrez, 2001)

Por un lado proclamamos los derechos humanos, de entre ellos el derecho a la intimidad de la persona, y por otro con las técnicas que nos son propias propiciamos, siquiera sea inconscientemente, la vulneración de ese derecho (pensemos en fotografías aéreas, satélites, micrófonos de móviles, etc.). Ya no somos solo un número para un banco, un nombre y apellidos sustituibles por el número del DNI. Somos todo lo que tiene el fisco de nosotros, todo lo relacionado a nuestro carnet de conducir, nuestro historial de la Seguridad Social… las veces

[16]Desde 1928 se conocen las intervenciones de líneas telefónicas por parte de la policía para luchar contra el crimen. Su evolución es lenta, pero constante. En 1968 se registran en Estados Unidos unas 900 escuchas realizadas legalmente por la policía. Poco después, el mismo concepto se traslada a las conversaciones vía internet con, por ejemplo, "sniffers" legales.

[17] Debe hacernos pensar esto en por qué las aplicaciones que se sirven de PGP, como encriptación, tienen problemas transfronterizos al considerarlos el legislador del otro lado del charco como armas.

que hemos consultado una cartelera de cine, si hemos visto un vídeo de Johnny Cash a través de Youtube, si tu madre consulta el horóscopo, si tienes marcas biológicas en la sangre, tu retrato antropológico… todo susceptible de ser codificado y de generar con ello espectros económicos, sumándolos a informes tuyos que andan dispersos, incluso antiguos como tus antecedentes patológicos familiares, los datos de tu propia gestación, incluso rumores sobre tu carácter. Somos, en sí, un gigantesco y voraz banco de datos donde caben todos los hechos y dichos de tu vida (Vázquez & Barroso , 1992)

Día a día, voluntaria o involuntariamente, facilitamos a grandes bases de datos información sobre nuestros deseos, nuestras creencias e ideologías, dejando un rastro vivo de los restaurantes donde comemos, que libro compramos, con quien hablamos de forma supuestamente privada con aplicaciones de mensajería, cuánto dinero tenemos, por donde hemos paseado. Esto nos trae ecos de Foucalt(Foucalt, 2012), el efecto del panóptico, donde metemos a un preso en una celda permanentemente vigilada, asegurando así el funcionamiento automático del poder, pues el prisionero se sabe continuamente observado. La conclusión obvia, que la vigilancia puede considerarse simultáneamente deficiente y excesiva, puede aplicarse a los tratamientos de datos sin control, prácticamente sin variar ni una coma. Con una lectura directa, estamos ante la creciente demanda de seguridad y con ella la necesidad de vigilancia; y por otro lado los efectos que dicha vigilancia tiene sobre la libertad individual y colectiva. La cuestión de la privacidad queda entonces atrapada en un oxímoron que es “vigilar para liberar”. (Colmenarejo Fernández, 2017)

Aquí entra en juego el perfil del profesional. Un profesional de la información tiene de alguna manera un puesto de árbitro en ese nuevo juego que se configura. Dicho de otra manera, si deseamos vivir en una sociedad justa, sin atropellos, donde las normas se respeten, libre y donde un poderoso por el mero hecho de serlo no “valga más” que un humilde, necesitamos buenos profesionales. Buenos, en doble sentido: buenos porque se posee un dominio excelente de la técnica y buenos como personas, que son capaces de mirarse al espejo sabedoras de que enfrente no tienen a nadie que quiebra la ética y la deontología profesional. Porque si solo somos buenos como técnicos, despreciando las normas de comportamiento, estamos arrojando al contenedor la parte más importante de nuestra humanidad y colocando cuñas para quebrar nuestra sociedad.

Obviamente, si planteáramos en clase de forma abierta la pregunta ¿Qué es una persona buena?, saldrían tantas respuestas como alumnos. No, no hay, al menos soy incapaz de darla yo, una respuesta única a esa pregunta. Hay muchísimas consideraciones a ser tenidas en cuenta. De hecho, sobre estas materias, las dudas crecen. Como nos recuerda (López Calvo, 2018) incluso en las personas con formación tecnológica y jurídica al respecto, hay opiniones divergentes, incluso en el ámbito judicial. Como la reciente Sentencia del Tribunal Europeo de Derechos Humanos que condena a España a indemnizar a cinco cajeras que robaban a su empleador por vulnerar el derecho a su privacidad al ser grabadas con cámaras ocultas o la habilitación de cesión a la Agencia Tributaria por Airbnb de los datos de sus clientes o por el Consejo General del Poder Judicial de los datos de abogados incluidos en Lexnet.

Nos planteamos una y otra vez debates viejos como la humanidad. Esa combinación entre ética, ley, decisiones personales y decisiones políticas nos acompañan desde el antiguo Egipto,

desde los códigos primitivos, donde ya se alude a razones morales. En el caso de la privacidad, desde el artículo de (Warren & Brandeis, 1890) es leído por muchos como un derecho moral a ser protegido por la ley[18]. Por organizar un poco las ideas, y siguiendo a (Colmenarejo Fernández, 2017), enumeraremos unas razones morales para la protección de los datos personales:

- Prevención de daños. Por ejemplo, garantizando que las contraseñas de acceso son seguras, o que la geolocalización no es activada por los dispositivos sin consentimiento del usuario.
- Evitar la desigualdad informativa. Los datos personales se han convertido en mercancías. Las personas suelen estar en posición de desventaja frente a empresas o gobiernos. Las leyes tienen por objeto establecer las condiciones equitativas para la redacción de contratos relativos a la transmisión y el intercambio de datos personales.
- Evitar la injusticia informativa, que puede conllevar discriminación. La información personal proporcionada en un contexto (p.e. durante un análisis médico) puede cambiar su significado en otro contexto (p.e. en procesos de contratación o en transacciones comerciales[19]) y desembocar en discriminación.
- No intromisión en la autonomía moral. La falta de privacidad puede exponer los individuos a fuerzas externas que influyen en sus elecciones. Pensemos en las noticias falsas que apoyan a un candidato frente a otro, que consiguen ser las más difundidas. Se muestran además a aquellos usuarios que pueden estar potencialmente de acuerdo, trayéndonos ecos de lo que llamamos "posverdad".

Recordemos que el procesamiento de datos exige que se especifique su propósito, se límite su uso, se notifique a los individuos y se permite corregir inexactitudes.

Solemos encontrar reticencias. Es habitual aludir a la neutralidad de los datos y de la tecnología para justificar lo innecesario de la ética en lo que se denominan ciencias empíricas. Los datos tienen una fuente, son obtenidos de personas o de actividades que hacen esas personas con unos determinados métodos y con una o más finalidades. Eso debería bastar, para algunos. El problema es que el gran tamaño y su cada vez mayor número provocan cambios en las actividades relacionadas con nuestra identidad. La sociedad, a veces de forma imperceptible, sufre cambios en la valoración de lo que es la privacidad, que conlleva controlar datos de otros y tan solo se despierta ante elementos críticos como la necesidad gestionar nuestra reputación. (Colmenarejo Fernández, 2017)

[18] Podemos pensar sin ir más lejos en la tan manida por las películas de Hollywood Cuarta Enmienda, de 1789, texto aprobado definitivamente por Jefferson en 1792 como parte de la Carta de Derechos redactados para controlar los abusos gubernamentales a los ciudadanos tras la Guerra de la Independencia, que dice así: *El derecho de los habitantes de que sus personas, domicilios, papeles y efectos se hallan a salvo de pesquisas y de aprehensiones arbitrarias será inviolable, y no se expedirán al efecto mandamientos que no se apoyen en un motivo verosímil, estén corroborados mediante juramento o protesta y describan con particularidad el lugar que debe ser registrado y las personas o cosas que deben ser detenidas o embargadas.*

[19] ¿cómo justificar la correlación de datos entre la información de un historial sanitario de un ciudadano con la información sobre sus búsquedas en google? Recordemos webs como patientslike me (Patients Like Me), de donde se robaron datos para su venta a compañías sanitarias. Esto debería hacernos reflexionar, entre otras cosas, sobre la relación de la exportación de datos con la portabilidad como nuevo derecho de protección de datos.

Podríamos aducir una supuesta objetividad de los métodos cuantitativos. Esa supuesta objetividad se fundamenta en la forma que tienen los sistemas de información de eludir o evitar la intervención humana. Esto vendría a afianzar esos paradigmas que nos hablan del determinismo tecnológico. Debemos asumir que los atributos técnicos de la tecnología deben ser analizados social y éticamente, y no solo técnicamente, pues las innovaciones tecnológicas lejos de ser neutrales siempre están orientadas hacia un fin político. (Colmenarejo Fernández, 2017). Además, hoy, con la "nube", la dispersión de servidores a lo largo del globo, que nos hace concebir a las bases de datos como algo sin un entorno físico, nos provoca un distanciamiento extra en lo moral. Nos Recuerda Colmenarejo una cita de Aranguren, según la cual ante un estímulo los humanos hemos de conformar necesariamente la realidad antes de tomar una decisión, hemos de pararnos a pensar, detenernos a justificar nuestra acción ante un abanico de posibilidades que se ubica en la irrealidad. Dice Aranguren que la primera dimensión de la libertad de las personas se da precisamente en este liberarse del estímulo que supone la reflexión. La segunda dimensión de la libertad que no se es propia se hace efectiva cuando tomamos una decisión, cuando decidimos actuar de un modo y no de otro, cuando justificamos nuestros actos está la dimensión moral, que nos es inherente a todos los seres humanos, nuestra capacidad para decidirnos entre irrealidades posibles distinguiendo entre bien, mal y o aquello que atiende exclusivamente a nuestros intereses. Y dicho esto ¿Cómo conformamos una realidad "no tangible"?

Parece pues que, por una parte, la neutralidad de la tecnología, que supuestamente no tiene moral, y por otra la intangibilidad del bien a proteger, nos permite ponernos de perfil. Craso error. Vamos a apoyarnos para desmontar esto en (De la Cueva, 2018). Por una parte, las soluciones dadas por los sistemas informáticos a unas necesidades de gestión de la información no tienen respaldo jurídico alguno, son meras interpretaciones de un humano, el que construyó ese algoritmo. Eso rompe en mil pedazos la idea de la neutralidad de la tecnología. Es más, nos convierten en presos de unas imposiciones técnicas que no admiten su discusión pues se muestran como irrebatibles, lo que nos lleva a una verdadera dictadura de la máquina. Nos queda pendiente el, permítaseme el juego de palabras, vaporoso asunto de la nube. Que no lo es tanto, pues que no veamos las máquinas, no significa que estas no existan y por tanto, queden libres de sujeciones legales o morales.

No hace tanto, se nos decía que en Internet podíamos pasar por lo que quisiéramos. Una top model, un fuerte camionero, un niño pequeño, un actor o un amante de las focas. Hoy, eso ha dejado de ser cierto. Si somos un amate de las focas, se sabrá. Se sabrá además cuáles son nuestras focas favoritas, en que paralelo se encuentran, cómo se alimentan, que seguimiento les hacemos, cuántas veces hemos ido a verlas y que hemos escrito de ellas. Hasta que ropa llevábamos puesta cuando escribíamos de ellas. ¿Cómo se construyen esos registros? ¿Qué transparencia tiene el ciudadano de ellos? Hay una serie de problemas al respecto que (Colmenarejo Fernández, 2017) enumera:

- Los usuarios no han llegado a comprender cómo afectan estas violaciones de privacidad tanto de individuos como al comportamiento social de estos individuos.
- Existe una falta de transparencia en cuanto a política de privacidad, la información respecto los análisis predictivos.

- Datos falsos. Resultados de análisis falsos pueden ser compartidos a veces de forma automática. Esto dificulta que los usuarios puedan ejercer su derecho a corregir errores o falsedades que les afecten mediante un adecuado procedimiento.
- Posibilidad de programar análisis que permiten predecir con exactitud de forma automática un amplio rango de atributos sensibles cómo, p.e., la orientación sexual, creencias religiosas, ideología política, uso de drogas, test inteligencia, etcétera.
- Desajuste de las políticas reclamadas por los proveedores, y los controles reales disponibles para preservar la privacidad de los usuarios.
- Existencia de un incentivo policial similar para usar técnicas avanzadas de vigilancia[20].
- Limitaciones para permitir el análisis de datos privados, que hacen que esas técnicas sean vulnerables.
- Leyes de privacidad que se ven rápidamente superadas y que dejan de ajustarse al espíritu de las leyes originales.

Planteémonos ahora otra duda: si una persona cede intencionalmente información ¿qué derecho tienen otros a hacer esa información pública? ¿Nuestra mera existencia constituye entonces un acto creativo? Habría que hablar del derecho a la propiedad de los datos halando de la libre exposición de estos para hacer el uso de ellos de la forma que consideremos. El desafío llega al tratar el espinoso tema de la publicidad actual, directa hacia nosotros con los datos que conscientemente muchas veces les hemos dado. Esto es, quizá hay que protegernos de nosotros mismos, mediante tecnología está diseñada con requisitos de privacidad en el software y el hardware. Para hacer más cómodo esto, (Colmenarejo Fernández, 2017) propone una taxonomía de la privacidad de acuerdo con los diferentes momentos:

1. Recolección: vigilancia e interrogación con objeto de captar datos.
2. Proceso: recopilación, identificación, seguridad, uso secundario y exclusión.
3. Difusión: violaciones de confidencialidad, revelación, exposición indebida, facilidad de acceso, chantaje, apropiación y distorsión.
4. Intrusión e interferencia en la toma de decisiones.

¿Qué caracteriza hoy el uso de las bases de datos? Según (Colmenarejo Fernández, 2017), se puede resumir en “Las cinco V”: volumen, velocidad, variedad, veracidad y valor.

Códigos de conducta

Acabamos de ver cómo, en toda actuación profesional, no solo basta cumplir con la ley. La ley es lo que nos controla desde fuera, pero hay un control superior que es el interior. En lo que respecta al mundo de la protección de datos, con una necesaria proactividad de los responsables, la existencia de unos códigos que ayuden a delimitar unos cauces adecuados se convierte en algo, más que importante, casi imprescindible. Así, el Reglamento incita a asociaciones representen a responsables o encargados a que elaboren códigos de conducta[21],

[20] Es de interés visualizar el documental Pre-Crimen (Hielscher & Heeder, 2018)
[21] Podemos enlazar esto con los criterios para la construcción de códigos deontológicos o de buena práctica profesional, en los que debe figurar: (Garriga Domínguez, 2010)

con el fin de facilitar su aplicación efectiva, interpretando las características específicas en cada sector y las necesidades específicas, sobre todo, de las PYME´s

En estos códigos es de interés establecer las obligaciones de los responsables y encargados.

Para elaborarlos, o modificarlos si procede, es preciso consultar a las partes interesadas.

Algunos elementos a considerar en estos códigos:

1. el tratamiento leal y transparente;
2. los intereses legítimos perseguidos por los responsables;
3. la recogida de datos personales;
4. la seudonimización de datos personales;
5. la información proporcionada al público y a los interesados;
6. el ejercicio de los derechos de los interesados;
7. la información proporcionada a los niños y la protección de estos;
8. la notificación de violaciones de la seguridad de los datos personales
9. la transferencia de datos personales a terceros países

Las asociaciones y otros organismos que proyecten elaborar un código de conducta o modificar o ampliar un código existente presentarán el proyecto de código o la modificación o ampliación a la autoridad de control competente. Si el proyecto de código o la modificación o ampliación es aprobado, la autoridad de control registrará y publicará el código. El Comité archivará en un registro todos los códigos de conducta, modificaciones y ampliaciones que se aprueben, y los pondrá a disposición pública por cualquier medio apropiado.

Certificación

Se promueve la creación de mecanismos de certificación en materia de protección de datos y de sellos y marcas de protección de datos a fin de demostrar el cumplimiento de lo dispuesto en el presente Reglamento en las operaciones de tratamiento de los responsables y los encargados.

Estos mecanismos de certificación, sellos o marcas de protección de datos tienen el objeto de demostrar la existencia de garantías adecuadas ofrecidas por los responsables o encargados no sujetos al presente Reglamento. Esta certificación será voluntaria y estará disponible a través de un proceso transparente. Se expedirá a un responsable o encargado de tratamiento por un período máximo de tres años y podrá ser renovada en las mismas condiciones, siempre y cuando se sigan cumpliendo los requisitos pertinentes. La certificación será retirada, cuando no se cumplan o se hayan dejado de cumplir los requisitos para la certificación.

• Condiciones de organización
• Régimen de funcionamiento
• Procedimientos aplicables
• Normas de seguridad de los ficheros
• Obligaciones de los responsables del fichero y de las demás personas que intervengan en el tratamiento o uso de datos personales.
• Las garantías para el ejercicio de los derechos de las personas afectadas.

El Comité archivará en un registro todos los mecanismos de certificación y sellos y marcas de protección de datos y los pondrá a disposición pública por cualquier medio apropiado.

Los organismos de certificación sean acreditados por la autoridad de control, por el organismo nacional de acreditación (Reglamento (CE) nº 765/2008 del Parlamento Europeo y del Consejo con arreglo a la norma EN ISO/IEC 17065/2012), o por ambos. Esta acreditación se expedirá por un período máximo de cinco años y podrá ser renovada en las mismas condiciones.

Situación y conclusiones

El ser humano parece deja de ser soberano para pasar a ser un flujo de datos en una unidad controlada. Mientras las empresas privadas crecen en poder no solo económico, sino también político y social, como podemos ver por los mensajes dominantes que nos rodean… o por las posibilidades de ganar elecciones usando las redes sociales…

Está en manos del profesional conducir esta situación a buen término, pero… las noticias que nos rodean llevan a gran confusión. Leemos en la prensa datos sorprendentes y titulares aún más llamativos que nos hacen pensar que las empresas parecen dividirse entre las que se han enterado de que existe una legislación europea de protección de datos e intentan hacer algo, con diverso éxito, y los que aun "pasan", por no hablar de casos peores (recordemos el asunto de Cambridge Analytica con los datos tomados de Facebook)

Hay que tener en cuenta la dificultad de armonizar en una legislación las 27 precedentes de los distintos países de la unión, al tiempo que vigilar que los cambios producidos por esta se lleven a cabo de forma razonable. Todos recibimos en su momento una lluvia de peticiones de consentimiento que, al tiempo que nos recuerda nuestra vida digital y tantos años de regalar nuestros datos por internet, nos hacen ver que entramos en una nueva era.

Muchos aspectos cambiantes a considerar hemos visto, aspectos a ser tamizados por la ley 3/2018, por ejemplo, sobre el espinoso tema de los difuntos, al facilitar que los herederos puedan dirigirse al responsable de tratamiento, excepto si el finado no dijo otra cosa o hay una ley que lo impida. También aparecen cambios con respecto a los menores (menores, sus tutores o el Ministerio Fiscal; lo mismo para discapacitados menores) donde se rebaja la edad crítica de 14 a 13 años.

Este tipo de legislación es susceptible de recibir muchos cambios, bien por la promulgación de nuevas leyes, directivas…, bien por la corrección de las actuales (por ejemplo,(Europea, 2018)). Es muy importante para el profesional no bajar la guardia al respecto.

Es, de nuevo, el profesional la pieza clave para que este complicado mecanismo de relojería no atrase, no adelante… y no se pare.

Un punto de interés para el mismo lo tenemos en las memorias anuales de la AEPD.

Un ejemplo de próxima actualización lo tenemos con el "e-privacy".(Comisión Europea, 2017). Aún en proceso, este futuro Reglamento se centra especialmente las comunicaciones digitales y los parámetros de compatibilidad entre privacidad y economía digital, regulando aspectos tales como la protección de la privacidad en determinados servicios online o en los datos de los navegadores. Actualmente se aplica una directiva del año 2002, como puede entenderse,

obsoleta en muchos aspectos, por eso desde 2009 se están dando pasos para sustituirla, esta vez como Reglamento, para evitar problemas a la hora de ejecución simultánea en los distintos países de la Unión. Algunos de los aspectos a renovar es la mejora de los navegadores en lo que respecta a la protección de datos, pues debe dejar de importar el dispositivo desde el que se emplee. Es algo que entra en lo llamado privacidad por diseño y que busca que los usuarios no tengan que visitar innumerables y cambiantes menús para proteger sus datos. También aparecen reglas estrictas para las cookies.

Herramientas de utilidad

Para finalizar, damos una serie de pistas sobre herramientas para localizar legislación y normas.

La principal es la página del BOE, donde podemos encontrar la legislación actualizada, al tiempo que disponible en compendios ("códigos"): www.boe.es

Para la legislación de la Unión, hay un buscador similar, multiidioma: https://eur-lex.europa.eu/homepage.html?locale=es

Autenticados en la red de la UPV y desde dentro de la misma, podremos acceder a los buscadores de AENOR, para normas técnicas y ARANZADI, de donde se destaca su archivo de jurisprudencia.

Herramientas de la AEPD (Facilita, evaluación de impactos, análisis de riesgos…): disponibles en: https://gestiona.aepd.es/

Otras normas de interés:

Además de las reseñadas en el tema, cabe destacar:

- Directrices sobre el consentimiento en el sentido del Reglamento (UE) 2016/679(GRUPO DE TRABAJO DEL ARTÍCULO 29 SOBRE PROTECCIÓN DE DATOS, 2017)
- Orientaciones de la Comisión sobre la aplicación directa del Reglamento general de protección de datos: (Comisión Europea, 2018)
- Para desarrolladores de aplicaciones móviles: Hay un documento del grupo 29 imprescindible: (ARTICLE 29 DATA PROTECTION WORKING PARTY, 2013)
- REGLAMENTO (CE) No765/2008 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 9 de julio de 2008por el que se establecen los requisitos de acreditación y vigilancia del mercado relativos a la comercialización de los productos y por el que se deroga el Reglamento (CEE) n339/93(PARLAMENTO EUROPEO Y CONSEJO DE LA UNIÓN EUROPEA, 2008)
- Requisitos para organismos que certifican productos, procesos o servicios (AENOR, 2012)

Otros textos de interés:

Para profundizar en determinados temas:

- AGPD: Procedimiento por incorporación a un grupo de Whatsapp(Agencia Española de Protección de Datos, 2017)
- AGPD: Procedimiento por transmisión de fotos por Whatsapp(Agencia Española de

Protección de Datos, 2017)
- AGPD: Procedimiento sancionador contra Google Street View (Agencia Española de Protección de Datos, 2017)
- Circular del ministerio fiscal sobre intervención de comunicaciones electrónicas (FISCALÍA GENERAL DEL ESTADO, 2013)
- Derecho al olvido. Caso Mario Costejá: (Google vs Mario Costejá, 2014)
- La corte de apelación de los Estados Unidos declara que los "likes" de Facebook están protegidos por la Primera Enmienda: (Bland vs Roberts, 2013)
- Libertad de información, derecho a la propia imagen y autocensura de los medios: (Salvador, Rubí, & Ramírez, 2011)
- Menores en internet: (Davara Fernández de Marcos, Madrid)
- Sentencia: derecho al olvido digital: (Derecho al olvido digital. Digitalización de hemeroteca sin utilizar códigos ni instrucciones que..., 2015)
- Sobre el uso de cámara oculta: Tesis doctoral (Gómez Sáez , 2014)
- Sobre tratamiento de los datos sanitarios: (Medinacelli Díaz, 2016)

Preguntas de tipo test. Ejemplos.

El Reglamento Europeo de Protección de Datos se aplica a

a) Las personas jurídicas
b) Las personas físicas
c) a) y b) son correctas
d) La inscripción en el Registro general

Respuesta correcta: b). Página 2.

Pertinencia es sinónimo de:

a) Veracidad
b) Seguridad
c) Lealtad
d) Ninguna de las anteriores

Respuesta correcta: d). Página 11.

Los momentos del Tratamiento de Protección de Datos serían

a) Cesión, tratamiento y utilización
b) Recogida, disociación y utilización
c) Recogida, tratamiento y utilización
d) Recogida, tratamiento y portabilidad

Respuesta correcta: c). Página 14

El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento

a) la rectificación de los datos personales inexactos que le conciernan
b) la disociación de los datos personales inexactos que le conciernan
c) la disociación de los datos personales exactos que le conciernan

d) Todas las anteriores son correctas

Respuesta correcta: a). Página 19

Hace falta un delgado de protección de datos

a) si se trata de un tratamiento desde la administración pública,
b) cuando se trabaja con datos de un elevado número de personas,
c) cuando se trabaja con un elevado número de datos especiales
d) Todas las anteriores son correctas

Respuesta correcta: d). Página 25.

ANEXO. Actuaciones técnicas del profesional.

Vamos a tratar en este apartado de los elementos de más importancia para el profesional. Nos focalizaremos en la evaluación de impacto, dejando para mejor ocasión un desarrollo de la necesidad de establecer mediante contrato la obligación del análisis de riesgos y otras tareas importantes como el llevar a cabo el registro de actividad o notificar violaciones de seguridad y las elementales de garantía de la seguridad de los datos tratados y cooperación con la autoridad de control. Elementos como la aplicación de la portabilidad con sus consiguientes derivadas de empleo de formatos estructurados de uso común, de lectura mecánica… deben quedar al buen saber y hacer del profesional.

Evaluación de impacto (EIPD)

Se trata de evaluar de manera anticipada cuáles son los potenciales riesgos a los que están expuestos los datos personales en función de las actividades de tratamiento que se llevan a cabo con los mismos. Una EIPD es un proceso utilizado para reforzar y demostrar el cumplimiento.

De forma obvia, esto implica un análisis de riesgos, el cual permite identificar los riesgos que se ciernen sobre los datos de los interesados y establecer una respuesta adoptando las salvaguardas necesarias para reducirlos hasta un nivel de riesgo aceptable.

El RGPD prevé que las Evaluaciones de Impacto se lleven a cabo “antes del tratamiento”. Hay un par de documentos imprescindibles para el profesional. Por una parte, la Guía que la AEPD publicó (AEPD, 2017)y, por otra, las directrices que sobre el EIPD dio el Grupo del Artículo 29 (Grupo "Protección de datos" del artículo 29, 2017). Por otra parte, y para el momento concreto de la notificación de brechas de seguridad, recordemos que también existe una guía al respecto (AEPD & INCIBE, 2017).

¿Cuándo se debe hacer?

La Evaluación de Impacto debe llevarse a cabo cuando sea probable que un tipo de tratamiento por su naturaleza, alcance, contexto o fines, entraña un alto riesgo para los derechos y libertades de las personas físicas.

Si al realizarla se ve que el tratamiento entrañaría un alto riesgo si el responsable no toma medidas para para mitigarlo.

Para determinar si es necesario llevar a cabo la evaluación de Impacto o no, se puede seguir una breve metodología de análisis en dos fases (art. 35. RGPD), (art 28 Ley 3/2018):

Fase 1. Analizar las listas de tratamientos previstos en la regulación;

1.1) Evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones.

1.2) Tratamiento a gran escala de las categorías especiales de datos, o de los datos personales relativos a condenas e infracciones penales.

1.3) Observación sistemática a gran escala de una zona de acceso público.

Fase 2. Análisis de la naturaleza, alcance, contexto y fines de tratamiento: si se utilizan TIC´s o si por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas.

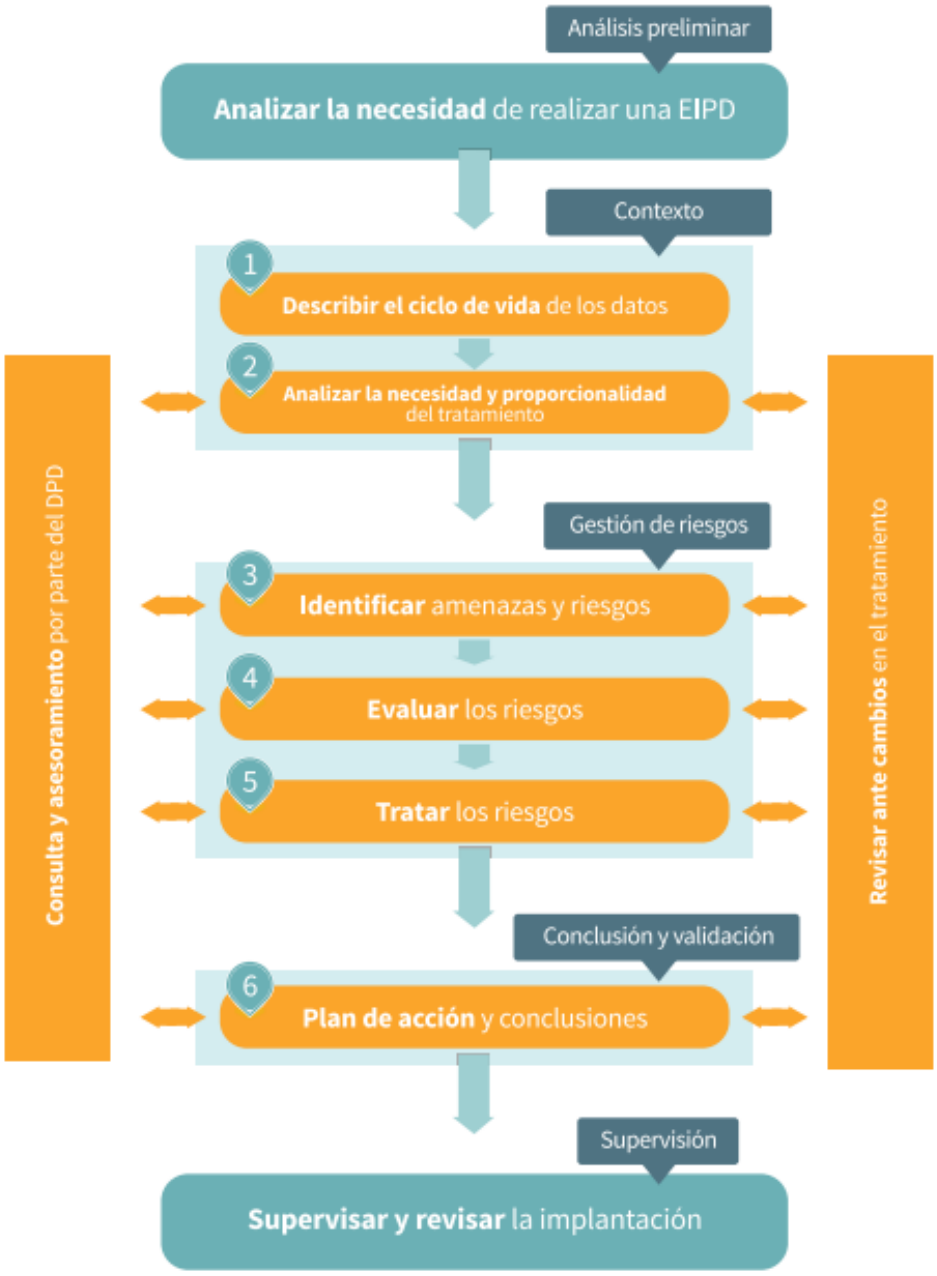


Ilustración 22 Flujo a seguir en una EIPD. Fuente: AEPD, guía práctica para las EIPD

¿Qué debe incluir como mínimo?

1. Descripción sistemática de las operaciones de tratamiento previstas, de los fines del mismo, y si procede, el interés legítimo perseguido por el responsable del tratamiento.

2. Evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad.

3. Evaluación de los riesgos para los derechos y libertades de los interesados.

4. Medidas previstas para afrontar los riesgos, demostrando la conformidad con el Reglamento General.

Medidas paliativas que determine la autoridad de control

Existe la necesidad de adoptar aquellas medidas paliativas o correctivas del tratamiento pretendido, cuando el mismo lleve consigo un alto riesgo de vulneración de los derechos y libertades de los interesados o titulares de los datos, en busca de aminorar los riesgos y en su caso, los perjuicios que, en su caso, se hubiera podido causar a los titulares de los datos, si los tratamientos se hubieran llevado a cabo de manera efectiva.

Son medidas correctoras o moderadoras del riesgo. Muchas veces la gravedad del impacto puede evitarse con un mejor diseño del mismo. Todas estas actuaciones deberán quedar incorporadas y acreditadas documentalmente en las correspondientes subcarpetas de esta carpeta, a los efectos de su debida constancia.

¿Qué criterios adoptar?

a) Reducir al máximo el tratamiento de datos personales.

b) Pseudo anonimizar lo antes posible los datos personales.

c) Dar transparencia a las funciones y el tratamiento de datos personales.

d) Permitir a los interesados supervisar el tratamiento de datos.

e) Crear y mejorar elementos de seguridad.

Además, aquellos criterios que la AEPD indica: Licitud, lealtad y transparencia; Limitación de la finalidad (los datos se recogen con un fin determinado); Minimización de datos; Exactitud; Limitación del plazo de conservación; Integridad y confidencialidad.

Directrices del grupo 29

En este apartado vamos a tratar de resumir los aspectos más importantes del imprescindible documento ya citado *Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del Reglamento (UE) 2016/679* (Grupo "Protección de datos" del artículo 29, 2017). El resumen es más que eso: es una síntesis de párrafos destacados de la guía, de la que recomendamos encarecidamente su lectura y estudio.

Empezamos definiendo lo que es un riesgo y su gestión.

Un «riesgo» es un escenario que describe un acontecimiento y sus consecuencias, estimado en términos de gravedad y probabilidad. La «gestión de riesgos» puede definirse como las actividades coordinadas para dirigir y controlar una organización respecto al riesgo. Para nosotros esta lectura va tamizada por el artículo 35 del RGPD, que se refiere a un probable alto riesgo «para los derechos y libertades de las personas». En esa referencia a «los derechos y libertades» de los interesados no solo se apunta a los derechos a la protección de datos y a la intimidad, sino a otros derechos fundamentales como la libertad de expresión, la libertad de pensamiento, la libertad de circulación, la prohibición de discriminación, el derecho a la libertad y la libertad de conciencia y de religión.

La AEPD tiene una guía magnífica muy recomendable, la Guía práctica de análisis de riesgos en lo tratamientos de datos personales sujetos al AEPD (AEPD, 2017), de donde sacamos esta imagen:

Ilustración 23 Riesgos y su gestión. Fuente: Guía práctica de análisis de riesgos...

La guía del grupo 29 nos muestra otra imagen muy aclaratoria.

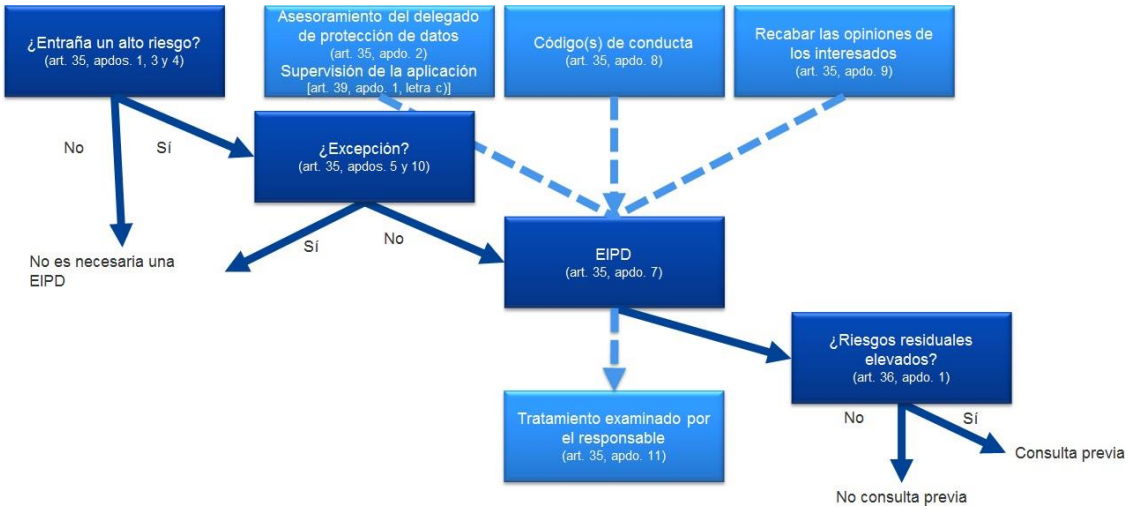


Ilustración 24 Principios básicos relacionados con la EIPD en el RGPD . Fuente: Directrices...

Vamos a ir respondiendo, siguiendo milimétricamente la guía, las preguntas más importantes.

¿Qué aborda una EIPD? ¿Una única operación de tratamiento o un conjunto de operaciones de tratamiento similares?

Puede utilizarse una única EIPD para evaluar múltiples operaciones de tratamiento que sean similares en términos de naturaleza, alcance, contexto, fines y riesgos. Un ejemplo: se puede para una compañía de ferrocarriles cubrir la videovigilancia de todas sus estaciones con solo una EIPD. Esto sería igualmente aplicable a operaciones de tratamiento similares aplicadas por varios responsables.

Una EIPD también puede servir para evaluar el impacto relativo a la protección de datos de un producto tecnológico, de tal forma que el responsable del tratamiento que instala el producto sigue teniendo la obligación de llevar a cabo su propia EIPD relativa a la aplicación específica, pero esta puede basarse en una EIPD preparada por el proveedor del producto.

¿Qué operaciones de tratamiento deben someterse a una EIPD?

Salvo excepciones, todas aquellas que «probablemente entrañen alto riesgo». A menos que la operación de tratamiento cumpla una excepción, se debe realizar una EIPD cuando una operación de tratamiento «entrañe probablemente un alto riesgo»

¿Cuándo resulta obligatoria una EIPD? Cuando el tratamiento «entrañe probablemente un alto riesgo». En los casos en los que no esté claro si se requiere una EIPD, el GT29 recomienda realizar una.

Para entender qué conjunto de operaciones de tratamiento requerirían una EIPD debido a su inherente alto riesgo, se deben considerar los nueve criterios siguientes:

1. Evaluación o puntuación, incluida la elaboración de perfiles y la predicción, especialmente de «aspectos relacionados con el rendimiento en el trabajo, la situación económica, la salud, las preferencias o intereses personales, la fiabilidad o el comportamiento, la situación o los movimientos del interesado». Algunos ejemplos de esto podrán incluir a una

institución financiera que investigue a sus clientes en una base de datos de referencia de crédito o en una base de datos contra el blanqueo de capitales y la financiación del terrorismo o sobre fraudes.

2. Toma de decisiones automatizada con efecto jurídico significativo o similar: tratamiento destinado a tomar decisiones sobre los interesados que produce «efectos jurídicos para las personas físicas» o que les afectan «significativamente de modo similar». Por ejemplo, el tratamiento puede provocar exclusión o discriminación contra las personas.

3. Observación sistemática: tratamiento usado para observar, supervisar y controlar a los interesados, incluidos los datos recogidos a través de redes u «observación sistemática [...] de una zona de acceso público»

4. Datos sensibles o datos muy personales: esto incluye las categorías especiales de datos personales definidas en el artículo 9 (por ejemplo, información sobre las opiniones políticas de las personas), así como datos personales relativos a condenas e infracciones penales según la definición del artículo 10. Un ejemplo sería un hospital general que guarda historiales médicos de pacientes o un investigador privado que guarda datos de delincuentes.

5. Tratamiento de datos a gran escala: determinar si el tratamiento se realiza a gran escala:

5.1. El número de interesados afectados, bien como cifra concreta o como proporción de la población correspondiente;

5.2. El volumen de datos o la variedad de elementos de datos distintos que se procesan;

5.3. La duración, o permanencia, de la actividad de tratamiento de datos;

5.4. El alcance geográfico de la actividad de tratamiento.

6. Asociación o combinación de conjuntos de datos, por ejemplo procedentes de dos o más operaciones de tratamiento de datos realizadas para distintos fines.

7. Datos relativos a interesados vulnerables:

8. Uso innovador o aplicación de nuevas soluciones tecnológicas u organizativas, como combinar el uso de huella dactilar y reconocimiento facial.

9. Cuando el propio tratamiento «impida a los interesados ejercer un derecho o utilizar un servicio o ejecutar un contrato». Un ejemplo de esto sería cuando un banco investiga a sus clientes en una base de datos de referencia de crédito con el fin de decidir si les ofrece un préstamo.

En la mayoría de los casos, un responsable del tratamiento puede considerar que un tratamiento que cumpla dos criterios requerirá la realización de una EIPD. Sin embargo, en algunos casos, un responsable del tratamiento puede considerar que un tratamiento que cumpla solo uno de estos criterios requiere una EIPD.

Ejemplos sobre como evaluar si una operación de tratamiento concreta requiere una EIPD:

Ejemplo	Criterios	¿EIPD necesaria?
Hospital que trata los datos genéticos y sanitarios de sus pacientes	Datos sensibles o datos muy personales. Datos relativos a interesados vulnerables. Tratamiento de datos a gran escala.	SI
Sistema de cámaras en autovías. Existe un sistema inteligente para seleccionar coches y reconocer matrículas.	Observación sistemática. Uso innovador o aplicación de soluciones tecnológicas u organizativas.	SI
Observación de actividades de empleados: puesto de trabajo, internet…	Observación sistemática. Datos relativos a interesados vulnerables.	SI
Recogida de datos de los medios sociales públicos para elaborar perfiles.	Evaluación o puntuación. Tratamiento de datos a gran escala. Asociación o combinación de conjuntos de datos. Datos sensibles o datos muy personales	SI
Base de datos nacional de calificación crediticia o sobre fraudes	Evaluación o puntuación. Toma de decisiones automatizada con efecto jurídico significativo o similar. Impide a los interesados ejercer un derecho o utilizar un servicio o ejecutar un contrato. Datos sensibles o datos muy personales	SI
Datos personales de pacientes o clientes por un solo médico, otro profesional de la salud o abogado	Datos sensibles o datos muy personales. Datos relativos a interesados vulnerables.	NO
Revista en línea que use una lista de distribución para enviar un resumen diario	Tratamiento de datos a gran escala.	NO
Web de comercio electrónico que muestra anuncios de piezas de coches clásicos que supone una elaboración de perfiles limitada basada en elementos vistos o adquiridos en su propio sitio web.	Evaluación o puntuación.	NO

No se requiere una EIPD en los siguientes casos:

- cuando «no sea probable que el tratamiento entrañe un alto riesgo para los derechos y libertades de las personas físicas»;

- cuando la naturaleza, el alcance, el contexto y los fines del tratamiento sean muy similares al tratamiento para el que se ha realizado la EIPD.

- cuando las operaciones de tratamiento hayan sido comprobadas por la autoridad de control antes de mayo de 2018 en condiciones específicas que no hayan cambiado

- cuando una operación de tratamiento tenga una base jurídica en el Derecho de la Unión o en el Derecho del Estado miembro, y cuando ya se haya realizado una EIPD

- cuando el tratamiento se incluya en la lista opcional (establecida por la autoridad de control) de operaciones de tratamiento para las que no se requiere una EIPD

¿Qué pasa con las operaciones de tratamiento ya existentes?

El requisito de realizar una EIPD se aplica a operaciones de tratamiento existentes que probablemente entrañan un alto riesgo para los derechos y libertades de las personas físicas y para las que se ha producido un cambio de los riesgos, teniendo en cuenta la naturaleza, el alcance, el contexto y los fines del tratamiento. Por razón de buenas prácticas, una EIPD debe ser continuamente revisada y reevaluada con regularidad.

¿Cómo se debe llevar a cabo una EIPD?

Momento: antes del tratamiento. La EIPD debe iniciarse tan pronto como sea viable en el diseño de la operación de tratamiento incluso aunque algunas de las operaciones de tratamiento no se conozcan aún. Llevar a cabo una EIPD es un proceso continuo, no una medida excepcional.

Consejo: resulta una buena práctica definir y documentar otras funciones y responsabilidades específicas. P.e.:

- en el caso de que unidades empresariales específicas propusieran llevar a cabo una EIPD, dichas unidades deberían aportar información a la EIPD y participar en el proceso de validación de dicha evaluación;

- en su caso, se recomienda recabar el asesoramiento de expertos independientes de distintas profesiones (abogados, expertos en TI, expertos en seguridad, sociólogos, expertos en ética, etc.).

- las funciones y responsabilidades de los encargados del tratamiento deben definirse contractualmente.

- el responsable principal de la seguridad de la información (CISO), en caso de ser nombrado, así como el delegado de protección de datos, podrían sugerir que el responsable llevara a cabo una EIPD sobre una operación de tratamiento específica, y deberían ayudar a las partes interesadas en la metodología, ayudar a evaluar la calidad de la evaluación de riesgo y si el riesgo residual es aceptable, y a desarrollar conocimientos específicos para el contexto del responsable del tratamiento;

¿Cuál es la metodología para llevar a cabo una EIPD?

El RGPD establece las características mínimas de una EIPD (artículo 35, apartado 7, y considerandos 84 y 90). En la guía se ofrece un gráfico que ilustra el proceso iterativo genérico para realizar una EIPD:

Ilustración 25 Proceso iterativo genérico para realizar una EIPD. Fuente: Guía...

Existen una serie de componentes de la EIPD que se solapan con componentes bien definidos de gestión del riesgo (p. ej., ISO 31000). Hay una serie de marcos relativos a la EIPD en la Unión Europea que hay que considerar[22].

[22] **Ejemplos de marcos genéricos de la UE:**
- DE: Standard Data Protection Model (modelo estándar de protección de datos), V.1.0 – versión de prueba, 2016. https://www.datenschutzzentrum.de/uploads/SDM-Methodology_V1_EN1.pdf
- ES: Guía para una Evaluación de Impacto en la Protección de Datos Personales (EIPD), Agencia española de protección de datos (AGPD), 2014. https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf

- FR: Privacy Impact Assessment (PIA) (evaluación de impacto relativa a la intimidad), Commission nationale de l'informatique et des libertés (CNIL), 2015. https://www.cnil.fr/fr/node/15798
- UK: Conducting privacy impact assessments code of practice (realización de evaluaciones de impacto relativas a la intimidad: código de práctica), Oficina del Comisario de Información (ICO), 2014. https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

Ejemplos de marcos de sectores específicos de la UE:
- Privacy and Data Protection Impact Assessment Framework for RFID Applications (marco de evaluación de impacto relativo a la intimidad y la protección de datos para las aplicaciones RFID). http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp180_annex_en.pdf
- Modelo de evaluación del impacto sobre la protección de datos para redes inteligentes y para sistemas de contador inteligente http://ec.europa.eu/energy/sites/ener/files/documents/2014_dpia_smart_grids_forces.pdf

Esto puede provocar un lío, de hecho se pueden usar diferentes metodologías para ayudar a la aplicación de los requisitos básicos establecidos en el RGPD. Se han identificado criterios comunes con el fin de permitir la existencia de estos distintos enfoques, al tiempo que se permite a los responsables del tratamiento cumplir con el RGPD. Aclaran los requisitos básicos del Reglamento, pero ofrecen un alcance suficiente para las diferentes formas de aplicación. Estos criterios pueden usarse para mostrar que una metodología de EIPD particular cumple los estándares exigidos por el RGPD. Depende del responsable del tratamiento elegir una metodología, pero esta debe cumplir los criterios establecidos en el anexo 2 de la guía[23].

Asimismo, una norma internacional ofrecerá directrices sobre las metodologías utilizadas para llevar a cabo la EIPD (ISO/CEI 29134).

[23] **Criterios para una EIPD aceptable**

El GT29 propone los siguientes criterios que los responsables del tratamiento pueden usar para evaluar si una EIPD, o una metodología usada para realizar una EIPD, es suficientemente exhaustiva para cumplir con el RGPD:

- se ofrece una descripción sistemática del tratamiento
  - se tienen en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento
  - se registran los datos personales, los destinatarios y el periodo durante el cual se conservarán dichos datos;
  - se ofrece una descripción funcional de la operación de tratamiento;
  - se identifican los medios de los que dependen los datos personales (hardware, software, redes, personas, papel o canales de transmisión del papel);
  - se tiene en cuenta el cumplimiento de los códigos de conducta aprobados
- se evalúan la necesidad y la proporcionalidad
  - se determinan las medidas previstas para cumplir el, teniendo en cuenta:
  - las medidas que contribuyen a la proporcionalidad y la necesidad del tratamiento sobre la base de:
    - fines determinados, explícitos y;
    - legalidad del tratamiento;
    - datos adecuados, pertinentes y limitados a lo necesario
    - duración limitada de la conservación
  - medidas que contribuyen a los derechos de los interesados:
    - información facilitada al interesado
    - derecho de acceso y a la portabilidad de los datos
    - derecho de rectificación y de supresión
    - derecho de oposición y a la limitación del tratamiento
    - relaciones con los encargados del tratamiento
    - garantías concurrentes en las transferencias internacionales
    - consulta previa
- se gestionan los riesgos para los derechos y libertades de los interesados
  - se aprecian el origen, la naturaleza, la particularidad y la gravedad de los riesgos o, más concretamente, de cada riesgo (acceso ilegítimo, modificación no deseada y desaparición de datos) desde la perspectiva de los interesados;
    - se tienen en cuenta los orígenes de los riesgos
    - se identifican efectos posibles sobre los derechos y libertades de los interesados en caso de que se produzcan hechos que incluyan el acceso ilegítimo, la modificación no deseada o la desaparición de datos;
    - se identifican las amenazas que pueden provocar el acceso ilegítimo, la modificación no deseada o la desaparición de datos;
    - se estiman la probabilidad y la gravedad
  - se determinan las medidas previstas para tratar esos riesgos;
- participan las partes interesadas

No existe la obligación de publicar la EIPD, pero publicar un resumen podría fomentar la confianza, y se debe comunicar la EIPD completa a la autoridad de control en caso de consulta previa o si así lo solicita la APD. La publicación de una EIPD no representa un requisito jurídico del RGPD, ya que es una decisión que corresponde al responsable del tratamiento. Sin embargo, los responsables deben considerar al menos la publicación de algunas partes, como un resumen o una conclusión de su EIPD.

¿Cuándo debe consultarse a la autoridad de control?

Cuando los riesgos residuales sean elevados. Un ejemplo de riesgo residual elevado inaceptable incluye casos en los que los interesados pueden encontrarse con consecuencias importantes, o incluso irreversibles, de las que no puedan recuperarse (p. ej.: un acceso ilegítimo a datos que suponga una amenaza para la vida de los interesados, un despido, un peligro financiero) o cuando parezca obvio que existirá un riesgo (p. ej.: por no poder reducir el número de personas que acceden a los datos debido a sus modos de intercambio, uso o distribución, o cuando no se corrige una vulnerabilidad conocida).

Cuando el responsable del tratamiento no pueda hallar suficientes medidas para reducir los riesgos hasta un nivel aceptable (es decir, los riesgos residuales siguen siendo elevados), se debe consultar a la autoridad de control.

Otros elementos de interés a considerar:

A modo de cajón de sastre, figuran elementos que no deben perderse de vista por el profesional

Tratamiento de categorías especiales.

Hablamos de elementos relacionados con la medicina preventiva o laboral, con los muy sensibles de salud, política, religión… y su relación con el interés público, y el frecuentemente olvidado asunto de las condenas e infracciones penales.

Consideremos que hay categorías de tratamiento que precisan una alta especialización, como los tratamientos con alto riesgo, las transferencias internacionales de datos, la elaboración de perfiles, la gestión de datos tratados por grupos de empresas o de datos de titularidad o interés público.

Hay una larga serie de elementos recomendables, desde la conocida guía de la Agencia Catalana de Protección de Datos para los centros educativos (Agencia Catalana de Protección de Datos, 2018) a normas internacionales como la ISO/IEC 29187 (Information technology -- Identification of privacy protection requirements pertaining to learning, education and training)

Protección de datos desde el diseño y por defecto

Se trata de algo a contemplar antes de determinar el tratamiento, incluyendo medidas técnicas y organizativas. Se trata de quedarse solo con los datos necesarios.

- se recaba el asesoramiento del delegado de protección de datos;
- se recaban las opiniones de los interesados o sus representantes .

Ejemplos:

Protección de datos desde el diseño: mediante el uso de seudonimización (sustitución del material de identificación personal) y de cifrado (codificación de mensajes de forma que solo las personas autorizadas puedan leerlos).

Protección de datos por defecto: animando a una plataforma de redes sociales a configurar los parámetros del perfil de los usuarios en el entorno que más proteja la intimidad, por ejemplo limitando desde el primer momento la accesibilidad del perfil de los usuarios para que por defecto no sea accesible a un número indefinido de personas.

Guías y documentación de alto interés para el profesional.

Un elemento de alto interés son las evaluaciones de impacto. Para ello proponemos tres elementos casi imprescindibles. Por una parte, la guía de la propia AEPD (Guía práctica para las evaluaciones de impacto en la protección de los datos sujetas al RGPD) (AEPD, 2017), por otra la aún más amplia guía de la Agencia Catalana de Protección de Datos (Evaluación de impacto relativa a la protección de datos) (Autoritat Catalana de Protecció de Dades, 2018) y por último la aplicación open source de la CNIL, lo que podemos considerar la agencia francesa. (CNIL, 2019)

Sobre el deber de informar. A quien, como y cuando, incluyendo la Gestión de los derechos: que, como, donde, cuando… la AEPD tiene una magnífica guía: Guía para el cumplimiento del deber de informar (AEPD, 2016).

La responsabilidad del responsable: los contratos con encargado, revisión de medidas, políticas de protección de datos, corresponsables, autorizaciones previas… podemos consultar las Directrices para la elaboración de contratos entre responsables y encargados de tratamiento (AEPD, 2016).

Notificación de brechas de seguridad. Además de distintos formularios de la AEPD, podemos consultar las Directrices sobre la notificación de las violaciones de la seguridad de los datos personales de acuerdo con el reglamento 2016/679 (Grupo de trabajo sobre protección de datos del artículo 29, 2018). También sobre brechas de seguridad son de interés una serie de normas técnicas: la familia UNE 71505. Sistema de Gestión de Evidencias Electrónicas (AENOR, 2013), las ISO IEC 29147:2018 Information technology - Security techniques - Vulnerability disclosure (ISO, 2018) e ISO IEC 29100 Framework sobre protección de datos de información personal (ISO , 2015). Es de mucho interés a este respecto el Reglamento (UE) No 611/2013 relativo a las medidas aplicables a la notificación de casos de violación de datos personales en el marco de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo sobre la privacidad y las comunicaciones electrónicas (Parlamento Europeo, 2013).

Más sobre riesgos: de alto interés relacionarlo con nuestra normativa propia de seguridad (Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información) (BOE, 2018) , el Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas (BOE, 2011), la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas (BOE, 2011), la Directiva (UE) 2016/1148 relativa a las medidas destinadas a garantizar un elevado

nivel común de seguridad de las redes y sistemas de información en la Unión (Parlamento Europeo, 2016) y no menos importante, la Guía de Seguridad de las TIC CCN-STIC 817: Esquema Nacional de Seguridad. Gestión de Ciberincidentes (CCN, 2018).

Sobre el consentimiento, es de alto interés estudiar las directrices sobre el consentimiento del Grupo 29 (GRUPO DE TRABAJO DEL ARTÍCULO 29 SOBRE PROTECCIÓN DE DATOS, 2017).

Para trabajo con perfiles es muy importante la consulta de las Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679 (Parlamento Europeo, 2018).

Bibliografía

PARLAMENTO EUROPEO Y CONSEJO DE LA UNIÓN EUROPEA. (9 de julio de 2008). REGLAMENTO (CE) No765/2008. - *REGLAMENTO (CE) No765/2008 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 9 de julio de 2008 por el que se establecen los requisitos de acreditación y vigilancia del mercado relativos a la comercialización de los productos y por el que se deroga el Reglamento* . Bruselas, Unión Europea: Diario Oficial de la Unión Europea.

AENOR. (Diciembre de 2012). Evaluación de la Conformidad. *UNE-EN ISO/IEC 17065*. Madrid, España: AENOR.

AENOR. (2013). *UNE 71505. Sistema de Gestión de Evidencias Electrónicas.* Madrid: AENOR.

AEPD. (2016). *Directrices para la elaboración de contratos entre responsables y encargados de tratamiento.* Madrid: AEPD.

AEPD. (2016). *Guía para el cumplimiento del deber de informar.* Madrid: AEPD.

AEPD. (2017). *Guía práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD".* Madrid: AEPD.

AEPD. (2017). *Guía práctica para las evaluaciones de impacto en la protección de los datos sujetas al RGPD.* Madrid: AEPD.

AEPD. (2018). *Listado de cumplimiento normativo.* Madrid: AEPD.

AEPD, & INCIBE. (2017). *Guía para la gestión y notificación de brechas de seguridad.* Madrid: AEPD.

Agencia Catalana de Protección de Datos. (2018). *Pautas de protección de datos para los centros educativos.* Barcelona: APDCAT.

Agencia Española de Protección de Datos. (2017). Denuncia del AYUNTAMIENTO DE LA FONT DE LA FIGUERA. *PS/00576/2017*. Madrid, España: Agencia Española de Protección de Datos.

Agencia Española de Protección de Datos. (2017). Google Street View. *Procedimiento Nº PS/00541/2010.* Madrid, España: Agencia Española de Protección de Datos.

Agencia Española de Protección de Datos. (2017). Infracción de Administraciones Públicas instruido por la Agencia Española de Protección de Datos al AYUNTAMIENTO DE BOECILLO. *Procedimiento Nº AP/00023/2017*. Madrid, España: Agencia Española de Protección de Datos.

Agencia Española de Protección de Datos. (26 de mayo de 2018). *Agencia Española de Protección de Datos.* Recuperado el 18 de julio de 2018, de https://www.aepd.es/

ARTICLE 29 DATA PROTECTION WORKING PARTY. (27 de Febrero de 2013). Opinion 02/2013 on apps on smart devices. Bruselas, Unión Europea: Consejo de Europa.

Autoritat Catalana de Protecció de Dades. (2018). *Evaluación de impacto relativa a la protección de datos.* Barcelona: APDCAT.

Barlow , J. P. (Noviembre de 1993). A plain text on crypto policy. *Communications of the ACM, 36*(11), 21-26.

Bland vs Roberts, Appeal: 12-1671 Doc: 59 (UNITED STATES COURT OF APPEALS FOR THE FOURTH CIRCUIT 18 de septiembre de 2013).

BOE. (14 de diciembre de 1999). Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. *«BOE» núm. 298, de 14/12/1999*. Madrid, España: BOE.

BOE. (12 de julio de 2002). Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico. Madrid, España: BOE.

BOE. (2011). *Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.* Madrid: BOE.

BOE. (2011). *Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.* Madrid: BOE.

BOE. (5 de Diciembre de 2018). Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. *Ley Orgánica 3/2018*. Madrid: BOE.

BOE. (2018). *Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.* Madrid: BOE.

Bowyer, K. W. (1995). *Ethics and Computing: Living Responsibly in a Computerized World.* Los Alamitos, CA, USA.: IEEE Computer Society Pres.

CCN. (2018). *Guía de Seguridad de las TIC CCN-STIC 817: Esquema Nacional de Seguridad. Gestión de Ciberincidentes.* Madrid: CCN.

CNIL. (1 de junio de 2019). *Privacy Impact assessment (pia)*. Obtenido de https://www.cnil.fr/en/privacy-impact-assessment-pia

Colmenarejo Fernández, R. (2017). *Una ética para Big Data.* Barcelona: UOC.

Comisión Europea. (10 de enero de 2017). Propuesta de REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE. *Reglamento sobre la privacidad y las comunicaciones electrónicas*. Bruselas, Unión Europea: Comisión Europea.

Comisión Europea. (24 de enero de 2018). Mayor protección, nuevas oportunidades: Orientaciones de la Comisión sobre la aplicación directa del Reglamento general de protección de datos a partir del 25 de mayo de 2018. *COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO*. Bruselas, Unión Europea: Comisión Europea.

Davara Fernández de Marcos, L. (Madrid). *Menores en Internet.* 2017: AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS.

Davara Rodríguez, M. Á. (1998). *La protección de datos en Europa.* Madrid: Asnef Equifax.

De la Cueva, J. (mayo-junio de 2018). Código fuente, algoritmos y fuentes del Derecho. *El Notario del Siglo XXI*(77).

De Miguel Molina, M., & Oltra Gutiérrez, J. V. (2007). *Deontología y Aspectos Legales de la Informática: cuestiones jurídicas, técnicas y éticas básicas.* Valencia: Servicio de Publicaciones de la Universidad Politécnica de Valencia.

De Miguel Molina, M., Oltra Gutiérrez, J. V., & Sarabdeen, J. (2010). An exploratory study on the privacy of children's images in Spain's most widely used social network sites (Tuenti and Facebook). *International Review of Law, Computers&Technology 3(24)*, 277-285.

Delgado Carravilla, E., & Puyol Montero, J. (2018). *La Implantación del Nuevo Reglamento General de Protección de Datos de la Unión Europea.* Valencia: Tirant.

Derecho al olvido digital. Digitalización de hemeroteca sin utilizar códigos ni instrucciones que..., STS 4132/2015 - ECLI:ES:TS:2015:4132 (Tribunal Supremo. Sala de lo Civil 15 de octubre de 2015).

Diario Oficial de la Unión Europea. (27 de abril de 2016). *Reglamento General de Protección de Datos (RGPD).* Recuperado el 4 de abril de 2018, de https://www.boe.es/doue/2016/119/L00001-00088.pdf

Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención. (27 de abril de 2016). *PARLAMENTO EUROPEO Y CONSEJO DE LA UNIÓN EUROPEA*. Bruselas, Unión Europea: Diario Oficial de la Unión Europea.

Europea, C. d. (19 de abril de 2018). Corrigendum Reglamento General de Protección de Datos. Bruselas, UE: Consejo de la Unión Europea.

FISCALÍA GENERAL DEL ESTADO. (11 de enero de 2013). SOBRE PAUTAS EN RELACIÓN CON LA DILIGENCIA DE INTERVENCIÓN DE LAS COMUNICACIONES TELEFÓNICAS. *CIRCULAR 1/2013,*. Madrid, España: FISCALÍA GENERAL DEL ESTADO.

Foucalt, M. (2012). *Vigilar y castigar.* Madrid: Biblioteca Nueva.

Frosini, V. (1982). *Cibernética, Derecho y sociedad.* Madrid: Tecnos.

García Mirete, C. M. (2014). *Bases de Datos Electrónicas Internacionales.* Valencia: Tirant lo Blanch.

Garriga Domínguez, A. (2010). *Fundamentos éticos y jurídicos de las TIC.* Cizur Menor (NAvarra): Thomson Reuters.

Goizueta Vértiz, J., González Murua, A. R., & Pariente, D. I. (2013). *El espacio de libertad, seguridad y justicia: Schengen y protección de datos.* Cizur Menor (Navarra): Thomson Reuters.

Gómez Sáez , F. (2014). Los reportajes de investigación con cámara oculta y sus repercusiones en los derechos fundamentales. *Tesis Doctoral*. Madrid, España: UNED.

Google Spain SL y Google Inc. contra Agencia Española de Protección de Datos (AEPD) y Mario Costeja González, Asunto C-131/12 (Tribunal de Justicia de la Unión Europea (Gran Sala) 2014).

Google vs Mario Costejá, C-131/12 (Gran Sala. Tribunal de Justicia -ue 31 de mayo de 2014).

GRUPO DE TRABAJO DE PROTECCIÓN DE LAS PERSONAS (Grupo de trabajo del artículo 29). (10 de abrl de 2018). Directrices sobre el consentimiento en el sentido del Reglamento (UE) 2016/679. *17/ES. WP259 y rev.01*. Bruselas, Unión Europea: European Comission.

GRUPO DE TRABAJO DEL ARTÍCULO 29 SOBRE PROTECCIÓN DE DATOS. (28 de noviembre de 2017). Directrices sobre el consentimiento en el sentido del Reglamento (UE) 2016/679. Bruselas, Unión Europea: Consejo de la Unión Europea.

Grupo "Protección de datos" del artículo 29. (2017). *Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) WP 248.* Bruselas: Comisión Europea.

Grupo de trabajo sobre protección de datos del artículo 29. (2018). *Directrices sobre la notificación de las violaciones de la seguridad de los datos personales de acuerdo con el reglamento 2016/679.* Bruselas: UE.

Hobbes, T. (2003). *Leviatán.* Barcelona: Losada.

ISO . (2015). *ISO IEC 29100 Framework sobre protección de datos de información personal.* Madrid: ISO.

ISO. (2018). *ISO IEC 29147:2018 Information technology - Security techniques - Vulnerability disclosure.* Madrid: ISO.

Landau, S., Kent, S., Brooks, C. C., Charney, S., Denning, D. E., Diffie, W., . . . Sobel , D. L. (Agosto de 1994). Crypto policy perspectives. *Communications of the ACM, 37*(8), 115-121.

López Calvo, J. (mayo-junio de 2018). Un Reglamento exponente, víctima y resultado de su tiempo. *El notario del siglo XXI*(77).

Medinacelli Díaz, K. I. (2016). *El tratamiento de los datos sanitarios.* Madrid: Agencia Española de Protección de Datos.

Moore , M. (Dirección). (2007). *Sicko* [Película].

Negroponte, N. (2003). Cómo vencer en la revolución digital. Madrid: Conferencia ExpoManagement 2003.

Oltra Gutiérrez, J. V. (2001). Echelon hoy. *Novática: Revista de la Asociación de Técnicos de Informática, 153* , 52-55.

Ortega y Gasset, J. (1968). *Meditación de la técnica.* Madrid: Revista de Occidente.

Parlamento Europeo. (24 de junio de 2013). Reglamento (UE) No 611/2013 relativo a las medidas aplicables a la notificación de casos de violación de datos personales en el marco de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo sobre la privacidad y las comunicaciones electrónicas. Bruselas: UE.

Parlamento Europeo. (2016). *DIRECTIVA (UE) 2016/1148 DEL PARLAMENTO EUROPEO Y DEL CONSEJO.* Bruselas: UE.

Parlamento Europeo. (2018). *Directrices sobre decisiones individuales automatizadas y elaboración de perfiles.* Bruselas: Parlamento Europeo.

PARLAMENTO EUROPEO Y CONSEJO DE LA UNIÓN EUROPEA. (31 de diciembre de 2003). Directiva 2003/98/CE del Parlamento Europeo y del Consejo, de 17 de noviembre de 2003, relativa a la reutilización de la información del sector público. Bruselas, Unión Europea: Diario Oficial de la Unión Europea.

Real Academia Española. (2017). *Diccionario de la Real Academia Española*. Recuperado el 17 de julio de 2018, de http://dle.rae.es/

Recurso de casación por infracción de preceptos constitucionales e infracción de Ley, STS 1942/2016 - ECLI:ES:TS:2016:1942 (Tribunal Supremo. Sala de lo Penal 3 de mayo de 2016).

Rincón, R. (26 de junio de 2018). *El País*. Recuperado el 18 de julio de 2018, de El Constitucional extiende el derecho al olvido a las hemerotecas digitales: https://elpais.com/politica/2018/06/26/actualidad/1530007122_707929.html

Salvador, P., Rubí, A., & Ramírez, P. (2011). Imágenes veladas. *InDret*.

Secretaría de Estado de Cultura. (s.f.). *Biblioteca Virtual de Prensa Historica*. Recuperado el 18 de julio de 2018, de http://prensahistorica.mcu.es/es/consulta/busqueda.cmd

The International Trade Administration. (27 de julio de 2016). *EUROPEAN UNION: TRANSFERRING PERSONAL DATA FROM THE EU TO THE US*. Recuperado el 20 de julio de 2018, de https://www.export.gov/article?id=European-Union-Transferring-Personal-Data-From-the-EU-to-the-US

Vázquez, J. M., & Barroso , P. (1992). *Deontología de la informática. Esquemas.* Madrid: Instituto de Sociología Aplicada.

Warren, S. D., & Brandeis, L. D. (15 de Diciembre de 1890). The Right to Privacy. (T. H. Association, Ed.) *Harvard Law Review, 4*(5), 193-220.

Contenido