

OpenCourseWare

DERECHO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

Coordinadora Curso: -Prof^a (PhD) María Nieves de la Serna Bilbao

**Titular de Derecho Administrativo UC3M// Departamento de
Derecho Público**

**Co-directora del Máster Universitario en Derecho
Telecomunicaciones, Protección de Datos, Audiovisual y Sociedad
de la Información// Instituto Pascual Madoz**

**LECCIÓN 2: PROTECCIÓN DE DATOS: RÉGIMEN
GENERAL**

*Elaborado por PhD. M^a NIEVES DE LA SERNA BILBAO
Profesora Titular de Derecho Administrativo// Departamento de Derecho
Público*

*Codirectora del Máster Universitario en Derecho Telecomunicaciones,
Protección de Datos, Audiovisual y Sociedad de la Información// Instituto
Pascual Madoz
Universidad Carlos III de Madrid*



Esta obra está bajo una [licencia de Creative Commons
Reconocimiento-NoComercial-CompartirIgual 3.0 España](https://creativecommons.org/licenses/by-nc-sa/3.0/es/).



SUMARIO:

I.- INTRODUCCIÓN Y ANÁLISIS DE LOS ANTECEDENTES DEL DERECHO A LA PROTECCIÓN DE DATOS EN EUROPA

1.- Presentación

2.- Primeras regulaciones; el Consejo de Europa –CdE-

3.- El Convenio 108 del Consejo de Europa, de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal

4. Regulaciones adoptadas a nivel internacional

I. Presentación

*«La protección de datos nunca debería verse como una regulación estática, sino siempre como un proceso dinámico que no tiene fin»¹ **

El origen del derecho a la protección de datos se suele situar con el desarrollo de la informática y los peligros que aquella supone o puede suponer para los derechos fundamentales o no de las personas, en particular, el derecho a la intimidad, honor, imagen, protección de datos (conocida comúnmente como derecho a la vida privada). La informática y más tarde internet (lo que se conoce hoy en día como la digitalización) han traído y continuarán trayendo importantes avances e innovaciones para la sociedad y para los ciudadanos que les ha mejorado (y continuará mejorando), substancialmente en todos los órdenes de la vida –calidad, productividad, servicios, información, etc.-. No obstante, la digitalización necesita para avanzar obtener, guardar y tratar datos con múltiples objetivos, algunos muy beneficiosos, pero, también, otros peligrosos para la sociedad y las personas, en particular, cuando se trata de datos personales que ponen en peligro la intimidad en sentido amplio y el libre desarrollo de la personalidad. Como respuesta a estos tratamientos y para limitar los potenciales peligros frente a la recopilación y el usos de datos se aprobaron diferentes normas destinadas a regular lo que se denominó, en un primer momento en Europa, el “derecho a la autodeterminación informativa”², reconocido posteriormente en España³ y en Europa⁴ como el “derecho a la protección de datos personales”.

¹ *Spiros Simitis en el transcurso de la Conferencia de Primavera de las Autoridades Europeas de Protección de Datos, celebrada en Cracovia del 25 al 26 de abril de 2005; Agencia de Protección de Datos de la Comunidad de Madrid (2008) Revista Datos Personales –Enero-

² Denominación utilizada por primera vez por el Tribunal Constitucional Alemán en la sentencia de 1983, al analizar los datos censales en conexión con el derecho fundamental al respeto de la personalidad recogido en la Constitución.

³ Expresión utilizada por el Reglamento europeo General de Protección de Datos. También es el término que el Tribunal Constitucional Español utiliza para referirse a este Derecho en la célebre sentencia 292/2000, de 30 de noviembre.

⁴ RGPD

No encontramos, por tanto, ante un derecho relativamente nuevo pero no por ello sin recorrido⁵. Al contrario, dados los importantes avances, progresos e innovaciones que la tecnología ha tenido –y continúa teniendo- al igual que el uso generalizado en todos los ámbitos de la vida de las personas, ésta sigue planteando incesantemente interrogantes y peligros frente al Derecho y, en particular, frente a los derechos de las personas. Esta situación determina para el Derecho la necesidad de abordar importantes cambios (y seguirá en ese camino) para limitar los peligros que aquellos avances suponen para la sociedad y los derechos de las personas. Nos encontramos, por tanto, ante un

⁵ Algunos autores, dada la relación del derecho a la protección de datos con el derecho a la intimidad, concretan como primer antecedente de este derecho el artículo «The Right to Privacy» -El derecho a la intimidad- publicado en 1890 de WARREN, S.D.; BRANDEIS, L.D. «The right to privacy» in *Harvard Law Review* (1890 [15 diciembre 1890]), Vol. 4, No. 5, p. 193-220. Versión española en WARREN, S.D.; BRANDEIS, L.D., *El derecho a la intimidad* (Madrid, Cívitas, 1995). En el mismo, se planteaba el reconocimiento del derecho a ser dejado en paz -la intimidad- y la necesaria protección que el ordenamiento jurídico debe ofrecer frente a los inventos y métodos comerciales, como el advenimiento de la fotografía instantánea y la circulación generalizada de periódicos que ocurrían en aquel entonces. Señalan los autores que aquellas invenciones habían contribuido a la invasión de la intimidad de las personas y concretamente expresaban que «La prensa está traspasando, en todos los ámbitos, los límites de la propiedad y de la decencia. El chismorreó ha dejado de ser ocupación de gente ociosa y depravada para convertirse en una mercancía, buscada con ahínco e, incluso, con descaro... Con el fin de entretener al indolente, columna tras columna se llenan de chismes insustanciales, obtenidos, únicamente, mediante la intromisión en el ámbito privado.» y subrayan «Es nuestro propósito considerar si la ley existente ofrece un principio que puede invocarse adecuadamente para proteger la privacidad del individuo; y, si lo hace, cuál es la naturaleza y el alcance de dicha protección», para concluir que el derecho a ser dejado en paz es «un principio que puede invocarse para proteger la privacidad del individuo de la invasión, ya sea por la prensa demasiado emprendedora, el fotógrafo o el poseedor de cualquier otro dispositivo moderno para grabar o reproducir escenas o sonidos».

Aquel ensayo tiene una influencia y trascendencia jurídica incuestionable que da lugar a un planteamiento original en el que no sólo se reconoce una dimensión individual o subjetiva del derecho a la intimidad, sino que también plantea, la dimensión social y colectiva del citado derecho en tanto que protege el propio mantenimiento y avance del sistema democrático, ya que la privacidad contribuye también a limitar la actuación de los poderes públicos y a definir el atributo de la ciudadanía. Un estudio más en profundidad puede verse en Saldaña, M Nieves, «*The right to privacy*»: la génesis de la protección de la privacidad en el sistema constitucional norteamericano, el centenario legado de Warren y Brandeis, en *Revista de Derecho Político*, núm. 85, 2012 UNED, quien señala que se trata de un ensayo fundacional de la protección de la privacidad en los Estados Unidos y el artículo doctrinal más influyente de la literatura jurídica norteamericana. Sin duda su influencia ha sido incuestionable, ha originado la preocupación colectiva por el reconocimiento y garantía de la esfera privada, ha generado al menos cuatro acciones civiles para su protección y ha encuadrado y fundamentado el discurso constitucional del derecho a la privacidad en los Estados Unidos durante todo el siglo XX.

ámbito que obliga al Derecho a adoptar nuevas normas, modificar las existentes, etc, es decir, actualizarse, al ritmo de la evolución tecnológica.

En definitiva, el Derecho a la protección de datos es un derecho moderno y activo⁶ en el que, con carácter general, todo tratamiento, recogida, custodia o cesión de datos de carácter personal, cualquier sea el dato (íntimo o no) se debe sujetar a la normativa vigente reguladora de la materia. Es así que, en principio, cualquier tratamiento de datos personales, aunque no afecte a la vida privada de las personas o al libre desarrollo de su personalidad, debe cumplir, obligatoriamente, con lo dispuesto por la normativa correspondiente. Esto no significa que los datos personales no puedan ser recopilados o tratados, sino que, por el contrario, determina que para llevar a cabo un uso o tratamiento de datos personales, es necesario cumplir con lo dispuesto en la normativa de protección de datos.

⁶ Véase al respecto TJUE, las conclusiones de la Abogada General en asunto Volker und Markus Schecke GbR y Hartmut Eifert contra Land Hessen -C92/09 y C93/02- cit en Manual de legislación europea en materia de protección de datos (2019); edit. Agencia de los Derechos Fundamentales de la Unión Europea y Consejo de Europa; Luxemburgo; pág. 22.

2.- Primeras regulaciones; el Consejo de Europa –CdE-

ANTECEDENTES DERECHO PROTECCIÓN DE DATOS

- 1.- Primeras regulaciones; el Consejo de Europa –CdE-
- 2.- El Convenio 108 del Consejo de Europa, de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal
- 3. Algunas regulaciones adoptadas a nivel internacional

Se suele mencionar como primeros antecedentes de regulación del derecho a la protección de datos las Resoluciones aprobadas por el Consejo de Europa –CdE- para salvaguardar los derechos de las personas frente al auge de la tecnología. Se trata de la Resolución 509/1968 de la Asamblea denominada “*Los derechos humanos y los nuevos logros científicos y técnicos*”, la Resolución R (73) 22, relativa a “la protección de la vida privada de las personas físicas respecto de los bancos de datos electrónicos en el sector privado”; la Resolución R (73) 23, sobre medidas de armonización en el ámbito de la informática jurídica en los Estados miembros del Consejo de Europa y la Recomendación R (74) 29, relativa a la protección de la vida privada de las personas físicas respecto a los bancos de datos electrónicos en el sector público.

En la primera Resolución 509/1968, si bien no se mencionaba directamente el concepto protección de datos, sí se concretaba la necesidad de adoptar mecanismos de protección frente al uso de las tecnologías para proteger su potencial agresividad a la vida privada y a otros derechos de las personas.

Respecto del segundo grupo de resoluciones aprobadas a principios de los años setenta se concretan, en todas ellas se concretaban, tanto para el sector privado como para el sector público, pautas que se debían tener presente cuando se utilizase la informática para recolectar datos personales, así como las limitaciones en el tratamiento de aquellos.

Aquellas Resoluciones y la Recomendación fueron consideradas como el verdadero origen del movimiento legislativo en materia de protección de datos en Europa. En ellas se recogían principios -aún hoy vigentes-, como la calidad de los datos personales, la exigencia de exactitud y puesta al día o la adecuación de los datos tratados a la finalidad para la que se recogieron. Igualmente se contenían exigencias, también hoy vigentes, como obtener y tratar los datos con una base legitimadora o la adopción de medidas de seguridad adecuadas a los tipos de datos contenidos en los ficheros, entre otros.

Posteriormente, el Consejo de Europa –CdE- aprobó un importante número de Recomendaciones centradas en regular la protección de datos en sectores concretos de gran trascendencia para las personas como el relativo al ámbito médico, al policial, al laboral, estadístico, de telecomunicaciones, entre otros muchos⁷.

⁷ En este sentido cabe mencionar las siguientes: Recomendación núm. R(81) 1, de 23 de enero, que trata el tratamiento automatizado de los bancos de datos médicos; la Recomendación núm. R(83) 10, de 23 de septiembre, relativa a la protección de datos personales utilizados con fines de investigación y estadísticos; la Recomendación núm. R(86) 1, de 23 de enero, sobre la protección de datos personales relacionados con la Seguridad Social; la Recomendación R(87) 15, de 17 de septiembre, sobre utilización de datos personales por la policía; la Recomendación R(89) 2, de 18 de enero, relativa a la protección de datos personales utilizados con fines laborales; número la Recomendación R(91) 10, de 9 de septiembre, relativa a la cesión de datos pertenecientes al sector público; la Recomendación R(95) 4, de 7 de febrero, relativa a la protección de datos personales en el sector de telecomunicaciones; la Recomendación núm. R(97) 5, de 13 de febrero, relativa a la protección de datos sanitarios; la Recomendación R(97) 18, de 30 de septiembre, relativa a la protección de datos personales con fines estadísticos, entre muchas otras.

3.- El Convenio 108 del Consejo de Europa, de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal

En el año 1981 el Consejo de Europa aprueba un documento de gran trascendencia en materia de protección de datos. Se trata del Convenio 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal; único instrumento internacional jurídicamente vinculante para los Estados que lo han ratificado. El Convenio 108 tuvo como propósito establecer unidad entre las legislaciones de los países adheridos, así como extender la garantía de la protección de datos a todos los ciudadanos. No obstante, cabe señalar que no resulta posible solicitar amparo ante el Tribunal Europeo de Derechos Humanos (en adelante, TEDH) por vulneración de algún precepto del Convenio, pero el propio TEDH lo considera una parte importante del derecho al respeto a la vida privada y familiar recogido en el artículo 8 del CEDH, precepto que concreta:

- 1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.*
- 2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás.*

Es preciso señalar que el Convenio 108 del Consejo de Europa también tiene un papel destacado a nivel internacional ya que al estar abierto a que se adhieran Partes no Contratantes del Consejo de Europa, sirve como base para

promover la protección de datos a escala mundial. Recordemos que el Convenio tiene por finalidad proteger la libre circulación de los datos personales para favorecer el comercio y el libre mercado y para ello, cada Estado parte y los Estados que se adhieran deben adaptar su legislación interna al contenido del Convenio con el fin de cumplir con los objetivos del mismo⁸.

Con carácter general el Convenio 108 debe ser respetado tanto por el sector público como el sector privado. Igual obligación corresponde a las autoridades judiciales y a las Fuerzas y Cuerpos de Seguridad. En cuanto a su contenido el mismo señala principios que se deben respetar en todo tratamiento de datos personales -calidad, lealtad, licitud, conservación, entre otros-; reconoce la existencia de datos sensibles y les otorga una protección especial; reconoce derechos a los titulares de los datos que pueden ser ejercitados ante quien recoge o trata los datos como el derecho de acceso, de rectificación, de supresión y de oposición, entre otros. Sin embargo, es preciso desatacar que el mismo no contiene ninguna referencia a la adopción de medidas de seguridad.

El Convenio 108 del Consejo del año 1981 fue objeto de diversas modificaciones, de las que cabe destacar la del año 1999, en el que la Unión Europea pasa a ser parte del mismo, la del año 2001, por el que se adopta un Protocolo adicional con la finalidad de introducir la regulación sobre los flujos transfronterizos a los Estados no Partes, así como la obligación de crear autoridades de control específicas en materia de protección de datos. Finalmente, en el año 2011, se inicia un proceso de actualización de su contenido para adaptarlo al desarrollo de las tecnologías de la información y la comunicación que culmina en el año 2018 con la aprobación de un Protocolo Adicional que da lugar al denominado Convenio 108 + (plus), el 10 de octubre del citado año. En este último instrumento se reforzó la protección de los datos personales ante la diversificación e incremento de las actividades de

⁸ Actualmente forman parte del mismo 51 países partes del Convenio 108, la Unión Europea y otros países no miembros del CdE como Uruguay, Túnez, Senegal, etc.

procesamiento de datos y de circulación de la información. También se incorporó los objetivos adoptados en la reforma normativa llevada a cabo en la Unión Europea en materia de protección de datos que culmina en 2016 con la aprobación del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos⁹). Es así que, se puede afirmar, que actualmente existe coherencia y compatibilidad entre la regulación del CdE y de la Unión Europea.

En líneas generales el Convenio 108+ (plus), vino a reforzar las exigencias en las medidas de seguridad que se deben adoptar; a concretar las responsabilidades de las entidades que trabajan con datos personales; a exigir rendición de cuentas de los sujetos que manipulan datos; eso sí, siempre con la idea de la proyección universal que este instrumento tiene. El Convenio 108+ continúa con su cometido inicial, es decir, de proteger a las personas en todo tratamiento de datos; de facilitar el flujo transfronterizo y de reforzar al mismo tiempo la efectiva aplicación del Convenio.

4.- Regulaciones adoptadas a nivel internacional

Las instituciones internacionales también se han preocupado por la circulación de los datos personales. La irrupción de la tecnología y la incidencia que aquella tiene sobre la vida privada de las personas se valora con preocupación, en particular, en la económica. Es así que, en los años ochenta, la Organización para la Cooperación y el Desarrollo Económico, en adelante OCDE, aprobó, primero en 1980, las Directrices sobre protección de la privacidad y flujos transfronterizos de datos personales (Directrices sobre

⁹ DO L 119 de 4.5.2016, p. 1

privacidad; en 1985, la Declaración sobre flujos de datos transfronterizos y, en 1998, la Declaración ministerial sobre la protección de la privacidad de las redes globales¹⁰. Recientemente y como consecuencia de los importantes desarrollos tecnológicos que plantean nuevos retos y oportunidades, se aprobaron las denominadas Directrices del siglo XXI. Con ellas se quiere fortalecer y proteger la privacidad global y se articulan distintos mecanismos de cooperación con otras organizaciones internacionales para adoptar políticas coherentes que permitan garantizar el respeto de la vida privada de las personas y la protección de datos en línea. Finalmente, señalar que en el año 2020 la OCDE, ante la situación de pandemia, aprobó las Directrices de seguimiento COVID: protección de la privacidad y de los datos durante el uso de aplicaciones y datos biométricos.

Por su parte, Naciones Unidas también ha mostrado su preocupación por el uso de la informática y los perjuicios que su uso ocasiona en los distintos ámbitos de la vida de las personas y adoptó diversos documentos relevantes. Entre ellos, merece mencionar los denominados “Principios rectores sobre la reglamentación de los ficheros computarizados de datos personales”, adoptados por Resolución A/Res/45/1995, de 14 de diciembre 1990, de la Asamblea General; las Declaraciones de gran impacto a nivel mundial como la Declaración Universal sobre el Genoma Humano y los Derechos Humanos, adoptada por unanimidad por la Asamblea General el 11 de noviembre de 1997; la Declaración Internacional sobre los Datos Genéticos Humanos de 16 de octubre de 2003 o la Declaración Universal sobre Bioética y Derechos Humanos, de 19 de octubre de 2005. Todas ellas han marcado un antes y un después en el mundo jurídico y, desde luego, en materia de protección de datos.

La Organización de Estados Americanos OEA, también aborda estos temas y es preciso destacar, entre muchos otros documentos, los Principios de la OEA sobre la privacidad y la protección de los datos personales adoptados en 2014,

¹⁰ Un pequeño resumen de estos documentos puede consultarse <https://www.oecd.org/sti/ieconomy/15590267.pdf>

cuyo objetivo es concretar unas bases que sirvan a los diferentes Estados para adoptar leyes que protejan la privacidad de las personas.

Más recientemente, organizaciones mundiales como la Organización Mundial de la Salud –OMS–, la Organización de Naciones Unidas –ONU–, la Organización Internacional de Migraciones –OIM–, la UNESCO y otras, adoptaron, ante la situación de pandemia vivida, una Declaración Conjunta sobre protección de datos y privacidad en respuesta a la COVID-19, en la que se solicita respeto al derecho a la privacidad y otros derechos humanos y se recuerda cómo se deben utilizar los datos personales para tratar el COVID-19, así como las medidas preventivas que se deben adoptar y evitar para no afectar negativamente los derechos reconocidos a las personas. En este contexto la OMS también publicó unas consideraciones éticas en una Guía para utilizar las tecnologías digitales de rastreo de proximidad para la localización de contactos en la COVID-19¹¹ que también apuntan a proteger los derechos de las personas.

En definitiva, la preocupación por la recogida y uso de los datos personales, así como los destinos de los mismos, está presente en todas aquellas instituciones internacionales con el fin de proteger a las personas frente a cualquier vulneración de los derechos humanos reconocidos, pero sin olvidar la importancia que tiene la libre circulación de los datos, necesario en un mundo globalizado.

¹¹ <https://www.who.int/publications/i/item/WHO-2019-nCoV-Ethics-Contact-tracing-apps-2020.1>