CAPÍTULO 1.
NUEVO ESCENARIO NORMATIVO

1.1. PRIVACIDAD Y PROTECCIÓN DE DATOS EN EL PANORAMA INTERNACIONAL

Han pasado más de ciento veinte años desde que Ilmo. Juez Sr. COOLEY postulaba lo que podría traducirse como el *"derecho a no ser molestado" o "derecho a dejarte en paz"*[1] y el artículo que expresaba una nueva concepción de derechos *"The Right to Privacy"*[2], viéndose ambos trasladados con toda su fuerza, a fecha presente, con el denominado "derecho al olvido" o derecho de supresión al tratamiento de datos personales[3] y, especialmente, respecto a la privacidad de los individuos.

Han tenido que pasar aproximadamente un siglo y medio para que el derecho a la protección de datos de carácter personal haya sido reconocido formalmente como derecho fundamental del individuo, separado o disgregado de otros derechos fundamentales —intimidad—, gracias entre otras, a la importante Sentencia del Tribunal Constitucional 292/2000, la cual estableció, entre otros considerandos, el grado de afectación de dicho derecho, siendo el ámbito de aplicación del derecho a la protección de datos de carácter personal más amplio que el derecho a la intimidad. Este avance supuso eliminar la acotación del derecho a la protección de datos de carácter personal como derecho a la autodeterminación informativa y, por ende, otorgar al individuo la garantía de ostentar el *"poder de control"* respecto a la disposición de los mismos y, especialmente, en cuanto a su uso ilícito[4].

A través del presente capítulo efectuaremos un recorrido por los más importantes hitos que han contribuido al reconocimiento del derecho de

---

1. «The right to be let alone», recogido en la obra A treatise on the Law or the wrongs which arise independent of contract. 2ª Edición. Callaghan. Páginas 899. Chicago, 1988."
2. "The Right to Privacy". Mr. Warren and Mr. Brandeis. Harvard Law Review. Vol. IV. 15 de Diciembre, 1890 No. 5.
3. Sentencia del Tribunal de Justicia de la Unión Europea de fecha 13 de mayo del 2014. Asunto C-131/12 proveniente de cuestión prejudicial planteada por la Audiencia Nacional. Partes: Google INC y Google Spain, SL frente a Agencia de Protección de Datos Personales y Sr. Costeja González.
4. Sentencia del Tribunal Constitucional 292/2000 de 30 de noviembre. *"[…] En cambio, el derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado […]".*

los datos de carácter personal como derecho fundamental del individuo —Declaración de Derechos Humanos, Tratados y Acuerdos Internacionales; Ámbito europeo y nacional—.

La Declaración Universal de Derechos Humanos —DUDH—, adoptada y proclamada, en 183ª Asamblea General de las Naciones Unidas, recogía el derecho a no recibir injerencias, tanto en su vida privada como familiar y, respecto al derecho de libertad de información y expresión, a no ser molestado por las opiniones vertidas, a través de su artículo 12 *"Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques"*. Por su parte, España ratificó el Tratado Internacional de Derechos Civiles y Políticos —TIDCP— en el cual se incluían menciones a derechos similares a los establecidos en la DUDH. Igualmente, España ratificó en el año 1979 el Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales —CPDHLF—, efectuado en Roma el 4 de noviembre de 1950, en el cual se reconocían los derechos individuales insertos: respecto a la vida privada y la intimidad así como la libertad de expresión e información. El reconocimiento internacional del derecho fundamental de intimidad como garante de la personalidad de toda persona ha visto trasladada su eficacia y ampliada su ámbito de aplicación al tratamiento de la información y de los datos de carácter personal. Así, por ejemplo la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura —UNESCO—, integrada por 194 países, siendo una organización especializada de las Naciones Unidas, en la que los distintos miembros establecen estándares o reglas comunes en distintos ámbitos, siendo estos trasladados como instrumentos normativos —Declaraciones y Recomendaciones—. Entre estos instrumentos destacan la Declaración Universal sobre el Genoma Humano y los Derechos Humanos; Declaración Universal sobre Bioética y Derechos Humanos; Declaración Internacional sobre los Datos Genéticos Humanos y otras adicionales que se encuadran dentro de los medios de comunicación social; uso de las nueva tecnologías; ciberespacio.

Hay que tener en cuenta que la Declaración Universal de Derechos Humanos no es un tratado, por lo tanto, no ha sido ratificada. Sin embargo, ha inspirado muchos otros tratados internacionales de derechos humanos legalmente vinculantes. Hoy en día, todos los Estados miembros de la Organización de las Naciones Unidas han ratificado al menos uno de los tratados internacionales sobre derechos humanos y, de hecho, el 80% de ellos ha ratificado cuatro o más.

También se hace necesario destacar dentro de la ONU y dentro de la Organización para la Cooperación y Desarrollo Económicos —OCDE—, las Directrices respecto a la Protección de Datos que, a pesar que las mismas no son vinculantes jurídicamente, sí, por el contrario, establecen recomendaciones que se deberían tener en cuenta por los países en los ámbitos a los que se dirigen dichas directrices: Directrices de Protección de Datos de la ONU y Directrices de protección de datos y circulación transfronteriza de datos personales de la OCDE. Así mismo, existen organizaciones internacionales de colaboración con la finalidad de abordar, estudiar e investigar lo relativo a la afectación del tratamiento de datos de carácter personal.

Con respecto a las Directrices de la ONU en materia de protección de datos personales adoptadas mediante resolución 45/95 de la Asamblea General, de 14 de diciembre de 1990, resaltaríamos que la práctica de las mismas se dejan a la iniciativa de cada Estado, ofreciendo entre otras orientaciones aquellas relacionadas con el principio de legalidad y lealtad, principio de exactitud, principio de especificación de la finalidad y principio de no discriminación.

Con respecto a la aplicación de normativas de protección de datos personales en el mundo, hay que tener en cuenta que los países cuentan con normas específicas, así como la mayoría de ellos cuentan con sus propias autoridades de control, debiendo destacar el gran nivel de implicación en materia de protección de datos de los países europeos, debiendo destacar igualmente un alto nivel de desarrollo en materia de

privacidad tanto en América del Norte, Canadá, Iberoamérica, Pacífico y algunas regiones de África.

En América del Norte y, especialmente Estados Unidos se puede destacar el gran manejo de datos de carácter personal frete a una legislación federal, normativas sectoriales que regulan diferentes ámbitos como la Ley de Protección de la Privacidad de Menores de los Estados Unidos (COPPA), la Ley de Transferencia y Responsabilidad del Seguro Médico en EE.UU. (HIPAA) o la Ley de Cumplimiento Fiscal de Cuentas en el Extranjero (FATCA):

- COPPA: no se permite la recogida de datos ni ubicación física del menor son previo consentimiento de los padres y/o tutores.
- HIPAA: estipula que, salvo excepciones, la información está al alcance de los médicos, no pudiendo llevarse a cabo comunicaciones de los mismos sin el previo consentimiento del paciente.
- FATCA: prohíbe que en los recibos de tarjetas de crédito se vean los últimos dígitos del número, limitando la visualización a los primeros cinco dígitos.

Hay que tener en cuenta, como anécdota que, los Estados Unidos de América no cuentan con ninguna autoridad de control en materia de protección de datos por lo que los conflictos acerca de la privacidad y datos personales han de resolverse directamente ante los juzgados, no existiendo un baremo en la imposición de multas por gravedad de las acciones.

Hay que destacar que en 1999 se iniciaron negociaciones entre Europa y los Estados Unidos de América en orden a conseguir una declaración de adecuación del nivel de protección de datos personales, que culminó en el conocido Puerto Seguro, por el cual aquellas empresas que estuvieran adheridas a dicho a protocolo garantizaban una *"presunción de adecuación"* al nivel de protección exigido por la Directiva 95/46, permitiéndose así la libre transferencia internacional de datos a

dichos operadores. En el 2016 El Tribunal de Justicia de la Unión Europea (TJUE) declaró inválida la Decisión de la Comisión 2000/520/CE que establecía el nivel adecuado de protección de las garantías para las transferencias internacionales de datos a EE.UU. ofrecidas por el acuerdo de Puerto Seguro, por lo que en julio de ese mismo año la Comisión publicó la Decisión 2016/1250 sobre la adecuación de la protección conferida por un nuevo esquema denominado *"Escudo de Privacidad UE-EE.UU."* para la circulación de datos entre Europa y Estados Unidos de América se dispusieron tres métodos, cláusulas contractuales, normas corporativas vinculantes y el Escudo de Privacidad. Este Escudo de Privacidad funciona más o menos como el Puerto Seguro, las empresas deben adherirse primero, teniendo sus obligaciones y siendo el Departamento de Comercio de los EE.UU. el responsable de gestionar y administrar el Escudo de Privacidad y de garantizar que las empresas respeten sus compromisos. Dicho Escudo de Privacidad *(Privacy Shield)* puede verse afectado por el asunto Facebook y Cambridge Analytics.

Con respecto a Iberoamérica, se puede decir que desde el año 2003 ha ido creciendo la adopción de legislaciones en materia de protección de datos personales, así como la implantación de autoridades de control, gracias a la RIPD (Red Iberoamericana de Protección de Datos), la cual surge con motivo del acuerdo alcanzado en el Encuentro Iberoamericano de Protección de Datos celebrado en La Antigua, Guatemala, del 1 al 6 de junio de 2003, con la asistencia de representantes de 14 países iberoamericanos y destacando la importancia de las iniciativas regulatorias iberoamericanas para proteger la privacidad de los ciudadanos, entendiendo la protección de datos personales como un derecho fundamental, llevando a cabo entre otras funciones la de promover los desarrollos normativos necesarios para garantizar, dentro de un contexto democrático, una regulación en materia de protección de datos personales.

Atendiendo que cada país adopta su propia normativa, unos nombrando autoridad de control otros no, puede resultar quizá más revelador

el dato de aquellos países para los cuales el Grupo de Autoridades del artículo 29 los ha considerado con un nivel adecuado de protección de datos personales, lo cual le permitirá transferir datos desde los Estados miembros de la Unión Europea sin necesidad de ningún tipo de trámite o autorización especial. Los países que hasta la fecha son considerados con un nivel adecuado son los siguientes: Andorra, Argentina, Canadá (Sector privado), Suiza, Islas Feroe, Guernsey, Israel, Isla de Man, Jersey, Nueva Zelanda y Uruguay.

1.2. LA PROTECCIÓN DE DATOS EN EUROPA

Dentro del ámbito europeo se han hecho verdaderos esfuerzos para que el derecho a la protección de datos de carácter personal fuera reconocido como un derecho fundamental —autodeterminación informativa— e independiente del derecho a la intimidad[5]. A lo largo de los años, el derecho a la protección de datos de carácter personal como derecho fundamental y derecho de autodeterminación, por parte del titular de los datos personales, se veía subsumido en la prohibición de injerencia por parte de terceros o, lo que es lo mismo, aglutinado dentro del derecho fundamental a la intimidad. No será hasta la Directiva 95/46/CEE, consecuencia del Convenio Nº 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, cuando formalmente y expresamente se reconozca el derecho a la protección de datos de carácter personal como independiente.

Como curiosidad, cabe destacar que la República Federal de Alemania en 1970 fue el primer país europeo que aprobó una ley nacional sobre protección de datos de carácter personal, denominándose esta *"Datenschutz"* y crea un Comisario de Protección de Datos. Esta ley

5. Primer hito importante del derecho a la protección de datos de carácter personal. Resolución de 8 de mayo sobre tutela de los derechos del individuo frente al creciente progreso técnico en el sector de la informática, aprobada por el Parlamento Europeo en el año 1979.

regulaba el uso de datos de los ciudadanos por las instituciones públicas. Ley conocida como Land de Hesse. En el año 1973 Suecia aprobó la primera ley que regulaba el tratamiento de datos de carácter personal, creándose la primera autoridad en dicha materia: *"Datainspektionen"*. A partir del año 1970 entrarían en vigor otras leyes de protección de datos nacionales de estados europeos.

Antes de continuar con la evolución y principales referencias legislativas dentro del ámbito europeo, es importante conocer las fuentes del derecho comunitario con la finalidad de *"situar"* en todo momento la prevalencia de las mismas y su repercusión a nivel nacional.

El derecho comunitario está integrado, tanto por el derecho originario —Tratados Fundacionales— como por el derecho derivado —las normas europeas adoptadas por las Instituciones para el ejercicio de las competencias que les confieren los Tratados—. Dentro de las normas europeas destacan:

- **Reglamentos**: Actos aplicables directamente en todos los Estados miembros y de manera uniforme.
- **Directivas**: Actos que fijan los objetivos a alcanzar, pero que dejan a los Estados miembros la elección de los medios para alcanzarlos.
- **Decisiones**: Actos que obliga únicamente al destinatario.
- **Recomendaciones y los Dictámenes**, los cuales no son vinculantes.
- **Jurisprudencia del Tribunal de Justicia de las Comunidades Europeas**: Acuerdos Internacionales de la Unión; Convenios entre los Estados miembros; Resoluciones, Declaraciones, Conclusiones y Comunicaciones interpretativas de la Comisión.

1.3. EL RGPD Y SU ADAPTACIÓN POR LOS DIFERENTES PAÍSES EUROPEOS

Hay que destacar que el RGPD tiene un alcance paneuropeo, si bien tal y como se indica a lo largo de su cuerpo normativo, sus normas podrán ser bien especificadas bien restringidas a través de cuerpos normativos nacionales, pero en ningún caso, podrán ser contradictorias con el RGPD. Por tanto, el RGPD resalta a lo largo de sus diferentes considerandos así como de su cuerpo normativo la importancia de la uniformidad aplicativa alejándose de la fragmentación derivada de la Directiva 95/46/CE, de ahí la importancia que fuere un reglamento el instrumento normativo a través del cual se regulara la protección de datos personales a nivel europeo.

Centrándonos en el enfoque del presente apartado, hay que destacar el Considerando 8 del RGPD donde se puede decir que se da el *"pistoletazo de salida"* y la posibilidad que los distintos Estados miembros puedan aprobar sus propios cuerpos normativos para limitar o bien dar algo de luz al reglamento, tan esperado y a la vez opaco en algunos términos.

"Considerando 8. En los casos en los que el presente Reglamento establece que sus normas sean especificadas o restringidas por el Derecho de los Estados miembros, estos, en la medida en que sea necesario por razones de coherencia y para que las disposiciones nacionales sean comprensibles para sus destinatarios, pueden incorporar a su Derecho nacional elementos del presente Reglamento".

Por lo tanto, estará prohibido para los Estados miembros la repetición del texto del RGPD en su propia normativa nacional, al no ser que dichas repeticiones sean estrictamente necesarias en aras a la coherencia o en orden a poder hacer que las legislaciones nacionales sean comprensibles para aquellos a los que se aplican. Dejándose la interpretación del RGPD en manos de los tribunales europeos y no del legislador de cada uno de los Estados miembros.

Además de los países integrantes de la Unión Europea, la Comisión Europea proseguirá su trabajo para la integración del RGPD en los países integrantes de la EFTA (Islandia, Liechtenstein y Noruega), tan pronto entre en vigor la aplicación del RGPD en el Acuerdo del Espacio Económico Europeo, pudiendo los datos circular libremente entre los países de la UE y del Estado Económico Europeo de la misma manera que lo hacen entre los Estados miembros de la Unión Europea.

Dentro de las previsiones que la Comisión Europea ha tenido en cuenta, se encuentra también la posible retirada del Reino Unido de la Unión Europea, que se tiene previsto que se lleve a cabo el 31 de marzo de 2019, por lo que en el momento que entre en aplicación el RGPD le será todavía aplicable en su totalidad al Reino Unido, aunque aparentemente solo por un periodo de 10 meses, por lo que el Reino Unido ya ha trabajado en un texto normativo *"The Data Protection Bill"* que es muy parecido al RGPD, de tal forma que una vez que el Reino Unido se retire de la Unión Europea, en caso que finalmente lo haga, no existan demasiadas diferencias debiendo tener en cuenta que sí le serán de aplicación una vez esté fuera de la UE, las transferencias internacionales para con sus relaciones con la Unión Europea.

Hay que destacar que muy probablemente la Comisión Europea acabe considerando al Reino Unido como un país con un nivel adecuado de protección, como ya hiciera anteriormente con Suiza, Canadá, Argentina, Guernsey, Isla Man, Jersey, Islas Feroe, Andorra, Israel, Uruguay, Nueva Zelanda y Estados Unidos *(Privacy Shield)*, si bien durante el transcurso de su aprobación, como ya he comentado anteriormente, se considerarán transferencias internacionales de datos.

1.4. LA PROTECCIÓN DE DATOS EN ESPAÑA

El derecho interno no ha sido ajeno a los cambios que se producían desde los años 70 hasta hoy, habiendo recorrido un camino paralelo en

cuanto al reconocimiento del derecho a la protección de datos de carácter personal como derecho sustantivo, como derecho de autodeterminación informativa. Dicho derecho ha virado como "derecho complementario" al derecho a la intimidad como consecuencia de la injerencia de la informática en la vida privada a un derecho sustantivo, en el que el titular de los datos personales dispone del "poder" de la información que proporciona y que terceros tratan.

De hecho, España, al igual que Portugal[6], en el periodo de la segunda generación de normas, promulga sendas Constituciones en las que se hacen *"eco"* de la utilización de la informática y su injerencia en la intimidad del individuo. La Constitución Española —CE— lo incluye en el artículo 18, dentro del Capítulo II Derechos y Libertades, dándole una relevancia como derecho fundamental al derecho a la intimidad, el cual será garantizado y añade en el apartado 4 del citado artículo, que la ley será el instrumento para garantizar dicho derecho fundamental que pudiere verse mermado por uso de la informática.

Artículo 18.1 CE. 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.

Por su parte, el derecho a la intimidad, primero, al igual que el derecho a la protección de datos personales cuando sea reconocido como derecho sustantivo se ve excepcionado cuando convergen con ellos otros derechos fundamentales: libertad de información, la seguridad del estado, la averiguación de delitos.

---

6. Constitución Portuguesa del año 1976, en cuyo artículo 35 consagra la libertad informática y las garantías del individuo frente a la misma.