
UCAM
UNIVERSIDAD CATÓLICA
DE MURCIA

ESCUELA INTERNACIONAL DE DOCTORADO
Programa de Doctorado en Ciencias Sociales

# El derecho de acceso a la Información Nacional y supranacional. Los casos de España y Panamá y el difícil equilibrio entre la Open Data y la salvaguarda de la seguridad

Autor:
D. Juan Manuel Antonio Solaeche y Bielsa

Director:
Dr. D. Cesar Augusto Giner Alegría

Murcia, junio de 2019


UCAM
UNIVERSIDAD CATÓLICA
DE MURCIA

ESCUELA INTERNACIONAL DE DOCTORADO
Programa de Doctorado en Ciencias Sociales

# El derecho de acceso a la Información Nacional y supranacional. Los casos de España y Panamá y el difícil equilibrio entre la Open Data y la salvaguarda de la seguridad

Autor:
D. Juan Manuel Antonio Solaeche y Bielsa

Director:
Dr. D. Cesar Augusto Giner Alegría

Murcia, junio de 2019

UCAM
UNIVERSIDAD CATÓLICA
DE MURCIA

# AUTORIZACIÓN DEL DIRECTOR DE LA TESIS PARA SU PRESENTACIÓN

El Dr. D. César Augusto Giner Alegría como Director de la Tesis Doctoral titulada "El derecho de acceso a la Información Nacional y supranacional. Los casos de España y Panamá y el difícil equilibrio entre la Open Data y la salvaguarda de la seguridad" realizada por D. Juan Manuel Antonio Solaeche y Bielsa en el Departamento de Criminología, **autoriza su presentación a trámite** dado que reúne las condiciones necesarias para su defensa.

**LO QUE FIRMO, PARA DAR CUMPLIMIENTO A LOS REALES DECRETOS 99/2011, 1393/2007, 56/2005 Y 778/98, EN MURCIA A 5 DE JUNIO DE 2019**

Dr. D. César Augusto Giner Alegría

UCAM EIDUCAM Escuela Internacional de Doctorado

**Resumen**

Las garantías de acceso a la información de los ciudadanos que implementan los Estados por motivos de seguridad, nos enfrenta a una línea gris donde es difícil dirimir cual derecho prevalece si la seguridad individual o la seguridad colectiva, siendo necesario reflexionar y establecer estándares para la gestión de la información pública relativa al ámbito de la seguridad de los estados y respetar a su vez el *par in parem non habet imperium* que obedece al principio de igualdad soberana, entre estos lo que genera entonces el interés de establecer hasta qué punto el Estado puede y tiene la legitimidad de brindar confidencialidad a los datos sobre determinadas informaciones de sus ciudadanos y residentes que no colisionen con la seguridad nacional y por ende la seguridad internacional. En esta investigación comparada nos hemos enfocado tanto en los nuevos desafíos de la seguridad que obligan a los estados a desplegar limitaciones a las leyes de acceso a la información, para informaciones susceptibles de categorizarse como de interés restringido para la población en general, dado que si bien reconocemos en esta tesis, el derecho de acceso a la información por parte de los ciudadanos, defendemos así mismo la necesidad de establecer un elenco armonizado internacionalmente, de leyes legitimas de reserva al acceso a la información por parte de los ciudadanos, que son comúnmente aceptadas por el derecho internacional, cuando estas estén referidas a la seguridad nacional, pues en el escenario de los nuevos retos de la seguridad nacional e internacional, emergen como una de las informaciones más sensibles y susceptibles de ser salvaguardada por interés general. El acceso a la información, al facilitar el escrutinio público de los actos del Estado, no sólo previene abusos por parte de funcionarios públicos, sino que además permite que la población intervenga en la definición de las políticas del Estado y, por ende, constituye un elemento clave para la preservación efectiva de la seguridad nacional, la participación democrática y la formulación de políticas sólidas. Para proteger el pleno ejercicio de los derechos humanos, en ciertas circunstancias, podría ser necesario mantener información en secreto para salvaguardar intereses legítimos de la seguridad nacional. Encontrar un punto de equilibrio adecuado se torna aún

más difícil debido a que, en muchos países, los tribunales actúan con la menor independencia y la mayor deferencia frente a los reclamos del gobierno cuando este apela a argumentos de seguridad nacional. Esta deferencia se ve reforzada por disposiciones de las leyes sobre seguridad de numerosos países que prevén excepciones al derecho a la información y a las normas procesales comunes sobre prueba y derechos de los acusados ante la mínima demostración, o mera afirmación, por parte del gobierno de que existe un riesgo para la seguridad nacional. Cuando un gobierno apela excesivamente a argumentos de seguridad nacional, se pueden quebrantar las principales garantías institucionales contra el abuso gubernamental: la independencia de los tribunales, el estado de derecho, el control legislativo, la libertad de los medios de comunicación y el gobierno abierto. Al margen de los conceptos de Gobierno Abierto y Buen Gobierno, el principio de transparencia conlleva el reconocimiento de un derecho muy concreto: el acceso a la información y a los documentos que obren en poder de la Administración Pública. El objeto del presente estudio será, precisamente, el análisis de este derecho. Uno de los temas más controvertidos del debate parlamentario y extraparlamentario alrededor de la Ley de Transparencia vino dado por la determinación de la propia naturaleza del derecho de acceso a la información pública que se pretendía configurar en la ley. La cuestión giraba en torno a si debía considerarse como derecho fundamental, o simplemente como un derecho público subjetivo de creación legal no recurrible en amparo. Avancemos ya que la opción del legislador, así como la del Gobierno desde el inicio en el Anteproyecto, fue la de descartar de raíz que el derecho de acceso pudiera catalogarse como fundamental, evitando también con ello, al tiempo, la tramitación de la ley como orgánica. En este sentido la Ley de Transparencia regula los límites en los artículos 15 (protección de datos personales), 17 (causas de inadmisión), 19.4 (tramitación de las solicitudes) y, sobre todo, en el 14, que lleva precisamente por título "límites al derecho de acceso." Éste es el que se encarga de recoger todo el listado cerrado de excepciones con el objeto de proteger otros bienes y valores susceptibles de protección. Su regulación está directamente inspirada en el CEADP, imitando todas las características ya apuntadas. Se trata de límites relativos, no absolutos ("el derecho de acceso podrá ser limitado cuando acceder a la información suponga un perjuicio para…"), por lo que ningún campo queda vedado por completo y ad limine al conocimiento de la ciudadanía. Los intereses que constituyen tales límites

relativos son los siguientes: “la seguridad nacional; la defensa; las relaciones exteriores; la seguridad pública; la prevención, investigación y sanción de los ilícitos penales, administrativos o disciplinarios; la igualdad de las partes en los procesos judiciales y la tutela judicial efectiva; las funciones administrativas de vigilancia, inspección y control; los intereses económicos y comerciales; la política económica y monetaria; el secreto profesional y la propiedad intelectual e industrial; la garantía de la confidencialidad o el secreto requerido en procesos de toma de decisión; la protección del medio ambiente.” Volviendo al ámbito supranacional en este caso a otro de los interesas que vehiculan esta tesis, nos fijaremos en el ámbito centroamericano en concreto al caso de Panamá, en donde la acción de Habeas Data se establece mediante Ley No. 6 de 22 de enero de 2002, por medio de la cual se dictan normas para la transparencia en la gestión pública, se establece la acción de Habeas Data.

**Palabras clave:** habeas Data, Open Data; Ley de secretos oficiales, Panamá, Ley de Trasparencia

**Abstract**

The guarantees of access to citizen information implemented by States for security reasons, we face a gray line where it is difficult to determine which right prevails if individual security or collective security, it is necessary to reflect and establish standards for management of public information related to the scope of the security of the states and respect in turn the pair in parem non habet imperium that obeys the principle of sovereign equality, among these what then generates the interest of establishing to what extent the State can and It has the legitimacy to provide confidentiality to data on certain information from its citizens and residents that do not collide with national security and therefore international security. In this comparative research we have focused so much on the new security challenges that force states to deploy limitations to the laws of access to information, for information that can be categorized as of restricted interest for the general population, given that if we recognize in this thesis, the right of access to information by citizens, we also defend the need to establish an internationally harmonized list of legitimate laws of reservation to access to information by citizens, which are commonly accepted by international law, when these are related to national security, because in the scenario of the new challenges of national and international security, emerge as one of the most sensitive information and susceptible to be safeguarded by the general interest. Access to information, by facilitating public scrutiny of the acts of the State, not only prevents abuses by public officials, but also allows the population to intervene in the definition of State policies and, therefore, constitutes a key element for the effective preservation of national security, democratic participation and the formulation of sound policies. To protect the full exercise of human rights, in certain circumstances, it may be necessary to keep information secret in order to safeguard legitimate interests of national security. Finding an adequate balance point becomes even more difficult because, in many countries, the courts act with the least independence and the greatest deference to the claims of the government when it appeals to national security arguments. This deference is reinforced by provisions of the security laws

of many countries that provide for exceptions to the right to information and common procedural rules on evidence and rights of the accused at the slightest demonstration, or mere affirmation, by the government that there is a risk to national security. When a government appeals excessively to national security arguments, the main institutional guarantees against government abuse can be broken: the independence of the courts, the rule of law, legislative control, the freedom of the media and open government. Apart from the concepts of Open Government and Good Governance, the principle of transparency entails the recognition of a very specific right: access to information and to documents held by the Public Administration. The object of the present study will be, precisely, the analysis of this right. One of the most controversial issues in the parliamentary and extraparliamentary debate surrounding the Transparency Law was determined by the nature of the right of access to public information that was intended to be set out in the law. The question revolved around whether it should be considered as a fundamental right, or simply as a subjective public right of non-actionable legal creation in amparo. Let's move forward since the option of the legislator, as well as that of the Government from the beginning in the Draft, was to discard at the outset that the right of access could be classified as fundamental, also avoiding, at the same time, the processing of the law as organic In this sense, the Law of Transparency regulates the limits in articles 15 (protection of personal data), 17 (causes of inadmissibility), 19.4 (processing of applications) and, especially, in 14, which takes precisely by title " limits to the right of access. "This is the one in charge of collecting all the closed list of exceptions in order to protect other goods and values susceptible to protection. Its regulation is directly inspired by the CEADP, imitating all the characteristics already mentioned. These are relative, not absolute limits ("the right of access may be limited when accessing information supposes harm to ..."), so that no field is completely and ad limine restricted to the knowledge of citizens. The interests that constitute such relative limits are the following: "national security; the defense; external relations; public safety; the prevention, investigation and punishment of criminal, administrative or disciplinary offenses; the equality of the parties in judicial proceedings and effective judicial protection; the administrative functions of surveillance, inspection and control; economic and commercial interests; economic and monetary policy; professional secrecy and intellectual and industrial property; the guarantee of confidentiality or the secrecy

required in decision-making processes; the protection of the environment. "Returning to the supranational field in this case to another of the interests that convey this thesis, we will look at the Central American area in particular to the case of Panama, where the action of Habeas Data is established by Law No. 6 of January 22, 2002, through which rules are issued for transparency in public management, the action of Habeas Data is established.

**Keywords:** habeas Data, Open Data; Law of official secrets, Panama, Law of Transparency

# ÍNDICE

## AGRADECIMIENTOS

A mi director de tesis, el doctor C.A. Giner por haberme iluminado en esta investigación, tan indudablemente compleja, mostrándome un apoyo fraternal incondicional. Mi deuda será inolvidable por el conocimiento, el cariño y la amistad compartida a lo largo de este camino que iniciamos juntos. Me ha hecho apreciar la palabra *Maestro* en toda su amplitud académica e histórica, como guía, camino, tradición y discípulo.

También a mi mujer, Lali y mis hijos Juan y Eduardo y mi familia, por los momentos que les robé durante el estudio y análisis de toda esta materia y no pude disfrutar de ellos tanto como hubiera querido. Por su paciencia y apoyo, y en especial a mi hermano Ángel Ramón a quien perdí por esa alimaña de enfermedad que se le llevó antes que pudiéramos celebrar juntos esta obra.

No podría olvidar a mis amigos y compañeros que desde la Sociedad de Estudios Internacionales de España y Panamá me han aportado material histórico inigualable para contrastar los diversos aspectos recogidos en esta obra. Los fraternos doctor E. Lau, S. Mejía y M. Cohen-Henriquez, embajador de Panamá en España. Así como a Monseñor C. Martin Muñoz cuya pérdida irreparable nos dejó una profunda herida académica y de amistad; a los doctores E. Mercader y J.J. Delgado por sus sabios consejos y experiencia que complementaron el camino de mi *Maestro* el doctor C.A. Giner.

Por último y como debo ir finiquitando este apartado de agradecimientos a todos mis compañeros y amigos que de una manera u otra me aportaron el apoyo y calor en los momentos difíciles para poder compaginar mi actividad académica en la Sociedad de Estudios Internacionales cuya presidencia de honor ostenta S.M. El Rey Don Juan Carlos I y el día a día en los viajes a uno y otro lado del Atlantico visitando y recopilando material para esta tesis.

Debo ese agradecimiento especial a mi Universidad Católica de Murcia por acogerme entre su alumnado y sentir ese calor apoyo y seguimiento para lograr ese tan celebrado éxito en mi tesis. ¡Gracias!.

# I.-
# INTRODUCCIÓN

# I.-INTRODUCCION

Las distintas restricciones sobre las garantías de acceso a la información de los ciudadanos que implementan los Estados por motivos de seguridad, nos enfrenta a una línea gris donde es difícil dirimir cual derecho prevalece si la seguridad individual o la seguridad colectiva, siendo necesario reflexionar y establecer estándares para la gestión de la información pública relativa al ámbito de la seguridad de los estados y respetar a su vez el *par in parem non habet imperium* que obedece al principio de igualdad soberana, entre estos. También es obvio y somos conscientes de que el terrorismo, la delincuencia organizada y la corrupción entre otras acciones no legítimas, han utilizado las protecciones que la ley otorga para poder ocultar los beneficios de sus acciones, o el financiamiento de sus atentados. Lo que genera entonces el interés de establecer hasta qué punto el Estado puede y tiene la legitimidad de brindar confidencialidad a los datos sobre determinadas informaciones de sus ciudadanos y residentes que no colisionen con la seguridad nacional y por ende la seguridad internacional. En esta investigación comparada nos hemos enfocado tanto en los nuevos desafíos de la seguridad que obligan a los estados a desplegar limitaciones a las leyes de acceso a la información, para informaciones susceptibles de categorizarse como de interés restringido para la población en general, dado que si bien reconocemos en esta tesis, el derecho de acceso a la información por parte de los ciudadanos, defendemos así mismo la necesidad de establecer un elenco armonizado internacionalmente, de leyes legitimas de reserva al acceso a la información por parte de los ciudadanos, que son comúnmente aceptadas por el derecho internacional, cuando estas estén referidas a la seguridad nacional, pues en el escenario de los nuevos retos de la seguridad nacional e internacional, emergen como una de las informaciones más sensibles y susceptibles de ser salvaguardada por interés general.

La seguridad nacional y el derecho a saber de la sociedad a menudo se consideran objetivos contrapuestos. Si bien a veces puede haber cierto grado de tensión entre el interés de un gobierno por preservar el carácter reservado de cierta información por razones de seguridad nacional y el derecho de la población a acceder a información en poder de autoridades públicas, un examen exhaustivo del pasado reciente indica que los intereses legítimos de seguridad nacional, en la

práctica, se ven favorecidos cuando la sociedad está bien informada sobre las actividades del Estado, incluidas aquellas llevadas a cabo para resguardar la seguridad nacional.

El acceso a la información, al facilitar el escrutinio público de los actos del Estado, no sólo previene abusos por parte de funcionarios públicos, sino que además permite que la población intervenga en la definición de las políticas del Estado y, por ende, constituye un elemento clave para la preservación efectiva de la seguridad nacional, la participación democrática y la formulación de políticas sólidas. Para proteger el pleno ejercicio de los derechos humanos, en ciertas circunstancias, podría ser necesario mantener información en secreto para salvaguardar intereses legítimos de la seguridad nacional.

Encontrar un punto de equilibrio adecuado se torna aún más difícil debido a que, en muchos países, los tribunales actúan con la menor independencia y la mayor deferencia frente a los reclamos del gobierno cuando este apela a argumentos de seguridad nacional.

Esta deferencia se ve reforzada por disposiciones de las leyes sobre seguridad de numerosos países que prevén excepciones al derecho a la información y a las normas procesales comunes sobre prueba y derechos de los acusados ante la mínima demostración, o mera afirmación, por parte del gobierno de que existe un riesgo para la seguridad nacional.

Cuando un gobierno apela excesivamente a argumentos de seguridad nacional, se pueden quebrantar las principales garantías institucionales contra el abuso gubernamental: la independencia de los tribunales, el estado de derecho, el control legislativo, la libertad de los medios de comunicación y el gobierno abierto.

Al margen de los conceptos de Gobierno Abierto y Buen Gobierno, el principio de transparencia conlleva el reconocimiento de un derecho muy concreto: el acceso a la información y a los documentos que obren en poder de la Administración Pública. El objeto del presente estudio será, precisamente, el análisis de este derecho.

El primer texto jurídico de protección de datos que encontramos en Europa es la “Datenshutz” dictado por el Parlamento de la República Federal Alemana, y promulgada el 7 de octubre de 1970, y que es el antecedente directo de la Ley

Federal de 1977. En Suecia, la normativa de protección de datos personales y de protección a la intimidad, es de 1973.

En los Estados Unidos de Norteamérica, el caso Watergate es el antecedente que lleva a la protección del derecho a la intimidad mediante el "Privacy Act" de 1974.

Ahora bien, vale anotar que la particularidad que tienen todas las legislaciones referidas es, en efecto, el reconocimiento del derecho a la intimidad y la protección de datos personales; no obstante, no establecieron una acción judicial de protección o tutela del derecho que consagraron.

Es la Constitución de Portugal de 2 de abril de 1976, la primera Constitución en establecer, en el contexto de la constitucionalidad, el derecho de los ciudadanos de controlar sus datos personales que se encuentren en registros y documentos públicos, así como la finalidad del uso de esa información, con el recurso procesal de poder exigir la rectificación, como la actualización de los datos.

Luego, la Constitución española en 1978, recoge esa previsión constituyente y se establece como un procedimiento constitucional; y son las constitucionales de Portugal de 1976 y de España de 1978 las constituciones que influyen, directamente, en el constitucionalismo latinoamericano, al punto que la Constitución de Portugal incide, directamente, en el constituyente brasileño de 1988, que introduce en el constitucionalismo latinoamericano la institución del "Habes Data".

En 1981, las representaciones acreditadas de Alemania, España, Francia, Noruega y Suecia, celebraron el Convenio No. 108, "para la protección de las personas con respecto al tratamiento de datos automatizados de carácter personal", mediante el cual se procura el respeto a la intimidad y a la vida privada de los ciudadanos a través de la protección de los de sus datos personales, y se crea a favor del ciudadano afectado la posibilidad de presentar un recurso como garantía de protección de esos derechos detallados en el Convenio.

En la República Federativa de Alemania, la jurisprudencia del Tribunal Constitucional Federal Alemán, desde 1983, al declararse competente para conocer recursos de amparo contra la Ley de Censo de Población, Profesional y

lugares de trabajo, la justicia constitucional alemana reconoció, dentro del derecho a la personalidad general, lo que denominó el "derecho a la autodeterminación de la información".

Es la Constitución brasileña de 1988, la que introduce en América Latina, a modelo de un proceso constitucional, la acción o recurso de "Habeas Data", como mecanismo mediante el cual se instituye un medio de protección del derecho de controlar los datos o informaciones personales en registros o bancos de datos, consagrando la institucionalidad del Estado. En Panamá la acción de Habeas Data se establece mediante Ley No. 6 de 22 de enero de 2002, por medio de la cual se dictan normas para la transparencia en la gestión pública, se establece la acción de Habeas Data y se dictan otras disposiciones.

Llevando este hilo conductor nuevamente a nuestro ámbito, el 27 de julio de 2012, el Consejo de Ministros aprobó el Proyecto de Ley de Transparencia y Acceso a la Información Pública y Buen Gobierno (en adelante, Proyecto de Ley de Transparencia). La aprobación de una norma de estas características, tras varias tentativas vendrá cargada de significado, máxime teniendo en cuenta los incesantes reclamos por parte de la sociedad de mayor transparencia en las instituciones públicas. La dimensión constitucional de la configuración actual del derecho de acceso a la información pública tras la reciente entrada en vigor de la Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la Información Pública y Buen Gobierno.

Uno de los temas más controvertidos del debate parlamentario y extraparlamentario alrededor de la Ley de Transparencia vino dado por la determinación de la propia naturaleza del derecho de acceso a la información pública que se pretendía configurar en la ley. La cuestión giraba en torno a si debía considerarse como derecho fundamental, o simplemente como un derecho público subjetivo de creación legal no recurrible en amparo. Avancemos ya que la opción del legislador, así como la del Gobierno desde el inicio en el Anteproyecto, fue la de descartar de raíz que el derecho de acceso pudiera catalogarse como fundamental, evitando también con ello, al tiempo, la tramitación de la ley como orgánica.

En este sentido la Ley de Transparencia regula los límites en los artículos 15 (protección de datos personales), 17 (causas de inadmisión), 19.4 (tramitación de las solicitudes) y, sobre todo, en el 14, que lleva precisamente por título "límites al

derecho de acceso." Éste es el que se encarga de recoger todo el listado cerrado de excepciones42 con el objeto de proteger otros bienes y valores susceptibles de protección. Su regulación está directamente inspirada en el CEADP, imitando todas las características ya apuntadas. Se trata de límites relativos, no absolutos ("el derecho de acceso podrá ser limitado cuando acceder a la información suponga un perjuicio para…"), por lo que ningún campo queda vedado por completo y ad limine al conocimiento de la ciudadanía. Los intereses que constituyen tales límites relativos son los siguientes:

> "la seguridad nacional; la defensa; las relaciones exteriores; la seguridad pública; la prevención, investigación y sanción de los ilícitos penales, administrativos o disciplinarios; la igualdad de las partes en los procesos judiciales y la tutela judicial efectiva; las funciones administrativas de vigilancia, inspección y control; los intereses económicos y comerciales; la política económica y monetaria; el secreto profesional y la propiedad intelectual e industrial; la garantía de la confidencialidad o el secreto requerido en procesos de toma de decisión; la protección del medio ambiente".

La previsión constitucional del art. 105 b) recoge, in fine, que el derecho queda reconocido "salvo en lo que afecte a la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de las personas." La Constitución es clara al respecto: estos tres grupos de materias no son un límite absoluto, sino relativo, pues de lo contrario no hubiera utilizando la expresión "en lo que afecte." Por tanto, el legislador tenía la puerta vedada (y aún la tiene) a la hora de reconocer por bloques materias sobre las que, de ninguna forma, pudiera ejercerse el derecho de acceso.

Por otra parte, y como interés también en esta tesis a nivel supranacional cabría distinguir entre la normativa aprobada en el seno de organizaciones internacionales tales como Naciones Unidas o el Consejo de Europa y la regulación de la Unión Europea en la materia. En el ámbito de las organizaciones internacionales, el reconocimiento de este derecho es el resultado de la evolución normativa desde la Declaración Universal de los Derechos Humanos (DUDH), con el reconocimiento de la Libertad de Expresión –que incluye el derecho a recibir información y difundirla (artículo 19)– hasta la aprobación de normas

específicas sobre acceso a información en ámbitos concretos como la Convención de las Naciones Unidas sobre el Acceso a la Información, la Participación Pública en la toma de decisiones y el acceso a la Justicia, también conocida como Convención de Aarhus.

En el seno del Consejo de Europa la evolución de los instrumentos normativos que regulan el derecho a la información y el derecho de acceso a la documentación pública es parecida. Así, el Convenio Europeo de Derechos Humanos, establece en su artículo 10 el derecho a la Libertad de Expresión que, al igual que la DUDH, incluye la libertad de recibir y comunicar información; a partir de ahí, se irán delimitando los instrumentos que abogan por el reconocimiento del derecho a acceder a los documentos en poder de las administraciones: la Declaración del Comité de Ministros sobre Libertad de Expresión e Información, la Recomendación n.º R (81) 19, sobre el acceso a la información en poder de las autoridades públicas, la Recomendación nº R (2000)13 sobre política europea en el acceso a archivos y la Recomendación nº R (2000) sobre el acceso a los documentos públicos. Esta batería normativa se completa con el Convenio del Consejo de Europa sobre el Acceso a los Documentos Públicos, de 18 de junio de 2009.

El Convenio prevé una excepción general a estos límites: la concurrencia de un interés público superior que justifique el acceso a los documentos. Es previsible que este tipo de cláusula dé lugar a debates a la hora de determinar el alcance de la excepción, esto es, a la hora de definir qué debemos entender por interés público superior.

Volviendo al ámbito supranacional en este caso a otro de los interesas que vehiculan esta tesis, nos fijaremos en el ámbito centroamericano. Como decíamos en Panamá la acción de Habeas Data se establece mediante Ley No. 6 de 22 de enero de 2002, por medio de la cual se dictan normas para la transparencia en la gestión pública, se establece la acción de Habeas Data y se dictan otras disposiciones.

La Ley 6 de 2002 tiene como antecedentes inmediatos:

• El Proyecto Ley No. 48, por el cual se desarrolla el Derecho a la Libertad de Información derivado de fuentes públicas, se obliga a las instituciones del Estado a facilitar información, se señalan las modalidades de participación

ciudadana en la acción pública y se reforman los artículos segundo y tercero del Decreto Ejecutivo No. 99 de 13 de septiembre de 1999.

• El Proyecto Ley No. 49, por medio del cual se establece la Acción de Habeas Data.

De la fusión de ambos proyectos de ley nace lo que hoy conocemos como la Ley 6 de 22 de enero de 2002, que en su artículo 17, establece:

Artículo 17. Toda persona estará legitimada para promover acción de Hábeas Data, con miras a garantizar el derecho de acceso a la información previsto en esta Ley, cuando el funcionario público titular o responsable del registro, archivo o banco de datos en el que se encuentra la información o dato personal reclamado, no le haya suministrado lo solicitado o si suministrado lo requerido se haya hecho de manera insuficiente o en forma inexacta.

Es con la reforma constitucional de 15 de noviembre de 2004, que se eleva a rango constitucional el instituto del Habeas Data, y aparece fundamentalmente establecido en los artículos 42, 43 y 44 del texto de la Constitución Política de Panamá.

El artículo 42 del texto constitucional, conforme a la reforma del 2004, se refiere al acceso a la información personal y establece que

> "Toda persona tiene derecho a acceder a la información personal contenida en bases de datos o registros públicos y privados, y a requerir su rectificación y protección, así como su supresión, de conformidad con lo previsto en la Ley.
>
> Esta información sólo podrá ser recogida para fines específicos, mediante consentimiento de su titular o por disposición de autoridad competente con fundamento en lo previsto en la Ley".

En tanto que el artículo 43 del texto constitucional, conforme a la reforma del 2004, se refiere al derecho de solicitar información de acceso público o de interés colectivo, y establece que

> "Toda persona tiene derecho a solicitar información de acceso público o de interés colectivo que repose en bases de datos o registros a cargo de servidores públicos o de personas privadas que presten servicios públicos,

> siempre que ese acceso no haya sido limitado por disposición escrita y por mandato de la Ley, así como para exigir su tratamiento leal y rectificación".

Adviértase que los artículos 42 y 43 del texto constitucional distingue entre información personal y pública; y es por ello que el artículo 42 instituye que, cuando se trata de información personal, toda persona tiene derecho a acceder a su información personal contenida en bases de datos o registros públicos y privados, y a requerir su rectificación y protección, así como su supresión, de conformidad con lo previsto en la Ley; mientras que cuando se trata de información pública el artículo 43 establece que toda persona tiene derecho a solicitar información de acceso público o de interés colectivo que repose en bases de datos o registros a cargo de servidores públicos o de personas privadas que presten servicios públicos, siempre que ese acceso no haya sido limitado por disposición escrita y por mandato de la Ley, así como para exigir su tratamiento leal y rectificación.

Es a consecuencia del incumplimiento de la protección del derecho fundamental del derecho de acceso a la información personal o pública establecido en los artículos 42 y 43 de la Constitución que, entonces, se aplica el artículo 44 de la Constitución; y es que si, en efecto, no se reconoce el derecho fundamental de acceso a la información personal o pública es cuando se ejerce el derecho previsto en el artículo 44 que, propiamente, instituye el Habeas data como mecanismo jurisdiccional de protección del derecho fundamental al acceso a la información.

Dice el artículo 44 del texto constitucional que

> "Toda persona podrá promover acción de hábeas data con miras a garantizar el derecho de acceso a su información personal recabada en bancos de datos o registros oficiales o particulares, cuando estos últimos traten de empresas que prestan un servicio al público o se dediquen a suministrar información.
>
> Esta acción se podrá interponer, de igual forma, para hacer valer el derecho de acceso a la información pública o de acceso libre, de conformidad con lo establecido en esta Constitución.
>
> Mediante la acción de hábeas data se podrá solicitar que se corrija, actualice, rectifique, suprima o se mantenga en confidencialidad la información o datos que tengan carácter personal.

> La Ley reglamentará lo referente a los tribunales competentes para conocer del hábeas data, que se sustanciará mediante proceso sumario y sin necesidad de apoderado judicial".

Es así, entonces, que el Habeas Data, desde el texto constitucional, opera como un principio y como un derecho. En cuanto es un principio constitucional se expresa en el mandato de orden universal que dice que todas las personas tienen acceso a su información personal y pública; lo cual implica un deber de obligatorio cumplimiento para todas las autoridades en el cumplimiento y tutela de ese mandato principialista establecido en el texto constitucional. En cuanto derecho, el acceso a la información personal y pública se traduce en un derecho subjetivo que en la praxis implica deberes de cumplimiento de las autoridades, de atender y cumplir con el derecho de acceso a la información; porque su incumplimiento implica la libertad de ejercer la garantía jurisdiccional de Habeas Data para hacer efectivo el derecho tutelado en la constitución.

Por otra parte, e igualmente como eje temático de esta tesis, observamos los Principios globales sobre seguridad nacional y el derecho a la información, emitidos el 12 de junio de 2013, fueron redactados por 22 organizaciones durante un periodo de dos años, en el que se contó con la asesoría de más de 500 expertos de al menos 70 países. El proceso de redacción culminó con una reunión en la ciudad sudafricana de Tshwane, de la que estos Principios tomaron su nombre, y moderadas por la Iniciativa Pro-Justicia de la Sociedad Abierta, y con la ayuda de los cuatro relatores especiales para la promoción y protección de la libertad de expresión y/o la libertad de prensa y el relator especial sobre la promoción y protección de los derechos humanos y libertades fundamentales en la lucha contra el terrorismo:

- El Relator Especial de las Naciones Unidas (ONU) para la Libertad de Opinión y de Expresión,
- El Relator Especial de las Naciones Unidas (ONU) sobre la promoción y protección de los derechos humanos y libertades fundamentales en la lucha contra el terrorismo,
- La Relatora Especial de la Comisión Africana de Derechos Humanos y de los Pueblos sobre Libertad de Expresión y Acceso a la Información (ACHPR),

• La Relatora Especial de la Organización de los Estados Americanos (OEA) para la Libertad de Expresión y

• La Representante de la Organización para la Seguridad y la Cooperación en Europa (OSCE) para la libertad de los medios.

# II.-
# JUSTIFICACIÓN Y RELEVANCIA DE LA TESIS DOCTORAL

## II.-JUSTIFICACIÓN Y RELEVANCIA DE LA TESIS DOCTORAL

Esta tesis doctoral se fundamentará por tanto en las conclusiones obtenidas en tres capítulos de libro, relativos a las leyes de acceso a la información púbica en un ámbito comparado, así como las distintas restricciones normativas que se supeditan a esta por interés general.

En un primer capítulo de esta compilación observaremos el fenómeno de la Información clasificada de las organizaciones internacionales y su protección, en donde las organizaciones internacionales y supranacionales de las que España forma parte, en particular la Organización del Tratado del Atlántico Norte (OTAN), la Unión Europea (UE), la Agencia Espacial Europea (ESA) y la Organización Conjunta de Cooperación en materia de Armamento (OCCAR) han desarrollado un esquema, y la normativa correspondiente, para la protección de la Información Clasificada, la cual se aplica a las personas, las instalaciones, los sistemas de información y comunicación y las empresas que han de acceder, manejar o generar dicha Información Clasificada. Todos los estados que forman parte de estas organizaciones tienen como cometido velar por la protección de la Información Clasificada de la organización y de sus programas clasificados, y para ello han de desarrollar y aplicar la legislación nacional necesaria, así como concluir los acuerdos de seguridad, bilaterales o multilaterales, que se requieran con terceros estados u organizaciones internacionales.

El segundo de los capítulos que forman parte de esta compilación es el resultado de dos estancias en el Centro de Políticas Públicas y Transparencia de la Universidad de Panamá, y que representara el primer estudio comparado entre Panamá y España respecto a sus leyes de acceso a la información, donde trataremos las leyes de acceso a la información en Panamá y entre otros, su excepción de protección de datos personales bancarios, lo que ha generado el fenómeno de los denominados como “papeles de Panamá”, para sintetizar en concreto la pertinencia de observar las leyes panameñas de acceso a la información y su acomodo ante los retos de la seguridad regional e internacional.

El tercero y último de los capítulos que compondrán esta tesis doctoral será un trabajo que observe la armonización de las políticas públicas en el ámbito regional americano, una vez que en el primer capítulo de esta compilación hemos tratado el fenómeno de las restricciones a la información, en un ámbito

supranacional haciendo incidencia en las organizaciones de las que España forma parte, mientras que en este tercer capítulo propondremos una investigación incardinada a un ámbito americano de las que Panamá forma parte, trayendo a colación las deliberaciones del comité jurídico interamericano y las leyes modelo interamericanas sobre acceso a la información confrontándolos con los principios de Johannesburgo que definen la legitimidad de la restricción de determinadas informaciones que comprometan la integridad territorial ante amenazas a su seguridad, confrontándola con los "Principios de Tshwane", sobre la seguridad nacional y el derecho a la información emitidos el 12 de junio de 2013, y redactados por 22 organizaciones y expertos de 70 países.

# III.-
# OBJETIVOS CIENTÍFICOS DE ESTA TESIS DOCTORAL

# III.- OBJETIVOS CIENTÍFICOS DE ESTA TESIS DOCTORAL

## 3.1. OBJETIVOS

### 3.1.1.- Objetivo general

Observar en un ámbito comparado, las excepciones reconocidas y aceptadas por el derecho internacional a la restricción del acceso a la información sobre determinas informaciones susceptibles de ser quebrantadas por la amenaza del terrorismo internacional.

### 3.1.2.- Objetivos trasversales

Representar el primer estudio comparado entre Panamá y España respecto a sus leyes de acceso a la información, donde trataremos las leyes de acceso a la información en Panamá y entre otros, su excepción de protección de datos personales bancarios, lo que ha generado el fenómeno de los denominados como "papeles de Panamá", para sintetizar en concreto la pertinencia de observar las leyes panameñas de acceso a la información y su acomodo ante los retos de la seguridad regional e internacional.

Verificar los planteamientos teóricos y prácticos con el objetivo de contribuir a la robustez que sustenta los principios sobre la reserva o restricción del acceso a la información alusiva a la seguridad nacional, en detrimento de los principios que sustentan las leyes de acceso a la información

Observar la necesidad de que los Estados establezcan protocolos y estándares mínimos, que deberán cumplir entre aquellos que se dediquen al manejo de datos e información, y de qué manera podrá efectuarse una supervisión efectiva sin que la misma se entienda como una vulneración a las garantías fundamentales, o derecho a la intimidad de las personas**.**

# IV.-
# PREGUNTAS DE INVESTIGACIÓN

## IV.-PREGUNTAS DE INVESTIGACIÓN

P1- El terrorismo, la delincuencia organizada y la corrupción entre otras acciones no legítimas han utilizado las protecciones del derecho a la información que la ley otorga, para poder ocultar los beneficios de sus acciones, ¿Sería posible una open data general para evitar estos casos?

P2.- Los planteamientos teóricos y prácticos sobre la reserva o restricción del acceso a la información alusiva a la seguridad nacional, en detrimento de los principios que sustentan las leyes de acceso a la información ¿son coherentes con las normativas internacionales sobre los derechos humanos?

P3.- ¿Sería coherente armonizar normativas y establecer estándares a nivel supranacional entre las disposiciones legales que obligan a la rendición de cuentas, el acceso a la información y la trasparencia, y las disposiciones que protegen los intereses de seguridad nacional de los estados democráticos?

# V.-
# METODOLOGÍA DE LA INVESTIGACIÓN

## V.-METODOLOGIA DE LA INVESTIGACIÓN

El proyecto de tesis doctoral que aquí se presenta, consistirá en un trabajo original elaborado a partir del conjunto de publicaciones del doctorando, relacionadas en una misma línea temática, perteneciente esta al plan de investigación de la tesis doctoral y que está constituido por tres capítulos de libro, relacionados con el objeto de la tesis, que serán publicados en editoriales de reconocido prestigio y que cuentan con sistemas de selección de originales por el método de evaluación externa o revisión ciega por pares.

El estudio que vamos a realizar constituirá un análisis cualitativo, del objeto de la tesis, manejando fuentes documentales a través de un análisis inductivo-deductivo, basado en las fuentes de nuestro ordenamiento jurídico, así como de los estudios doctrinales existentes sobre la materia, ofreciendo un exhaustivo análisis sustantivo de los documentos estudiados, que exponga los resultados ofrecidos a través de las distintas publicaciones que se aúnan como hilo conductor de esta Tesis Doctoral.

Dentro de las técnicas metodológicas que hemos utilizado, destaca la observación documental a través de:

- Meta-análisis: búsqueda documental y tratamiento de datos
- El análisis de contenidos: unidades de análisis, categorización, codificación y cuantificación
- El análisis secundario: fuentes de datos, análisis e interpretación

La documentación analizada incluye la plasmación de las discusiones doctrinales sobre la materia, referenciadas en distintas monografías y revistas especializadas, nacionales e internacionales, al objeto de sustentar el rigor científico a la presente obra que configure una investigación sustentada en los capítulos de libro componen la misma.

# CAPITULO I.-
# LA GOBERNANZA DE LA SEGURIDAD EN UN MUNDO GLOBALIZADO

# CAPITULO I.- LA GOBERNANZA DE LA SEGURIDAD EN UN MUNDO GLOBALIZADO

## 1.1. LA GLOBALIZACIÓN Y SU GOBERNANZA

### 1.1.1. El papel de los Estados en la globalización

Garantizar la seguridad es sinónimo de desarrollo en sentido amplio donde se verá que existe la obligación de poner la seguridad en relación con la gobernanza como forma alternativa de gobernar dentro del contexto globalizador, y del rol emergente de actores no estatales en la construcción global de la misma. La gobernanza global de la seguridad en el siglo XXI responde a la necesidad de incluir actores no estatales en la coproducción de la misma, y de un mayor protagonismo del rol de los actores locales en su construcción global. Dado el uso generalizado del término globalización en nuestro lenguaje diario, es habitual relacionarla con el plano económico, si bien, se utiliza de igual forma para referirse a los aspectos sociales, culturales y tecnológicos de alcance planetario, de ahí que sea necesario revisar el estado del arte acerca del concepto. Así, algunos autores entienden que la globalización es solo una de las dimensiones de entre muchas cosas fundamentales que están sucediendo en el mundo al día de hoy[1], o que es una palabra que define nuestro tiempo y la forma en que vivimos, nos ofrece una visión extensiva y del sentido vasto que la detalla, en buena medida gracias a la capacidad de trasmisión favorecida por la tecnología y la liberalización de los intercambios de bienes, servicios y capitales[2].

Los factores que han producido los cambios que han dado lugar a este nuevo paradigma han tenido dos dimensiones diferentes, una extensiva (cuantitativa) y otra de cambio estructural (cualitativa). La primera de ellas como transformación de las fuerzas productivas y los modos de vida resultantes, alteraron las condiciones de desenvolvimiento de la economía, la sociedad, la cultura, la geopolítica mundial y la completa unificación del mercado mundial[3].

---

[1]Friedman, T. L. (2006).La Tierra es plana: breve historia del mundo globalizado del siglo XXI. Martínez Roca.

[2]De la Dehesa, G., & Krugman, P. (2007). Comprender la globalización. Alianza Editorial.

[3]Dabat, A. (2000). Globalización: Capitalismo informático-Global y nueva configuración espacial del mundo. México: Universidad Nacional Autónoma de México.

Este argumento de la globalización se ha acelerado por la caída de las barreras comerciales, la expansión del libre comercio y la armonización del comercio en la era electrónica[4], la reducción de la burocracia relacionada con el comercio internacional y el aumento de la velocidad y forma en que las comunicaciones transmiten los cambios a cualquier parte del mundo y aunque en efecto, se produzcan toda esta serie de circunstancias, existen autores que opinan que conceptualmente se reconoce el hecho de que la globalización es un proceso complejo y a largo plazo[5]. Todo esto hace de la globalización un proceso incompleto y asimétrico[6].

Cabe destacar que el efecto interdependencia es el rasgo que más identifica la globalización, y también es comprensible que aquellos autores que creen que todavía se encuentra en una fase embrionaria y además asimétrica responden a que los Estados, sus comunidades, y su grado de desarrollo, social, económico y político es muy dispar. Así, todo parece indicar que interconexión sí, aunque asimetría también, prueba de ello serán los resultados de la encuesta global Mi Mundo desarrollada por la ONU para un mundo mejor, con el fin de elaborar una agenda global del desarrollo post 2015.[7]

Existe una percepción que el Estado es cada vez más inoperante en lo global y cada vez menos representativo en lo nacional, para ilustrar esta evolución[8], en donde los principales procesos de transformación contemporánea de la sociedad y Estado encontramos,

> "la democratización política, redimensionamiento del tamaño y los alcances del gobierno, la liberación de los mercados, la globalización económica y telecomunicativa, el crecimiento de la independencia y la autonomía social, la individualización de los estilos de vida, la formación de estados supranacionales, el establecimiento de redes civiles o ciudadanas

[4]Paliwoda, S. J., &Slater, S. (2009). Globalisation through the kaleidoscope. International Marketing Review,26(4/5), 373-383.
[5] De Lombaerde, P., &Iapadre, P. L. (2012). Indicadores de la globalización. Cuadernos de Economía,31(SPE57), p 13
[6]Romero, A., & Vera-Colina, M. A. (2012). La globalización posible: límites y alternativas. Cuadernos de Economía, 31(58), p 49.
[7](http://www.myworld2015.org/)
[8]Castells, M. (1999). Globalización, identidad y estado en América Latina. Santiago de Chile: PNUD.

transfronterizas y mundiales, el aumento de la influencia de los organismos internacionales"[9].

En definitiva, el Estado "ya no es esa sociedad perfecta", ya que no se basta a sí mismo para garantizar la seguridad, el bienestar, la justicia, la conservación del medio ambiente, etc. de ahí que necesite delegar para poder hacer frente a un ambiente global complejo[10]. De hecho, la integración y la irrupción en la esfera internacional de actores no estatales, organizaciones intergubernamentales, organizaciones no gubernamentales, empresas transnacionales, han adquirido mayor protagonismo político y económico en el mundo contemporáneo[11].

En este mundo interdependiente, la soberanía de iure y la de facto como idea y como praxis, sigue siendo una fuerza poderosa y competente, especialmente respecto a la capacidad del Estado para ejercer su poder coercitivo[12]. Las restricciones provenientes del sistema internacional y de las tendencias a la transnacionalización y a la globalización no significan hasta ahora el total debilitamiento o la condena a la extinción del Estado-nación ni de su soberanía y autonomía de ejercicio.

### 1.1.2. La Gobernanza como red de actores

La definición más reciente de gobernanza proviene del Diccionario de la lengua española, como el arte o manera de gobernar que se propone como objetivo el logro de un desarrollo económico, social e institucional duradero, promoviendo un sano equilibrio entre el Estado, la sociedad civil y el mercado de la economía, sin embargo, esta conceptualización se ve desbordada por el dinamismo de las interacciones entre actores institucionales y no institucionales, así como por la calidad de las redes que desarrollan políticas públicas. Un buen ejemplo de intento por asir la gobernanza, desde una perspectiva conceptual ya

[9]Aguilar, L. F. (2010). El futuro de la gestión pública y la gobernanza después de la crisis. Frontera norte, 22(43), p 210.

[10]Salgado, A.R. (2005) "Globalización y crisis de la política: la necesidad de instaurar el espacio público", VII Congreso Español de Ciencia Política y de la Administración. Democracia y Buen Gobierno.

[11]Sandel, M.J. (1996), Democracy's discontent: America in search of a public philosophy, Belknap Press.

[12]Kaplan, M. (1994). La soberanía estatal-nacional: retos e interrogantes. Problemas actuales del derecho constitucional. Estudios en homenaje a Jorge Carpizo, 225-234.

ha sido desarrollado por Naciones Unidas en su documento elaborado por el Comité de Expertos en Administración Pública de la ONU sobre compendio de terminología básica de gobernanza y administración pública[13]. En suma, la gobernanza es una particular manera de gobernar, que se caracteriza por la interdependencia entre actores, los cuales se coordinan y negocian con la intención de lograr los objetivos propuestos, en un contexto que ha pasado del mando y control tradicional al de coordinación. Cuál es la parte que corresponde a la gobernabilidad y a la gobernanza en la construcción de una situación de seguridad ciudadana. Queda claro que abordar la gobernabilidad de la seguridad no se refiere al conjunto de acciones que de manera clásica se abordan cuando se hace referencia a la seguridad ciudadana (acciones de prevención y de coerción).Esta nueva modalidad de gobernar, crea de modo implícito la necesidad inequívoca de establecer relaciones, y así entender las necesidades, plantear soluciones colectivas, buscar el consenso, etc.

## 1.2. LA SEGURIDAD

### 1.2.1 La Seguridad y su significado

"La seguridad es un derecho, tanto de los individuos, como de las comunidades, para alcanzar una calidad de vida acorde a la dignidad de ciudadanos"[14].

La inseguridad ciudadana es un fenómeno multicausal y multifacético. Intervienen múltiples actores en el problema y se requiere, en la lógica contemporánea de una seguridad transversal, numerosas interacciones entre actores públicos, privados y sociales. De ahí la importancia de definir bien la problemática y de resaltar las conflictividades y los nudos principales en la toma de decisiones. Obviamente, tratándose de una construcción social, es esperable que cada actor desarrolle una percepción muy diferente del problema[15]. De igual

[13]Consultar: http://unpan1.un.org/intradoc/groups/public/documents/un/unpan025249.pdf

[14]Ruiz, J. C., &Vanderschueren, F. (2007). Base conceptual de la seguridad. Consolidación de los gobiernos locales en seguridad ciudadana. Red, 14, pp 11-12.

[15]Velásquez, E. (2007b) "Gobernabilidad de la seguridad ciudadana en Bogotá 1992-2007: Una primera lectura". En: Velásquez, E. & Godard, H.(eds). Gobernabilidad territorial en las ciudades andinas. Organización y recomposiciones territoriales y socio-políticas. Bogotá: IFEA-U. Externado.

modo el concepto puede ser ampliado tomando en consideración la seguridad nacional y defensa de la nación, a través de las fuerzas armadas o el uso de la fuerza para controlar a los ciudadanos de un estado, implicando en ello a los servidores públicos de la seguridad, las fuerzas de seguridad y los ejércitos[16].

En esta línea argumental, dentro del sistema hobbesiano, la esencia de la seguridad se encuentra en la mutua relación entre protección y obediencia y en ella se encuentra la esencia del pacto social y la esencia del poder político[17]. Por su parte, Emmanuel Kant, se apropia de la seguridad y se la atribuye al Estado como competencia para garantizar a sus ciudadanos los derechos que les son inalienables, ideas compartidas con Hobbes. No obstante, Kant crea además la idea de crear lazos entre Estados como medio para lograr un orden no sólo interno, sino además de carácter internacional, donde se demuestra que la seguridad tiene gran importancia en nuestra calidad de vida, en el desarrollo económico y social en la sociedad de hoy, y de la libertad misma, sin condiciones de seguridad no queda garantizado el ejercicio de las libertades públicas ni las individuales.

### 1.3. LA GOBERNANZA DE LA SEGURIDAD

La gobernanza de la seguridad implica a diferentes actores donde los mismos interactúan, y es en este proceso que, al compartir normas, valores e identidad, entre un grupo de Estados, hay menos probabilidad de la guerra o la violencia mutua, y posteriormente se abre el camino hacia una comunidad de seguridad[18], el cual está centrado en el Estado, más que en la orientación de gobernanza de la seguridad, que se extiende a un actor de múltiples niveles estatales, no estatales, públicos y privados, y en donde actualmente preocupan a las grandes potencias, la actividad de grupos armados que representan intereses políticos, religiosos o culturales, armas de destrucción masiva y terroristas internacionales.

---

[16]Brooks, D.J.(2010).What is security: Definition through knowledge categorization. Security Journal, 23(3), 225-239.

[17]Arbeláez Herrera, Á. M. (2009). La Noción de Seguridad en Thomas Hobbes. Revista de la Facultad de Derecho y Ciencias Políticas, p 34.

[18]Kirchner, E. J. (2006). The Challenge of European Union Security Governance..*JCMS: Journal of common market studies*, *44*(5), 947-968.

También se ha mencionado que la gobernanza de la seguridad es como un gobierno en red, de redes interorganizacionales y autoorganizadas, integradas por actores públicos y privados como gobierno relacional, y ante un escenario de riesgos dispersos dentro de esa red, exige establecer un rol a los encargados de garantizar la seguridad dentro de la misma, incluso la propia sociedad ha abierto un nuevo espacio político donde articular estrategias para afrontar los desafíos del gobierno urbano, debates sobre delincuencia, inseguridad, para que pasen de ser tratados desde el ámbito público al privado[19]. La formulación de políticas públicas caracterizado por la cooperación entre diferentes actores interdependientes es un campo dominado por una serie vasta de redes e instituciones entrelazadas que transcienden la clásica división público/privada y que generan mezclas híbridas compuestas por una pluralidad de agencias, profesiones y líderes de la sociedad civil[20].

En cuanto al ámbito internacional, más allá de las fronteras de los Estados donde la amplitud de la autoridad gubernamental se encuentra mermada por los límites que le impone el principio de territorialidad y el ejercicio de soberanía, parece intuir que una situación de anarquía domina la esfera internacional. Sin embargo, Webber afirma que existe "un mínimo orden que sustenta la vida global", él mismo, cita a Bob Jessop introduciendo el concepto de heterarquía, la cual supone la existencia de múltiples centros de poder y multiplicidad de acciones combinadas y coordinadas adoptadas en respuesta a los desafíos cada vez más complejos de gobernar en un mundo globalizado. Entiende Webber, que la gobernanza de la seguridad se compone de cinco características[21]:

1. Heterarquía, redes interconectadas.
2. La interacción de un gran número de actores, tanto públicos como privados.
3. Institucionalización tanto de carácter formal como informal.

[19]Virta, S. (2002). Local security management: Policing through networks. Policing: An International Journal of Police Strategies& Management,25(1), 190-200.
[20]Dabat, A. (2000). Globalización: Capitalismo informático-Global y nueva configuración espacial del mundo.México: Universidad Nacional Autónoma de México.
[21]Webber, M., Croft, S., Howorth, J., Terriff, T., &Krahmann, E. (2004). The governance of European security. Review of international studies, 30(01), 3-26.

4. Las relaciones entre los actores caracterizados por sus ideales estructurados por normas e interpretaciones, además de regulaciones formales.
5. El propósito colectivo, los intereses comunes.

Así, para entender la gobernanza de la seguridad, habría que diferenciar entre estructura y proceso. Como estructura hay que admitir la existencia de la multiplicidad de instituciones relacionadas, y como proceso, la necesidad de una regulación en los procesos de coordinación, al objeto de adecuarlos para lograr una resolución eficiente de los objetivos acordados por los diferentes actores en acción. Al mismo tiempo, los órganos responsables que formulan aplican y supervisan la política de seguridad con el fin de garantizar el bienestar y la seguridad de los individuos de modo aislado y en sociedad, deben garantizar su gobernabilidad a través del buen gobierno (Resolución 2000/ 64 de la Comisión).

### 1.3.1. La Gobernabilidad de la seguridad pública

Actualmente la gobernabilidad como hemos comprobado no depende únicamente de la actuación del gobierno, sino de la interacción que se da entre este y los nuevos actores que se presentan en la escena estatal. Partiendo de este contexto, es necesario ahora determinar hasta qué punto la seguridad influye en la gobernabilidad. Para ello es preciso mencionar cuáles son los factores relacionados con el tema de seguridad que disminuyen la confianza en el gobierno[22]. La percepción de inseguridad se da por la interacción entre varios factores relacionados con las actividades de los delincuentes, el trabajo de los cuerpos de seguridad, las políticas públicas en la materia y la distribución de los recursos por parte de las autoridades para atacar este problema. Es por estos motivos que se considera que la inseguridad pública y la violencia generan un cierto grado de ingobernabilidad y esta, a su vez, con protesta civil o sin ella, propicia condiciones adecuadas para el fenómeno de actividades delictivas o, como ya se ha dicho, para estigmatizar a ciertos grupos de la población que al verse excluidos, se colocan en una situación más propicia para ser víctimas de la

[22]Garay Maldonado. D., Seguridad Pública y Gobernabilidad. En estado Constitucional, Derechos Humanos, Justicia y vida universitaria. Instituto de investigaciones jurídicas. Estudios en homenaj a Jorge Carpizo. UNAM. 2015. P 311.

delincuencia, que bien puede atacarlos o ver en ellos una rica veta de elementos, a los cuales orillan, a través de la violencia u otros tipos de coacción, a formar parte de grupos criminales; esto es, que existe una relación bidireccional entre los altos índices de delincuencia y la ingobernabilidad[23]. Cuestión distinta, es si en el conjunto sistema internacional y de las redes que lo conforma necesitan de un órgano/s supranacional que moderen/pongan orden en dichas interacciones, de alguna u otra forma y dejando al margen ciertos Estados que han estado y ejercen una especial vigilancia más allá de sus fronteras. Se han creado organizaciones internacionales que ejercen presión sobre los Estados y por ende de los distintos líderes de la red, y que como se ha dicho, a medida que adquieren mayor protagonismo erosionan la soberanía de los Estados.

### 1.3.2. Cuáles son los Retos en materia de gobernabilidad de la seguridad

Asumiendo por tanto que el gobierno no es el único actor que debe operar en la nueva dinámica social que es necesaria para lograr aumentar los índices de seguridad, es imprescindible, como se ha mencionado, concebir mecanismos de negociación y cooperación entre los diversos actores públicos y privados para reducir la conflictividad, y, con ello, la violencia.[24] Para lograrlo es fundamental conseguir una mayor participación ciudadana, pues se ha demostrado que la política de seguridad en buena medida operará en función tanto de la configuración social y cultural del espacio en el que desee aplicarse como de la relación que tenga con la ciudadanía. La seguridad como ámbito discrecional del Estado, y la tradicional tríada policía-justicia-sistema penitenciario, ha comenzado a abrir paso a nuevas formas de intervención de nuevos actores en la lucha contra el delito y en la construcción de la seguridad ciudadana.

Podría plantearse que, en contravía al tradicional esquema vertical y discrecional, se viene abriendo paso un esquema transversal de la política pública de seguridad ciudadana. Se podría hablar hoy de la seguridad transversal. Por ello, una visión de la seguridad ciudadana es necesaria desde la perspectiva de la

[23] Valdez Zepeda, Andrés, "Seguridad pública y gobernabilidad: teorías, relaciones y aproximaciones" *Estudios Politicos* sexta época, num 24, mayo-agosto de 200. P281

[24] Garay Maldonado. D., Seguridad Pública y Gobernabilidad. En estado Constitucional, Derechos Humanos, Justicia y vida universitaria. Instituto de investigaciones jurídicas. Estudios en homenaj a Jorge Carpizo. UNAM. 2015. P 314

gobernabilidad y la gobernanza. Una relación entre gobernabilidad y seguridad aparece como necesaria. Autores como Krahmann se han ocupado de los aspectos globales de la gobernabilidad y la seguridad, principalmente en una perspectiva internacional e incluyendo aspectos más tradicionales de la defensa y la seguridad nacional.[25]

Esta dinámica también puede aplicarse en sentido inverso, si se considera que los gobiernos autoritarios y represivos favorecen la pasividad ciudadana para obtener el control autoritario del espacio público, pues los miedos demasiado explícitos o las demandas de orden muy urgentes hacen desaparecer las libertades. Además, una ciudadanía socialmente activa reclama una seguridad construida de manera compartida entre los distintos actores y sectores que la componen, lo que se torna indispensable dada la situación global[26], donde la gobernabilidad en el ámbito de las relaciones internacionales se ha focalizado en la construcción de sistemas de reglas.

### 1.4. CONCLUSIONES PRELIMINARES

La naturaleza multidimensional de la globalización y la pluralidad de contextos sobre los que recae su marco teórico, complica la descripción y concreción del repertorio de factores que se producen como consecuencia de los distintos ámbitos relacionados en este artículo, si bien, resultó oportuno ponerla en relación con el binomio Estado-sociedad, figuras preponderantes en el mundo de hoy, convino ilustrar el cambio sufrido del modelo de Estado-nación el cual se encuentra en fase de transformación profunda para adaptarse a un modelo más horizontal y moldeable. Así, el mapa político actual es difícil de describir y analizar, dado que es reflejo de tendencias e impulsos complejos y contradictorios entrelazados, a falta de regulación internacional que permita solucionar los problemas de aplicación estatal, provocada por los propios límites que le impone el principio de legalidad al que se encuentran sometidos los sistemas penales tradicionales derivados la concepción clásica de soberanía de Estado-nación, se generan crisis de legitimidad institucional ante la falta de acción estatal por

[25]Krahmann, E. (2003). Conceptualizing security governance. Cooperation and conflict, 38(1), 5-26.
[26]Pascual Esteve, J M. (2010) «El buen gobierno 2.0: La gobernanza democrática territorial». Ed. Tirant Lo Blanch, Valencia, p 38.

hechos de esta relevancia, y de la que se hacen eco los medios de comunicación. De hecho, los cambios sociopolíticos acaecidos durante el transcurso del estado moderno y posmoderno, se han caracterizado por ser rápidos y profundos, además de constantes. Así, pues, y en el marco de nuevas entidades espaciales y territoriales, surgen otras formas de poder y de ejercicio de poder y organizaciones tales como el Consejo Europa, Naciones Unidas, Tribunales Internacionales, Organismos Intergubernamentales, Organismos no Gubernamentales, etc, se han convertido en actores imprescindibles en la gestión de lo público, formando parte de la nueva forma de gobernar, la gobernanza.

# CAPÍTULO II.-
# EQUILIBRIO ENTRE INFORMACIÓN Y SEGURIDAD NACIONAL

# CAPITULO II.- EQUILIBRIO ENTRE INFORMACIÓN Y SEGURIDAD NACIONAL

## 2.1. INTRODUCCIÓN

Los riesgos globales enfrentan a los Estados a un nuevo entorno estratégico cada vez más abierto e incierto que genera una sensación de inseguridad. Las medidas a adoptar pueden ser de distinta naturaleza, pero casi todas ellas han venido auspiciadas por la necesidad de garantizar la seguridad nacional. La restricción de las libertades desde los acontecimientos del 11-S y los siguientes grandes atentados terroristas, han desdibujado los esquemas tradicionales del binomio libertad / seguridad, han coadyuvado a reforzar este segundo concepto en detrimento del primero[27].

> "El miedo al terrorismo global no puede dar lugar a que los Estados al sentirse amenazados actúen sin el debido respeto a los derechos fundamentales, legislando de forma excepcional. El miedo se convierte en un generador de políticas que olvidan los espacios de libertad, haciendo primar la seguridad"[28].

La Lucha contra el terrorismo debe llevarse a cabo siempre dentro de los límites del estado de derecho y de la democracia constitucional.

> "El miedo, la sensación de inseguridad, la obsesión por la seguridad total tras brutales masacres, si bien puede aumentar los controles policiales o las intervenciones preventivas, no se puede ignora que los titulares de derechos fundamentales, inalienables, inviolables son inderogables"[29].

En este orden de cosas es conveniente recordar la Decisión-Marco del Consejo de la Unión Europea, de 13 de junio de 2002, (reformada en 2008), en

---

[27] Sobre las diferentes respuestas ofrecidas en la lucha contra el terrorismo internacional tras el 11-S puede verse, entre otros, el trabajo KENT R (2014): «The 9/11 effect in comparative perspective: some thoughts on terrorism in Canada, Spain and the United States», en REVENGA SÁNCHEZ, M (Director), Terrorismo y Derecho bajo la estela del 11 de septiembre, Valencia, Tirant lo Blanch, pp. 21-60.

[28] CURBET, J.: Temeraris atemorits. L'obsessió contemporània per la seguretat, Girona, CCG Edicions, 2007.

[29] ver RUIZ MIGUEL, C (2003): «El derecho a la protección de los datos personales en la Carta de derechos fundamentales de la Unión Europea», Revista de Derecho Comunitario, n.º 14, pp. 7-43.

materia de lucha contra el terrorismo, que intenta definir las reglas para homogeneizar la prevención y represión de los delitos de terrorismo por los Estados miembros, preocupándose al fin por respetar los derechos fundamentales[30]. La coordinación policial y judicial, mediante la Decisión Marco 2002/584/JAI del Consejo, de 13 de junio de 2002 y denominada como euroorden de extradición, ha permitido aplicar medidas eficaces de lucha desde las estructuras jurisdiccionales sobre sujetos vinculados con el terrorismo o con la criminalidad transnacional[31].

### 2.2. COMO EL "REFORZAMIENTO DE LA SEGURIDAD" ANTE EL TERRORISMO, PUEDE PONER EN DUDA EL DISEÑO DEL ESTADO CONSTITUCIONAL Y DEMOCRÁTICO DE DERECHO

Hoy se nos plantean dudas razonables sobre el mantenimiento de los esquemas institucionales del Estado de Derecho en su versión anterior al desarrollo de dichas medidas para luchar contra las nuevas versiones del fenómeno terrorista, o contra la criminalidad organizada transnacional, como graves problemas globales, con lo que entendemos que en ocasiones

> "se ha aprovechado el contexto para extremar de paso medidas tradicionalmente consideradas como extraordinarias, normalizándolas y así primar el principio de eficacia en la reacción ante posibles amenazas normalizando las medidas de excepción[32]".

En similar sentido Revenga Sánchez aludiendo que "lo que dota de sentido a las medidas excepcionales es su carácter limitado en el tiempo y su función de instrumento para la recuperación de la normalidad"[33].

---

[30]Garantizados por el Convenio Europeo de Derechos Humanos y las Libertades Fundamentales, y la Carta de Derechos Fundamentales aprobada en Niza en 2002 e incorporada al Tratado de Lisboa en 2009.

[31]Vease comunicación de la Comisión al Parlamento Europea, al Consejo y al Comité Económico y Social Europeo y al Comité de las Regiones, bajo el título: "Prevenir la radicalización hacia el terrorismo y el extremismo violento: una respuesta más firme de la UE", de 15 de enero de 2014

[32]VERGOTTINI, G. D., Guerra y Constitución, Nuevo conflicto y defensa de la democracia, Il Mulino, Bologna, 2004, p. 21.

[33]REVENGA SÁNCHEZ., M., Garantizando la libertad y la seguridad de los ciudadanos en Europa: Nobles sueños y pesadillas en la lucha contra el terrorismo. Parlamento y Constitución, n.20,2006-2007, p.61

El miedo al terrorismo puede originar que los Estados amenazados por el mismo sufran una "política del miedo", una sensación de "emergencia constante", constituyendo ésta situación el caldo de cultivo para legislar de forma excepcional, produciéndose así un verdadero proceso de marginalización de los derechos fundamentales. El miedo deviene así un generador de políticas que olvidan los espacios de Libertad, primando la seguridad. *La lucha contra el terrorismo no puede renunciar a dos requisitos ineludibles: el uso de medios no terroristas y el respeto al marco que impone la democracia constitucional*[34].

La *política de seguridad nacional* ha pasado a ser objetivo principal de la política judicial, en perjuicio de los derechos civiles y las garantías constitucionales. Como ha escrito Miguel Revenga, *lo que llaman en los Estados Unidos* "guerra contra el terrorismo" *ha producido ya allí ciertas transformaciones en un modo de concebir la libertad política con una tradición de más de doscientos años*[35].

Se ha creado una inteligencia nacional ampliada, que se extiende a todo tipo de información, con independencia de la fuente de la que proceda y que incluye información obtenida dentro y fuera de Estados Unidos, bajo el argumento de la defensa de la seguridad nacional[36] y en donde la tecnología al servicio de la vigilancia, hace que nuestra vida sea "transparente". La vigilancia afecta a todos los resortes de la vida actual, y llega un momento que ya no depende directamente de técnicas de procesamiento en manos del hombre, sino de máquinas a las que hay que controlar muy de cerca para que no acaben con la libertad humana[37].

### 2.2.1. Los principios que rigen el tratamiento de datos

El descubrimiento de escuchas masivas en el extranjero por parte de la agencia estatal de información NSA, y los escándalos por la revelación de secretos (casos Assange y Snowden) no ha generado más que incertidumbre y

[34]WALZER, M., Terrorismo y Guerra Justa, Breus CCBB, Barcelona 2006, p.22
[35]REVENGA SÁNCHEZ., M., Garantizando la libertad y la seguridad …ob cit p.59
[36]Véase; AKERMAN, B: Antes que nos ataquen de nuevo. La defensa de las libertades en tiempos de terrorismo, Barcelona, Península, 2007; VERVALE J.: La legislación antiterrorista en Estados Unidos, ¿Inter arma silent leges?, Buenos Aires, Ediciones del Puerto, 2006..
[37]WHITAKER, R., El fin de la privacidad: cómo la vigilancia total se está convirtiendo en realidad, Paidós, Barcelona,1999, p.11.

desconfianza en amplios sectores de la población mundial. En el espionaje masivo de datos el ciudadano siente que el halo de privacidad con el que actúa e interactúa en su vida privada —y que es lo que le hace sentirse en libertad—está en peligro. Es cuando la pretendida búsqueda de la seguridad nacional acaba erosionando la «seguridad» que uno tiene en que hay un espacio en el que puede actuar sin controles y que hay una información que corresponde a ese espacio privado y que no goza de mayor relevancia o de la que no se pueden derivar mayores consecuencias. El conjunto de metadatos que se pueden almacenar sobre los ciudadanos es incalculable y puede ir desde una información muy sensible (ej. datos sobre salud) hasta otros datos que aisladamente considerados pudieran parecer no tener gran valor, como por ejemplo quién es el titular de un determinado móvil.

Cabe plantearse como interpreta Serra Cristóbal,

> "si del tratamiento de estos datos se puede producir una invasión en mi vida privada, dado que la jurisprudencia y numerosos textos supranacionales han considerado el tratamiento de los datos de carácter personal como una cuestión en la que puede verse afectado el ámbito de la intimidad/privacidad[38] del individuo"[39].

Si, además, se cruzan determinados datos de tráfico (identificación de llamadas, interlocutores en mensajes electrónicos…) y se tratan los mismos mediante determinados programas o técnicas informáticas que permiten conocer los interlocutores en una comunicación electrónica o incluso el contenido de la comunicación misma, podría quedar menoscabado el derecho a la inviolabilidad del secreto de las comunicaciones. Es indudable que, de un modo u otro, la recolección y almacenamiento de datos sobre comunicaciones, —que, entre otros, se produce por los servicios de inteligencia—, puede ir más allá de la mera recolección de datos o incluso tratarse de un control prospectivo del contenido mismo de las comunicaciones. Los servicios de inteligencia durante sus

[38]Sobre el ámbito de la privacidad o vida privada, vease, MARTÍNEZ MARTÍNEZ, R., (2005): Una aproximación crítica a la autodeterminación informativa, Madrid, Civitas, pp. 35-44.
[39]Vease RUIZ MIGUEL, C., (2003): «El derecho a la protección de los datos personales …ob cit, pp. 7-43.

actividades de vigilancia,[40] deben velar por el respeto a la legalidad vigente y a que el tratamiento de los datos goce de todas las garantías, —máxime, cuando afectan a la intimidad y más aún, si interfieren en el secreto de las comunicaciones—.

Cuando se trata de recabar datos derivados de comunicaciones que puedan afectar al secreto de éstas (escuchas telefónicas o electrónicas), nuestra Constitución exige la autorización de un juez, sin necesidad de distinguir entre interceptaciones individuales de comunicaciones o vigilancia masiva de comunicaciones (art. 18.3 CE). Y cuando dichos controles tienen que ser realizados por los servicios de inteligencia en el marco de sus funciones, la Ley Orgánica 2/2002, reguladora del control judicial previo del Centro Nacional de Inteligencia, indica que

> "el Secretario de Estado Director del Centro Nacional de Inteligencia deberá solicitar al Magistrado del Tribunal Supremo competente, conforme a la Ley Orgánica del Poder Judicial, autorización para la adopción de medidas que afecten a la inviolabilidad del domicilio y al secreto de las comunicaciones, siempre que tales medidas resulten necesarias para el cumplimiento de las funciones asignadas al Centro".

Además, el TEDH ha realizado también un loable trabajo de protección de los derechos humanos en el marco de la lucha contra el terrorismo y, en concreto, en la protección de intimidad/privacidad cuando se llevan a cabo programas de vigilancia general o interceptaciones estratégicas, exigiendo no solo una habilitación legal, sino una previsión legal que sea precisa y respetuosa con los derechos fundamentales[41].

---

[40]El sistema de escuchas telefónicas SITEL utilizadas por las fuerzas de seguridad del Estado y por los servicios del Centro Nacional de Inteligencia españoles es un avanzado sistema electrónico que permite interceptar y grabar en tiempo real cualquier conversación telefónica, correo electrónico o mensaje de móvil, además de almacenar en formato digital todos los datos de esas comunicaciones para su posterior análisis. En todo caso, en principio, este sistema de vigilancia sólo puede ser utilizado con autorización judicial previa. Una descripción técnica de este sistema pude encontrarse en la STS 250/2009, de 13 de marzo. Citado en; SERRA CRISTÓBAL, R., "La opinión pública ante la vigilancia masiva de datos. El difícil equilibrio entre acceso a la información y seguridad nacional". En *Revista de Derecho Político* N.º 92, enero-abril 2015, p 99.

[41]SSTEDH asunto; Valenzuela Contreras c. España, de 30 de julio de 1998; SSTEDH asunto; Padro Bugallo c. España, de 18 de febrero de 2003; SSTEDH asunto; Dulkarin Coban c. España, de 26 de septiembre de 2006 etc.

De las regulaciones jurídicas anteriores podemos afirmar la necesidad ineluctable de que la lucha contra el terrorismo en sus diversas manifestaciones, se debe realizar dentro de los límites del Estado de Derecho y de la democracia constitucional. La doctrina del Tribunal Europeo de Derechos Humanos nos parece un buen referente para no caer en los abusos de la lucha contra la inseguridad y en especial el terrorismo: la garantía del derecho a la seguridad de los ciudadanos como deber del Estado, el respeto íntegro a los derechos y libertades reconocidos en el convenio, así como las garantías y controles precisos en las limitaciones o restricciones de los derechos de las personas (intimidad, secreto de las comunicaciones, protección de datos personales, privación de libertad) y aunque el Tribunal Europeo de Derechos Humanos ha reconocido que tal tipo de vigilancia prospectiva es a veces necesaria, exigiendo una previsión legal que la regule y que sea precisa y respetuosa con los derechos fundamentales, que exista proporcionalidad en el ejercicio de tales prácticas y una autoridad externa independiente que las supervise.[42]

En este sentido nuestra LO 15/1999, de protección de datos, no se aplica a los ficheros sometidos a la normativa sobre materias clasificadas o a los establecidos para la investigación del terrorismo (art. 2), los principios básicos que informan dicha Ley no dejan de tener pertinencia también en ese tipo de información recabada, almacenada y tratada por los servicios de inteligencia. Son principios que informan, entre otras cosas, cuándo se pueden recopilar datos, cuándo pueden cederse, o qué medidas de seguridad se adoptan para evitar el acceso de terceros. Estos principios son los de consentimiento, necesidad, y seguridad y todos ellos lógicamente dentro de la finalidad expresa por su autorización, para la que fueron recabados.

[42]SSTEDH asunto Murray c. the United Kingdom, 28 de octubre de1994, La Corte, en primer lugar, reiterar su reconocimiento de que el uso de información confidencial es esencial en la lucha contra la violencia terrorista y la amenaza que el terrorismo organizado representa para la vida de los ciudadanos y para la sociedad democrática en su conjunto. Esto no significa, sin embargo, que las autoridades investigadoras tengan carta blanca…». SSTEDH asunto Kopp C. Switzerland, 25 de marzo de 1998, «la grabación y otras formas de interceptación de conversaciones telefónicas constituyen una grave injerencia en la vida privada y la correspondencia y en consecuencia debe ser basada en una «ley» que sea particularmente precisa. Es indispensable contar con reglas claras y detalladas sobre el tema, sobre todo porque la tecnología disponible para ello se está haciendo cada vez en más sofisticada. Citado en; SERRA CRISTÓBAL, R., "La opinión pública ante la vigilancia masiva de datos… ob cit. p 101

El principio de consentimiento, al igual que queda excepcionado por la Ley de Protección de datos para los ficheros de los cuerpos de seguridad del Estado, también queda excepcionado por la Ley reguladora del Centro Nacional de Inteligencia por el carácter secreto de toda información de inteligencia que generen dichos servicios (art. 5). Por lo tanto, no podemos decir que exista un derecho a acceder a los ficheros producto de la vigilancia prospectiva para inteligencia, como tampoco es necesario nuestro consentimiento para que se recaben esos datos.

El principio de necesidad, que exige que solo se puedan tratar datos cuando sean adecuados, pertinentes y no excesivos, obligaría a analizar en cada caso si estamos ante una actividad de recogida y tratamiento de datos que responda a un interés que justifique suficientemente la necesidad de llevarla a cabo, dado que es necesaria la justificación porque, como hemos indicado, de tal vigilancia y tratamiento de datos pueden derivarse posibles daños para los derechos de los ciudadanos, fundamentalmente para la salvaguarda de la privacidad/ intimidad y el derecho a la autodeterminación informativa de los titulares de tales datos, y en ocasiones para el secreto de las comunicaciones. Afirmando Serra Cristóbal, *que la recogida y tratamiento de datos personales y de comunicaciones, debiera producirse sólo cuando sea realmente necesario para la salvaguarda de la seguridad*.

El principio de seguridad, exige que los datos con los que operan los servicios de inteligencia por su carácter sensible se salvaguarden mediante modos de encriptación. *La preocupación por la seguridad de las bases de datos sobre información clasificada ha estado presente en la UE desde hace años, en cuyo marco se han ido adoptando normas de seguridad para la protección de la información clasificada*[43]. La Orden Ministerial 76/2006, de 19 de mayo, la política de seguridad de la información del Ministerio de Defensa, mejoro las previsiones que existían en cuestión de seguridad de la información[44], mientras que el Real Decreto 3/2010, de 8 de enero, se centró en regular el Esquema Nacional de Seguridad en el ámbito

[43]Decisión del Consejo 2001/264/EC, sobre las normas de seguridad del Consejo. Estas normas fueron modificadas en 2011, Decisión del Consejo 2011/292/UE, de 31 de marzo de 2011, sobre las normas de seguridad para la protección de la información clasificada de la UE. Citado en; Serra Cristóbal, R., "La opinión pública ante la vigilancia masiva de datos… ob cit. p 104

[44]Entre otras, las que se contemplaban en el Decreto 242/1969, de desarrollo de la Ley de Secretos oficiales; Orden Ministerial 12/1982, de 21 de octubre, del manual de seguridad industrial de las Fuerzas Armadas; Ley 15/1999, de protección de datos, ibídem p 105

de la Administración electrónica, generando confianza sobre los medios electrónicos en la relación entre el ciudadano y la Administración Pública.

### 2.2.2. La sociedad del control

La sociedad del siglo XXI camina hacia lo que Mattelart y Vitalis definen como un "mundo vigilado", *sociedad bajo el control de las nuevas tecnologías que hacen que nuestra intimidad sea mucho más permeable, donde cada vez se asienta más el principio del control,*[45] siguiendo lo afirmado por Silva Sánchez, *uno de los rasgos más significativos de las sociedades de la era postindustrial es la sensación general de inseguridad, esto es, la aparición de una forma especialmente aguda de vivir el riesgo*[46]. Las palabras pronunciadas por el Comisario europeo responsable del área de investigación P. Busquin, el 3 de febrero de 2004 no dejan duda a lo manifestado anteriormente

> "adoptar una cultura de la seguridad, movilizar a las fuerzas de la industria de la seguridad y la excelencia de la investigación europea, los acontecimientos han situado a la seguridad en la primera fila de las preocupaciones prácticas en Europa y en el mundo. La video-vigilancia globalizada como un medio de actuación policial "comporta una seria renuncia al modelo constitucional de garantía de las libertades"[47].

No olvidemos que las tecnologías de la información vuelven transparentes nuestras vidas.[48] En palabras de Whitaker, en lo que alude como "arquitectura del control",

> "la interceptación de las comunicaciones sin autorización es posible ahora cuando se trate de investigaciones nacionales o internacionales cuya finalidad sea la salvaguarda de la seguridad nacional, para los datos registrados como mensajes de voz, o correos electrónicos"[49],

[45]MATTELART, A Y VITALIS.A., De Orwell al cibercontrol. Gedisa. 2015
[46]SILVA SANCHEZ, J M., La expansión del Derecho penal. Aspectos de la política-criminal de las sociedades postindustriales, 2ª ed., Madrid 2001. Citado en SERRA CRISTÓBAL, R… p.91
[47]Citado en GUDIN, F., La lucha contra el terrorismo en la sociedad de la información, Edisofer, Madrid, 2006, p.174
[48]La Directiva europea de 15 de marzo del 2006 obliga a los Estados miembros a almacenar durante dos años los datos de comunicación de sus ciudadanos.
[49]WHITAKER, R El fin de la privacidad: … ob cit, p.11.

por lo que se deduce que todos los medios de comunicación que emplee el sospechoso pueden ser interceptados. Para analizar cuándo cabe tal limitación de las libertades para proteger a la seguridad nacional podrían ser útiles las reflexiones de Rawls sobre la llamada «regla del peligro claro y presente»[50]. Tal y como nos traslada Serra Cristóbal, aplicando análogamente la teoría de Rawls, *a la limitación de otros derechos ante un peligro claro y presente como lo supone el terrorismo internacional*.

Esta teoría, ya esgrimida por el Tribunal Supremo norteamericano diciendo que, *en cada caso, (los tribunales) deben preguntarse si la gravedad del mal reducida por su improbabilidad, justifica tal invasión de (la libre expresión) como la necesaria para evitar el peligro*[51]. Según esta doctrina, basta con que el mal probable sea suficientemente. Es necesario, por tanto, siguiendo a la citada autora,

> "que se trate de una situación de emergencia en el que se plantea una amenaza presente o previsible de grave perjuicio, pudiendo limitarse el contenido de un derecho, si ello es necesario para evitar una pérdida mayor y más significativa, bien directa o indirecta, de esas libertades".

Por lo tanto, también a nuestro juicio, solo cuando exista una probabilidad razonablemente constatable de que se produzca un daño en la seguridad de los ciudadanos a través de posibles ataques terroristas, cabría adoptar medidas que limiten o perjudiquen los derechos de los ciudadanos.

### 2.3. LAS NUEVAS POLÍTICAS EN LA LUCHA CONTRA EL TERRORISMO

En los Estados Unidos, las medidas antiterroristas han provocado que muchas autoridades locales rechacen la aplicación de parte de la legislación "convencional" y sostengan –como el Fiscal general Ashcroft- que la política de seguridad nacional ha pasado a ser objetivo principal de la política judicial, en perjuicio de los derechos civiles y las garantías constitucionales. Según Revenga, *lo que llaman en los Estados Unidos* "guerra contra el terrorismo", *ha producido ya allí ciertas transformaciones en un modo de concebir la libertad política con una tradición de*

[50]RAWLS, J (ed. 1996): Sobre las libertades, Barcelona, Paidós, pp. 97 y ss. Citado en SERRA CRISTÓBAL, R… p.92

[51]Caso Dennis v. United States, 341 U. S. 494 en 510, cit. 183 F. 2, en 212. ibidem… p.92.

*más de doscientos años* [52] . Estas medidas incidieron en la antesala de la reconsideración de derechos fundamentales como libertad y seguridad personales, aumentándose el tiempo de duración de la detención preventiva, la tutela judicial efectiva, con la creación de tribunales de excepción, o el derecho a un proceso debido con todas las garantías al ser afectados los sistemas de recursos o pruebas, o el secreto de las comunicaciones telefónicas y a través de Internet, permitiendo la interceptación de comunicaciones telefónicas sin mandato judicial[53].

La Comisión creada en EEUU a raíz de los ataques del 11-S, instaurada a finales de 2002, elaboró un exhaustivo y completo catálogo de las circunstancias que los produjeron. Esa Comisión hizo públicas sus conclusiones a finales de julio del 2004, entre las que se incluían 41 recomendaciones, en su mayoría dirigidas a la Intelligence Community. Todo este proceso cristalizó en la Intelligence Reformand Terrorism Prevention Act del 2004 (IRTPA). En ella, se contiene una definición de inteligencia nacional ampliada, que se extiende a todo tipo de información, *con independencia de la fuente de la que proceda y que incluye información obtenida dentro y fuera de Estados Unidos, comprendiendo de manera especial la relativa a la seguridad nacional*[54]. El presidente Bush el 26 de octubre el Presidente sancionó la Patriot Act. Se trata de una ley extensa y compleja que confiere inusuales poderes ejecutivos a estructuras operativas de control y a los servicios de inteligencia, derivando esta misma a la adopción en varios Estados de Fellow Patriot Act, que han introducido previsiones similares en materia de registros, embargos, poderes especiales y excepcionales del gobernador[55].

La Patriot Act consta de diez Títulos que modifican unas 15 leyes federales ya existentes, entre ellas, el Wiretap Statute, el Computer Fraud and Abuse, el Foreing Intelligence Surveillance Act, el pen Register and Trap and Trace Statute, the Immigration and Nationality Act, el Mioney laundering Act y el Bank Secrecy

[52]REVENGA SÁNCHEZ, M., Garantizando la libertad y la seguridad de los ciudadanos en Europa: Nobles sueños y pesadillas en la lucha contra el terrorismo. Parlamento y Constitución, n.20,2006-2007, p.59.

[53]ÁLVAREZ, E Y GONZÁLEZ, H., Legislación terrorista comparada después de los atentados del 11 de septiembre y su incidencia en el ejercicio de los derechos fundamentales, Real Instituto Elcano, Área de Terrorismo Internacional, ARI n.7/2006 Madrid,2006, p.2.

[54]

[55]VERVAELE, J., La legislación antiterrorista en Estados Unidos…ob cit, p.12.

Act En su Título II se amplía notablemente la posibilidad de investigación digital, sin exigir en todos los supuestos la autorización judicial. La interceptación de las comunicaciones sin autorización es posible ahora cuando se trate de investigaciones nacionales o internacionales cuya finalidad sea la salvaguarda de la seguridad nacional, para los datos registrados como mensajes de voz, o correos electrónicos. La Patriot Act no exige órdenes de interceptación ni siquiera se requiere la autorización para la interceptación de comunicaciones de sujetos sospechosos de haber cometido abusos informáticos. Todos los medios de comunicación que emplee el sospechoso pueden ser interceptados, y quien lleve a cabo la interceptación no debe quedar identificado en la solicitud ni en la orden de interceptación.

Las repercusiones de la Patriot Act también se han dejado notar en el ámbito de la protección de fronteras y leyes de inmigración. En estas áreas se amplían de 24 horas a 7 días el plazo para comunicar los motivos de la detención administrativa. En el plazo de estos 7 días, el interesado debe ser acusado de un delito o bien ser conducido ante el Ministerio Público en el procedimiento de expulsión. Sin embargo y por motivos de seguridad nacional el Fiscal general puede ampliar el plazo de detención a 6 meses y prorrogarlo varias veces. Amparados en esta legislación, el Fiscal general y el INS (Inmigration and Naturalization Service) ostentan un poder de detención a largo plazo sin precedentes, sin posibilidad de defensa y sin obligación de declarar expresamente en qué se basa con exactitud la amenaza para la seguridad nacional.

> "La política antiterrorista desarrollada por los Estados Unidos ha supuesto en los últimos años un profundo cambio que ha afectado también a las reglas del ordenamiento de la ONU al justificar con la máxima amplitud el recurso a la fuerza e incluso en casos extremos a la "guerra preventiva", como se teoriza en la doctrina estratégica de Estados Unidos"

(The Nacional Security Strategy of the United States of America, septiembre 2002)[56].

En similar sentido, la política antiterrorista seguida por el Reino Unido en los últimos tiempos ha merecido la crítica del Comisario de Derechos Humanos del Consejo cuando el Primer Ministro Tony Blair presentó un proyecto de ley

[56]VERGOTTINI, G, D., Guerra y Constitución... ob cit.pág. 21.

sobre seguridad, crimen y antiterrorismo (Antiterrorism, Crime and Security Act) que supuso la petición a la Cámara de los Comunes de la derogación del art. 5 de la Convención Europea de los Derechos Humanos y Libertades Fundamentales, que garantiza el derecho a la libertad y prohíbe la detención sin proceso judicial, en base a lo dispuesto en el artículo 15 de la Convención Europea que permite que los Gobiernos puedan derogar el citado artículo en tiempos de guerra o emergencia pública

> "la referida norma legal, una vez aprobada, supone un aumento importante de los poderes de policía por cuanto esta puede acceder sin control judicial alguno a interceptar los números de teléfono a los que llaman los vigilados y, en el ámbito de las garantías procesales",

sin embargo, esa Ley antiterrorista del 2001 fue declarada nula por el Tribunal de la Cámara de los Lores por ser incompatible con el Convenio Europeo de Derechos Humanos al permitir la detención de sospechosos de terrorismo de una manera que discriminaba en materia de nacionalidad o estatus de inmigración, al haberse recluido en cárceles británicas a nueve ciudadanos extranjeros sospechosos de terrorismo durante tres años sin proceso judicial, aunque ya previamente la Comisión de Apelación Especial de Inmigración de 2002 había declarado que era injustamente discriminatoria con los extranjeros que vivían en el Reino Unido.

Posteriormente, el 11 de marzo del 2005, sería aprobada en el Reino Unido la Ley de Prevención del Terrorismo (Prevention Terrorism Act), aplicable tanto a los nacionales como extranjeros, la cual ante la imposibilidad de detener a los sospechosos de delitos de terrorismo sin una decisión judicial, introduce la figura de las llamadas "órdenes de control", que permiten vigilar a los extranjeros, controlar sus movimientos e incluso arrestarlos en su domicilio *La Ley antiterrorista Alemana, permite el arresto domiciliario sin cargos de sospechosos terroristas y una serie de "*medidas de control*", como el toque de queda, la vigilancia con medios electrónicos o la prohibición de usar Internet"*[57]**.** A diferencia de la Ley de 2001, no distingue en su aplicación entre ciudadanos británicos y extranjeros, para evitar el argumento utilizado por la Cámara de los Lores cuando afirmó que la Ley de 2001 discriminaba entre uno y otros, en su aplicación. Tanto la ley del 2001

[57] ALVAREZ, E., y GONZÁLEZ, H., ob. cit.pág.5

como la del 2005 a juicio de Amnistía Internacional, contienen disposiciones de amplísimo alcance que contravienen la legislación de derechos humanos y que han producidos abusos graves. El 11 de junio de 2008 el Gobierno del Reino Unido, veía por decreto ampliado el tiempo máximo de detención para sospechosos de terrorismo sin cargos de 28 a 42 días. No cabe duda de que todo lo expuesto comporta un ataque frontal a los postulados sobre los que se cimienta el Estado de Derecho, que se refleja en la disminución de las garantías hasta ahora consagradas, a través de los derechos fundamentales básicos.

> "Asistimos a un momento crucial en la defensa de las libertades por cuanto los postulados en los que se asienta la lucha contra el terrorismo en EEUU y Reino Unido, como hemos observado, dejan a la deriva el barco de las libertades y de los derechos humanos".

En Alemania con la aprobación el 19 de diciembre del 2008 por parte del parlamento alemán de la nueva ley de la BKA (policía criminal) vio ampliadas las competencias policiales, posibilitando "en casos de urgencia" el espionaje on line de ordenadores, sin necesidad de autorización judicial, mientras que, en sintonía con el resto de países de la unión, las compañías de telefonía deben mantener seis meses inalterables sus bancos de datos por si la policía necesitase recurrir a ellos. Son muy interesantes las reflexiones del filósofo alemán Meter Sloterdijk cuando e relación a esta aprobación manifestó que *lo que caracteriza nuestra época es el triunfo de la seguridad sobre la libertad. Los ciudadanos se han convertido en súbditos de la seguridad. La libertad es víctima de nuestro siglo*[58].

Por su parte, la nueva Ley antiterrorista aprobada en Francia en 2005 autorizó la videovigilancia en los transportes públicos, en las estaciones, Ministerios, comercios, sinagogas, iglesias y mezquitas. La Policía tiene acceso directo a las imágenes. La nueva Ley aprobada no sólo aborda la videovigilancia sino que además establece la obligación de que los operadores de telecomunicaciones conserven durante un año los contenidos de las conexiones a Internet, las conversaciones telefónicas de los usuarios y especialmente, reforzando esa inspección en los cibercafés. Los propietarios están obligados a conservar esos datos de transmisión. Los teléfonos celulares también son objeto de vigilancia por esta ley. Además, las compañías aéreas, ferroviarias y marítimas

[58] ibidem. p 97

deben guardar los datos de sus clientes al menos durante doce meses. Asimismo, la ley amplía el plazo de presentación de los detenidos ante la Justicia de cuatro a seis días. La referida ley supone también, la posibilidad de que los servicios policiales puedan instalar sistemas de vigilancia fotográfica de vehículos, fotografiar a sus ocupantes y guardar las imágenes durante ocho días sin tener que pedir un mandamiento judicial. En este orden de cosas, hemos de recordar que la Directiva europea de 15 de marzo del 2006 obliga a los Estados miembros a almacenar durante dos años los datos de comunicación de sus ciudadanos.

# CAPÍTULO III.-
# LA ESTRATEGIA DE SEGURIDAD NACIONAL Y EL ACCESO A LA INFORMACIÓN CONCERNIENTE A LA SEGURIDAD NACIONAL

# CAPÍTULO III.- LA ESTRATEGIA DE SEGURIDAD NACIONAL Y EL ACCESO A LA INFORMACIÓN CONCERNIENTE A LA SEGURIDAD NACIONAL

## 3.1. INTRODUCCIÓN

El miedo al terrorismo puede originar que los Estados amenazados por el mismo sufran una "política del miedo", una sensación de "emergencia constante", constituyendo ésta situación el caldo de cultivo para legislar de forma excepcional, produciéndose así un verdadero proceso de marginalización de los derechos fundamentales. El miedo deviene así un generador de políticas que olvidan los espacios de Libertad, primando la seguridad. La lucha contra el terrorismo no puede renunciar a dos requisitos ineludibles: el uso de medios no terroristas y el respeto al marco que impone la democracia constitucional.

Hoy se nos plantean dudas razonables sobre el mantenimiento de los esquemas institucionales del Estado de Derecho para luchar contra las nuevas versiones del fenómeno terrorista, o contra la criminalidad organizada transnacional, como graves problemas globales, con lo que entendemos que, en ocasiones,

> "se ha aprovechado el contexto para extremar de paso medidas tradicionalmente consideradas como extraordinarias, normalizándolas y así primar el principio de eficacia en la reacción ante posibles amenazas normalizando las medidas de excepción"[59].

En similar sentido, Revenga Sánchez aludiendo que *lo que dota de sentido a las medidas excepcionales es su carácter limitado en el tiempo y su función de instrumento para la recuperación de la normalidad*[60].

La *política de seguridad nacional* ha pasado a ser objetivo principal de la política judicial, en perjuicio de los derechos civiles y las garantías constitucionales. Como ha escrito Miguel Revenga, *lo que llaman en los Estados*

---

[59] VERGOTTINI, G. D., Guerra y Constitución, Nuevo conflicto y defensa de la democracia, Il Mulino, Bologna, 2004, p. 21.

[60] REVENGA SÁNCHEZ., M., Garantizando la libertad y la seguridad de los ciudadanos en Europa: Nobles sueños y pesadillas en la lucha contra el terrorismo. Parlamento y Constitución, n.20,2006-2007, p.61

*Unidos "*guerra contra el terrorismo*" ha producido ya allí ciertas transformaciones en un modo de concebir la libertad política con una tradición de más de doscientos años*[61].

Se ha creado una inteligencia nacional ampliada, que se extiende a todo tipo de información, con independencia de la fuente de la que proceda y que incluye información obtenida dentro y fuera de Estados Unidos, bajo el argumento de la defensa de la seguridad nacional[62] y en donde la tecnología, al servicio de la vigilancia, hace que nuestra vida sea "transparente". La vigilancia afecta a todos los resortes de la vida actual y llega un momento que ya no depende directamente de técnicas de procesamiento en manos del hombre, sino de máquinas a las que hay que controlar muy de cerca para que no acaben con la libertad humana[63].

### 3.2. EL "REFORZAMIENTO DE LA SEGURIDAD" Y EL DISEÑO DEL ESTADO CONSTITUCIONAL Y DEMOCRÁTICO DE DERECHO

Los riesgos globales enfrentan a los Estados a un nuevo entorno estratégico cada vez más abierto e incierto que genera una sensación de inseguridad. Las medidas a adoptar pueden ser de distinta naturaleza, pero casi todas ellas han venido auspiciadas por la necesidad de garantizar la seguridad nacional. La restricción de las libertades desde los acontecimientos del 11-S y los siguientes grandes atentados terroristas, han desdibujado los esquemas tradicionales del binomio libertad / seguridad, coadyuvando a reforzar este segundo concepto en detrimento del primero[64].

> "El miedo al terrorismo global no puede dar lugar a que los Estados al sentirse amenazados actúen sin el debido respeto a los derechos fundamentales, legislando de forma excepcional. El miedo se convierte en

[61]REVENGA SÁNCHEZ., M., Garantizando la libertad y la seguridad …ob cit p.59

[62]Véase; AKERMAN, B: Antes que nos ataquen de nuevo. La defensa de las libertades en tiempos de terrorismo, Barcelona, Península, 2007; VERVALE J.: La legislación antiterrorista en Estados Unidos, ¿Inter arma silent leges?, Buenos Aires, Ediciones del Puerto, 2006.

[63]WHITAKER, R., El fin de la privacidad: cómo la vigilancia total se está convirtiendo en realidad, Paidós, Barcelona,1999, p.11.

[64]Sobre las diferentes respuestas ofrecidas en la lucha contra el terrorismo internacional tras el 11-S puede verse, entre otros, el trabajo KENT R (2014): «The 9/11 effect in comparative perspective: some thoughts on terrorism in Canada, Spain and the United States», en REVENGA SÁNCHEZ, M (Director), Terrorismo y Derecho bajo la estela del 11 de septiembre, Valencia, Tirant lo Blanch, pp. 21-60.

> un generador de políticas que olvidan los espacios de libertad, haciendo primar la seguridad"[65].

La Lucha contra el terrorismo debe llevarse a cabo siempre dentro de los límites del estado de derecho y de la democracia constitucional.

> "El miedo, la sensación de inseguridad, la obsesión por la seguridad total tras brutales masacres, si bien puede aumentar los controles policiales o las intervenciones preventivas, no se puede ignora que los titulares de derechos fundamentales, inalienables, inviolables son inderogables"[66].

En este orden de cosas es conveniente recordar la Decisión-Marco del Consejo de la Unión Europea, de 13 de junio de 2002, (reformada en 2008), en materia de lucha contra el terrorismo, que intenta definir las reglas para homogeneizar la prevención y represión de los delitos de terrorismo por los Estados miembros, preocupándose, al fin, por respetar los derechos fundamentales[67]. La coordinación policial y judicial, mediante la Decisión Marco 2002/584/JAI del Consejo, de 13 de junio de 2002 y denominada como euroorden de extradición, ha permitido aplicar medidas eficaces de lucha desde las estructuras jurisdiccionales sobre sujetos vinculados con el terrorismo o con la criminalidad transnacional[68]. Por otro lado, estamos ante una ley que aplica inicialmente la Estrategia de Seguridad Nacional. Un proyecto compartido (ESN 2013), en adelante ESN 2013; y ahora la nueva Estrategia de Seguridad Nacional, un proyecto compartido de todos y para todos (ESN 2017), y que, en la medida en que plantea una reacción institucional del Estado en su conjunto, pone en manos del Gobierno y, en especial, de su presidente y del Consejo de Seguridad Nacional, como comisión delegada del mismo, unas facultades necesarias para exponenciar la gobernanza de la seguridad.

---

[65] CURBET, J.: Temeraris atemorits. L'obsessió contemporània per la seguretat, Girona, CCG Edicions, 2007.

[66] ver RUIZ MIGUEL, C (2003): «El derecho a la protección de los datos personales en la Carta de derechos fundamentales de la Unión Europea», Revista de Derecho Comunitario, n.º 14, pp. 7-43.

[67] Garantizados por el Convenio Europeo de Derechos Humanos y las Libertades Fundamentales, y la Carta de Derechos Fundamentales aprobada en Niza en 2002 e incorporada al Tratado de Lisboa en 2009.

[68] Vease comunicación de la Comisión al Parlamento Europea, al Consejo y al Comité Económico y Social Europeo y al Comité de las Regiones, bajo el título: "Prevenir la radicalización hacia el terrorismo y el extremismo violento: una respuesta más firme de la UE", de 15 de enero de 2014

### 3.3. EL CONCEPTO DE SEGURIDAD NACIONAL

El orden mundial multipolar del siglo XXI obliga a analizar el concepto de seguridad desde una perspectiva amplia y dinámica para cubrir todos los ámbitos concernientes a la seguridad del Estado y de sus ciudadanos, que son variables según las rápidas evoluciones del entorno estratégico. En relación con el Estado, las dinámicas son reflejo, según palabras de Bauman[69]

> "a todos los efectos prácticos ha cambiado su antiguo rol de defensor y guardián de la seguridad por el de uno más (puede que el más eficaz) de los muchos agentes que contribuyen a elevar la inseguridad, la incertidumbre y la (des)protección a la categoría de condiciones humanas permanentes".

Esta tesitura propia global refleja la paradoja de las dicotomías significativas de la globalización interdependiente, pero fragmentada.

El concepto de *Seguridad Nacional* se define, en el art. 3 de la ley, en los siguientes términos:

> "la acción del Estado dirigida a proteger la libertad, los derechos y el bienestar de los ciudadanos, a garantizar la defensa de España y sus principios y valores constitucionales, así como a contribuir junto a nuestros socios y aliados a la seguridad internacional en cumplimiento de los compromisos asumidos; concepto que hasta la fecha no había sido objeto de una regulación normativa integral".

Se trata, según se insiste, de un "objetivo compartido" entre las diversas Administraciones, estatal, autonómica y local, los órganos constitucionales, en especial las Cortes Generales, el sector privado y la sociedad civil. El art. 4 afirma que la *política de Seguridad Nacional* es una política pública bajo la dirección del presidente del Gobierno y la responsabilidad del Gobierno, en la que, eso sí, participan todas las Administraciones Públicas "de acuerdo con sus competencias" y la sociedad en general. Por consiguiente, plantea que el Gobierno promueva una "cultura de Seguridad Nacional" en la que se implique de forma directa a la sociedad. La cooperación con las Comunidades Autónomas se realiza por medio de la *Conferencia Sectorial para asuntos de la Seguridad Nacional*. El Gobierno, una vez declarada la situación de interés para la Seguridad Nacional,

[69]BAUMAN, ZYGMUNT (2017): *Retrotopía*, Barcelona. Paidós. pp. 31

en caso de graves amenazas, podría dar órdenes directas a los funcionarios de otras administraciones o sectores. Por consiguiente, deberán ser objeto de un desarrollo posterior los mecanismos de cooperación establecidos, para que todas las instituciones y sujetos participantes en la garantía de la "Seguridad Nacional" participen positivamente[70]. Hay que hacer frente común a los ataques a la ciberseguridad, la seguridad económica y financiera, la seguridad marítima, el espacio aéreo, la seguridad energética, sanitaria, de preservación del medioambiente, o a las infraestructuras críticas.

Necesitamos un debate profundo sobre la *cultura de la seguridad*, como una cuestión de Estado, al margen de ideologías, para de una vez comprender que hay que construir estructuras adecuadas para hacer frente a los graves ataques y amenazas globales mencionadas. La declaración de la "situación de interés para la Seguridad Nacional" por parte del Gobierno ha de tener el necesario control parlamentario (art. 24.3), así como, en su caso, judicial.

### 3.3.1. La *Seguridad Nacional,* proyecto integral

La entrada en vigor de la *Estrategia de Seguridad Nacional* de 2013 permitió ajustar la visión integral que emanaba de este concepto de seguridad, permitiendo la significación de la *Seguridad Nacional* como la salvaguarda de la libertad y seguridad ciudadana, los principios y valores del Estado de derecho, los intereses nacionales y los compromisos internacionales. Fue en 2014, cuando la coordinación estratégica y conceptual de la *Seguridad Nacional* experimentó un avance destacado por el impulso de una ley propia: la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, dentro de las competencias exclusivas que la Carta Magna otorga al Estado en materia de Defensa y Fuerzas Armadas[71] y Seguridad Pública[72]. La ESN 2013 articula la *Seguridad Nacional* como política de Estado y reasigna todos los recursos a disposición del ente público de forma efectiva para su preservación.

---

[70] Web oficial del Departamento de Seguridad Nacional. Gabinete de la Presidencia del Gobierno. Gobierno de España. Sistema de Seguridad Nacional. [en línea, 12.09.2018] http://www.dsn.gob.es/es/sistema-seguridad-nacional

[71] CE 1978 art. 149.1.4

[72] CE 1978 art. 149.1.29

Este nuevo texto legal abordo en términos generales potenciar las capacidades de España para responder ante los desafíos y amenazas intrincadas que vivimos hoy, y define competencias en materias como la ciberseguridad, la seguridad marítima y la seguridad financiera, el medio ambiente, la energía, los transportes y las telecomunicaciones.

Su principal objetivo[73] es configurar la *Seguridad Nacional* como un nuevo espacio de acción pública dirigido a la armonización de objetivos, recursos y políticas ya existentes en materia de seguridad y cuya responsabilidad se deberá compartir por los órganos constitucionales, en especial, las Cortes Generales, las diferentes Administraciones Públicas, el sector privado y la sociedad civil dentro del marco internacional vigente. Este esfuerzo de integración reviste mucha importancia, por la compleja naturaleza de los riesgos y amenazas, los cuales impiden que sean contrarrestados con los instrumentos de los que dispone tradicionalmente el Estado.

En esta línea, es necesaria una eficiente coordinación de la estructura territorial del Estado, prevista en la Constitución, para afianzar una correcta respuesta integral. Conforme a esta visión integral se define la política de *Seguridad Nacional*, en su título Preliminar, como una política pública de Estado bajo la dirección del Presidente del Gobierno. La garantía de *Seguridad Nacional*, que se establecía en la propia ESN 2013 reclamaba el compromiso y la responsabilidad al más alto nivel. El Presidente la liderará y la impulsará[74] y, bajo su dirección, el Gobierno será responsable de su cumplimiento, implicando a

[73]La vicepresidenta del Gobierno destaca la finalidad de la Ley 36/2015 en el siguiente extremo textual: "Se pretende dotar al Estado con herramientas adecuadas para los nuevos riesgos y amenazas y tiene por fin el funcionamiento óptimo de los recursos de la Administración en la defensa de nuestros valores democráticos y recoge también una mejor coordinación cuando hay varios organismos implicados" Fuente Periodística." La Ley de Seguridad Nacional: mejorará la respuesta ante riesgos sin suspender derechos". Informativos 24 horas. RTVE. Agencia. Fecha 16.01.2015. [En línea, 2.08.2018]
http://www.rtve.es/noticias/20150116/ley-seguridad-nacional-mejorara-respuesta-ante-riesgos-sin-suspender-derechos/1082600.shtml

[74]Una de las características destacables de la Seguridad Nacional es que potencia la capacidad del liderazgo presidencialista del gobierno. En base a nuestra legislación corresponde al presidente la dirección de la acción del gobierno y la coordinación de las funciones de los demás miembros del mismo, de acuerdo con el artículo 2, de la Ley 50/1997, de 27 de noviembre, del Gobierno, en desarrollo del art. 97 CE. Esta competencia que también subyace en la Seguridad Nacional refleja desde el ámbito jurídico el llamado principio de dirección presidencial.

todas las Administraciones públicas del Estado en su cooperación con solidaridad y lealtad institucional, así como a todos los ciudadanos.

La *Seguridad Nacional* es un servicio público, que debe ser objeto de una política de Estado, lo que requiere la planificación y definición de principios y líneas de actuación permanentes capaces de dar respuestas integrales a los desafíos actuales. Es importante una continuidad en el tiempo y superar los marcos temporales y las políticas singulares de cada gobierno. Por este motivo, la *Seguridad Nacional* se apoya en el compromiso y el consenso de todos, para actuar de forma concertada y cohesionada.

La Estrategia de Seguridad Nacional del 2013[75] fue el marco político estratégico de referencia de la *Seguridad Nacional* como política de Estado y como muestra de gobernanza de la seguridad[76]. Este ámbito político se ocupa de "formular e implementar una estrategia nacional para crear un entorno favorable para los intereses nacionales […], la política de seguridad nacional es una parte de la política general del Estado; mientras que la Estrategia Nacional integra fines como la supervivencia, seguridad, integridad, bienestar o estabilidad de un Estado con los medios disponibles, sean militares o no"[77]. A través de ella, cada gobierno expresa "la visión que tiene del contexto estratégico que le rodea, los riesgos y oportunidades, el protagonismo que quiere ejercer y las prioridades que establece"[78].

### 3.3.2. La definición de la *Seguridad Nacional* como política pública

En efecto, estamos ante una política pública dirigida por el Presidente del Gobierno y por el *Consejo de Seguridad Nacional* a partir del concepto de «coordinación reforzada». La *Seguridad Nacional* deviene, así, un objetivo compartido entre los poderes públicos, la sociedad y también las Comunidades Autónomas, que supondrá la obligación de las autoridades competentes de

[75]Son documentos públicos de naturaleza política, no jurídica ya que su objetivo fundamental es orientar la conducción política.
[76]Ley 36/2015. Art. 4.3.
[77]Arteaga, F.; Fojón, E. (2007). *El Planeamiento de la Política de Defensa y Seguridad en España*. Instituto Universitario General Gutiérrez Mellado, Madrid, UNED. pp.37
[78]Arteaga, F. (2011): "Propuesta para la implantación de una Estrategia de Seguridad en España". *DT* 19/2011, Real Instituto Elcano, Madrid. pp.9

aportar los medios humanos y materiales necesarios que se encuentren bajo su dependencia, para la efectiva aplicación de los mecanismos de actuación, como una medida funcional y temporal en el marco del concepto que reitera la sentencia de "coordinación reforzada" y sin que pueda menoscabar las competencias autonómicas. Cooperación, que no imposición, como expresa la existencia de la *Conferencia Sectorial para asuntos de la Seguridad Nacional*. Por ello el art. 18 de la Ley 36/2015 configura el *Sistema de Seguridad Nacional,* al cual nos referiremos a continuación.

### 3.3.3. El Sistema de Seguridad Nacional en la Estrategia de Seguridad Nacional 2017

Desde el 2013 y hasta la actualidad, el entorno es más complejo y volátil. En el ámbito de la seguridad cambiante actual es "más convulso, caracterizado por la velocidad del cambio, los choques estratégicos y la proliferación de crisis"[79].

España, identificada como un país con vocación global, sigue estando condicionada su Seguridad Nacional por su singular enclave geoestratégico, crucial para definir prioridades y planificar los ámbitos temáticos de esta materia. La *Seguridad Nacional* se puede "ver comprometida" por ítems diferenciales según sean de naturaleza geopolítica, económica o social, entre otros.

Las amenazas que pueden tambalear la *Seguridad Nacional*, o los desafíos[80] que intervienen en la vulneración o materialización de otras amenazas; la particular importancia del valor de los espacios comunes globales, susceptibles de apropiación, como son el ciberespacio, el espacio marítimo y el espacio aéreo, cuyo buen uso es fundamental para la seguridad, han sido tensionados como espacios comunes globales objeto de competencia y confrontación. En esta tesitura, es igualmente relevante la importancia substancial de las infraestructuras críticas, por su provisión de servicios esenciales a la sociedad; sin olvidar el papel que tiene España como punto de mira, como antes lo fueron otros Estados europeos, en la oleada de atentados terroristas yihadistas, el último que azotó

[79]ESN 2017. op.cit. pp. 37

[80]La ESN 2017 establece la terminología de amenazas y desafíos en lugar de riesgos por una causa de ajuste de la terminología más significativa.

nuestro país, en agosto del 2017 en la ciudad de Barcelona, siendo uno de los principales problemas a los que se enfrenta la comunidad internacional.

Esta complejidad incierta del presente incentivó la necesidad de revisar la ESN 2013, antes de los cinco años previstos, y alumbró la *Estrategia de Seguridad Nacional. Un proyecto compartido de todos y para todos* (2017)[81].

Su procedimiento de elaboración fue gracias a la puerta que deja abierta la Ley 36/2015 de Seguridad Nacional, "cuando lo aconseje las circunstancias cambiantes del entorno estratégico" y, sin duda alguna, fue lo que consideró el *Consejo de Seguridad Nacional*, en su reunión ordinaria del 20 de enero del 2017, tras la aprobación del Informe Anual de Seguridad Nacional 2016[82].

En este sentido, también era fundamental establecer una Estrategia de Seguridad Nacional enmarcada en esta Ley, que permitiese ajustar y encauzar la garantía de participación del

> "conjunto de las Administraciones Públicas en los asuntos propios de dicha política pública de nuevo cuño y, en definitiva, de estructurar la organización y funcionamiento del *Sistema de Seguridad Nacional* como principal apoyo del Gobierno a la hora de impulsar el enfoque integral de la gestión de crisis".

Con la reciente Estrategia de Seguridad Nacional 2017, los principios rectores de *la política de Seguridad Nacional* permiten a España situarse, en materia de seguridad, en el contexto internacional actual y son los siguientes:

- ✓ Desarrollar el modelo integral de gestión de crisis;
- ✓ Promover una Cultura de Seguridad Nacional;

---

[81]El BOE del 16 de febrero de 2017 publica el acuerdo del CSN por el que aprueba el procedimiento de elaboración viene refrendado por la Orden PRA/116/2017 del Ministerio de la Presidencia y para las Administraciones Territoriales, de 9 de febrero, BOE 33/2017 de 16 de febrero de 2017. El 1 de diciembre de 2017, el DSN sometió a la consideración del CSN la nueva ESN 2017; para su remisión inmediata al Consejo de Ministros y su posterior aprobación mediante el Real Decreto 1008/2017, de 1 de diciembre, por el que se aprueba la Estrategia de Seguridad Nacional 2017. BOE núm. 309. Fecha de Publicación: 21.12.2017. Referencia: BOE-A-2017-15181; todo ello según acuerdo establecido en el art. 146 de la Ley 36/2015.

[82]Presidencia del Gobierno. *Informe Anual de Seguridad Nacional 2016*, aprobado por el Consejo de Seguridad Nacional en su reunión de 20 de enero de 2016 [En línea, 2.07.2018] http://www.dsn.gob.es/es/documento/informe-anual-seguridad-nacional-2016

- ✓ Favorecer el buen uso de los espacios comunes globales;
- ✓ Impulsar la dimensión de seguridad en el desarrollo tecnológico;
- ✓ Fortalecer la proyección internacional de España.

Además, aparte de incluir ámbitos tradicionales de actuación, como son la Defensa Nacional, la lucha contra el terrorismo, la ciberseguridad, o la lucha contra el crimen organizado. Establece hasta quince ámbitos pertinentes para ajustarse a las nuevas necesidades de la *Seguridad Nacional* como pueden ser la preservación del medio ambiente[83], incidiendo en la lucha contra el cambio climático, la seguridad frente a epidemias o pandemias y la seguridad del espacio aéreo.

En cuanto al *Sistema de Seguridad Nacional* (SSN), cabe resaltar que la dimensión orgánica que proyectaba la ESN 2013 permitía garantizar la defensa de España y sus principios y valores constitucionales. De esta forma, no sólo se trata la *Seguridad Nacional* desde una forma integral y como una política pública de Estado, sino que involucra a todas las AA.PP. y a la sociedad en general.

El *Sistema de Seguridad Nacional* es el conjunto de órganos, organismos, recursos y procedimientos, integrados en la estructura prevista en la Ley 36/2015, de Seguridad Nacional, que permite a los órganos competentes en materia de *Seguridad Nacional* ejercer sus funciones. Le corresponde evaluar los factores y situaciones que puedan vulnerar la *Seguridad Nacional*, recabar y analizar la información que permita ponderar las decisiones oportunas para dirigir y coordinar la respuesta del Estado frente las situaciones de crisis contempladas en esta ley, así como detectar las necesidades y proponer las medidas sobre planificación y coordinación con el conjunto del sector público, con la finalidad de garantizar la disponibilidad y el correcto funcionamiento de los recursos disponibles del sistema[84]. La reciente ESN 2017 ajusta la orgánica del *Sistema de Seguridad Nacional* a ámbitos óptimos de actuación y de gobernanza de la seguridad.

[83]La ESN 2017 se la considera, básicamente, una Estrategia de Seguridad Humana, por la inclusión del ámbito de la salud y el medioambiente. La Seguridad Humana es clave por primera vez en el *Informe del Programa de Desarrollo Humano* (PNUD) de la ONU de 1994, en el que también se aprobó el *Índice de Desarrollo Humano* conocido como IDH.

[84]Ley 36/2015. Art.19. y STC 184/2016 ya citadas.

El *Consejo de Seguridad Nacional*[85], en su condición de Comisión Delegada del Gobierno, es el máximo órgano que asume la defensa y la seguridad del Estado. El Consejo nació con el compromiso firme de desarrollar una propuesta de la, ya presente, Ley 36/2015 de Seguridad Nacional según establece la ESN 2013 y es en esta norma, en concreto, en su art. 20, donde se desarrollan su estructura, sus funciones y su composición. El Presidente del Gobierno dirige el *Sistema de Seguridad Nacional* y es asistido por el *Consejo de Seguridad Nacional* para acometer sus competencias.

La entrada en vigor de la Estrategia de Seguridad Nacional 2017 establece que "se abordará el diseño de la posición estratégica nacional respecto de la gobernanza y uso de los espacios comunes globales". Con este objetivo, se complementará, en primer lugar, la arquitectura orgánica y gobierno del *Consejo de Seguridad Nacional* con la génesis de un *Consejo de Seguridad Aeroespacial*. Y en segundo lugar, se ajustará el marco estratégico sectorial de los denominados espacios comunes a esta nueva Estrategia; supuesto que obligará tanto a revisar la vigente *Estrategia de Seguridad Marítima Nacional y de Ciberseguridad Nacional* como la *Estrategia de Seguridad Energética Nacional*, así como el desarrollo de una *Estrategia de Seguridad Aeroespacial Nacional*.

La composición del *Consejo de Seguridad Nacional* (CSN) viene regulada conforme a lo previsto en el apartado 8 del art. 21 de la Ley 36/2015, de Seguridad Nacional. El CSN informará a S.M. el Rey, como mínimo una vez al año, a propuesta de la Presidencia. Si S.M. el Rey asistiera a una de las convocatorias, lo

[85]El Consejo de Ministros, del 31 de mayo de 2013, aprobó la regulación del Consejo de Seguridad Nacional (CSN) mediante Real Decreto 385/2013, de 31 de mayo, de modificación del Real Decreto 1886/2011, de 30 de diciembre, por el que se establecen las Comisiones Delegadas del Gobierno, en su condición de Comisión Delegada del Gobierno para la Seguridad Nacional. La creación y puesta en funcionamiento del Consejo de Seguridad Nacional viene determinado por el soporte del art. 6, en conexión con el art. 1.3 ambos preceptos de la Ley 50/1997, de 27 de noviembre, del Gobierno que condiciona la naturaleza del Consejo en Comisión Delegada del Gobierno siendo necesaria la modificación del Real Decreto 1886/2011, de 30 de diciembre, por el que se establecen las Comisiones Delegadas del Gobierno. El Ejecutivo acordó con el PSOE su creación en el marco de la nueva ESN. Fue constituido, el 11 de julio de 2013, en un acto en el palacio de la Zarzuela, presidido por su Majestad el Rey D. Juan Carlos y con la presencia del Príncipe de Asturias, acompañados por el Presidente del Gobierno y vicepresidente del Gobierno, ministros y los jefes de las Fuerzas Armadas y del Centro Nacional de Inteligencia Véase "Nace el Consejo de Seguridad Nacional presidido por el Rey". Fuente periodística. elPaís, fecha 11.07.2013. [en línea, 28.02.2018] https://politica.elpais.com/politica/2013/07/11/actualidad/1373527931_448816.html

presidiría. Su convocatoria es bimestral o cuando se considere necesario relativo a la *Seguridad Nacional*. Sus funciones[86] consistirán en asistir al Presidente del Gobierno en la dirección de la *política de Seguridad Nacional*, en promover e impulsar la revisión de la ESN e impulsar Estrategias de segundo nivel para su aprobación, aprobar el Informe Anual de Seguridad para su presentación y el posterior debate en las Cortes Generales, realizar el control óptimo del funcionamiento del *Sistema de Seguridad Nacional*, así como las que sean atribuidas por el ordenamiento jurídico o por el propio Presidente.

La Ley 36/2015[87], de 28 de septiembre, de Seguridad Nacional, además de definir la *Seguridad Nacional*, de establecer los principios básicos de la política pública de este ámbito, también encauza y garantiza la participación del conjunto de las Administraciones públicas en los asuntos propios de dicha política. Es decir, es un mandato legal que atañe al Consejo al que le corresponde supervisar y coordinar al *Sistema de Seguridad Nacional*, como eje vertebrador de la ejecución de dicha política pública. Esta misma norma también contempla en el art.11.1, el mandato legal para que las respectivas Administraciones públicas competentes –enunciadas en el art.10- establezcan los mecanismos de coordinación e intercambio de información con el *Sistema de Seguridad Nacional* y, en especial, en relación con los sistemas de vigilancia y alerta ante posibles riesgos y amenazas.

Según se establece en la Orden PRA/16/2017[88], de 9 de febrero, el cumplimiento de dicho mandato legal está marcado por dos factores actualmente, en primer lugar, la constitución de la *Conferencia Sectorial para asuntos de la Seguridad Nacional* como instrumento de colaboración entre las CC.AA. y, en segundo lugar, llevar a cabo la ejecución de la homologación de los instrumentos de gestión de crisis que están plenamente relacionados con la participación de la

[86]Establecidas las responsabilidades competenciales en la propia ESN 2013.

[87]Concretamente el 20 de septiembre y el 5 de diciembre de 2013, el Consejo de Seguridad Nacional, bajo la presidencia del Presidente del Gobierno, fue convocado para adoptar acuerdos relativos al propio funcionamiento del Consejo, así como de sus recursos para el cumplimiento de sus funciones. Entre estos acuerdos subrayamos la creación de una Comisión Técnica para la elaboración del borrador de anteproyectos de la ya mencionada Ley 36/2015, de Seguridad Nacional, entre otros.

[88]Ministerio de la Presidencia y para las Administraciones Territoriales. Orden PRA/116/2017, de 9 de febrero, por la que se publica el Acuerdo del Consejo de Seguridad Nacional de Implementación de los mecanismos para garantizar el funcionamiento integrado del Sistema de Seguridad Nacional. BOE núm. 38. Publicado el 14 de febrero de 2017. Referencia: BOE-A-2017-1460.
https://www.boe.es/diario_boe/txt.php?id=BOE-A-2017-1460

Administración autonómica en los elementos que implementen el *Sistema de Seguridad Nacional*. Este precepto,

> "sintoniza a la perfección con la doctrina del Tribunal Constitucional expresada en la sentencia de 3 de noviembre de 2016 y que reafirma la constitucionalidad de los artículos 4.3, 15.b) y 24.2 de la Ley de Seguridad Nacional"[89].

Todo este contexto configura la necesidad de afrontar una segunda fase "de concreción de los mecanismos de enlace y coordinación" del conjunto de las AA.PP, correctamente homologados, con el *Sistema de Seguridad Nacional*.

En cuanto al *Departamento de Seguridad Nacional*[90] (DSN), creado en 2012[91], es el órgano de asesoramiento al Presidente del Gobierno en materia de *Seguridad Nacional* y ejercerá las funciones de Secretaría Técnica y órgano de trabajo permanente del Consejo y de sus órganos de apoyo, así como las demás funciones previstas en la normativa que le sea de aplicación. Como órgano de asesoramiento a la Presidencia del Gobierno, le corresponde dar el apoyo inmediato, óptimo e integral en materia de *Seguridad Nacional*, para la adecuada toma de decisiones, así como, además, entre otras responsabilidades[92]:

a) Elaborar estudios e informes de seguridad nacional.
b) Realizar la "alerta temprana" y el seguimiento de los riesgos y amenazas y situaciones de crisis en total coordinación con autoridades y órganos correspondientes.

---

[89] STC 184/2016

[90] Aplicación del Real Decreto 571/2013, de 26 de julio, de modificación del Real Decreto 83/2012, de 13 de enero, por el que se reestructura la Presidencia del Gobierno. BOE núm. 184, Publicado el 2 de agosto de 2013. Referencia: BOE-A-2013-8506 [en línea, 13.03.2018] https://www.boe.es/boe/dias/2013/08/02/pdfs/BOE-A-2013-8506.pdf. El DSN es el primer eslabón del proyecto de Seguridad Nacional. El DSN fue creado en 2012 para dar cumplimiento a la necesidad de reforzar la orgánica de la Presidencia del Gobierno para asistir al Presidente del Gobierno en su responsabilidad de dirigir la política de Seguridad Nacional de nuestro país. (Consultar el nuevo R.D. 766/2017, de 28 de julio, por el que se reestructura la Presidencia del Gobierno).

[91] Consultar Real Decreto 1119/2012, de 20 de julio, de modificación del Real Decreto 83/2012, de 13 de enero, por el que se reestructura la Presidencia del Gobierno. [en línea, 13.03.2018] https://www.boe.es/boe/dias/2012/07/23/pdfs/BOE-A-2012-9816.pdf.

[92] Web oficial del Departamento de Seguridad Nacional. Gabinete de la Presidencia del Gobierno. Gobierno de España. [en línea, 2.02.2018] http://www.dsn.gob.es/es/sistema-seguridad-nacional/departamento-seguridad-nacional

c) Asistir al Director del Gabinete de la Presidencia en calidad de Secretario del Consejo de Seguridad Nacional así como en representación del Gabinete en el ámbito de la seguridad.

d) Contribuir en propuestas normativas sobre la materia respectiva.

e) Analizar los riesgos y amenazas y los denominados potenciadores.

f) En relación a la gestión de situaciones de crisis, aporta la visión integral y transversal de la gestión de crisis y apoya todo el despliegue del Comité especializado.

g) Coordina los trabajos de elaboración de la Estrategia de Seguridad Nacional, así como las denominadas de segundo nivel.

h) Coordina la elaboración de los Informes Anuales de Seguridad Nacional.

El *Departamento de Seguridad Nacional*[93] por sus competencias vinculantes como órgano de asesoramiento al Presidente del Gobierno en materia de *Seguridad Nacional* y como Secretaría Técnica del *Consejo de Seguridad Nacional*, es el "centro neurálgico" que debe "entroncar" los mecanismos de enlace y coordinación entre los entes públicos de acuerdo con el art. 20.4 de la Ley 36/2015, de 28 de septiembre, para garantizar el funcionamiento integrado del *Sistema de Seguridad Nacional.*

### 3.4. POLÍTICAS EN LA LUCHA CONTRA EL TERRORISMO

Saliendo momentáneamente de nuestro ámbito y a modo de comparación, observamos como en los Estados Unidos, "las medidas antiterroristas han provocado que muchas autoridades locales rechacen la aplicación de parte de la legislación "convencional" y sostengan –como el Fiscal general Ashcroft- que la política de seguridad nacional ha pasado a ser objetivo principal de la política judicial, en perjuicio de los derechos civiles y las garantías constitucionales". Según Revenga, "lo que llaman en los Estados Unidos "guerra contra el

[93]Web oficial del Departamento de Seguridad Nacional. Gabinete de la Presidencia del Gobierno. Gobierno de España. Sistema de Seguridad Nacional. [en línea, 12.09.2018]
http://www.dsn.gob.es/es/sistema-seguridad-nacional

terrorismo", ha producido ya allí ciertas transformaciones en un modo de concebir la libertad política con una tradición de más de doscientos años"[94].

Estas medidas incidieron en la antesala de la reconsideración de derechos fundamentales, como libertad y seguridad personales, aumentándose el tiempo de duración de la detención preventiva, la tutela judicial efectiva, con la creación de tribunales de excepción, o el derecho a un proceso debido con todas las garantías al ser afectados los sistemas de recursos o pruebas, o el secreto de las comunicaciones telefónicas y a través de Internet, permitiendo la interceptación de comunicaciones telefónicas sin mandato judicial[95].

La Comisión creada en EEUU, a raíz de los ataques del 11-S, instaurada a finales de 2002, elaboró un exhaustivo y completo catálogo de las circunstancias que los produjeron. Esa Comisión hizo públicas sus conclusiones a finales de julio del 2004, entre las que se incluían 41 recomendaciones, en su mayoría dirigidas a la Intelligence Community. Todo este proceso cristalizó en la Intelligence Reformand Terrorism Prevention Act del 2004 (IRTPA). En ella, se contiene una definición de inteligencia nacional ampliada, que se extiende a todo tipo de información, *con independencia de la fuente de la que proceda y que incluye información obtenida dentro y fuera de Estados Unidos, comprendiendo de manera especial la relativa a la seguridad nacional*[96]. El presidente Bush el 26 de octubre el presidente sancionó la *Patriot Act*.

Se trata de una ley extensa y compleja que confiere inusuales poderes ejecutivos a estructuras operativas de control y a los servicios de inteligencia, derivando esta misma a la adopción en varios Estados de Fellow Patriot Act, que han introducido previsiones similares en materia de registros, embargos, poderes especiales y excepcionales del gobernador[97].

La Patriot Act consta de diez Títulos que modifican unas 15 leyes federales ya existentes, entre ellas, el Wiretap Statute, el Computer Fraud and Abuse, el

[94]REVENGA SÁNCHEZ, M., Garantizando la libertad y la seguridad de los ciudadanos en Europa: Nobles sueños y pesadillas en la lucha contra el terrorismo. Parlamento y Constitución, n.20,2006-2007, p.59.

[95]ÁLVAREZ, E Y GONZÁLEZ, H., Legislación terrorista comparada después de los atentados del 11 de septiembre y su incidencia en el ejercicio de los derechos fundamentales, Real Instituto Elcano, Área de Terrorismo Internacional, ARI n.7/2006 Madrid,2006, p.2.

[96]

[97]VERVAELE, J., La legislación antiterrorista en Estados Unidos…ob cit, p.12.

Foreing Intelligence Surveillance Act, el pen Register and Trap and Trace Statute, the Immigration and Nationality Act, el Money laundering Act y el Bank Secrecy Act En su Título II se amplía notablemente la posibilidad de investigación digital, sin exigir en todos los supuestos la autorización judicial. La interceptación de las comunicaciones sin autorización es posible ahora cuando se trate de investigaciones nacionales o internacionales cuya finalidad sea la salvaguarda de la seguridad nacional, para los datos registrados como mensajes de voz, o correos electrónicos. La Patriot Act no exige órdenes de interceptación ni siquiera se requiere la autorización para la interceptación de comunicaciones de sujetos sospechosos de haber cometido abusos informáticos. Todos los medios de comunicación que emplee el sospechoso pueden ser interceptados, y quien lleve a cabo la interceptación no debe quedar identificado en la solicitud ni en la orden de interceptación.

Las repercusiones de la Patriot Act también se han dejado notar en el ámbito de la protección de fronteras y leyes de inmigración. En estas áreas se amplían de 24 horas a 7 días el plazo para comunicar los motivos de la detención administrativa. En el plazo de estos 7 días, el interesado debe ser acusado de un delito o bien ser conducido ante el Ministerio Público en el procedimiento de expulsión. Sin embargo y por motivos de seguridad nacional el Fiscal general puede ampliar el plazo de detención a 6 meses y prorrogarlo varias veces. Amparados en esta legislación, el Fiscal general y el INS (Inmigration and Naturalization Service) ostentan un poder de detención a largo plazo sin precedentes, sin posibilidad de defensa y sin obligación de declarar expresamente en qué se basa con exactitud la amenaza para la seguridad nacional.

> "La política antiterrorista desarrollada por los Estados Unidos ha supuesto en los últimos años un profundo cambio que ha afectado también a las reglas del ordenamiento de la ONU al justificar con la máxima amplitud el recurso a la fuerza e incluso en casos extremos a la *guerra preventiva*, como se teoriza en la doctrina estratégica de Estados Unidos"

(The Nacional Security Strategy of the United States of America, septiembre 2002)[98].

[98]VERGOTTINI, G, D., Guerra y Constitución... ob cit.pág. 21.

En similar sentido, la política antiterrorista seguida por el Reino Unido en los últimos tiempos ha merecido la crítica del Comisario de Derechos Humanos del Consejo cuando el Primer Ministro Tony Blair presentó un proyecto de ley sobre seguridad, crimen y antiterrorismo (Antiterrorism, Crime and Security Act) que supuso la petición a la Cámara de los Comunes de la derogación del art. 5 de la Convención Europea de los Derechos Humanos y Libertades Fundamentales, que garantiza el derecho a la libertad y prohíbe la detención sin proceso judicial, en base a lo dispuesto en el artículo 15 de la Convención Europea que permite que los Gobiernos puedan derogar el citado artículo en tiempos de guerra o emergencia pública. Posteriormente, el 11 de marzo del 2005, sería aprobada en el Reino Unido la Ley de Prevención del Terrorismo (Prevention Terrorism Act), aplicable tanto a los nacionales como extranjeros, la cual, ante la imposibilidad de detener a los sospechosos de delitos de terrorismo sin una decisión judicial, introduce la figura de las llamadas "órdenes de control ", que permiten vigilar a los extranjeros, controlar sus movimientos e, incluso, arrestarlos en su domicilio. *La Ley antiterrorista alemana, permite el arresto domiciliario sin cargos de sospechosos terroristas y una serie de "medidas de control", como el toque de queda, la vigilancia con medios electrónicos o la prohibición de usar Internet* [99].

A diferencia de la Ley de 2001, no distingue en su aplicación entre ciudadanos británicos y extranjeros, para evitar el argumento utilizado por la Cámara de los Lores, cuando afirmó que la Ley de 2001 discriminaba entre uno y otros en su aplicación. Tanto la ley del 2001 como la del 2005, a juicio de Amnistía Internacional, contienen disposiciones de amplísimo alcance que contravienen la legislación de derechos humanos y que han producidos abusos graves. El 11 de junio de 2008, el Gobierno del Reino Unido veía por decreto ampliado el tiempo máximo de detención para sospechosos de terrorismo sin cargos de 28 a 42 días. No cabe duda de que todo lo expuesto comporta un ataque frontal a los postulados sobre los que se cimienta el Estado de Derecho, que se refleja en la disminución de las garantías hasta ahora consagradas, a través de los derechos fundamentales básicos.

[99] ALVAREZ, E., y GONZÁLEZ, H., ob. cit.pág.5

> "Asistimos a un momento crucial en la defensa de las libertades por cuanto los postulados en los que se asienta la lucha contra el terrorismo en EEUU y Reino Unido, como hemos observado, dejan a la deriva el barco de las libertades y de los derechos humanos".

En Alemania, con la aprobación el 19 de diciembre del 2008 por parte del parlamento alemán de la nueva ley de la BKA (policía criminal), vio ampliadas las competencias policiales, posibilitando, "en casos de urgencia", el espionaje online de ordenadores sin necesidad de autorización judicial, mientras que, en sintonía con el resto de los países de la unión, las compañías de telefonía deben mantener seis meses inalterables sus bancos de datos por si la policía necesitase recurrir a ellos. Son muy interesantes las reflexiones del filósofo alemán Meter Sloterdijk cuando, en relación con esta aprobación, manifestó que *lo que caracteriza nuestra época es el triunfo de la seguridad sobre la libertad. Los ciudadanos se han convertido en súbditos de la seguridad. La libertad es víctima de nuestro siglo*[100].

Por su parte, la nueva Ley antiterrorista aprobada en Francia en 2005 autorizó la videovigilancia en los transportes públicos, en las estaciones, Ministerios, comercios, sinagogas, iglesias y mezquitas. La policía tiene acceso directo a las imágenes. La nueva Ley aprobada, no sólo aborda la videovigilancia, sino que, además, establece la obligación de que los operadores de telecomunicaciones conserven durante un año los contenidos de las conexiones a Internet, las conversaciones telefónicas de los usuarios y, especialmente, reforzando esa inspección en los cibercafés. Los propietarios están obligados a conservar esos datos de transmisión. Los teléfonos celulares también son objeto de vigilancia por esta ley. Además, las compañías aéreas, ferroviarias y marítimas deben guardar los datos de sus clientes, al menos, durante doce meses. Asimismo, la ley amplía el plazo de presentación de los detenidos ante la Justicia de cuatro a seis días. La referida ley supone, también, la posibilidad de que los servicios policiales puedan instalar sistemas de vigilancia fotográfica de vehículos, fotografiar a sus ocupantes y guardar las imágenes durante ocho días sin tener que pedir un mandamiento judicial. En este orden de cosas, hemos de recordar que la Directiva europea de 15 de marzo del 2006 obliga a los Estados miembros a almacenar durante dos años los datos de comunicación de sus ciudadanos.

[100] ibidem. p 97

## 3.5. EL TRATAMIENTO DE DATOS EN LA SEGURIDAD

El descubrimiento de escuchas masivas no ha generado más que incertidumbre y desconfianza en amplios sectores de la población mundial. En el espionaje masivo de datos el ciudadano siente que el halo de privacidad con el que actúa e interactúa en su vida privada —y que es lo que le hace sentirse en libertad— está en peligro. Es cuando, la pretendida búsqueda de la seguridad nacional, acaba erosionando la «seguridad» que uno tiene en que hay un espacio en el que puede actuar sin controles y que hay una información que corresponde a ese espacio privado y que no goza de mayor relevancia o de la que no se pueden derivar mayores consecuencias. El conjunto de metadatos que se pueden almacenar sobre los ciudadanos es incalculable y puede ir desde una información muy sensible (ej. Datos sobre salud) hasta otros datos que, aisladamente considerados, pudieran parecer no tener gran valor, como por ejemplo quién es el titular de un determinado móvil.

Cabe plantearse, como interpreta Serra Cristóbal,

> "si del tratamiento de estos datos se puede producir una invasión en mi vida privada, dado que la jurisprudencia y numerosos textos supranacionales han considerado el tratamiento de los datos de carácter personal como una cuestión en la que puede verse afectado el ámbito de la intimidad/privacidad[101] del individuo"[102].

Si, además, se cruzan determinados datos de tráfico (identificación de llamadas, interlocutores en mensajes electrónicos…) y se tratan los mismos mediante determinados programas o técnicas informáticas que permiten conocer los interlocutores en una comunicación electrónica o, incluso, el contenido de la comunicación misma podría quedar menoscabado el derecho a la inviolabilidad del secreto de las comunicaciones. Es indudable que, de un modo u otro, la recolección y almacenamiento de datos sobre comunicaciones, —que, entre otros, se produce por los servicios de inteligencia—, puede ir más allá de la mera recolección de datos o, incluso, tratarse de un control prospectivo del contenido

[101]Sobre el ámbito de la privacidad o vida privada, vease, MARTÍNEZ MARTÍNEZ, R., (2005): Una aproximación crítica a la autodeterminación informativa, Madrid, Civitas, pp. 35-44.

[102]Vease RUIZ MIGUEL, C., (2003): «El derecho a la protección de los datos personales …ob cit, pp. 7-43.

mismo de las comunicaciones. Los servicios de inteligencia durante sus actividades de vigilancia,[103] deben velar por el respeto a la legalidad vigente y a que el tratamiento de los datos goce de todas las garantías, —máxime, cuando afectan a la intimidad y más aún, si interfieren en el secreto de las comunicaciones—.

Cuando se trata de recabar datos derivados de comunicaciones que puedan afectar al secreto de estas (escuchas telefónicas o electrónicas), nuestra Constitución exige la autorización de un juez, sin necesidad de distinguir entre interceptaciones individuales de comunicaciones o vigilancia masiva de comunicaciones (art. 18.3 CE). Y cuando dichos controles tienen que ser realizados por los servicios de inteligencia en el marco de sus funciones, la Ley Orgánica 2/2002, reguladora del control judicial previo del Centro Nacional de Inteligencia, indica que

> "el Secretario de Estado Director del Centro Nacional de Inteligencia deberá solicitar al Magistrado del Tribunal Supremo competente, conforme a la Ley Orgánica del Poder Judicial, autorización para la adopción de medidas que afecten a la inviolabilidad del domicilio y al secreto de las comunicaciones, siempre que tales medidas resulten necesarias para el cumplimiento de las funciones asignadas al Centro".

Además, el Tribunal Europeo de Derechos Humanos (TEDH) ha realizado también un loable trabajo de protección de los derechos humanos, en el marco de la lucha contra el terrorismo y, en concreto, en la protección de intimidad/privacidad cuando se llevan a cabo programas de vigilancia general o

[103]El sistema de escuchas telefónicas SITEL utilizadas por las fuerzas de seguridad del Estado y por los servicios del Centro Nacional de Inteligencia españoles es un avanzado sistema electrónico que permite interceptar y grabar en tiempo real cualquier conversación telefónica, correo electrónico o mensaje de móvil, además de almacenar en formato digital todos los datos de esas comunicaciones para su posterior análisis. En todo caso, en principio, este sistema de vigilancia sólo puede ser utilizado con autorización judicial previa. Una descripción técnica de este sistema pude encontrarse en la STS 250/2009, de 13 de marzo. Citado en; SERRA CRISTÓBAL, R., "La opinión pública ante la vigilancia masiva de datos. El difícil equilibrio entre acceso a la información y seguridad nacional". En *Revista de Derecho Político* N.º 92, enero-abril 2015, p 99.

interceptaciones estratégicas, exigiendo no solo una habilitación legal, sino una previsión legal que sea precisa y respetuosa con los derechos fundamentales[104].

De las regulaciones jurídicas anteriores, podemos afirmar la necesidad ineluctable de que la lucha contra el terrorismo, en sus diversas manifestaciones, se debe realizar dentro de los límites del Estado de Derecho y de la democracia constitucional. La doctrina del TEDH nos parece un buen referente para no caer en los abusos de la lucha contra la inseguridad y en especial el terrorismo: la garantía del derecho a la seguridad de los ciudadanos como deber del Estado, el respeto íntegro a los derechos y libertades reconocidos en el convenio, así como las garantías y controles precisos en las limitaciones o restricciones de los derechos de las personas (intimidad, secreto de las comunicaciones, protección de datos personales, privación de libertad) , aunque el TEDH ha reconocido que tal tipo de vigilancia prospectiva es a veces necesaria, exigiendo una previsión legal que la regule y que sea precisa y respetuosa con los derechos fundamentales, que exista proporcionalidad en el ejercicio de tales prácticas y una autoridad externa independiente que las supervise.[105]

En este sentido, nuestra LO 15/1999, de protección de datos, no se aplica a los ficheros sometidos a la normativa sobre materias clasificadas o a los establecidos para la investigación del terrorismo (art. 2), los principios básicos que informan dicha Ley no dejan de tener pertinencia también en ese tipo de información recabada, almacenada y tratada por los servicios de inteligencia. Son principios que informan, entre otras cosas, cuándo se pueden recopilar datos, cuándo pueden cederse o qué medidas de seguridad se adoptan para evitar el

[104]SSTEDH asunto; Valenzuela Contreras c. España, de 30 de julio de 1998; SSTEDH asunto; Padro Bugallo c. España, de 18 de febrero de 2003; SSTEDH asunto; Dulkarin Coban c. España, de 26 de septiembre de 2006 etc.

[105]SSTEDH asunto Murray c. the United Kingdom, 28 de octubre de1994, La Corte, en primer lugar, reiterar su reconocimiento de que el uso de información confidencial es esencial en la lucha contra la violencia terrorista y la amenaza que el terrorismo organizado representa para la vida de los ciudadanos y para la sociedad democrática en su conjunto. Esto no significa, sin embargo, que las autoridades investigadoras tengan carta blanca…». SSTEDH asunto Kopp C. Switzerland, 25 de marzo de 1998, «la grabación y otras formas de interceptación de conversaciones telefónicas constituyen una grave injerencia en la vida privada y la correspondencia y en consecuencia debe ser basada en una «ley» que sea particularmente precisa. Es indispensable contar con reglas claras y detalladas sobre el tema, sobre todo porque la tecnología disponible para ello se está haciendo cada vez en más sofisticada. Citado en; SERRA CRISTÓBAL, R., "La opinión pública ante la vigilancia masiva de datos… ob cit. p 101.

acceso de terceros. Estos principios son los de consentimiento, necesidad y seguridad y todos ellos, lógicamente, dentro de la finalidad expresa por su autorización, para la que fueron recabados.

El principio de consentimiento, al igual que queda excepcionado por la Ley de Protección de datos para los ficheros de los cuerpos de seguridad del Estado, también queda excepcionado por la Ley reguladora del Centro Nacional de Inteligencia por el carácter secreto de toda información de inteligencia que generen dichos servicios (art. 5). Por lo tanto, no podemos decir que exista un derecho a acceder a los ficheros producto de la vigilancia prospectiva para inteligencia, como tampoco es necesario nuestro consentimiento para que se recaben esos datos.

El principio de necesidad, que exige que solo se puedan tratar datos cuando sean adecuados, pertinentes y no excesivos, obligaría a analizar en cada caso si estamos ante una actividad de recogida y tratamiento de datos que responda a un interés que justifique suficientemente la necesidad de llevarla a cabo, dado que es necesaria la justificación porque, como hemos indicado, de tal vigilancia y tratamiento de datos pueden derivarse posibles daños para los derechos de los ciudadanos, fundamentalmente, para la salvaguarda de la privacidad/ intimidad y el derecho a la autodeterminación informativa de los titulares de tales datos y, en ocasiones, para el secreto de las comunicaciones. Afirmando Serra Cristóbal, *que la recogida y tratamiento de datos personales y de comunicaciones, debiera producirse sólo cuando sea realmente necesario para la salvaguarda de la seguridad.*

El principio de seguridad exige que los datos con los que operan los servicios de inteligencia por su carácter sensible se salvaguarden mediante modos de encriptación. *La preocupación por la seguridad de las bases de datos sobre información clasificada ha estado presente en la UE desde hace años, en cuyo marco se han ido adoptando normas de seguridad para la protección de la información clasificada*[106].

La Orden Ministerial 76/2006, de 19 de mayo, la política de seguridad de la información del Ministerio de Defensa, mejoro las previsiones que existían en

[106]Decisión del Consejo 2001/264/EC, sobre las normas de seguridad del Consejo. Estas normas fueron modificadas en 2011, Decisión del Consejo 2011/292/UE, de 31 de marzo de 2011, sobre las normas de seguridad para la protección de la información clasificada de la UE. Citado en; Serra Cristóbal, R., "La opinión pública ante la vigilancia masiva de datos… ob cit. p 104

cuestión de seguridad de la información[107], mientras que el Real Decreto 3/2010, de 8 de enero, se centró en regular el Esquema Nacional de Seguridad en el ámbito de la Administración electrónica, generando confianza sobre los medios electrónicos en la relación entre el ciudadano y la Administración Pública.

### 3.6. BIG DATA COMO HERRAMIENTA DE LA SEGURIDAD Y LA DEFENSA

De manera genérica, podemos decir que la aplicación de "Big Data" a la defensa y seguridad persigue capturar y utilizar grandes cantidades de datos para poder aunar sensores, percepción y decisión en sistemas autónomos y para incrementar significativamente el que el entendimiento de la situación y contexto del analista y el combatiente o el agente del orden[108]. Para poder trabajar con la creciente complejidad y abundancia de datos, es necesario un mayor enfoque en la comprensión de la situación, especialmente, en aquellos ámbitos donde los objetivos (blancos, enemigos, criminales, etc.) son en apariencia de pequeña escala y/o de carácter ambiguo. En este sentido, para un mayor cribado direccionado a la creación de inteligencia de las fuentes abiertas que trataremos, aludiremos la inteligencia denominada OSINT, acrónimo derivado de su nombre en inglés *Open-source Intelligence*[109].

Aunque *osint*, ya hemos abundado, no es un término nuevo, si cabe, igualmente se ve necesaria su redefinición, dado que la consideración que se le

---

[107]Entre otras, las que se contemplaban en el Decreto 242/1969, de desarrollo de la Ley de Secretos oficiales; Orden Ministerial 12/1982, de 21 de octubre, del manual de seguridad industrial de las Fuerzas Armadas; Ley 15/1999, de protección de datos, ibídem p 105

[108]CARRILLO RUIZ, J,A et al.: "Big data en los entornos de defensa y seguridad" documento resultado del grupo de trabajo sobre big data, de la comisión de investigación de nuevas tecnologías del centro superior de estudios de la defensa nacional. (CESEDEN) Documento de Investigación del Instituto Español de Estudios Estratégicos (IEEE) 03/2013. Pag 44.

[109]Tipo de inteligencia elaborada a partir de información que se obtiene de fuentes de información de carácter público, comprendiendo cualquier tipo de contenido, fijado en cualquier clase de soporte, papel, fotográfico, magnético, óptico etc. que se transmita por el medio y que se puede acceder en modo digital o no, y a disposición pública, difundido por canales restringidos o gratuitos. Podemos considerar fuentes abiertas de ámbito OSINT:

- Datos extraíbles de la Internet abierta, frecuentemente de la web abierta.
- Estudios e informes, *white papers,* revistas especializadas y otras fuentes de literatura gris.
- Repositorios abiertos, tanto públicos como privados.
- Registros administrativos públicamente accesibles.

prestaba radicaba principalmente en que, desde antaño, mantenía un concepto tradicional de recopilación de información, igualmente de fuentes abiertas, pero basado, fundamentalmente, en el estudio de televisión y prensa extranjera, entrevistas con los hombres de negocios o turistas a la vuelta de un viaje o colaboraciones con expertos académicos. Son embargo, el aumento actual de la capacidad de almacenamiento de información residenciado en las fuentes abiertas web, y que ha crecido exponencialmente en los últimos años, genera cada día una enorme cantidad de información consciente o inconscientemente [110] , evidenciándose las potencialidades de Internet y sus alcances globales, convirtiéndolo en una suerte de actor en el escenario internacional en el marco de la era de la información.

El principal documento[111] de la OTAN sobre OSINT[112] identificaba cuatro categorías en las fuentes abiertas:

- OSD (Open Source Data; Datos de fuentes abiertas): impresión en bruto, radiodifusión, informe oral u otra forma de información de una fuente primaria, como una fotografía, una grabación, una imagen de satélite comercial, etc.

- OSIF (Open Source Information; Información de fuentes abiertas): integrada por datos que se agrupan generalmente por medio de un proceso de edición que proporciona algún tipo de filtrado y validación, así como una gestión de su presentación.

- OSINT (Open Source Intelligence; Inteligencia de fuentes abiertas): información que deliberadamente ha sido obtenida, discriminada, extraída y desimanada a personas seleccionadas, todo ello con objeto de responder a una pregunta o tema específico.

---

[110]Como por ejemplo cuando se reserva un billete de avión, se paga con una tarjeta de crédito, se entra en un servidor para ingresar el e-mail, se participa o es participado en una red social, blogs, foros de Internet o sencillamente se interactúa ante la infinidad de sensores de las ciudades inteligentes (Smart Cities).

[111]En ; http://www.nato.int/cps/en/natohq/topics_68372.htm?selectedLocale=en
OTAN Open Source Inteligencia Manual,
OTAN Open Source Inteligencia Reader
OTAN Inteligencia explotación de la Guía de Internet.

[112]El concepto OSINT, tiene su origen en los Estados Unidos como método de inteligencia analítica estandarizado y diseñado para cumplir tareas específicas o toma de decisiones de apoyo. No debe ser confundido con el OSIF, que representa toda la información a disposición del público de código abierto que se basa los análisis OSINT.

• OSINT Validada (OSINT-V): información a la que se puede atribuir un muy alto grado de certidumbre. Puede ser producida por un profesional de inteligencia de todo tipo de fuente, con acceso a las clasificadas, trabajando para una nación o como personal de una coalición.

En este sentido, la creciente importancia de las fuentes abiertas ha llevado a la creación de organismos específicos, como el estadounidense Open Sources Center (OSC)[113], mientras que, en la Unión Europea, se han llevado a cabo iniciativas como el Eurosint[114], orientado a la cooperación europea en materia de inteligencia y al uso intensivo de las fuentes abiertas para elaborar inteligencia en la prevención de amenazas para la paz y la seguridad. Por ejemplo, uno de los *think tanks* más importantes del mundo, SIPRI[115] (Stockholm International Peace Research Institute), que es un instituto de estudios estratégicos, dedicado a la investigación de los conflictos, a la producción, comercio y control del armamento, al gasto militar, la prevención de los conflictos y la seguridad internacional. En el caso británico, podemos dar relevancia al NEC[116], que es una red que engloba 10 redes especializadas. Sin olvidar igualmente el potencial de la NSA[117] para abarcar también este campo de estrategia. La OTAN dispone del sistema se NNEC[118], similar en la teoría al sistema británico.

---

[113] Véase; https://www.cia.gov/news-information/featured-story-archive/2010-featured-story-archive/open-source-intelligence.html

[114] Véase; https://www.eurosint.eu/

[115] Ver en: http://www.sipri.org/

[116] En el NEC británico hay un enlace directo entre el nivel Estratégico y el Táctico, lo que abunda en la idea de que en las situaciones actuales de "asimetría", el nivel Táctico se convierte, muchas veces, en Operativo y que los medios tecnológicos del nivel Estratégico pueden trabajar directamente para el Táctico.

[117] La (NSA) National Security Agency es responsable de la protección, desarrollo y control de las comunicaciones militares y administrativas, el desarrollo de las tecnologías de la información, la seguridad de las redes informáticas, el espionaje vía satélite y la coordinación de la guerra en el espacio, entre los Estados Unidos y los servicios de información de Reino Unido, Canadá, Australia y Nueva Zelanda entre otros. En todo el mundo, todas las comunicaciones por correo electrónico, teléfono y fax son regularmente interceptadas por Echelon, cuyos ordenadores extraen de la masa de informaciones los mensajes que contengan palabras-clave sensibles".

[118] Para la OTAN, el NNEC representa el enfoque y la política común para armonizar el uso de las nuevas tecnologías, con la finalidad de usarlas en futuras misiones. El problema que se planteará es que la OTAN no tiene órganos propios de Inteligencia y que depende de los de las naciones aliadas.

### 3.6.1. Las nuevas tecnologías que almacenan datos y su encuadre dentro de la estrategia

Actualmente, los sistemas de ayuda al mando en la toma de decisiones, formados fundamental por los órganos de inteligencia, están evolucionando hacia un "sistema de sistemas", en el que se integran en una única red sensores, decisores, plataformas varias e inteligencia, con la finalidad de aumentar la capacidad de acción de las fuerzas para una mejor explotación de la información, mediante la superioridad que supone la obtención de información relevante y decisiva para el combate, a través de la explotación oportuna de inteligencia, siendo válido, tanto para la batalla convencional, como para el enfrentamiento asimétrico.

En la inteligencia de código abierto, la recopilación de información difiere, generalmente, de las diferentes disciplinas de la inteligencia que hemos referenciado, consolidándose en las agencias de inteligencia una nueva conceptualización de la estrategia operacional basada en estos recursos, básicamente, porque la obtención de información en bruto a analizar puede ser un desafío importante, especialmente si son objetivos no cooperativos, tanto si está residenciada en fuentes abiertas[119] o en la minería de datos[120]. En este mismo

[119]Por su parte MARTÍN DE SANTOS, I. Y VEGA, A. M.: «Las fuentes abiertas de información: un sistema de competencia perfecta», en Inteligencia y Seguridad: revista de análisis y prospectiva, número 8, pp. 91-112, junio-noviembre de 2010. "Las fuentes abiertas de información incluyen tanto la Internet superficial como la profunda (también llamada invisible), el correo electrónico, así como las fuentes de los medios de comunicación tradicionales, incluyendo los medios dirigidos a un público específico y boletines especializados y de los foros de discusión en línea. Se incluye la literatura gris, expertos (o especialistas) en determinados temas y cualquier persona que tenga conocimiento de algo por haber sido testigo directo de ello o haberlo vivido". Por otra parte, IRAVEDRA, J. C.: «Inteligencia de fuentes abiertas en la Unión Europea (proyecto Virtuoso)», Jornadas de Estudios de Seguridad, 17, 18 y 19 mayo de 2011, La seguridad y la defensa en el actual marco socioeconómico: nuevas estrategias frente a amenazas, Instituto Universitario «General Gutiérrez Mellado»- Universidad Nacional de Educación a Distancia, Madrid, 2011. dice que: "Fuentes abiertas son las que no están clasificadas".

[120]La minería de datos o data mining o "el arte de sacar conocimiento de grandes volúmenes de datos" es una técnica que "consiste en extraer información de los algoritmos que contienen las grandes bases de datos que acumulan la historia de las actividades de las organizaciones" MARTÍNEZ, GILBERTO L.: "Minería de datos: Cómo hallar una aguja en un pajar", Ingenierías, 53 2011. págs. 55-63 Las redes de transmisiones digitalizadas, con su gran capacidad y velocidad de transmisión, permiten que las comunicaciones tácticas y, dentro de ellas, de las utilizadas por los órganos de Inteligencia. Como ejemplo; en la primera guerra de Irak, una fuerza de 500.000 hombres

contexto de fuentes abiertas, se está produciendo un gran movimiento alrededor de lo que se conoce como Open Data, implicando que los datos puedan ser utilizados, reutilizados y redistribuidos libremente por cualquier persona y que se encuentran sujetos, cuando más, al requerimiento de atribución y de compartirse de la misma manera en que aparecen, siendo sus características fundamentales las siguientes:

- Disponibilidad y acceso: la información debe estar disponible como un todo y a un costo razonable de reproducción, preferiblemente, descargándola de internet. Además, la información debe estar disponible en una forma conveniente y modificable.

- Reutilización y redistribución: los datos deben ser provistos bajo términos que permitan reutilizarlos y redistribuirlos, e incluso integrarlos con otros conjuntos de datos.

- Participación universal: todos deben poder utilizar, reutilizar y redistribuir la información.

El termino recientemente acuñado en el diccionario LID de Inteligencia y Seguridad[121] de (SOCMINT) y definido como la "actividad de inteligencia referida a las redes sociales y medios sociales de comunicación de plataforma digital y los datos que las mismas generan" y que podríamos esquematizarlo según Álvarez y Perdomo[122] como la interacción entre las funciones y roles de las redes sociales, vuelcan la Inteligencia de Fuentes Abiertas (OSINT), creándose la Inteligencia en Redes Sociales (SOCMINT), las interrelaciones entre los medios de comunicación tradicionales y los medios con soportes en redes sociales y web 2.0 (social media/mass media), las operaciones de activismo en la red (hactivism) y la ingeniería social.

La web 2.0 supuso un cambio en el modo de comunicación de los usuarios en Internet, de forma que los usuarios dejan de ser meros receptores de

---

disponía de 100Mbits de banda ancha; unos 12 años más tarde, los 350.000 combatientes de la "Operation Irak Freedom", en la segunda guerra de Irak se apoyaban en 3.000Mbits.

[121] Vease: https://www.google.es/search?q=dicionario+LID+inteligencia&ie=utf-8&oe=utf-8&gws_rd=cr&ei=iX3UVbu8CobnUtTUr8gN#q=diccionario+lid+inteligencia+y+seguridad+pdf

[122] ALVAREZ ALVAREZ, L, A Y PERDOMO CORDERO, C.: "Inteligencia, Cibereguridad y Ciberdefensa; nuevas implicaciones conceptuales en las Estrategias de Seguridad Nacional." Universidad de Las Palmas de Gran Canaria, ULPGC.2002.

información y comienzan a ser generadores de esta; como ejemplo, lo supone el que hoy en día, la mayor parte de los usuarios forman parte de las redes sociales, disponen de sus propios blogs o participan en foros que provocan que el volumen de información disponible haya crecido de forma exponencial en los últimos años.

Este bruto ingente de información[123], que se puede obtener a través de la obtención, gestión, integración, análisis, filtrado, refinamiento y síntesis de la información ubicada en todo tipo de soportes y formas de transmisión y comunicación de información en las fuentes web[124], se cimienta, generalmente, en el pasado; pero, a los efectos de obtener inteligencia, es útil para comprender el presente y hacer predicciones futuras, ya que normalmente, las decisiones se basan en experiencias pasadas, siendo posible identificar tendencias, anomalías y amenazas, destacándose, por tanto, la importancia del papel de los profesionales que gestionen estas fuentes aplicadas a la seguridad, la defensa nacional así como la toma de decisiones en general.

Por su parte, OSINT acrónimo derivado de su nombre en inglés *Open-source Intelligence*[125] en los últimos años, a causa del desarrollo tecnológico en la era de la

[123]La proliferación del uso de Internet y la facilidad de publicación de contenidos a través de diferentes medios como redes sociales o blogs ha favorecido que se almacene una ingente cantidad de información online. Las cifras más significativas son las siguientes:

- Usuarios de Internet; aproximadamente 2.500 millones de usuarios.
- Únicamente el servidor Google, almacena 30 billones de páginas web, o lo que es lo mismo, más de 1.000 terabytes de información
- La red social Facebook tiene más de 1.000 millones de usuarios, 60 millones de páginas y 270.000 millones de fotos subidas.
- La red social Twitter tiene cerca de 240 millones de usuarios activos que escriben diariamente cerca de 600 millones de tweets.
- La red social Tumblr tiene cerca de 180 millones de blogs y alrededor de 55.000 millones de posts.
- La red social Flickr tiene casi 90 millones de usuarios y más de 10.000 millones de fotos.
- La red social Instagram cuenta con más de 350 millones de usuarios activos, que han subido 30 billones de fotos desde el 2010. Aproximadamente se suben a la red social 5 millones de fotos diariamente

Estos son algunos de los datos representativos más conocidos, sin mencionar la cantidad de información disponible en la DEEP WEB, así como también aquella información no accesible para el usuario común, pero existente dentro de la Web en capas invisibles o profundas, cuyos contenidos no son accesibles desde motores de búsqueda comunes y conocida como *WEB DATA MINING*.

[124]No olvidemos que la World Wide Web tiene un origen como experimento y herramienta militar.

[125]Tipo de inteligencia elaborada a partir de información que se obtiene de fuentes de información de carácter público, comprendiendo cualquier tipo de contenido, fijado en cualquier clase de soporte, papel, fotográfico, magnético, óptico etc. que se transmita por el medio y que se puede

información, la inteligencia *osint* amplía su rango de acción a una clase de Inteligencia que tiene por objeto la realización de productos de valor añadido a partir de información procedente igualmente de fuentes abiertas como las descritas, y particularmente las fuentes abiertas residenciadas en páginas web, contribuyendo así a ampliar el rango de necesidades actuales de información, como producto de inteligencia, que en su defecto, o sin dedicarle la atención oportuna, esta corre el riesgo de estar permanentemente desactualizada.

Determinados los alcances e importancia de OSINT, hemos de revelar nuevamente que este no es un concepto moderno, siquiera en su actual entendimiento, pues ya desde hace más de una década, la OTAN le concede especial relevancia, como lo evidencia el ejemplo del programa (EUSC) formado por un centro de satélites dedicado a la producción y explotación de inteligencia a partir de información de origen espacial, por medio del análisis de datos de satélites comerciales. También la Agencia Europea de Defensa (EDA) ha puesto en marcha programas de desarrollo de herramientas de prospectiva y análisis OSINF y de formación de inteligencia OSINT.

En este sentido y como impulsor, destacan principalmente los Estados Unidos, cuyos servicios de inteligencia han concedido una gran importancia a OSINT mediante la transformación, en 2005, del Servicio de Información de Emisiones del Exterior (FBIS) en el Centro de Fuentes Abiertas (OSC), incorporado OSIF y OSINT, en sus rutinas de Inteligencia militar, implantado la red IKN (Intelligence Knowledge Network), que proporciona servicios de inteligencia al Ejército. Francia, por su parte, está impulsando la plataforma HERISSON (Habile Extraction du Renseignement d´intéret Stratégique a partir de Sources Ouvertes Numérisées) de integración de información de fuentes abiertas. Veremos en el siguiente epígrafe algunas otras más relevantes al respecto de la inteligencia militar.

---

acceder en modo digital o no, y a disposición pública, difundido por canales restringidos o gratuitos. Podemos considerar fuentes abiertas de ámbito OSINT:

- Datos extraíbles de la Internet abierta, frecuentemente de la web abierta.
- Estudios e informes, *white papers,* revistas especializadas y otras fuentes de literatura gris.
- Repositorios abiertos, tanto públicos como privados.
- Registros administrativos públicamente accesibles.

• Requisitos: En esta etapa se establecen los parámetros mínimos y máximos que deben satisfacerse para conseguir el objetivo que ha activado el desarrollo del sistema.

• Fuentes de información: Esta etapa consiste en identificar a partir de los parámetros establecidos, las fuentes de interés que serán recopiladas.

• Adquisición: En esta etapa se obtiene la información a partir de los orígenes indicados.

• Procesamiento: Esta etapa consiste en dar formato a toda la información recopilada para que posteriormente pueda ser analizada discriminándola del bruto obtenido.

• Análisis: En esta etapa se genera inteligencia a partir de los datos recopilados y procesados, habiendo relacionado la información buscando los patrones que permitan llegar a conclusiones significativas.

• Inteligencia: Esta etapa consiste en presentar la información potencialmente útil y comprensible, para que pueda ser correctamente explotada

### 3.6.2. Relevancia estratégica de las bases de datos en fuentes abiertas

La doctrina discute acaloradamente, tanto los beneficios de la web, como los perjuicios que esta supone, pues el acceso de la información no es ajeno a ser utilizada de modo legal o ilegal, no pudiendo discriminar ningún servicio hasta la fecha la calidad del demandante de información. Este será un reto de futuro para la WWW, poder discriminar el usuario final basándose, igualmente, en las propias informaciones web para detectar quién es el usuario final o, al menos, si se discute la utilización más o menos legal de la información a la que accede. Estas son bases de datos que indizan estáticamente sus páginas por lo que, cuando buscamos información en cualquiera de los buscadores propuestos, únicamente se arroja información que pueda esta residenciada en ese buscador, omitiéndose gran cantidad de información residenciada en las restantes webs, así como en el internet profundo propio de la estructura de la *World Wide Web* en forma de tela de araña que, aunque pueda enlazar unas páginas con otras, hace que aquellas que no tengan enlaces indexados propios, no puedan ser localizados por los motores de búsqueda aunque sí permanezcan en la parte invisible de la Red.

También podemos utilizar los enlaces que aparecen en las páginas *web* de instituciones o *think tank*s más importantes de referencia, etc. por ejemplo *Completeplanet*[126] que tiene un apartado específico para bases de datos de temas militares, así como especialmente la página SIPRI[127], *(Stockholm International Peace Research Institute) que* es un instituto internacional de estudios estratégicos, dedicado a la investigación de los conflictos y al control de armamento y al desarme.

En la página *web* de SIPRI podemos consultar seis bases de datos.

*- SIPRI Facts on International Relations and Security Trends*

Base de datos que ofrece información sobre las relaciones internacionales y las tendencias de seguridad.

*- SIPRI Multilateral Peace Operations Database*

Base de datos que ofrece información sobre todas las operaciones de paz llevadas a cabo desde el año 2000, incluyendo la ubicación, las fechas de implementación y el funcionamiento, el mandato bajo el que se llevan a cabo, países participantes, el número de personas empleadas, costes económicos y bajas.

*- SIPRI Military Expenditure Database*

Base de datos que ofrece que recoge información sobre el gasto militar de 172 países desde el año 1988.

*- SIPRI Arms Transfers Database*

Base de datos sobre transferencias internacionales de armas, agrupadas en siete categorías de armas convencionales.

*- SIPRI Arms Embargoes Database*

Base de datos que ofrece información sobre todos los embargos de armas que han sido llevados a cabo por una organización internacional, como la Unión Europea o la Organización de Naciones Unidas, desde 1998.

*- SIPRI National Reports Database*

[126]Ver: *http://aip.completeplanet.com/*
[127]Ver: *http:// www.sipri.org/databases*

Base de datos que proporciona enlaces a todos los informes nacionales de acceso público sobre exportaciones de armas.

Otra página relevante en cuanto a información de interés para el analista de inteligencia lo supone *Jane's Intelligence Centre*, que dispone de una ingente cobertura informativa sobre todos los aspectos relacionados con la defensa, la seguridad y las Fuerzas Armadas a nivel mundial, etc. Resulta de gran utilidad para encontrar información, por ejemplo: presupuestos de los principales países del mundo en cuestiones de defensa, perfiles de países con una completa información sobre su situación política, económica, demográfica, militar, etc., imágenes sobre buques, vehículos terrestres y aviones, y sus detalles, así como qué vehículos militares, aeronaves y buques van a adquirir en el futuro a corto y medio plazo los principales países del mundo; información sobre las amenazas y riesgos que experimentan los principales países del mundo y qué capacidad tienen dichos países para hacer frente a estas amenazas; estabilidad de los Estados, crimen organizado, terrorismo, insurgencia, relaciones internacionales, etc.; datos de contacto e información sobre organizaciones de la industria aeroespacial y de la industria de la defensa: instituciones gubernamentales, fabricantes, distribuidores, compañías de servicios, etc.

Otra página relevante en cuanto a información proporcionada es el *GDI (Global Defense Information),* una base de datos sobre defensa y tecnología aeroespacial que contiene artículos y noticias sobre el sector.

También la página *ISCTRC (International Security And Counter Terrorism Reference Center)* proporciona información sobre todos los aspectos relacionados con la seguridad y la lucha contra el terrorismo. En la misma línea, la página *ProQuest Military Collection* es una base de datos especializada en seguridad y defensa, aeronáutica y vuelos espaciales, comunicaciones e ingeniería civil.

La página *Armed Conflict Database está elaborada por el International Institute for Strategic Studies de Londres* y es una base de datos que proporciona información sobre países en los que existe o ha existido algún conflicto bélico o actividad de grupos terroristas desde el año 1997. La página *Europa World Plus* cubre información política y económica de más de 250 países y territorios, desde Afganistán hasta Zimbabue. The Europa Regional Surveys of the World, aportan datos sobre los gobiernos, enlaces a otras instituciones, artículos, etc. La página *INS (International Relations and Security Network)* es un proyecto del CSS *(Center for*

*Security Studies),* en el ETH *(Swiss Federal Institute of Technology)* de Zurich, financiado conjuntamente por el Departamento Suizo de Defensa, Protección Civil y Deporte (DDPS) y ETH Zurich (Escuela Politécnica Federal) y donde podemos encontrar *think tanks*, agencias gubernamentales, organizaciones internacionales, organizaciones no gubernamentales información sobre el cambio climático, los movimientos migratorios, la seguridad alimenticia, e instituciones privadas.

Otra página interesante lo representa la *World Security Network,* una organización internacional, independiente, sin fines de lucro que trata las relaciones internacionales, temas puramente militares en cuanto al estudio de los conflictos, las operaciones de paz, los costes de las mismas y las políticas de seguridad. Forman parte de esta red instituciones como OTAN, el Center for Strategic and International Studies, la Defence Academy of the United Kingdom, el International Institute for Strategic Studies, la National Defense University, y UNISCI.

Como observamos, al alcance de un click tenemos fuentes de información abiertas, que pueden proveer de casi un 90% de la información necesaria para la toma de decisiones (deliberadamente buenas o deliberadamente malas) y para el diseño de políticas. Queda abierto, por tanto, el debate en dos sentidos, por un lado establecer si la sobreexposición de información relevante por parte de los gobiernos y entes sobre sus políticas de defensa y sus industrias armamentísticas, así como su declarado potencial de defensa, resulta antagónico con el propio carácter que se le debe suponer a tales asuntos, dado el desconocido perfil que pueda acceder a la información para ser usada con fines de dudosa confiabilidad; por otro lado, deberá acontecer desde el ámbito militar y el ámbito académico-legal un interesante debate para adelantar los parámetros que dilucidarán las respuesta de la inteligencia sobre los fenómenos y retos de la inteligencia que se avecinan, tales como las plataformas informáticas cuánticas, la guerra informática y digital o la ingeniería armamentista basada en la computación, las potencialidades de Internet y las fuentes abiertas de información en línea.

## 3.7. CONCLUSIONES PRELIMINARES

La *política de Seguridad Nacional* en España se perfila como una política pública de Estado que implica a todo el sector público y a la sociedad en pleno. La *Seguridad Nacional* es, por tanto, un proyecto compartido, *de todos y para todos*, que tiene como marco regulador La *Estrategia de Seguridad Nacional 2013* y la novedosa *Estrategia de Seguridad Nacional 2017*, recientemente publicada, así como lo establecido en la Ley 36/2015, de Seguridad Nacional que establecen, entre otros, una dimensión orgánica a través del *Sistema de Seguridad Nacional*. La concepción estratégica de *Seguridad Nacional* va más allá de una novación de la arquitectura securitaria del Estado y de establecer nuevos marcos competenciales; en realidad, se concibe como la acción del Estado dirigida a proteger la libertad y el bienestar de la población, a garantizar la defensa de España y sus principios y valores constitucionales, en el marco de una acción conjunta con nuestros aliados. En la actualidad, la importancia de los espacios comunes globales, como el ciberespacio, el espacio marítimo y el espacio aéreo y ultraterrestre han sido tensionados, al tiempo que se ha dado gran valor a las infraestructuras críticas, por su provisión de servicios esenciales a la sociedad. Esta tesitura obliga a potenciar un modelo integral de seguridad y a impulsar una *Cultura de seguridad nacional* en el que sea partícipe la sociedad en su conjunto.

En este nuevo proyecto de *Seguridad Integral* se puede desdibujar la línea roja entre seguridad y libertad, así como ser un ejemplo de cómo la seguridad ha calado tanto en el imaginario colectivo a proteger. La seguridad, la democracia y la libertad representan los tres pilares vertebradores de la sociedad para su desarrollo. Si uno de ellos es vulnerado, el Estado se muestra fallido. Frente a las multifacéticas amenazas y desafíos en las que el mundo global se enfrenta, el Estado debería poder ir a la avanzada. La política organiza la sociedad y el Derecho la regula. La gobernanza de la seguridad no es sólo sobrevivir y resistir frente a una tesitura compleja, sino demostrar la capacidad para mantener la resiliencia social e institucional.

Los riesgos globales enfrentan a los Estados a un nuevo entorno estratégico cada vez más abierto e incierto, que genera una sensación de inseguridad. Las medidas a adoptar pueden ser de distinta naturaleza, pero casi todas ellas han venido auspiciadas por la necesidad de garantizar la seguridad nacional,

constituyendo esta situación el caldo de cultivo para legislar de forma excepcional, produciéndose, así, un verdadero proceso de marginalización y desamparo en perjuicio de las garantías constitucionales. La actividad desplegada por algunas agencias de inteligencia pareciera que se ha desarrollado con base en una cuestionable legislación adoptada ante la urgencia y necesidad de combatir actos terroristas, lo que ha permitido el acceso a las comunicaciones y los documentos privados de las personas con el objetivo de proteger la seguridad interna de las naciones. Los gobiernos también se han beneficiado con la utilización de estas tecnologías, permitiendo una mejora considerable en la atención de sus fines y objetivos. Es así como, a pesar de las considerables ventajas que representan estas nuevas tecnologías, también han aparecido nuevos problemas y desafíos que causan preocupación en la población. De esta manera, los derechos y libertades fundamentales se han visto afectados de forma positiva y negativa. La vigilancia electrónica indiscriminada y arbitraria, tema de reciente data, inició un gran debate en la academia y diversos sectores de la sociedad. Uno de los derechos más afectados por el uso de las tecnologías de información y comunicación, ha sido el derecho de intimidad de las personas. Este derecho se ha visto vulnerado por diversas conductas de los gobiernos, las empresas y por los propios particulares. La sensación de inseguridad ha venido para quedarse. En esta nueva dimensión, el Estado deberá de ser permeable y sensible a las transformaciones profundas que la sociedad necesita para proteger el gran valor de la Libertad, núcleo de todos los Derechos Humanos.

Es, en este sentido, la seguridad un valor prioritario, siendo en muchos casos, el motivo central del pacto que justifica la aparición de la sociedad en el mundo moderno y el instrumento necesario para que otros valores menos accesorios, como por ejemplo la libertad, sean posibles, siendo aquí donde establecemos la conexión entre el valor principal de la seguridad y el valor accesorio de la libertad.

No es posible el desarrollo seguro de la comunidad sin la existencia de condiciones seguras y eso sitúa a la seguridad en el núcleo duro de los derechos fundamentales, como exigencia mínima para que una sociedad sea viable y condición sine quan non para que la libertad sea viable.

# CAPÍTULO IV.- PROTECCIÓN DE LA INFORMACIÓN CLASIFICADA DE LAS ORGANIZACIONES INTERNACIONALES Y SUS PROGRAMAS CLASIFICADOS

# CAPITULO IV.- PROTECCIÓN DE LA INFORMACIÓN CLASIFICADA DE LAS ORGANIZACIONES INTERNACIONALES Y SUS PROGRAMAS CLASIFICADOS

## 4.1. INTRODUCCIÓN

Vivimos inmersos en la sociedad de la información, principalmente gracias a las denominadas nuevas tecnologías. La información fluye de forma inmediata entre las personas que la poseen, incluso cuando estas personas forman parte de las Administraciones, de Organizaciones Internacionales o de empresas, lo cual provoca la sensación, se diría casi generalizada, de pensar que el acceso a toda la información es libre y constituye un derecho de todos y cada uno de nosotros. Nada más lejos de la realidad.

Es habitual que las legislaciones de los Estados impongan restricciones, cuando no prohibiciones, al libre acceso a la información por parte de los ciudadanos, y habitualmente son tres los motivos por los que se imponen dichas restricciones: 1) la propiedad intelectual, 2) los datos de carácter personal de los ciudadanos y 3) la Información Clasificada.

En el primero de los casos, la propiedad intelectual, las restricciones se imponen para permitir el beneficio económico de quien ha desarrollado un invento o ha producido una obra artística, y lo habitual es, en este caso, que se permita el acceso o el uso, del invento o de la obra artística, previo pago, como compensación, de lo demandando por su inventor o autor. El gran debate social que ha generado la denominada piratería de los contenidos musicales y cinematográficos todavía resuena entre los defensores del acceso libre a dichos contenidos, frente a los defensores del respeto a los derechos de autor. La ley de propiedad intelectual, junto a la ley de patentes y marcas regulan el acceso y uso de los derechos de propiedad intelectual de terceros garantizando los derechos de autor.

El acceso a los datos de carácter personal de los ciudadanos, datos que las diferentes administraciones públicas y muchas empresas tienen en cantidades ingentes, también se encuentra, en términos generales, limitado. El debate generado en torno al conocimiento de si una persona es portadora del VIH generó ríos de tinta cuando la preocupación por la posible pandemia de esta

enfermedad parecía justificar que todos conociéramos quiénes eran los portadores. Debido a los daños a las personas que puede ocasionar el acceso a los datos de carácter personal de los ciudadanos, dicho acceso se encuentra regulado mediante la ley de protección de datos. Finalmente nos encontramos que el acceso a la información que puede afectar gravemente a la seguridad y la defensa nacional también está limitado, y es esta clase de información la que se conoce como Información Clasificada. No es casual que en España la necesidad de proteger este tipo de información, que en ocasiones puede ser vital para garantizar la supervivencia del propio Estado, se encuentre recogida en la Constitución, la cual en su artículo 105b establece que "La ley regulará el acceso de los ciudadanos a los archivos y registros administrativos, salvo en lo que afecte a la seguridad y defensa del Estado". Tal disposición revela, como excepción a la norma general de publicidad de los actos de las administraciones públicas, el establecimiento de un criterio de cautela y reserva sobre aquellos asuntos que, de ser divulgados, pondrían en riesgo aquellos bienes que se desean proteger.

En este trabajo no vamos a cuestionar la necesidad o la existencia de la Información Clasificada, que como excepción de la norma general de publicidad es algo que está aquí, y está para quedarse, y nos centraremos en explicar cuáles son los instrumentos que nos permiten protegerla con un razonable nivel de seguridad (hay que recordar en este punto que la seguridad absoluta no existe) para tratar de alcanzar dos objetivos: divulgar el conocimiento a un grupo de potenciales lectores del trabajo que de una forma u otra acabarán accediendo a algún tipo de Información Clasificada, y, a la vista de la regulación existente sobre este asunto, disipar la sensación, bastante generalizada, de que el secreto puede ser utilizado abusivamente, lo cual llevaría a cuestionar la licitud de la existencia de asuntos que deban permanecer secretos.

Con el objeto de tratar de determinar la magnitud del problema al que nos enfrentamos, la protección de la Información Clasificada de las organizaciones internacionales y sus programas clasificados, la primera pregunta que nos hacemos es:

¿Cómo proteger una información que se encuentra en poder de alguien, digamos, una persona al servicio de las administraciones españolas?

Si está en poder de una sola persona realmente no resulta difícil evitar su divulgación. Esa persona realmente solo tiene que confiar en sí misma para protegerla adecuadamente. La realidad, sin embargo, es que la Información Clasificada normalmente ha de ser conocida y compartida por un grupo de personas, de las administraciones siguiendo nuestro ejemplo, y no solo por una, lo cual acrecienta el problema, y hace necesario que generemos un sistema en el que cada uno confíe en el resto, o al menos que cada uno confíe en el proceso para determinar la razonable fiabilidad de los demás como depositarios de la misma información. De este razonamiento se extrae como conclusión la necesidad de conceder habilitaciones personales de seguridad a las personas que han de conocer (o generar) Información Clasificada.

Ni que decir tiene que la Información Clasificada tiene que ser almacenada en alguna localización concreta y en algún tipo de soporte físico, a día de hoy principalmente digital, de forma que ese grupo de personas que han de manejar esa información puedan acceder a la misma de forma segura en estos lugares y en estos soportes. Este aspecto de la protección de la Información Clasificada es, sin duda, el más intuitivo, y nos lleva a concluir que es necesario disponer de un sistema de acreditación de los locales y los sistemas de información, de forma que tengamos la garantía de que están razonablemente protegidos cuando la Información Clasificada se encuentra en ellos.

Para seguir tratando de delimitar la extensión de nuestro problema, es necesario mencionar que las administraciones necesitan de las empresas para promover desarrollos, normalmente tecnológicos, que por su naturaleza son clasificados, y de esta realidad surge una nueva pregunta ¿Cómo proteger la Información Clasificada cuando la misma se encuentra, además de en las administraciones, en poder de las empresas y su personal?

Las empresas tienen sus propios intereses, lícitos por supuesto, normalmente de índole económico, los cuales representan un nuevo factor de riesgo para la Información Clasificada cuando es conocida, en realidad principalmente generada, por las empresas. En consecuencia, se hace necesario arbitrar un procedimiento para conceder a las empresas habilitaciones de seguridad que sirvan para garantizar la protección de la Información Clasificada manejada o generada por ellas en los locales de las administraciones o en los

suyos propios.

Finalmente, hay que reconocer que los proyectos de cierta envergadura son difícilmente abordables por un solo Estado dado el enorme esfuerzo económico que en algunos casos supone, por lo que cada vez es más habitual la participación de varios de ellos en desarrollos de naturaleza clasificada (por ejemplo el programa europeo de satélites Galileo, el programa EuroFigther o el programa A400M por mencionar solo algunos) con lo que nuestro problema vuelve a ensancharse, ahora traspasando fronteras.

La información Clasificada, en consecuencia, puede estar almacenada y ser conocida por personas y empresas de varios Estados, y para garantizar su seguridad necesitamos desarrollar normativas armonizadas entre todos los países que participan en un proyecto o programa clasificado, a la vez que necesitamos establecer un sistema de certificaciones cruzadas que permita reconocer como válidas las habilitaciones de seguridad de personas, locales, sistemas de información y empresas de unos países en otros. En los siguientes capítulos se examinarán cuáles son los instrumentos de que disponemos para poder satisfacer estas necesidades, mencionando, cuando sea menester, las carencias y deficiencias de los mismos.

## 4.2. CONCEPTOS GENERALES SOBRE INFORMACIÓN CLASIFICADA

### 4.2.1. Definición y Originador

Con el objeto de aclarar que entendemos por Información Clasificada introducimos la siguiente definición que se encuentra recogida en las normas de la Autoridad Nacional para la Protección de la Información Clasificada: "Información Clasificada es cualquier información o material respecto de la cual se decida que requiere protección contra su divulgación no autorizada y a la que se ha asignado una clasificación de seguridad".

Analizando esta definición observamos que el concepto de Información Clasificada abarca también los materiales que se decida proteger además de la información propiamente dicha. No ha de sorprender esta inclusión pues cualquier material es la manifestación física del diseño o invención de este, es decir la manifestación física de la información sobre su construcción y funcionamiento. Si esta información es clasificada también ha de serlo el material.

Por supuesto dentro de esta definición cabe cualquier soporte documental, por mencionar algunos, tal y como dice el desarrollo la Ley de Secretos Oficiales: "… impresos, manuscritos, papeles mecanografiados o taquigrafiados, planos, proyectos, esquemas, esbozos, diseños, bocetos, diagramas, cartas, croquis, mapas, fotografías y sus negativos…".

Sin embargo, lo realmente relevante de esta definición es, por un lado, la obligación de que se decida que una información requiere protección contra su divulgación, y por otro, la necesidad de otorgar un grado de clasificación a dicha Información Clasificada. La pregunta de quién decide qué información se ha de clasificar y en qué grado, nos lleva a la necesidad de definir las autoridades de clasificación de las que hablaremos más adelante.

Consideraremos originador de la Información Clasificada a la organización internacional, estado u organismo bajo cuya autoridad la Información Clasificada ha sido generada o producida y que determina quién ostenta la propiedad. Cuando sea difícil determinar el originador de la Información Clasificada la marca de clasificación lo determinará en último extremo.

El originador de la Información Clasificada es quien va a decidir cómo se ha de proteger la Información Clasificada de su propiedad, y normalmente lo hace mediante la elaboración de un conjunto de normas aplicables al efecto. Para evitar acumular Información Clasificada indefinidamente, la protección de la Información Clasificada ha de ser vista como un ciclo en el que dicha información va apareciendo y desapareciendo a lo largo del tiempo en función de diversos factores. Es habitual que en las diversas normativas se contemple la posibilidad de que las autoridades de clasificación determinen un periodo de tiempo para ir degradando la clasificación de seguridad de la información hasta que finalmente sea desclasificada. En la figura nº1 aparece una representación del ciclo de la Información Clasificada y su protección tal y como se concibe a día de hoy.

### 4.2.2. Tipos de Información Clasificada

El tipo de Información Clasificada está estrechamente ligado, por un lado, al originador de dicha información, y por otro, a la existencia de al menos una normativa para su protección (en la Unión Europea tenemos, de momento, tres

normativas diferentes, que aunque están armonizadas, presentan diferencias) que será el referente de obligado cumplimiento para su protección.

A tenor de lo dicho sobre los tipos de Información Clasificada nos encontramos que disponemos de Información Clasificada nacional, Información Clasificada de la Unión Europea, Información Clasificada de la OTAN, Información Clasificada de la Agencia Espacial Europea (ESA), Información Clasificada de otras organizaciones internacionales, e Información Clasificada de cualquiera de los Estados con los que España puede relacionarse en el terreno de la protección de la Información Clasificada, que por simplificar denominaremos Información Clasificada de "terceros estados".

También es claro de lo expuesto que existe normativa nacional, de las tres organizaciones internacionales mencionadas, y de las demás de las que España forma parte, y es así, si bien la normativa nacional cobra especial relevancia porque la normativa internacional remite a la nacional de cada Estado en muchas ocasiones.

Respecto a la Información Clasificada de "terceros estados" la normativa aplicable es el acuerdo bilateral de seguridad firmado con cada uno de los Estados con los que España ha tenido o tiene la necesidad de intercambiar Información Clasificada. Estos acuerdos bilaterales también remiten a la normativa de cada Estado para garantizar la protección de la Información Clasificada en muchos de sus apartados. Hablaremos de los acuerdos de seguridad bilaterales más adelante, y por ahora solo insistir en que la normativa nacional es una pieza clave del conjunto de normativas que hay establecidas para la protección de la Información Clasificada.

### 4.2.3. Grados de Información Clasificada

Como ya se ha mencionado, a la Información Clasificada se le asigna un grado que expresa la importancia de esta. En las organizaciones internacionales y supranacionales de las que forma parte España son en todos los casos cuatro los grados posibles de clasificación, y en la figura nº 2 se pueden consultar las denominaciones de estos grados de clasificación para la Información Clasificada de la Unión Europea, la OTAN y la Agencia Espacial Europea, mientras que en la figura nº 3 aparecen las denominaciones de la Información Clasificada de los

Estados que forman parte de la Unión Europea, la OTAN y la Agencia Espacial Europea. Estas dos tablas, que se encuentran en las Normas de la Autoridad Nacional de Seguridad para la protección de la Información Clasificada, representan la equivalencia de los cuatro grados de clasificación para todos los tipos de Información Clasificada incluidos, que en definitiva implica cual es el grado de protección que se ha de aplicar en cada caso.

La definición que encontramos tanto en la normativa de la Comisión Europea como en la normativa del Consejo de Europa para graduar la importancia de la Información Clasificada de la Unión Europea es la siguiente:

1. TRES SECRET UE/EU TOP SECRET: *información y material cuya revelación no autorizada pueda causar un perjuicio excepcionalmente grave a los intereses esenciales de la Unión Europea o de uno o varios Estados miembros*;

2. SECRET UE/EU SECRET: *información y material cuya revelación no autorizada pueda causar un perjuicio grave a los intereses esenciales de la Unión Europea o de uno o varios Estados miembros*;

3. CONFIDENTIEL UE/EU CONFIDENTIAL: *información y material cuya revelación no autorizada pueda causar perjuicio a los intereses esenciales de la Unión Europea o de uno o varios Estados miembros*;

4. RESTREINT UE/EU RESTRICTED: *información y material cuya revelación no autorizada pueda resultar desfavorable para los intereses de la Unión Europea o de uno o varios Estados miembros*.

Las denominaciones de la Información Clasificada de la Unión Europea se encuentran siempre tanto en idioma Inglés como en idioma Francés. Siendo muy parecidas las definiciones utilizadas por las otras dos organizaciones internacionales, las de la Unión Europea, como particularidad incluyen como parte de las definiciones tanto a la Unión propiamente dicha, como a cada uno de los Estados que la componen.

Vemos que la gradación de importancia abarca desde "causar perjuicios excepcionalmente graves", pasando por "causar un perjuicio grave" o simplemente "causar perjuicio", para finalizar por "resultar desfavorable", que a la postre son los únicos elementos de juicio de los que disponen las autoridades de clasificación para determinar con qué grado ha de clasificarse una

determinada información para que pase a ser clasificada.

Aparecen para España cuatro grados de clasificación, sin embargo, la Ley de Secretos Oficiales española, de la que hablaremos más adelante, únicamente contempla dos grados de clasificación SECRETO y RESERVADO que se encuentran definidos de la siguiente forma:

> 1. La clasificación de SECRETO se aplicará a todas las materias que precisen del más alto grado de protección por su excepcional importancia y cuya revelación no autorizada pudiera dar lugar a riesgos o perjuicios de la seguridad del Estado o pudiera comprometer los intereses fundamentales de la Nación en materia referente a la defensa nacional, la paz exterior o el orden constitucional.
>
> 2. La clasificación de RESERVADO se aplicará a las materias cuyo conocimiento o divulgación pudiera afectar a los referidos intereses fundamentales de la Nación, la seguridad del Estado, la defensa nacional, la paz exterior o el orden constitucional.

Estos dos grados de clasificación se corresponden con los de mayor importancia, y los dos grados inferiores denominados respectivamente CONFIDENCIAL y DIFUSIÓN LIMITADA únicamente aparecen recogidos en desarrollos legislativos de rango inferior a la Ley de Secretos Oficiales, concretamente en la Orden Ministerial 76/2006 sobre política de seguridad del Ministerio de Defensa, en las Normas de la Autoridad Nacional para la Protección de la Información Clasificada y en la Orden Ministerial IET/2377/2015, de 5 de noviembre, por la que se regula la protección de la información clasificada en el Ministerio de Industria, Energía y Turismo, que básicamente se adhiere a las normas de la Autoridad Nacional de Seguridad.

En la Orden Ministerial 76/2006 del Ministerio de Defensa, por poner un ejemplo, aparece la definición de materias objeto de reserva interna, a las cuales adjudicará los niveles de clasificación de CONFIDENCIAL y DIFUSIÓN LIMITADA con las siguientes definiciones:

> 1. El grado CONFIDENCIAL se aplicará a los asuntos, actos, documentos, informaciones, datos y objetos cuya revelación no autorizada pudiera dañar la seguridad del Ministerio de Defensa, perjudicar sus intereses o dificultar

el cumplimiento de su misión.

2. El grado DIFUSIÓN LIMITADA se aplicará a los asuntos, actos, documentos, informaciones, datos y objetos cuya revelación no autorizada pudiera ir en contra de los intereses y la misión del Ministerio de Defensa.

Esta circunstancia tiene repercusiones importantes pues, como se desprende de las definiciones de la Orden Ministerial 76/2006 para el caso del Ministerio de Defensa, únicamente en los departamentos antes mencionados, así como en la equivalencia contemplada en los acuerdos de seguridad bilaterales con "terceros estados" es de aplicación los dos niveles inferiores de Información Clasificada, CONFIDENCIAL y DIFUSIÓN LIMITADA, y por lo tanto solo en estos casos podemos hablar estrictamente de la existencia de cuatro niveles de clasificación, mientras que en el resto de las administraciones españolas solo existirían dos niveles, los que se encuentran recogidos en la Ley de Secretos Oficiales.

Sin embargo es posible que en virtud de algún proyecto multinacional, los ministerios que no tienen desarrollada normativa de protección pudieran llegar a recibir Información Clasificada de terceros países con un grado de clasificación para el que no están preparados al carecer de la normativa necesaria para su protección.

En estos casos, para evitar que se tengan que aplicar las medidas establecidas para el nivel de RESERVADO a los niveles inferiores de clasificación de terceros estados, se asume que serán de aplicación las normas de la Autoridad Nacional de Seguridad como forma de rellenar el vacío legislativo existente, si bien esta práctica es cuestionable desde un punto de vista jurídico.

### 4.3. AUTORIDADES DE CLASIFICACIÓN

La figura de la autoridad de clasificación es de vital importancia para que el proceso formal de clasificación expuesto en el siguiente apartado sea claro y El Reino Unido no utiliza el grado de clasificación "UK CONFIDENTIAL" en su sistema nacional. Maneja y protege los documentos con grado "CONFIDENCIAL o equivalente" acorde a la normativa de seguridad nacional establecido para "UK SECRET" transparente y no dé lugar a ningún tipo de inseguridad jurídica, ni a

quienes han de responsabilizarse de proteger la Información Clasificada, ni a quienes han de utilizarla en el desarrollo de su trabajo. Bélgica, Canadá, EEUU y Francia no utilizan el grado de clasificación "RESTRICTED" en su sistema nacional. Bélgica, Canadá, EEUU y Francia manejan y protegen los documentos con grado "DIFUSIÓN LIMITADA o equivalente" acorde a sus leyes y reglamentos nacionales en vigor, que no son menos exigentes que lo establecido en las normativas de seguridad de OTAN, UE o ESA. El reto más importante de las autoridades de clasificación es ceñirse a las definiciones de los grados de clasificación antes mencionadas para evitar caer en la sobreclasificación o en la infraclasificación de la información.

Es habitual que las autoridades de clasificación sean a su vez las encargadas de reclasificar y desclasificar la información que bajo su autoridad fue clasificada, garantizando de esta forma que quien apreció la necesidad de proteger una información sea quien reevalúe la necesidad de continuar protegiéndola. A su vez será esta autoridad quien determine la conveniencia de ceder o permitir el acceso a la Información Clasificada a "terceros", sean estos Estados u Organizaciones Internacionales, cuestión que habitualmente se hace mediante la firma de acuerdos de seguridad con dichos "terceros".

#### 4.3.1. Autoridades de clasificación nacionales

Para la Información Clasificada nacional, en el artículo cuarto de la Ley de Secretos Oficiales vienen mencionadas las autoridades de clasificación para los grados de SECRETO y RESERVADO, siendo, según dicha ley, el Consejo de Ministros y la Junta de Jefes de Estados Mayor las únicas autoridades reconocidas, sin que pueda ser transferida o delegada la facultad de clasificación para estos niveles.

Ciertamente la Junta de Jefes de Estado Mayor como órgano colegiado no existe desde hace ya años, concretamente desde el año 2008, aunque sí existe cada uno de los Jefes de Estado Mayor que componían dicha junta, por lo que a día de hoy únicamente el Consejo de Ministros puede clasificar en los grados de SECRETO y RESERVADO.

Es opinión del ponente de esta monografía que el Consejo de Ministros sólo debería reservarse la clasificación en exclusiva de grado SECRETO, sin capacidad

de delegarla, y debería estar permitido que además del Consejo de Ministros pudieran clasificar en grado de RESERVADO cada ministro en su ámbito de competencia con capacidad de delegar esta función a escalones inferiores de la Administración. Como veremos más adelante esta circunstancia es habitual en el ámbito internacional para los grados equivalentes a RESERVADO, es decir para grados de NATO SECRET, EU SECRET/UE SECRET y ESA SECRET.

Para la información clasificada de grados CONFIDENCIAL y DIFUSIÓN LIMITADA debemos acudir a las normativas departamentales antes mencionadas, para concluir que la delegación está permitida en todos los casos, y las autoridades, en general, son el presidente del gobierno, el/los vicepresidentes del gobierno, los ministros, los secretarios de estado, los subsecretarios y los jefes de de los estados mayores de fuerzas armadas y del Ministerio de Defensa.

Atendiendo estrictamente a la normativa y al ámbito de su aplicación, la realidad es que los ministerios que no tienen normativa departamental desarrollada, es decir todos excepto Defensa e Industria, no pueden clasificar en estos niveles inferiores y, en consecuencia, carecen de autoridades de clasificación con estas facultades.

### 4.3.2. Autoridades de Clasificación en el Ámbito Internacional

Así como están perfectamente definidas en la normativa nacional quiénes son las autoridades de clasificación, en la normativa internacional no es tan evidente, especialmente para las propias Organizaciones Internacionales y sus agencias. Es cierto que para cada Estado miembro, en general, serán las mismas autoridades nacionales las que clasifiquen con marca internacional cuando sea su responsabilidad hacerlo, puesto que las regulaciones internacionales remiten a las legislaciones nacionales en ausencia de regulación específica.

Sin embargo, la realidad del ámbito internacional es más compleja, es necesario armonizar las normativas de varios Estados, y es necesario aceptar como válida en España la clasificación efectuada por las autoridades de otros países con los que formamos parte de la misma Organización Internacional o Supranacional, así como la clasificación efectuada por las autoridades de la propia Organización Internacional, por lo que no siempre el nivel de las

autoridades de clasificación en las administraciones de otros países y de las organizaciones internacionales se corresponde con el aplicado en España.

Nos encontramos, por ejemplo, que en la Unión Europea la aprobación de la propuesta de clasificación del programa de satélites Galileo se realiza en última instancia en las sesiones del Consejo de Europa en el que se sienta el embajador de España ante la UE junto con el resto de los embajadores de los demás Estados de la Unión. Esta propuesta nos encontramos que tiene muchas partes clasificadas de grado "UE SECRET/EU SECRET" cuyo equivalente nacional es RESERVADO y en consecuencia, de acuerdo con la normativa nacional española, sólo el Consejo de Ministros debería clasificar en este grado sin que pueda delegar esta facultad.

Por poner otro ejemplo, en la Organización Conjunta de Cooperación en Materia de Armamento (OCCAR) de la que España forma parte junto con Alemania, Reino Unido, Francia, Italia y Bélgica, la aprobación en última instancia de las guías de clasificación de los programas conjuntos que desarrolla esta organización (por ejemplo el avión de transporte A400M) recae en la Junta de Supervisores (Board of Supervisors

-BoS- en su denominación en inglés) de la que forma parte el Director General de Armamento y Material del Ministerio de Defensa. Muchas partes de estos programas están clasificados en grado equivalente a RESERVADO, concretamente en grado "OCCAR SECRET" por lo que la clasificación debería corresponder al Consejo de Ministros exclusivamente.

En estos dos ejemplos, para armonizar el nivel de representación en estas organizaciones con el resto de los miembros de estas, se acepta que se ha delegado la facultad de clasificar en el embajador español de la representación española ante el Consejo de Europa, y en el Director de General de Armamento y Material en calidad de Director Nacional de Armamento.

La existencia en España de dos directivas de clasificación aprobadas por acuerdo del Consejo de Ministros, de las que hablaremos en el siguiente sub-apartado, soluciona la aparente delegación de funciones del Consejo de Ministros, cuando los asuntos clasificados se correspondan con los explicitados en dichas directivas. Sin embargo, para asuntos que no aparezcan en las directivas, o que aparezcan con un grado de clasificación distinto se habrían

delegado las funciones en contra de lo que establece la Ley.

En cuanto a la Información Clasificada generada y manejada en las propias organizaciones internacionales, observamos que en el caso de la OTAN, en el anexo E del documento CM (2002)-49, se establece que el Consejo del Atlántico Norte será la autoridad superior para autorizar la cesión de Información Clasificada de la alianza con capacidad de delegar esta función, mientras que en la Directiva de seguridad de la Información que desarrolla el documento antes mencionado se establece que: *las naciones OTAN y las agencias civiles y militares de la OTAN, tomarán medidas para asegurar que la información creada por, o proporcionada a la OTAN tiene correctamente asignada la clasificación de seguridad*, y para el caso particular de las agencias se exige que se restrinja la autoridad de decidir sobre la clasificación de seguridad a un número limitado de autoridades.

En el caso de la Unión Europea, en la normativa de la Comisión observamos que en su artículo 4.1 se establece que cada miembro de la Comisión Europea o los departamentos de la Comisión son responsables de que la Información Clasificada que ha creado esté correctamente marcada e identificada. No se establecen expresamente las autoridades de clasificación en esta normativa, pero se interpreta de la misma que todos los Directores Generales de los diferentes departamentos de la Comisión Europea son autoridades de clasificación.

Finalmente, en el caso de la ESA, esta organización por normativa interna solo clasifica su propia información en grado de "ESA RESTRICTED", siendo únicamente posible utilizar los otros grados para los programas que desarrolla, cuya clasificación se realiza de forma colegiada por las naciones que formen parte del programa.

Para finalizar hay que reconocer que la mayoría, por no decir la totalidad, de la Información Clasificada internacional de la que los Estados, entre ellos España, han de responsabilizarse de su protección por encontrarse en su territorio, se produce en el desarrollo de programas y contratos clasificados de estas mismas organizaciones internacionales, y, como explicaremos en un capítulo posterior dedicado a los programas y contratos clasificados internacionales, los Estados tienen un control total, de manera colegiada, en la definición de lo que se ha de clasificar en dichos programas y contratos.

### 4.4. PROCESO FORMAL DE CLASIFICACIÓN

El proceso formal de clasificación para la Información Clasificada nacional es sencillo, y consiste en que una Autoridad de Clasificación de las definidas anteriormente, en el ámbito de su competencia, emita el correspondiente documento en el que se establezca que la información relacionada con un asunto ha de ser clasificada especificando el grado y tipo de la misma.

Existen en la actualidad tres formas diferentes con las que las autoridades de clasificación pueden clasificar la información: la diligencia de clasificación, la directiva de clasificación y la ley, en este último caso únicamente para el grado de SECRETO (véase el artículo 1 de la ley de secretos oficiales).

En el primer caso la Autoridad de Clasificación clasifica "caso por caso", para lo cual se requiere de una propuesta de clasificación, siendo la diligencia de clasificación el documento por el que se certifica la aprobación, por la autoridad de clasificación, de una propuesta de clasificación.

Una directiva de clasificación es el documento por el que una autoridad de clasificación asigna un grado de clasificación a la información de asuntos o materias que, por su naturaleza, y a juicio de la citada autoridad, deba ser clasificada, sin que se requiera la elaboración de una propuesta de clasificación para cada uno de los casos.

Resulta muy útil la clasificación mediante una directiva de clasificación, y a día de hoy se encuentran en vigor dos directivas de clasificación aprobadas por acuerdo de Consejo de Ministros el 28 de noviembre de 1986, en las que se definen la mayoría de los asuntos que deben ser clasificados en los grados de RESERVADO y SECRETO por lo que no es necesario acudir repetidamente al Consejo de Ministros para que clasifique determinados asuntos.

No requiere de muchas explicaciones la clasificación por Ley, quizás nicamente el matiz de que esta forma de clasificar solo puede ser ejercida, obviamente, por quien tiene capacidad de legislar. Como ejemplo podemos mencionar la Ley 11/2002 de 6 de mayo reguladora del Centro Nacional de Inteligencia en la que en su artículo 3 se establece que la Directiva de Inteligencia elaborada por el Gobierno estará clasificada de SECRETO.

En el caso particular de España los parlamentos autonómicos tienen capacidad de legislar, por lo que cabe pensar que la Ley de Secretos Oficiales les

faculta para clasificar en grado de SECRETO mediante la aprobación de las leyes correspondientes. Sin embargo, dado que la Ley de Secretos Oficiales es anterior a la existencia de dichos parlamentos, no parece que esta posibilidad fuera el espíritu de dicha ley.

De esta última reflexión concluimos que la Ley de Secretos Oficiales no contempla la estructura de las diferentes administraciones del estado español, y en consecuencia únicamente la administración central estaría facultada para clasificar información de acuerdo con la ley actual. Sin embargo, hemos de mencionar que algunas de las comunidades autónomas tienen transferidas algunas competencias en materia de seguridad que pudieran ser objeto de protección mediante la aplicación de la Ley de Secretos Oficiales.

En el ámbito internacional el proceso formal de clasificación más importante es la elaboración y aprobación de la Guía de Clasificación de Seguridad (Security Classification Guide -SCG- en su denominación en inglés) de los programas y contratos en los que se maneja o genera Información Clasificada. Este documento, equivalente a una directiva de clasificación del programa, se elabora de forma colegiada entre todos los países que forman parte del mismo. Hablaremos de este documento en el apartado de seguridad de los programas internacionales.

### 4.5. EL PRINCIPIO DE NECESIDAD DE CONOCER Y SUS CONSECUENCIAS

La protección de la Información Clasificada descansa como piedra angular en el principio de "necesidad de conocer" (need-to-know en su denominación en inglés), que de forma intuitiva nos indica que solamente aquellas personas que realmente requieran la información en su desempeño profesional pueden acceder a la misma. Este principio no se fundamenta en jerarquía alguna, y en consecuencia es de aplicación a todos los escalones de cualquier departamento de las administraciones públicas, de las organizaciones internacionales o de las empresas que dispongan de Información Clasificada en sus instalaciones.

En las normas de la Autoridad Nacional de Seguridad el principio de necesidad de conocer aparece definido como "la determinación positiva por la

que el propietario, o en su defecto, el responsable de la custodia confirma que una persona necesita manejar determinada información clasificada para desempeñar servicios, tareas o cometidos oficiales". En consecuencia, nadie está autorizado a acceder a información clasificada por razón de su cargo o posición.

De la definición y del concepto podemos deducir, por un lado, que al recaer la responsabilidad de determinar la necesidad de conocer en todo aquel que la tenga en su custodia, la responsabilidad de su protección es compartida por todos los usuarios que la manejan, y por otro, que más tarde o más temprano todos los usuarios de alguna Información Clasificada se enfrentarán a la decisión de determinar la necesidad de conocer de otro usuario que le solicita acceder a la Información Clasificada bajo su custodia.

La estricta observancia del principio de necesidad de conocer, además de impedir el acceso a la Información Clasificada a usuarios no autorizados, sirve para limitar los daños que puede ocasionar un usuario confiable que hace un mal uso, fortuita o intencionadamente, de la Información Clasificada a la que ha accedido.

La determinación de la necesidad de conocer por parte de un usuario puede ser una tarea difícil en tanto que va en contra de nuestro comportamiento natural, aprendido desde pequeños, de pertenencia a determinados grupos sociales, y por eso, el incumplimiento del principio de necesidad de conocer en muchas ocasiones viene del intento de algunos usuarios de ser cooperativo y útil a otros, y no de una actuación deliberada para incumplirlo.

Lo expuesto hasta ahora sobre del principio de necesidad de conocer se corresponde con la característica excluyente del mismo, la más importante sin duda, es decir, la característica de que únicamente quien realmente necesite la información es quien debe acceder a ella, y no el resto.

Sin embargo, el principio de necesidad de conocer también presenta una característica incluyente, que se traduce en que todo el que tiene necesidad de conocer una determinada Información Clasificada ha de poder acceder a la misma de una forma u otra para poder desempeñar su trabajo adecuadamente. En algunos documentos esta característica suele denominarse como necesidad de compartir (need-to-share en su denominación en inglés) o responsabilidad de compartir.

La imposibilidad de acceder a la información clasificada por parte de aquellos que lo necesitan en el cumplimiento de sus obligaciones puede llevar al incremento de costes de los programas clasificados, la pérdida innecesaria de tiempo, la disminución de la competitividad de las empresas y la caída de la productividad en el desarrollo de los programas clasificados emprendidos por Estados y organizaciones internacionales. La necesidad de compartir Información Clasificada se ha demostrado especialmente importante en algunos terrenos, como la lucha contraterrorista y la contra inteligencia, en los que se tienen evidencias de que la dificultad, cuando no la imposibilidad, de compartir la Información Clasificada entre grupos de usuarios con necesidad de conocer dicha información, ha llevado a la imposibilidad de detectar y neutralizar algunos ataques terroristas de extrema gravedad, o algunas fugas de información a otros Estados.

La necesidad de conocer y la necesidad de compartir la Información Clasificada son dos caras de la misma moneda, y no resulta fácil encontrar el equilibrio entre la protección de la información y la distribución de esta entre todas las personas y organizaciones que puedan necesitarla.

### 4.6. LA INFORMACIÓN CLASIFICADA NACIONAL

Ya se ha mencionado que la legislación nacional es una pieza clave en la protección de la Información Clasificada de las organizaciones internacionales y supranacionales de las que España forma parte, así como de sus programas clasificados, puesto que las normativas, todas sin excepción, remiten a las legislaciones nacionales en innumerables ocasiones a través de su articulado.

Sin embargo, uno de los puntos sobre el que las normativas internacionales de la OTAN, la UE y la ESA no han remitido a las legislaciones nacionales es en la exigencia de nombrar una Autoridad Nacional de Seguridad encargada de velar por la protección de la Información Clasificada de estas organizaciones. La ausencia de esta autoridad, al menos de una forma explícita, en la legislación española obligó, como se expone más adelante en este trabajo, al nombramiento de esta para las tres organizaciones internacionales antes mencionadas.

Parecería entonces que en la actualidad existe la Autoridad Nacional de Seguridad para la protección de la Información Clasificada internacional, concretamente de la OTAN, la UE y la ESA, mientras que no existe para la protección de la Información Clasificada nacional. Sin embargo, a juicio del autor, la Autoridad Nacional de Seguridad para la protección de la Información Clasificada nacional es el Consejo de Ministros, único órgano existente con capacidad de clasificar de los dos mencionados en la ley.

Siendo pieza clave la legislación nacional, tenemos que admitir que la que está en vigor actualmente está obsoleta, al menos en el desarrollo reglamentario del Decreto 242, y está incompleta en la elaboración de normativa de rango inferior al desarrollo reglamentario, que sea de aplicación a la totalidad de las administraciones.

### 4.6.1. Ley de Secretos Oficiales y su Decreto de desarrollo

La Ley 9/1968 de 5 de abril, modificada por la Ley 48/1978 de 7 de octubre sobre Secretos Oficiales es el desarrollo legislativo más importante en materia de protección de Información Clasificada en España. De hecho es la Ley de Secretos Oficiales la que posibilita la existencia de Información Clasificada nacional.

La propia ley dispone que se desarrollen reglamentariamente los procedimientos y medidas necesarios para la aplicación de la ley, lo cual se materializó en el decreto 242/1969 de 20 de febrero.

Nos encontramos con una ley antigua, de hecho, es preconstitucional, si bien fue modificada en 1978, y sorprendentemente, a falta de ligeros retoques, sería perfectamente válida para dar la cobertura legal necesaria a los desarrollos legislativos de rango inferior que permitieran dar respuesta a las necesidades de los tiempos actuales.

La Ley de Secretos Oficiales está basada en la excepcionalidad de la clasificación, frente a la publicidad habitual de los trabajos de las administraciones, lo cual se ajusta a lo establecido en el artículo 105b de nuestra Constitución, como punto de partida. Sin embargo, en cuanto a las carencias principales de la Ley de Secretos Oficiales, fundamentalmente debido a su antigüedad, apreciamos las siguientes:

1. La ausencia de nombramiento, explícito o mediante desarrollo reglamentario, de la Autoridad Nacional de Seguridad para la protección de la Información Clasificada tanto nacional como internacional, junto a la posibilidad de delegar sus funciones, al menos parcialmente, en una autoridad delegada para la protección de la Información Clasificada. A juicio del autor la Autoridad Nacional de Seguridad debería recaer en el Consejo de Ministros, con capacidad de delegar sus funciones como ya se ha dicho.

2. El establecimiento de 4 niveles de clasificación de la Información Clasificada en lugar de tan solo 2, de forma que se pueda dar cobertura a los equivalentes internacionales que de facto se han aceptado en los desarrollos departamentales de rango inferior.

3. Establecer un conjunto de autoridades de clasificación en las administraciones en función del grado de clasificación de los cuatro propuestos en el apartado anterior, reservando la exclusividad del Consejo de Ministros, en calidad de Autoridad Nacional de Seguridad para la Protección de la Información Clasificada, únicamente para el grado máximo de SECRETO.

4. Ajustar la Ley a la estructura actual del Estado en la que las comunidades autónomas tienen capacidad de legislar, habiéndose transferido a las mismas algunas competencias en materia de seguridad.

5. Incluir, además de la referencia a las personas y locales de su artículo ocho, una clara referencia a la protección de los sistemas de información y comunicación que almacenan, manejan y transmiten Información Clasificada, de forma que se pueda elaborar normativa de rango inferior en este campo.

6. Incluir igualmente una referencia a la necesidad de que las empresas cumplan con las exigencias que se determinen para poder manejar y almacenar Información Clasificada, tanto nacional como internacional, en el desarrollo de los contratos que requieran el manejo o la generación de Información Clasificada.

En cuanto a lo que creemos que sobra en la actual ley, diremos que debería desaparecer del texto la Junta de Jefes de Estado Mayor que a día de hoy no

existe, y se debe cambiar el preámbulo de la ley en el que se menciona el Consejo Nacional del Movimiento, que tampoco existe a día de hoy.

El Decreto de desarrollo de la Ley de Secretos Oficiales es de 1969, y a pesar de que en la modificación de la Ley de Secretos Oficiales de 1978 se disponía su adecuación al nuevo texto de la ley, nunca se hizo tal adecuación.

Este Decreto de desarrollo (no es un Real Decreto pues en el momento de su elaboración España no había vuelto al sistema de monarquía parlamentaria consagrado en la Constitución de 1978) trata de desarrollar los procedimientos necesarios para el tratamiento y protección de las materias clasificadas.

El enfoque de este Decreto se centra casi exclusivamente en el personal de las administraciones, especialmente al de las fuerzas armadas, no mencionándose la industria y su personal en ningún apartado del decreto, cuando la realidad actual es que un porcentaje enorme de la Información Clasificada que se encuentra en territorio español está en poder de las empresas que desarrollan los programas y contratos clasificados para la administración española, para las organizaciones internacionales de las que España forma parte o para terceros estados.

Por otra parte, el decreto de 1969 solo contempla la posibilidad de recibir Información Clasificada de un país extranjero o de una Organización Internacional en el ámbito de la defensa (artículo 11e), cuando la realidad actual es otra bien distinta, y un porcentaje de la Información Clasificada que se recibe de terceras partes se enmarca en el ámbito civil, especialmente en el sector aeroespacial.

El Decreto 242 solamente prevé que se desarrolle normativa de rango inferior para la protección de la Información Clasificada en el ámbito de las Fuerzas Armadas y para las oficinas en el extranjero del Ministerio de Asuntos Exteriores y Cooperación, cuando a día de hoy observamos que es necesaria normativa de rango inferior en muchos más ámbitos, por no decir en la totalidad de los departamentos ministeriales.

En definitiva, es opinión del autor que el Decreto 242 ha de ser sustituido por un nuevo Real Decreto de desarrollo, centrando el mismo en el nombramiento de una Autoridad Nacional de Seguridad y las competencias de la misma, con capacidad de delegar sus funciones en una Autoridad Delegada,

entre las que se debe incluir la de elaborar normativa que sea de aplicación a toda la Administración, dejando los procedimientos concretos de tratamiento de la Información Clasificada, cambiantes para adecuarlos a los tiempos, con rango de Instrucción y elaborados por la Autoridad Nacional de Seguridad Delegada.

Las Normas de la Autoridad Nacional de Seguridad Delegada para la protección de la Información Clasificada de la OTAN, de la Unión Europea y de la Agencia Espacial Europea, vienen a representar de facto los procedimientos que se aplican para la protección de la Información Clasificada de toda clase, siendo necesario que a este desarrollo se le dé el respaldo necesario para los ámbitos en los que realmente no es Autoridad Nacional de Seguridad Delegada. Hablaremos de estas normas en el capítulo siguiente.

### 4.6.2. Política de seguridad del Ministerio De Defensa

La política de seguridad del Ministerio de Defensa se plasmó en la Orden Ministerial 76/2006, a la que siguieron desarrollos normativos de rango de instrucción de Secretario de Estado.

Esta Orden Ministerial viene a corregir la necesidad de que existan cuatro niveles de clasificación, nombra una única autoridad como responsable de la información del ministerio de Defensa, tanto clasificada como no clasificada de uso oficial, establece las autoridades de clasificación del ministerio de Defensa para los niveles inferiores de clasificación y define cinco áreas en las que es necesario desarrollar normativa con rango de instrucción de Secretario de Estado.

Se nombra como responsable de la información del ministerio con el cargo de Director de Seguridad de la Información del ministerio de Defensa (DISIDEF) al Secretario de Estado de Defensa, quien a su vez puede nombrar un responsable para cada una de las cinco áreas antes mencionadas.

Se establecen como autoridades de clasificación para los grados de CONFIDENCIAL y DIFUSIÓN LIMITADA al Ministro de Defensa, al Jefe del Estado Mayor de la Defensa, al Secretario de Estado de Defensa, al Subsecretario de Defensa, al Secretario General de Política de Defensa y a los tres jefes de los Estados Mayores de los tres ejércitos. En todos los casos con capacidad de delegar estas funciones.

Define, siguiendo la estela de la normativa de la Autoridad Nacional de Seguridad, las siguientes cinco áreas: Seguridad de la Información en las personas (SeginfoPer), Seguridad de la Información en los documentos (SeginfoDoc), Seguridad de la Información en los Sistemas de Información y Telecomunicación (SeginfoSit), Seguridad de la Información en las instalaciones (SeginfoIns) y Seguridad de la Información en poder de las empresas (SeginfoEmp).

En los desarrollos de estas cinco áreas se remite a la normativa de la Autoridad Nacional de Seguridad, especialmente en lo relativo a la concesión de las Habilitaciones de Seguridad a las Personas y a la concesión de Habilitaciones de Seguridad y Establecimiento a Empresas, habilitaciones que a día de hoy sólo concede la ANS.

Es claro que la normativa de la Autoridad Nacional de Seguridad debería ser el referente obligado en materia de protección de Información Clasificada nacional, es decir, "de jure", y no únicamente "de facto" como es en el momento actual.

### 4.6.3. La información clasificada en el Ministerio De Industria

Ante la necesidad de organizar la protección de la Información Clasificada, dada su creciente participación en programas y proyectos clasificados del ámbito civil, tanto nacionales como internacionales, el Ministerio de Industria decidió publicar la orden Ministerial IET/2377/2015, de 5 de noviembre, por la que se regula la protección de la Información Clasificada en el Ministerio de Industria, Energía y Turismo.

Esta orden ministerial crea en el Ministerio de Industria los dos grados de clasificación inferiores para complementar los establecidos en la Ley de Secretos Oficiales, adhiriéndose para su protección a las Normas de la Autoridad Nacional de Seguridad, a las que señala como referente.

Se nombra como Director de la Seguridad de la Información Clasificada en el Ministerio de Industria, Energía y Turismo al titular de la Subsecretaria, y se le encomienda la función de velar por el cumplimiento de la orden ministerial.

Se definen las autoridades de clasificación del ministerio para los nuevos grados de Información Clasificada formalmente creados, y se establecen los

requisitos para las personas, locales, sistemas de información y empresas para poder manejar o generar Información Clasificada, para lo cual en lugar de posibilitar desarrollos normativos de rango inferior, refiere, como ya se ha mencionado, a las Normas de la Autoridad Nacional de Seguridad como referente en todos esos ámbitos.

## 4.7. LA INFORMACIÓN CLASIFICADA INTERNACIONAL

La protección de la Información Clasificada de las Organizaciones Internacionales de las que España forma parte, en especial, aunque no exclusivamente, de la OTAN, Unión Europea y Agencia Espacial Europea, así como de terceros Estados, descansa en dos grandes pilares: por un lado la Autoridad Nacional de Seguridad y su normativa, y por otro los acuerdos bilaterales de seguridad para la protección de Información Clasificada.

Ya se ha mencionado que la legislación nacional es una pieza clave del engranaje, al referir a dicha legislación las diferentes normativas internacionales en materia de protección de Información Clasificada que España se ha comprometido a cumplir en virtud de los Acuerdos de Seguridad multilaterales firmados. De la misma manera los Acuerdos Bilaterales firmados por España con terceros Estados, una vez aprobados por las Cortes Generales, se convierten a todos los efectos en legislación nacional de obligado cumplimiento. Precisamente algunas de las carencias de la normativa nacional tuvieron que solucionarse de forma individual, caso por caso, como veremos a continuación.

### 4.7.1. Nombramiento de la Autoridad Nacional de Seguridad OTAN, UE y ESA

El 30 de mayo de 1982 España se adhiere al Tratado del Atlántico Norte y dicha adhesión obliga a España a cumplir con las normas de la OTAN, entre las que se encuentran las normas de protección de la Información Clasificada de la Alianza Atlántica, contenidas en el documento, que a día de hoy tras diversas revisiones, se denomina "*C-M(2002)49 Security within the north Atlantic Treaty Organization (NATO)*".

En dichas normas en el artículo 7.1.1 del anexo B (enclosure B, en su denominación en inglés) se establece la obligatoriedad de que cada nación

miembro de la Alianza nombre una Autoridad Nacional de Seguridad para la protección de la Información Clasificada de la Alianza. En España de acuerdo con la Ley de Secretos Oficiales, de la que ya hemos hablado, no existe de manera explícita la figura de Autoridad Nacional de Seguridad, y para poder dar cumplimiento a esta exigencia se decidió crearla.

Por acuerdo de Consejo de Ministros de 25 de Junio de 1982 se crea la Autoridad Nacional de Seguridad para la protección de la Información Clasificada de la OTAN, recayendo dicho nombramiento en los ministros de Defensa y Asuntos Exteriores conjuntamente. Dicho acuerdo permite la delegación de las funciones de la Autoridad Nacional de Seguridad, y mediante Orden Comunicada de Presidencia del Gobierno de fecha 11 de agosto de 1982 se materializa la delegación de forma nominal en el entonces Director del CESID (Centro Superior de Información de la Defensa).

El director del CESID decide crear, como órgano de trabajo específico para los asuntos de seguridad de la Información Clasificada de la OTAN, la Oficina Nacional de Seguridad (ONS), organismo que a la postre se encarga de cumplir y hacer cumplir los compromisos adquiridos por España en el ámbito internacional en materia de protección de Información Clasificada.

Las normas de la Unión Europea plasmadas, en su última versión, en la decisión del Consejo de 23 de septiembre de 2013 sobre las normas de seguridad para la protección de la Información Clasificada de la UE (2013/488/UE), establecen en su artículo 16-3-a que los Estados miembros: "designarán una ANS responsable de las medidas de seguridad para la protección de la Información Clasificada de la UE…"

Siguiendo la estela del nombramiento efectuado en 1982, por acuerdo del Consejo de Ministros de fecha 19 de abril de 2002 se crea la Autoridad Nacional de Seguridad para la protección de la Información Clasificada de la Unión Europea y la Unión Europea Occidental, recayendo nuevamente de forma conjunta en los ministros de Asuntos Exteriores y Defensa, y nuevamente con capacidad de delegar sus funciones en una autoridad delegada

Mediante la Orden Comunicada de 24 de mayo de 2002 se designa nuevamente autoridad delegada para la seguridad de la Información Clasificada para la Unión Europea y Unión Europea Occidental al entonces Secretario de

Estado Director del Centro Nacional de Inteligencia (organismo que sustituyó al CESID y que fue creado por la Ley 11/2002 de 6 de mayo reguladora del Centro Nacional de Inteligencia).

España ratificó su adhesión al Convenio de creación de la Agencia Espacial Europea (ESA) el 3 de marzo de 2005, siendo publicado en el Boletín Oficial del Estado número 53 el instrumento de adhesión. Esta adhesión exigía cumplir con la normativa de seguridad de la ESA, la cual nuevamente exigía el nombramiento de una Autoridad Nacional de Seguridad responsable de la seguridad de la Información Clasificada de la ESA.

La Autoridad Nacional de Seguridad para la seguridad de la Información Clasificada de la Agencia Espacial Europea se crea por acuerdo de Consejo de Ministros de fecha 18 de noviembre de 2005, recayendo el nombramiento de forma conjunta, tal y como se había hecho anteriormente para la OTAN y para la UE, en los ministros de Asuntos Exteriores y Cooperación y de Defensa, nuevamente con capacidad de delegar sus funciones.

Finalmente, mediante la ORDEN PRE/3289/2006, de 23 de octubre, se designa la Autoridad Delegada para la seguridad de la Información Clasificada de la Agencia Espacial Europea al Secretario de Estado Director del CNI. Esta última designación es al cargo y no a la persona, por lo que de forma automática cualquiera que ocupe el cargo de Secretario de Estado Director del CNI automáticamente pasa a ser la Autoridad Nacional de Seguridad Delegada para la protección de la Información Clasificada de la ESA.

Dado que los nombramientos para la OTAN y la UE eran nominales, los cambios de persona en el puesto de Secretario de Estado Director del CNI exigieron el nombramiento de cada uno de ellos como Autoridad Nacional de Seguridad para la OTAN y la UE, y en el año 2009, finalmente, se decide realizar el nombramiento al cargo en lugar de a la persona, lo cual se materializó en la Orden PRE/2130/2009, de 31 de julio, por la que se designa la Autoridad Delegada para la Seguridad de la Información Clasificada originada por las partes del Tratado del Atlántico Norte, por la Unión Europea y por la Unión Europea Occidental al Secretario de Estado Director del CNI.

El Centro Nacional de Inteligencia se encontraba adscrito al Ministerio de Defensa desde su creación por la Ley 11/2002, si bien dicha ley contemplaba la

posibilidad de que el CNI pasara a depender orgánicamente del Ministerio de la Presidencia. El 23 de diciembre de 2011 se produjo el cambio de adscripción como parte de las medidas adoptadas por el gobierno para reestructurar la Administración Central del Estado, pasando el CNI a depender del Ministerio de la Presidencia. Este cambio de adscripción suponía que orgánicamente el CNI se encontraba en el Ministerio de la Presidencia, pero en lo relacionado con la protección de la información clasificada de la OTAN, la UE y la ESA, en calidad de Autoridad Nacional de Seguridad Delegada, la dependencia seguía siendo de los ministros de Asuntos Exteriores y Defensa.

Esta circunstancia llevó a estudiar diferentes opciones para solucionar el asunto, y finalmente se decidió que la Autoridad Nacional de Seguridad, en los tres ámbitos mencionados, pasara a ser compartida por tres ministros, el de Presidencia del Gobierno, el de Asuntos Exteriores y Cooperación y el de Defensa. Esta decisión se plasmó en el Acuerdo de Consejo de Ministros de fecha 11 de mayo de 2012 por el que se modifican los tres acuerdos anteriores que se han mencionado.

En definitiva, la falta de regulación en la legislación nacional sobre la Autoridad Nacional de Seguridad para la protección de la Información Clasificada, en cualquier ámbito, nacional e internacional, ha ocasionado una cadena de nombramientos en sucesivos acuerdos de Consejo de Ministros, a los que siguieron las subsiguientes órdenes de designación de la Autoridad Nacional de Seguridad Delegada, en todos los casos, como ya se ha expuesto, en la figura del Secretario de Estado Director del CNI.

Esta designación, unido a la creación de la Oficina Nacional de Seguridad tiene una importancia trascendental en el cumplimiento de las obligaciones adquiridas por España en materia de protección de Información Clasificada en las tres organizaciones mencionadas, OTAN, UE y ESA, como veremos en los apartados siguientes.

Sin embargo, los nombramientos solo lo son para los tres ámbitos mencionados, OTAN, UE, ESA, mientras que en otras organizaciones como la OCCAR, al no haberse efectuado tal nombramiento, estrictamente hablando, la Autoridad Nacional de Seguridad no tiene las competencias necesarias para encargarse de la protección de la Información Clasificada de esta organización.

Esta misma situación de falta de nombramiento de la Autoridad Nacional de Seguridad española se produce en otras organizaciones internacionales a las que pertenece España y que disponen de Información Clasificada con marca propia. En todos los casos la Autoridad Nacional de Seguridad Delegada creada para la OTAN, UE y ESA, a pesar de la falta de nombramiento, se ha encargado de cumplir y hacer cumplir, en aplicación de su normativa, los requisitos de protección de la Información Clasificada de estas otras organizaciones internacionales.

### 4.7.2. Comités de Seguridad de la OTAN, UE y ESA

Las tres Organizaciones Internacionales para las que España nombró expresamente una Autoridad Nacional de Seguridad, crearon en su normativa un Comité de Seguridad en el que participan todas las naciones mediante el nombramiento de un representante de la Autoridad Nacional de Seguridad.

Todos los Comités de Seguridad tienen en común estar a cargo de la revisión de la política de seguridad de la Información Clasificada de la Organización Internacional, así como de elaborar directivas en los diferentes ámbitos de seguridad de la Información clasificada ya mencionados: en el personal, en las instalaciones, en los sistemas CIS y en la industria.

También es responsabilidad de los Comités supervisar la correcta aplicación de dicha normativa dedicando especial atención a los casos en los que se haya producido o existan razones de peso para pensar que se podría haber producido un acceso no autorizado a información clasificada. Todos los representantes españoles nombrados para los Comités de Seguridad de la OTAN, la Unión Europea y la ESA pertenecen a la Oficina Nacional de Seguridad.

Ha cobrado especial importancia la asistencia a estos comités para actualizar las Normas de la Autoridad Nacional de Seguridad, especialmente en lo relativo a la seguridad de la información Clasificada en la Industria, y evitar que los nuevos requisitos que se exigen a las empresas, o aquellos que se suavizan, no terminen siendo el arma arrojadiza contra el tejido industrial español con la que dejar fuera a las empresas españolas de los procesos de

contratación de las Organizaciones Internacionales.

Otras organizaciones internacionales a las que pertenece España como la OCCAR no han exigido expresamente el nombramiento de una Autoridad Nacional de Seguridad, en realidad porque han asumido que dicha Autoridad existe en cada uno de los Estados que forman parte de la organización. Sin embargo dentro de la OCCAR sí se ha creado un Comité de Seguridad para garantizar la protección de la Información Clasificada manejada o generada en los programas clasificados promovidos por esta organización, en el que participa un representante de la Autoridad Nacional de Seguridad, la cual estrictamente hablando no existe para la OCCAR, pues, como ya se ha dicho, los ámbitos para los que se ha creado la Autoridad Nacional de Seguridad son, como ya se ha dicho, la OTAN, la UE y la ESA.

### 4.7.3. Las Normas de la Autoridad Nacional de Seguridad

En todos los nombramientos de la Autoridad Nacional de Seguridad se facultó a la misma a elaborar la normativa necesaria para la protección de la Información Clasificada de la que se hacía responsable a la nueva Autoridad creada. Esta facultad a su vez fue delegada, junto con el resto de las funciones de la Autoridad Nacional de Seguridad en el Secretario de Estado Director del CNI, quien en uso de estas atribuciones decidió elaborar un conjunto normativo para dar cumplimiento a las exigencias de la OTAN, la UE y la ESA.

La primera cuestión, dado que hubo un total de tres nombramientos, uno para cada ámbito internacional OTAN, UE y ESA, fue decidir si se debían elaborar tres normativas diferentes, o únicamente una, y por razones prácticas, dado que en la mayoría de los casos son los mismos entes y personas los que manejan Información Clasificada de las tres organizaciones, se decidió que únicamente se elaboraría una normativa que cubriera las necesidades y obligaciones marcadas en las tres normativas de seguridad, una de cada organización.

Por antigüedad de la norma, la primera organización que elaboró normativa fue la OTAN, y realmente las de la Unión Europea y la Agencia Espacial Europea se derivan de ella con pequeños cambios para ajustarlas a sus respectivos ámbitos.

Todas estas normativas, además de incorporar disposiciones sobre el tratamiento de la Información Clasificada tales como marcado, identificación, reproducción, transporte, etc. contemplan la exigencia de medidas en los siguientes campos: seguridad de la Información Clasificada en el Personal, seguridad de la Información Clasificada en las Instalaciones, seguridad de la Información Clasificada en los sistemas CIS y Seguridad de la Información Clasificada en poder de la Industria.

Las Normas elaboradas por la Autoridad Nacional de Seguridad incorporan provisiones en todos estos campos, y son el referente para la protección de la Información Clasificada internacional, tanto de las organizaciones internacionales, como de terceros estados con los que se tiene suscrito un acuerdo bilateral para la protección de Información Clasificada. Además, como ya se ha mencionado anteriormente, debido a la ausencia de regulación en una gran parte de la administración española son el referente para aquellos departamentos ministeriales que no han desarrollado normativa de protección de Información Clasificada.

En los sub-apartados siguientes se van a dar unas pinceladas de lo contenido en las principales normas de la Autoridad Nacional de Seguridad.

*4.7.3.1. Protección de la Información Clasificada en el personal*

La protección de la Información Clasificada en las personas se apoya, una vez cumplidos los requisitos de elegibilidad exigidos en las Normas de la Autoridad Nacional de Seguridad, en tres grandes pilares: fiabilidad, concienciación e instrucción, siendo la fiabilidad el aspecto más importante y a la vez más difícil de determinar.

La fiabilidad, más bien la no presencia de indicios de falta de fiabilidad, la determina la Oficina Nacional de Seguridad mediante la investigación de la persona y su entorno, la cual se realiza con su consentimiento, de acuerdo con los criterios de fiabilidad estipulados en las normas de la Autoridad Nacional de Seguridad, concretamente en la NS02.

El consentimiento de la persona es necesario puesto que la concesión de una Habilitación Personal de Seguridad (HPS) no es un derecho y en consecuencia puede ser denegada. La concesión de la Habilitación Personal de

Seguridad representa el establecimiento de un vínculo de confianza mutuo entre la persona y la Administración: ésta última permitiendo el acceso a Información Clasificada, y la persona permitiendo ser investigada.

Una vez determinada la fiabilidad del solicitante, y concienciado e instruido convenientemente, la Autoridad Nacional de Seguridad, a propuesta de la ONS, concede a cada persona, por un determinado tiempo, una Habilitación Personal de Seguridad hasta un determinado grado y para un determinado tipo de Información Clasificada, que junto con la necesidad de conocer son los requisitos mínimos para que ésta pueda acceder a Información Clasificada de ese tipo y ese grado.

*4.7.3.2. Protección de la Información Clasificada en las instalaciones*

La protección de la información Clasificada en las instalaciones, tanto si estas son de las administraciones, como si pertenecen a una empresa, se basa en el establecimiento de una serie de medidas físicas de protección que han de quedar recogidas en un plan de protección que tiene que ser aprobado por la Oficina Nacional de Seguridad.

Las medidas físicas son más exigentes cuanto mayor es el grado de la Información Clasificada que se almacena en la instalación en cuestión, quedando recogidas estas medidas en las normas de la Autoridad Nacional de Seguridad, concretamente en la NS03.

Desde un punto de vista conceptual las medidas físicas pretenden disuadir, detectar, retardar y reaccionar. Disuadir al potencial intruso de iniciar su intento de entrar en la instalación protegida a la vista de las medidas de seguridad implementadas (algunas de ellas son intencionadamente evidentes), detectar inmediatamente el intento de intrusión en el caso de que se inicie dicha acción, retardar el máximo tiempo la posible intrusión para, finalmente, permitir reaccionar de forma adecuada e impedir la intrusión.

*4.7.3.3. Identificación y Tratamiento de la Información Clasificada*

Las tres organizaciones internacionales que exigieron a España el nombramiento de una Autoridad Nacional de Seguridad, a su vez exigieron que dicha autoridad estableciera un registro central de Información Clasificada de

estas tres organizaciones de forma que tuviera conocimiento de quién tiene Información Clasificada de las mismas.

Las normas de la Autoridad Nacional de Seguridad, concretamente la NS04, establece los procedimientos necesarios para que la Oficina Nacional de Seguridad pueda cumplir con el cometido de controlar la Información Clasificada internacional que se encuentra en territorio español bajo la custodia de organismos y empresas españolas.

En dicha norma también se especifican los procedimientos concretos para el marcado, identificación, reproducción, reclasificación, desclasificación, acceso, cesión, transmisión, transporte y destrucción de la Información Clasificada.

*4.7.3.4. Protección de la Información Clasificada en sistemas CIS*

Al igual que los locales donde se almacena Información Clasificada, los Sistemas de Información y Comunicación (CIS en sus siglas en inglés) donde se encuentra dicha Información Clasificada, han de ser previamente autorizados por la Autoridad Nacional de Seguridad.

La autorización de los sistemas CIS, dada la complejidad de los mismos y de las amenazas a las que pueden estar sometidos, requiere que sean acreditados técnicamente, lo cual es realizado por el Centro Criptológico Nacional (CCN), organismo adscrito al Centro Nacional de Inteligencia, referente nacional a día de hoy en ciberseguridad.

Las Normas de la Autoridad Nacional de Seguridad, concretamente la NS05, establece el proceso a seguir para solicitar la autorización para manejar Información Clasificada en un sistema CIS. Como complemento de esta norma, el CCN tiene un conjunto de normas técnicas sobre Seguridad de las Tecnologías de de la Información y Comunicación (STIC) con las que hay que cumplir, basadas todas ellas en un análisis de riesgos del sistema que se pretende acreditar.

La acreditación técnica del sistema CIS pretende garantizar la confidencialidad, integridad, disponibilidad, autenticidad y no repudio de la Información Clasificada almacenada, procesada y transmitida en el sistema CIS.

*4.7.3.5. Protección de la Información Clasificada en la Industria*

Ya se ha mencionado que permitir a las empresas manejar o generar Información Clasificada supone asumir ciertos riesgos inherentes a la propia naturaleza de las empresas. Sin embargo, no es menos cierto que sin la contratación de las empresas, especialmente de las más avanzadas tecnológicamente, sería imposible que los Estados abordaran el desarrollo de determinados proyectos.

Para lograr la confluencia de estas dos circunstancias, asumir el riesgo y poder cubrir la necesidad, se exige a las empresas obtener una Habilitación de Seguridad de Empresa (HSEM) antes de permitir que sus empleados puedan, a su vez, solicitar a través de la empresa una Habilitación Personal de Seguridad. Únicamente cuando ambas habilitaciones se hayan obtenido, la empresa podrá ser adjudicataria de alguno de los contratos públicos, tanto de las administraciones como de las organizaciones internacionales, en los que se va a manejar o generar Información Clasificada.

Además, cuando la empresa vaya a almacenar la Información Clasificada en sus propias instalaciones deberá obtener una Habilitación de Seguridad de Establecimiento (HSES), que, en términos generales, significa cumplir con los requisitos de seguridad física exigidos en la NS03 mencionados anteriormente en el apartado de protección de las instalaciones.

Al igual que en el caso de las personas, las empresas han de someterse voluntariamente a ser investigadas, investigación que realiza la Oficina Nacional de Seguridad de acuerdo con lo establecido en las Normas de Autoridad Nacional de Seguridad, concretamente en la NS06.

Dicha investigación pretende determinar cuatro aspectos de la empresa: personalidad jurídica, capacidad técnica, solvencia económica y fiabilidad, siendo la fiabilidad, como en el caso de las personas, el aspecto más importante, y para ello se estudia con detalle la distribución de la propiedad de la empresa, la composición del consejo de administración y los resultados de su actividad económica.

Los criterios de fiabilidad, o más bien, como ya se ha mencionado para el caso de las personas, la ausencia de datos que indiquen que la empresa no es fiable, se encuentran definidos en las Normas de la Autoridad Nacional de

Seguridad, concretamente en la NS06. Una vez superada la investigación, a propuesta de la ONS, la Autoridad Nacional de Seguridad concede a la empresa la Habilitación de Seguridad de Empresa que ha solicitado, lo cual permite a la misma participar en contratos en los que se maneje o genere Información Clasificada.

### 4.8. ACUERDOS BILATERALES SOBRE PROTECCIÓN DE INFORMACIÓN CLASIFICADA

El establecimiento del vínculo de confianza mutuo entre dos Estados que permita reconocer la capacidad de cada uno de ellos para manejar Información Clasificada del otro se plasma en un Acuerdo Bilateral sobre protección de Información Clasificada.

Dichos acuerdos de seguridad suelen abarcar tanto a las administraciones de los estados firmantes como a sus empresas, incluyendo a las personas que desempeñan sus cometidos tanto en unas como en otras.

Los acuerdos bilaterales de seguridad firmados por España son Tratados Internacionales, y por lo tanto con rango de ley, motivo por el que todos ellos en España han de ser ratificados tanto por el Congreso de los Diputados como por el Senado. Una vez cumplido este trámite (no solo en España sino también en el otro país firmante) el acuerdo es publicado en el Boletín Oficial del Estado entrando de esta manera en vigor.

Todos los Acuerdos son negociados por la Autoridad Nacional de Seguridad, en concreto por personal especializado de su órgano de trabajo, la Oficina Nacional de Seguridad, siendo necesario para comenzar la negociación argumentar la necesidad del acuerdo y solicitar el permiso del Consejo de Ministros.

Durante la negociación del texto, cada parte realiza los estudios que estimen necesarios tanto de la normativa como de los procedimientos existentes en la otra parte para proteger la información clasificada al objeto de identificar tanto las similitudes como las diferencias existentes entre ambas partes a la hora de proteger la información clasificad. En base a dichos estudios, se establecerá el ámbito del tratado y se redactarán las disposiciones correspondientes. Así pues, no existen dos Acuerdos iguales.

En el momento de redactar este trabajo hay un total de 32 Acuerdos bilaterales de Seguridad firmados con diferentes países, pudiéndose acceder a cada uno de ellos a través de la página web de la Oficina Nacional de Seguridad www.cni.es/es/ons.

### 4.8.1. Certificación cruzada de las habilitaciones de empresas y personas

Uno de los aspectos más importantes derivado tanto de la normativa sobre protección de Información Clasificada de las Organizaciones Internacionales a las que pertenece España, como de los propios acuerdos bilaterales para la protección de Información Clasificada firmados por España, es el reconocimiento en dichas Organizaciones Internacionales y terceros estados de las habilitaciones de seguridad concedidas en España a personas y empresas. En el caso de los españoles con Habilitación Personal de Seguridad, el reconocimiento de esta les permite, por ejemplo, poder optar a puestos en las Organizaciones Internacionales en los que se requiera acceder a Información Clasificada.

En el caso de las empresas la validez de su Habilitación de Seguridad de Empresa y las de su personal, permite a las mismas ser adjudicataria de aquellos contratos de las Organizaciones Internacionales y de terceros estados en los que se pida estar capacitado para el manejo de Información Clasificada.

Como contrapartida, son reconocidas en España las Habilitaciones de Seguridad de personas y empresas de los estados integrantes de las organizaciones internacionales a las que pertenece España, así como de los terceros estados con los que España tiene firmado un acuerdo bilateral para la protección de información Clasificada.

La certificación de dichas Habilitaciones de Seguridad de empresas y personas las realiza la Autoridad de Seguridad Nacional, puesto que es quien las concede, directamente a las autoridades de seguridad de las Organizaciones Internacionales y de los terceros estados, es decir, de autoridad a autoridad. A su vez las autoridades nacionales de seguridad de estos Estados certifican a la Autoridad española la validez de las habilitaciones de sus nacionales y de sus empresas.

Las Organizaciones Internacionales no conceden habilitaciones a empresas, siendo los Estados miembros de la misma, aplicando sus legislaciones nacionales,

quienes las conceden. En consecuencia, las Organizaciones Internacionales no certifican ningún tipo de habilitación de seguridad de empresa, y únicamente reciben la certificación de los Estados, previa solicitud de la misma, cuando es necesario.

## 4.9. LA SEGURIDAD EN LOS PROGRAMAS CLASIFICADOS

### 4.9.1. Esquema General

Es difícil encontrar desarrollos tecnológicos de cierta envergadura, especialmente en el ámbito de la defensa, que puedan ser abordados por un solo Estado, fundamentalmente debido al coste económico que supone. Por otra parte nos encontramos que ciertos desarrollos directamente nacen para dar servicio a un conjunto de Estados, lo cual implica que su desarrollo sea abordado de forma conjunta por todos los Estados que van a utilizar el servicio en cuestión.

En el primer caso de colaboración, para hacer viable económicamente un desarrollo complejo, podemos incluir el avión de combate EuroFigther EF2000, en cuyo desarrollo intervienen cuatro naciones, España, Alemania, Reino Unido e Italia, o el avión de transporte A400M, en cuyo desarrollo intervienen España, Alemania, Reino Unido, Francia y Turquía.

En el segundo de los casos de colaboración, podemos mencionar el programa de satélites Galileo de la Unión Europea, cuyo propósito es poder dar servicio al conjunto de los Estados miembros de la Unión, si bien algunos de los servicios que proporcionará este programa serán de acceso libre, como es el caso del posicionamiento que podrá ser utilizado libremente por cualquier usuario, como a día de hoy ocurre con el sistema de posicionamiento norteamericano GPS.

La gestión de los diferentes programas viene a organizarse de forma muy parecida en todos ellos, creándose una estructura multinacional en la que se distinguen claramente dos partes diferenciadas: por un lado la gestión técnica y económica, y por otro la gestión de la seguridad de la Información Clasificada. En dicha estructura, la gestión técnica y económica recae en la Oficina Conjunta del Programa, de la cual dependen las Oficinas Nacionales de dicho programa, mientras que la gestión de la seguridad de la Información Clasificada recae en el

grupo o comité de seguridad del programa, al cual asisten representantes de las Autoridades Nacionales de Seguridad de los participantes en el programa.

Cuando el programa se enmarca dentro de una determinada Organización Internacional, normalmente el comité de seguridad del programa se encuentra vinculado, cuando no subordinado, al comité de seguridad de la propia Organización Internacional

### 4.9.2. Normativa de Seguridad. El Comité de Seguridad del programa

Parece evidente, en el caso del programa Galileo, que se garantice la protección de la Información Clasificada de los programas de la Unión Europea aplicando la normativa de seguridad de la Unión Europea, y así es, pero no exclusivamente.

Estos programas cooperativos, como es el caso del programa Galileo, utilizan Información Clasificada nacional de algunos de los Estados que forman parte del programa, por ejemplo en el programa Galileo el único Estado con lanzadores de satélites al espacio es Francia, y la información Clasificada relacionada con estos lanzadores es francesa, pues en realidad los lanzadores existen con anterioridad al programa Galileo.

En el caso del avión de transporte A400M, proyecto gestionado por la Organización Conjunta de Cooperación en Materia de Armamento (OCCAR), de la que no forma parte Turquía, no parece tan evidente cual es la normativa de protección de Información Clasificada que se ha de aplicar, puesto que la de la OCCAR no es de aplicación, al menos de forma directa, en Turquía.

Debido a estas dos circunstancias, lo habitual para garantizar la seguridad de la Información Clasificada en los programas internacionales es que el comité de seguridad del programa en cuestión desarrolle una documentación de seguridad armonizada con todas aquellas que pudieran ser de aplicación: la de la Organización Internacional, la de los Estados participantes y la de terceros estados u organizaciones internacionales si fuera necesario.

Esta documentación de seguridad armonizada se denomina Instrucciones de Seguridad del Programa (Programme Security Instructions, PSI, en su denominación en inglés), y desde el momento de su aprobación por los Estados participantes en el programa pasa a ser la "normativa" de aplicación para la

gestión de la seguridad de la Información Clasificada manejada o generada en el programa.

El comité de seguridad del programa es el encargado de la elaboración de las Instrucciones de Seguridad del Programa, así como de su revisión cuando sea necesario. En dicho comité, como ya se ha dicho, participan las Autoridades Nacionales de Seguridad de todos los Estados participantes en el programa.

Como vemos, además de las normas de las Organizaciones Internacionales, la de los Estados, y los acuerdos bilaterales de protección de Información Clasificada, encontramos que tenemos una normativa específica para cada programa clasificado en que participa España. Por la precedencia de aplicación de la norma, para un determinado programa, evidentemente las instrucciones de seguridad de este son la fuente primaria.

Mencionar que las Instrucciones de Seguridad de los programas solo son de aplicación a las empresas que sean contratadas en el marco del programa, así como a la propia Organización Internacional que gestiona dicho programa. Nuevamente tenemos que mencionar que las Instrucciones de Seguridad de los Programas remiten a las legislaciones nacionales, y, por ejemplo, la concesión de las habilitaciones de seguridad a personas y empresas siempre corresponderá a los Estados participantes en el programa.

### 4.9.3. Oficina de Programa Conjunta Y Oficina de Programa Nacional

Ya se ha mencionado que la oficina de programa conjunta desarrolla los aspectos técnicos y económicos del programa, y desde el punto de vista de la protección de la Información Clasificado el aspecto que más nos interesa es la confección de la Guía de Clasificación de Seguridad.

Es evidente que han de ser los técnicos en una determinada materia quienes especifiquen que partes del desarrollo, por su especial sensibilidad, han de ser protegidas y en consecuencia clasificadas. Dicha definición se hace de forma colegiada entre todas las Oficinas Nacionales de un determinado programa, quedando plasmada la decisión conjunta en la Guía de Clasificación de Seguridad, que sirve como directiva de clasificación del programa. A partir de la aprobación de la misma todo lo contenido en ella ha de ser clasificado en el

grado especificado en la Guía de Clasificación de Seguridad.

La Oficina de Programa Conjunta y cada una de las Oficinas Nacionales han de garantizar que se exigen a las empresas contratistas los requisitos de seguridad establecidos para el programa en sus Instrucciones de Seguridad. En el siguiente capítulo abordaremos como se transfieren los requisitos de seguridad a la industria.

### 4.9.4. Información Clasificada y Contratación

La contratación con las empresas de bienes y servicios relacionados con la seguridad y defensa nacional de los Estados y la seguridad de las Organizaciones Internacionales, es decir la contratación cuando se va a manejar o generar Información Clasificada de los mismos, es la forma habitual mediante la cual la Información Clasificada es manejada y/o generada por las empresas.

Es fácil deducir que en el desarrollo de los programas clasificados, una vez recorridas una serie de etapas de diseño y definición de requisitos, incluyendo, por supuesto, el diseño y los requisitos de la seguridad de la Información Clasificada, se procede a la contratación de todas aquellas partes que han de ser desarrolladas por la industria, de las cuales algunas serán clasificadas, y en consecuencia manejarán o generarán Información Clasificada.

La contratación en este caso es extremadamente delicada porque además de los aspectos derivados de la propia contratación, aparecen dos nuevos asuntos sobre los que hay que prestar una atención especial: la seguridad del suministro y la seguridad de la Información Clasificada.

Sobre el primero de ellos no nos extenderemos mucho, simplemente mencionar que resulta difícil que se adjudique un contrato de, por ejemplo, un avión de combate a la empresa de un estado que no nos garantiza el suministro del propio avión o de sus repuestos, y que en consecuencia puede provocar la indisponibilidad o la inoperatividad del mismo. Es evidente que se requiere incorporar en este tipo de contratación algunas provisiones que nos garanticen la seguridad del suministro.

En cuanto a la protección de la Información Clasificada, la inclusión de requisitos específicos en este campo, necesarios para garantizar la seguridad y defensa nacional, la de nuestros aliados o la de las Organizaciones

Internacionales a las que pertenecemos, ocasiona diversos efectos derivados de esta circunstancia, siendo el más importante la generación de un mercado restringido al conjunto de empresas con capacidad de manejar Información Clasificada.

Es más, en algunas ocasiones la contratación cuando se ha de manejar Información Clasificada de una nación está cerrada a las empresas de otras en aplicación de su legislación nacional, incluso existiendo un acuerdo bilateral de protección de Información Clasificada. No debemos olvidar que la seguridad y defensa nacional son dos aspectos fuertemente ligados a la soberanía del Estado.

Evidentemente esta circunstancia puede ser utilizada torticeramente para provocar mercados esclavos, impidiendo la libre competencia y libre concurrencia de las empresas de unos países en otros. La Unión Europea, muy consciente de esta circunstancia, en el año 2009 aprobó la Directiva 81/2009/EC sobre contratación en los ámbitos de defensa y seguridad de la que hablaremos más adelante.

### 4.9.5. Transferencia de requisitos de Seguridad a la Industria

Las diferentes administraciones, desde las locales hasta las de la Unión Europea, pasando por supuesto por las administraciones nacionales, y en el caso particular de España por las administraciones autonómicas, entienden de normas. Las generan y las aprueban a diferentes niveles mediante los instrumentos legales que cada una de estas administraciones tiene a su disposición.

Sin embargo, las empresas entienden mejor sus obligaciones, incluso si son normas elaboradas y publicadas por las diferentes administraciones, cuando vienen reflejadas como parte de sus contratos en las cláusulas correspondientes, y es práctica habitual de las administraciones que se plasmen en las cláusulas de los contratos todos los requisitos del mismo.

En el caso particular de un contrato en el que se va a generar o acceder a Información Clasificada, las exigencias de seguridad se reflejan en las cláusulas de seguridad del contrato (Security Aspect Letter en su denominación en Inglés) que se han de incorporar al mismo. Para los programas en los que participan

varias naciones es habitual, como ya se ha mencionado, que se elaboren unas Instrucciones de Seguridad del Programa (Programme Security Instruction en su denominación en inglés) que se adjuntarán, total o parcialmente, a cada uno de los contratos que se deriven del programa en los que se maneje y/o genere Información Clasificada.

En algún caso podemos encontrar que las cláusulas contenidas en las instrucciones de seguridad de un programa difieren de las establecidas en la normativa nacional. En general esto ocurre por la necesidad de armonizar las normativas de los diferentes países que participan en el programa, pero no genera ninguna inseguridad jurídica a las empresas al utilizarse el principio de aplicación de la norma específica, en nuestro caso las instrucciones de seguridad del programa, cuando exista, y aplicación de la norma general en ausencia de norma específica.

### 4.9.6. Libre Competencia frente al Secreto

Es un principio fundamental de las economías modernas la garantía de la libre competencia de las empresas para acceder a la contratación con las administraciones públicas, tanto de los Estados como de las Organizaciones Internacionales y supranacionales con capacidad de contratar.

Este principio de libre competencia, que finalmente se materializa en la publicidad de las ofertas, la transparencia de los requisitos y la libre concurrencia de los licitadores parece enfrentarse de manera directa con la contratación cuando se ha de manejar Información Clasificada. Las empresas que carecen de Habilitaciones de Seguridad pueden ser excluidas de ciertos contratos por esta circunstancia.

Ciertamente, dentro de las capacidades técnicas que ha de tener una empresa para poder participar en un determinado proceso de contratación, la demostración de que posee los conocimientos, que tiene implantada la estructura de seguridad y que aplica los procedimientos adecuados para proteger la Información Clasificada puede ser considerada una más de ellas. Sin embargo, así como otras capacidades pueden ser ponderables, el cumplimiento de los requisitos de seguridad se aplica de forma estricta: si tiene las habilitaciones de seguridad puede ser adjudicatario del contrato, en caso contrario no.

Quiero mencionar que para poder garantizar la libre competencia en la práctica totalidad de los procesos de contratación cuando se ha de manejar Información Clasificada, la exigencia de disponer de las capacidades necesarias para manejarla debe figurar en la adjudicación de contrato, y no en la presentación de las ofertas a dicho contrato. No hacerlo de esta forma significa eliminar posibles competidores en la fase de licitación.

Únicamente es admisible que se exijan las habilitaciones de seguridad a personas y empresas en la fase de licitación cuando el propio pliego de condiciones técnicas esté clasificado por contener Información que ha de ser protegida. Es decir no se le podría entregar a una empresa que con carácter previo no disponga de las habilitaciones de seguridad pertinentes.

En el caso particular de España, todos los órganos de contratación tienen la obligación de firmar una carta de expectativas de participación en un contrato en el que se maneje Información Clasificada a las empresas que estén interesadas en licitar, de forma que puedan solicitar las habilitaciones necesarias de la empresa y su personal a la Autoridad Nacional de Seguridad. Este es el mecanismo por el que se trata de garantizar la libre competencia y la igualdad de oportunidades de las empresas.

### 4.9.7. Contratación en los sectores de Defensa y Seguridad

Dada la naturaleza clasificada de muchos suministros relacionados con la defensa y la seguridad, la Unión Europea decidió desarrollar una directiva sobre contratación en este campo y cuyo resultado fue la

> "Directive 2009/81/EC of the European Parliament and of the Council of 13 July 2009 on the coordination of procedures for the award of certain works contracts, supply contracts and service contracts by contracting authorities or entities in the fields of defence and security".

La capacidad y la fiabilidad de los operadores económicos para proteger la Información Clasificada son de hecho cruciales para la concesión y ejecución de muchos contratos de los ámbitos de la defensa y la seguridad. Al mismo tiempo la apertura de los mercados de defensa y seguridad de los Estados miembros de la UE se encontraba amenazada por la falta de un régimen en toda Europa para

la protección de la Información Clasificada.

Es prerrogativa de cada uno de los Estados de la Unión determinar qué información tiene que ser clasificada y en qué grado, y cada Estado, como ya se ha mencionado, concede sus propias habilitaciones a los contratistas con capacidad de proteger Información Clasificada. Estas habilitaciones de seguridad no son inmediatamente reconocidas entre Estados Miembro de la Unión Europea, si bien en muchos casos existen acuerdos bilaterales de protección de Información Clasificada, lo cual alivia el impacto negativo que sobre la efectividad de la directiva.

La directiva proporciona diversas garantías de seguridad de la Información Clasificada que posibilita a las autoridades de contratación limitar las exclusiones y las exenciones basadas en la exclusividad de los Estados en materia de defensa y seguridad contemplada en el tratado de la Unión, a casos realmente excepcionales.

La seguridad de la Información Clasificada aparece en diferentes partes de la directiva, son mencionados como requisitos en el artículo 7 de la directiva para las fases de licitación y contratación, puede ser causa de exclusión según el artículo 13 (cuando se invoque el artículo 346 del TFUE), puede ser una condición del contrato y un criterio de selección. La combinación de todas estas provisiones permite incorporar requisitos de protección de Información Clasificada en diferentes etapas de la contratación, desde la fase de licitación hasta la fase de ejecución del contrato.

La directiva 81/2009 debía ser transpuesta a las legislaciones nacionales en el mes de agosto de 2011, y en ese mes precisamente se publicó en España la ley 24/2011 de contratos de los sectores de defensa y seguridad, la cual es precisamente el desarrollo legislativo español para transponer la directiva.

Aunque no olvidemos que se trata de una ley de contratación, la misma incorpora requisitos en los campos de la seguridad del suministro y de la seguridad de la Información Clasificada, dado lo específico de los ámbitos que pretende regular.

En lo relativo a la protección de la Información Clasificada en la industria española, esta ley ha supuesto que la Autoridad Nacional de Seguridad y su normativa sean el único referente en este campo, ya sin excepción del tipo y clase

de Información Clasificada, al establecer la ley en su disposición adicional quinta que serán de aplicación a la industria española cuantas disposiciones establezca la Autoridad Nacional de Seguridad.

En la misma disposición adicional se establece que la Autoridad Nacional de Seguridad será la encargada de certificar las habilitaciones de seguridad de empresa y habilitaciones de seguridad de establecimiento de las empresas españolas, y en el caso de candidatos o licitadores no nacionales, le corresponderá a la Autoridad Delegada para la Seguridad de la Información Clasificada reconocer, al amparo de la normativa internacional vigente, las habilitaciones expedidas por otros Estados, así como certificar al órgano de contratación dicha circunstancia.

A pesar de que esta situación clara de respaldo de la Autoridad Nacional de Seguridad para la OTAN, UE y ESA en lo relativo a la protección de la Información Clasificada en la industria es positiva, nuevamente hemos de reconocer que hace falta que tal respaldo aparezca claramente establecido en la Ley de Secretos Oficiales. Después de todo la ley 24/2011 es una ley de contratación que incorpora algunas provisiones en el terreno de la seguridad de la Información Clasificada.

## 4.10. CONCLUSIONES

Se ha mencionado a lo largo del trabajo la importancia que tiene la legislación nacional en la protección de la Información Clasificada de las organizaciones internacionales y sus programas, y desafortunadamente hay que decir que siendo la pieza clave del engranaje de protección encontramos deficiencias y carencias en dicha legislación.

Está desajustado el esquema legislativo español necesario para dar respuesta a las exigencias actuales en materia de protección de la Información Clasificada de cualquier tipo y grado, nacional o internacional, el cual debería basarse en tres niveles de desarrollo:

1. La ley de Secretos Oficiales que dé cobertura legal al máximo nivel a lo previsto en el artículo 105b de la Constitución incorporando el nombramiento de la Autoridad Nacional de Seguridad.

2. Un Real Decreto que establezca las funciones de la Autoridad Nacional de Seguridad, incluyendo la posibilidad de delegar estas funciones en una Autoridad Delegada.

3. Cinco disposiciones de rango de instrucción de Secretario de Estado elaboradas por la Autoridad Delegada designada al efecto, en las que se incluyan instrucciones para la protección y el tratamiento de la Información Clasificada en soporte físico, en las personas, en las instalaciones, en los sistemas de información y telecomunicación y en la industria.

En cuanto al primer nivel, es necesario abordar una actualización de la Ley de Secretos Oficiales que se alinee de forma clara con los estándares internacionales de las organizaciones de las que España forma parte.

En particular es necesario que vengan reflejados los cuatro niveles de clasificación que contemplan las normativas internacionales, a la vez que se proceda al nombramiento de una Autoridad Nacional para la Protección de la Información Clasificada que solvente la situación actual de que exista dicha autoridad para la protección de la Información Clasificada de "otros" gracias a los sucesivos nombramientos por acuerdo de Consejo de Ministros, mientras que no existe de manera explícita para la protección de la Información Clasificada propia.

En esta reforma, a juicio del autor, se debería nombrar de manera explícita al Consejo de Ministros como Autoridad Nacional de Seguridad con capacidad de delegar sus funciones en una Autoridad Delegada, tal y como se ha venido haciendo hasta ahora para el ámbito internacional.

Dicha autoridad Nacional de Seguridad debe serlo para cualquier tipo de Información Clasificada, nacional e internacional, de la que España tenga que responsabilizarse de su protección por encontrarse en su territorio de soberanía, en virtud de la legislación nacional y los acuerdos internacionales firmados por España. La autoridad Nacional de Seguridad, es decir el Consejo de Ministros, solo se debería reservar en exclusiva la clasificación en el máximo grado de SECRETO pudiendo delegar las funciones de autoridad de clasificación para el grado de reservado.

Es necesario incorporar a la ley cobertura para desarrollos legislativos en los siguientes niveles en cuanto a la protección de la Información Clasificada en

los sistemas de información y comunicación y en la industria, puesto que estos dos ámbitos están ausentes en la actual ley.

En cuanto al segundo nivel es necesario abordar un nuevo desarrollo de la Ley que incorpore lo que es práctica habitual a día de hoy a través de las normas de Autoridad Nacional de Seguridad y exija su cumplimiento para el conjunto de las administraciones españolas con capacidad de acceder y generar Información Clasificada. Es decir, se necesita derogar el decreto actual (no se trata de un Real Decreto pues, como ya se ha dicho, es anterior a la actual monarquía parlamentaria consagrada en la Constitución de 1978) y elaborar un Real Decreto en el que se definan las funciones de la Autoridad Nacional de Seguridad, y cuáles de ellas se delegan en la Autoridad Delegada. Se deberían establecer las autoridades de clasificación para los dos niveles inferiores de clasificación y su capacidad para delegar estas funciones.

El tercer nivel de desarrollo se encuentra a día de hoy vigente y con el rango que se propone, es decir como instrucción del Secretario de Estado Director del CNI, en calidad de Autoridad Nacional de Seguridad Delegada, si bien dado que carece de la cobertura legal necesaria, estrictamente hablando, solo son de aplicación para la protección de la Información Clasificada internacional de la OTAN, la UE y la ESA, y de terceros estados con los que se tiene firmado un acuerdo bilateral de protección de Información Clasificada, pero no para la protección de la Información Clasificada nacional, ni para la de otras organizaciones internacionales que carecen de nombramiento expreso.

Es necesaria continuar la divulgación y concienciación en el mundo empresarial de las oportunidades que ha supuesto la apertura del mercado europeo en lo relativo a programas y contratos clasificados, de forma que se genere un tejido industrial preparado para poder competir internacionalmente en las oportunidades de negocio que se presentan fuera de España. Resulta de especial importancia los programas de la Unión Europea H2020 (Horizon 2020) dotados de un presupuesto astronómico, y en los que una parte de los proyectos vinculados a los mismos son clasificados.

La capacidad de proteger adecuadamente Información Clasificada de cualquier tipo, nacional o internacional, se ha convertido en un activo para las empresas, especialmente las de los sectores de defensa y aeroespacial, que si bien

se puede acreditar únicamente con ocasión de participar en un contrato en el que se maneje y/o genere información clasificada, disponer de esta capacidad sitúa a las empresas en una categoría superior.

# CAPÍTULO V.-
# DERECHO A LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

# CAPITULO V.- DERECHO A LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

## 5.1. INTRODUCCIÓN

El objeto de estudio de la "protección de datos de carácter personal", observa necesariamente la necesidad de profundizar en el origen y las diferentes normas que motivaron la creación del "Derecho a la Protección de Datos de Carácter Personal" como un derecho fundamental a nivel europeo y nacional. Para ello haremos un repaso de estas, donde podremos comprobar que existe cierto desfase normativo en la cronología de las normas que lo regulan, siendo más pronunciado a nivel nacional que europeo, ya que las tecnologías avanzan a gran velocidad, sin dar tiempo a regular adecuadamente. Aunque a lo largo de la historia también ha sido así, actualmente el tratamiento de los datos de carácter personal cada vez se realiza más rápido y a nivel global, exponiendo tratamientos de gran volumen de datos personales, que con los avances tecnológicos permiten un procesamiento de estos a través de diferentes técnicas de la era digital como por ejemplo el "*big data*", "internet de las cosas" o las "redes sociales". La regulación normativa de este derecho pretende proteger los intereses de los ciudadanos como titulares de sus datos y determinar las reglas u obligaciones que todos los actores deben cumplir. El estudio de la normativa refleja los cambios y giros que la legislación ha ido adoptando, siendo en esta última fase una normativa más de prevención que sancionadora.

## 5.2. EL ÁMBITO EUROPEO COMO INSPIRACIÓN

En el ámbito europeo, la privacidad y la protección de datos están configuradas nada menos que como un derecho fundamental. La primera conclusión que podemos extraer de ello es que en el ámbito europeo existe una distinción entre privacidad y protección de datos. Ambos conceptos son cercanos, pero no sinónimos. Mientras que la privacidad hace referencia de manera general a la protección de la esfera privada de la persona, la protección de datos incide específicamente en el procesamiento de datos relativos a un individuo identificado o identificable. En los próximos epígrafes, analizaremos la evolución

histórica de ambos derechos hasta llegar a la regulación más reciente en la materia

En los años 50, empezaron a aparecer las primeras normas que recogían los orígenes del derecho a la protección de datos, así en el año 1950, nacía el Convenio Europeo de Derechos Humanos, firmado en Roma, el 4 de noviembre del citado año. Este Convenio tenía como objetivo proteger los derechos humanos y las libertades fundamentales de las personas sometidas a la jurisdicción de los Estados miembros y permitir un control judicial del respeto de dichos derechos individuales. Concretamente, su art. 8 protege el derecho al respeto a la vida privada y familiar. Sin embargo, la jurisprudencia del Tribunal Europeo de Derechos Humanos ha entendido que, en el ámbito de este precepto, ha de entenderse incluido el derecho a la protección de los datos personales.

En 1957, unos años más tarde, el Tratado de Funcionamiento de la Unión Europea establecía, en su art. 16, que toda persona ostenta el derecho a la protección de los datos de carácter personal que le conciernan. Se trata éste de uno de los cuatro documentos que forman la constitución material de la Unión Europea, junto con el Tratado de la Unión Europea, el Tratado Constitutivo de la Comunidad Europea de la Energía Atómica (Euratom) y la Carta de Derechos Fundamentales de la Unión Europea.

Posteriormente, en 1980, la Organización para la Cooperación y el Desarrollo Económicos (OCDE) se convertía en el primer Foro internacional en emitir un documento al respecto, gracias a la publicación de sus Directrices de Privacidad. Si bien fue un hito relevante en el avance de este derecho, se trata de un documento no vinculante.

Asimismo, la OCDE también ha sido la primera organización en actualizar sus directrices en el año 2013, con el objeto de adaptarlas a la realidad tecnológica, económica y social. En la actualidad, la OCDE aglutina a 34 países, entre los que se encuentran España, Japón, México, Australia, Canadá o Estados Unidos.

En el ámbito comunitario existió una pronta preocupación por la influencia que las nuevas tecnologías supone en los derechos de las personas y ya desde 1973, el Parlamento Europeo mediante interpelación al Consejo de Europa solicitó detalles sobre actuaciones e iniciativas respecto de la regulación del derecho de acceso a la información personal. En los años sucesivos, el Parlamento Europeo

realizó estudios sobre el tratamiento de datos de carácter personal, incluso pensando en una posible Directiva (Directiva sobre Libertad Individual y la Informática) que homogenizase las diversas legislaciones que surgen en los Estados miembros regulando parte de la materia.

Los Trabajos realizados en Europa culminan con la creación del Convenio N.º 108 del Consejo de Europa y se pospone la adopción y elaboración de una Directiva. Con estos antecedentes surge el 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, se considera el primer instrumento a nivel internacional, jurídicamente vinculante en el ámbito de la protección de datos de carácter personal.

El Consejo de Europa tras cuatro años de negociaciones, adoptó el Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (Convenio N.º 108) y España firmó el Convenio el 28 de enero de 1982 y posteriormente lo ratificó en 1984, publicado en el Boletín Oficial del Estado número 274, de 15 de noviembre de 1985.

El Convenio N.º 108 entro en vigor el 10 de octubre de 1985, cuando se cumplió el requisito necesario para ello, que fuese firmado y ratificado por cinco Estados parte. Actualmente, son más de 51 Estados los que lo han adoptado, muchos de ellos no miembros del Consejo de Europa, como Uruguay, que se convirtió en el primer país latinoamericano que lo ha ratificado en el año 2013. En el art. 1 del Convenio se establece el objeto

> "garantizar, en el territorio de cada Parte, a cualquier persona física sean cual fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondiente a dicha persona ("protección de datos")".

El adoptar el Convenio 108, supone responsabilizarse y comprometerse respecto a la protección de datos personales y asumir obligaciones y medidas que garantizan la protección de los mismos, ante los tratamientos de datos personales que puedan realizar, ya sean entidades privadas o las Administraciones públicas quienes lo hagan. Para ello, en el Convenio se fijan una serie de principios básicos y requisitos que determinan si un tratamiento de datos se considera lícito.

Además, se establecen una serie de derechos respecto a las personas titulares de los datos, como el conocer que los datos personales están siendo tratados. También existe especial atención para los considerados datos sensibles, como, por ejemplo, los datos de salud, obligando a determinar medidas adicionales de protección en estos casos.

El 8 de noviembre de 2001, se adoptó un Protocolo Adicional a dicho Convenio en el que se destacan dos cuestiones fundamentales:

- Se insta la creación de autoridades de supervisión, que puedan ejercer sus funciones con plena independencia
- Se determina la prohibición de transferencias internacionales de datos a terceros países u organizaciones que no proporcionen un nivel adecuado de protección.

Podemos concretar las siguientes características del Convenio N.º 108:

- El Convenio N.º 108 limita de manera estricta la posibilidad de desligarse de la aplicación de las normas de protección de datos, de conformidad con los principios enunciados en el Convenio Europeo de Derechos Humanos.
- El Convenio N.º 108 tiene como objetivo proteger a las personas contra las intromisiones en su vida privada y contra el uso incorrecto de sus datos personales.
- El Protocolo Adicional al Convenio N.º 108, establece que los Estados Partes en el Convenio deberán establecer una o varias autoridades independientes con el objetivo de asegurar el respeto de los principios enunciados en el Convenio. Estas autoridades de control tienen el poder de investigar e intervenir, de interponer una acción judicial o de poner en conocimiento de las autoridades judiciales las violaciones de la legislación sobre la protección de datos.
- El Convenio N.º 108 presenta una ventaja esencial a través de la aplicación más allá de las fronteras en la era de la globalización y de la utilización de Internet: su dimensión transfronteriza, contienen garantías para proteger el movimiento transfronterizo de datos hacia terceros países. En principio, debe asegurarse un nivel de protección adecuado.
- El Convenio N.º 108 tiene un alcance de carácter universal al estar abierta la adhesión a los países no europeos, está abierto a la adhesión de los

Estados no miembros del Consejo de Europa, adaptándose plenamente a la realidad de hoy en día: los datos personales no conocen fronteras.

• El Convenio N.º 108 está siendo revisado continuamente para adaptarse a las nuevas realidades, dado que cada día surgen nuevos desafíos en materia de protección de datos, trabajando actualmente el Consejo de Europa en su modernización.

En los orígenes de la Directiva 95/46/CE, es necesario tener en cuenta que, en el mercado interior, dentro del cual se garantiza la libre circulación de mercancías personas, servicios y capitales, implica también la libre circulación de los datos de carácter personal de un Estado a otro. La utilización de tratamientos de datos en el sector económico privado y en el ámbito de la cooperación administrativa científica y técnica es cada vez más demandado y las diferencias jurídicas en la regulación que empiezan a existir en esta materia en cada Estado obstaculiza el flujo transfronterizo. En consecuencia, existe una necesidad de armonizar las legislaciones nacionales en materia de protección de datos de carácter personal y se empieza a considerar como algo prioritario en las instituciones comunitarias. Por lo tanto, se retoman las negociaciones que existían del final de los ochenta, alcanzándose un acuerdo la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en adelante Directiva 95/46/CE de Protección de Datos).

Sobre la base de los principios aportados por el Convenio N.º108, fue aprobada en el ámbito comunitario la Directiva 95/46/CE, que sienta las bases para lograr la coordinación de las legislaciones nacionales aplicables en materia de protección de datos en aras a garantizar la libre circulación de tales datos entre los Estados Miembros. Por su parte, la Directiva 94/46/CE amplia y concreta el ámbito que al respecto de la protección de datos ya había determinado el Convenio N.º 108. Y, que, debido a la diversidad legislativa de los Estados, así como respecto al desfase o generalidad del Convenio N.º 108 se hace necesario una normativa más concreta y detallada.

Los principios de protección de los derechos y libertades de las personas, y concretamente, del respeto a la intimidad, que se contienen en la Directiva, vienen

a ampliar los del convenio, y así se desprende del Considerando 11 de la misma. La Directiva establece como eje principal de su contenido el Derecho a la intimidad, sin que ello excluya la posibilidad de que entren en juego otros derechos.

La Directiva 95/46/CE constituye el texto de referencia, a escala europea, en materia de protección de datos personales. Crea un marco regulador destinado a establecer un equilibrio entre un nivel elevado de protección de la vida privada de las personas y la libre circulación de datos personales dentro de la Unión Europea (UE). Con ese objeto, la Directiva fija límites estrictos para la recogida y utilización de los datos personales y solicita la creación, en cada Estado miembro, de un organismo nacional independiente encargado de la supervisión de cualquier actividad relacionada con el tratamiento de los datos personales.

En el art. 32 de la Directiva 95/46/CE se establece la necesidad de que cada Estado miembro cumpla en el plazo de tres años con la transposición del contenido de la misma a su normativa nacional. Así, en España, aunque a destiempo, en el año 1999 se aprobó la Ley Orgánica 15/1999, del 13 de diciembre, de Protección de Datos de Carácter Personal, publicada en el BOE el 14 de diciembre, que veremos más adelante.

### 5.3. LA LEY ORGÁNICA 15/1999, DE 13 DE DICIEMBRE, DE PROTECCIÓN DE DATOS DE CARÁCTER

Personal (más conocida como LOPD), vigente en la actualidad, adapta la legislación española a la Directiva europea 95/46/CE, desarrollando la protección de datos más allá de los datos informatizados, incluyendo dentro de su ámbito de aplicación los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento automatizado o no, y toda modalidad de uso de estos.

Para entender la evolución de la normativa de protección de datos en Europa, es importante señalar la creación a través de la Directiva 95/46/CE del denominado "Grupo de la protección de las personas en lo que respecta al tratamiento de datos de carácter personal" (en adelante, Grupo del art. 29). Estará formado por un representante de la autoridad o autoridades de control designadas por cada Estado miembro, un representante de la autoridad o

autoridades creadas por las instituciones y organismos comunitarios y un representante de la Comisión, institución que ejerce las funciones de secretaría. Tomará sus decisiones por mayoría simple de los representantes de las autoridades de control y tiene naturaleza eminentemente consultiva. El Grupo actuará de forma independiente, mediante la elección de sus representantes (no designados por los Gobiernos).

Sus funciones son:

a) Estudiar toda cuestión relativa a la aplicación de las disposiciones nacionales de transposición con vistas a contribuir a la aplicación homogénea de la Directiva;

b) Emitir un dictamen destinado a la Comisión sobre el nivel de protección existente dentro de la Comunidad y en los países terceros;

c) Asesorar a la Comisión sobre cualquier proyecto de modificación de la Directiva, otras medidas adicionales o específicas y los proyectos de medidas comunitarias que afecten a los derechos y libertades de las personas físicas en lo que respecta al tratamiento de sus datos;

d) Emitir un dictamen sobre los códigos de conducta comunitarios (art. 30).

Este órgano consultivo puede actuar por iniciativa propia, formulando recomendaciones o a instancia de la Comisión. Así pues, no se trata de un órgano de cooperación entre Estados, sino que se le atribuyen funciones de control y vigilancia de la aplicación y cumplimiento de las disposiciones de la Directiva.

### 5.4. ANTECEDENTES NORMATIVOS EN LA LEGISLACIÓN ESPAÑOLA: ART. 18.4 CE

Por seguir un orden cronológico de los acontecimientos en el panorama legislativo nacional empezaremos por analizar como nuestra Constitución Española, recoge este derecho desde la perspectiva del riesgo que existía en el momento de su creación (1978), ya que se considera que la utilización de la informática puede suponer una agresión a la intimidad de los ciudadanos, personal o familiarmente, coartando el ejercicio de sus derechos.

Así, nuestra Constitución en el Capítulo II dedicado a Derechos y Libertades, dentro del Título bajo la rúbrica de "los derechos y deberes fundamentales" hace una referencia expresa al riesgo existente que existe

derivado de la informática respecto a la intimidad de la persona, determinando en el art. 18.4 que "La Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".

A través de esta fórmula se establece el reconocimiento a la protección de datos de carácter personal, sin reconocer un derecho autónomo, sino vinculado a la intimidad, al honor personal y familiar, será muchos años después (año 2000) a través del Tribunal Constitucional cuando se considere como derecho autónomo e independiente, como veremos seguidamente.

Hay parte de la Doctrina, que piensa que en este momento España todavía no tiene ni la madurez, ni conciencia social para considerar estos problemas, ni dicho derecho, ya que aún nuestro país se encuentra más preocupado en construir y garantizar los derechos tradicionales, de los que se había carecido con motivo de la Dictadura. Son momentos en los que si acaso se podía considerar que pudiera existir una utilización abusiva por los poderes públicos de los medios telemáticos.

Además, es importante tener en cuenta que cuando se crea la CE, todavía no se ha aprobado el Convenio N.º 108 del Consejo de Europa, aunque sí que existían ejemplos en el Derecho Comparado, como la Ley Federal alemana de 1977, la Privacy Act americana de 1974, o incluso en nuestra vecina Portugal que determina en su Constitución portuguesa este derecho de la protección frente al uso de la informática, con bastante detalle.

No será hasta el año 1992, cuando se desarrolle este mandato constitucional, que trajo como consecuencia la publicación y entrada en vigor de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento automatizado de Datos de Carácter Personal (más conocida como LORTAD), que aunque tardía permitió llenar una laguna en un derecho reconocido como fundamental.

Tal y como hemos visto en España, la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (LORTAD), desarrolla lo recogido en el art. 18.4 CE y establece, por primera vez, la limitación del uso de la informática para garantizar la intimidad personal. Se trata del primer texto que proclama los principios y derechos sobre protección de datos que han constituido la referencia para los textos posteriores.

Se ha planteado como un hecho extraño la aprobación de la LORTAD para cumplir con un mandato constitucional del año 1978, cuando ya en el año 1990 se había presentado en Europa una propuesta de Directiva sobre el tema. Sin embargo, hay varios motivos que argumentan esto, por un lado, ya empieza a existir en España una mayor conciencia social sobre el nuevo derecho y su importancia en un momento en el que se empieza a generalizar la informática y la telemática, además de producirse cierta litigiosidad constitucional en torno al tema.

Otra razón importante para la elaboración y aprobación de la LORTAD, fue que había sido objeto de firma en 1990 el Acuerdo de Schengen y también el Convenio para la Aplicación del Convenio de Schengen. Dichos Convenios exigen que todos los países que quieran participar en el mismo y que quieran beneficiarse de sus ventajas en orden al paso de fronteras, deben tener en cuenta las garantías de un sistema de protección de datos que satisfaga los requisitos y exigencias. España con su firma en el año 1991, había quedado comprometida a crear los instrumentos necesarios para satisfacer cuando menos las exigencias del Convenio Nº 108 del Consejo de Europa.

Una de las principales características de la LORTAD, es que sólo se refiere al tratamiento de datos en ficheros informatizados, no teniendo en cuenta los denominados ficheros manuales, que si serán determinantes en la Directiva 95/46/CE. Por lo que en España la LORTAD será derogada posteriormente por la Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal (LOPD), en cumplimiento y trasposición de la Directiva que si tiene en cuenta ambos tipos de tratamientos de datos (informatizados y manuales).

Otra de las características de la regulación establecida en la LORTAD, es el establecimiento de una Autoridad Independiente (orgánica y funcional), acuñando la denominación de Agencia, que dará paso la creación de nuestro Órgano de control, la Agencia Española de Protección de Datos.

En La LORTAD, también se insta a un desarrollo reglamentario posterior de alguno de sus preceptos que darán lugar a varios Reglamentos: El Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos (da lugar a la creación del Órgano de Control a nivel nacional en materia de protección de datos de carácter personal, más conocida como AEPD); El Real Decreto 1332/94 de 20 de junio de 1994 que

desarrolla la Ley Orgánica de Protección de Datos de Carácter Personal (más conocido como Reglamento de la LORTAD) y el Real Decreto 994/1999 de 11 de junio, por el que se aprueba el Reglamento de Medidas de Seguridad de los ficheros automatizados que contengan datos de carácter personal (más conocido como el Reglamento de Medidas de Seguridad). En cualquier caso, el desarrollo reglamentario de la Lortad en algunos casos fue muy lento.

El derecho consagrado en la Constitución (art. 18.4) parecía carecer de autonomía limitándose a establecer una garantía de otros derechos: La Ley limitará el uso de la informática para garantizar la intimidad y el honor personal y familiar y el pleno ejercicio de los derechos. Parecía así configurarse como una institución vicarial de otros derechos. Esta cuestión debatida, queda clara a partir de la Sentencia 292/200, de 30 de noviembre, del Tribunal Constitucional.

La Sentencia 292/200, indica claramente que el "derecho fundamental a la protección de datos, a diferencia del derecho a la intimidad, atribuye a su titular un haz de facultades que consiste en su mayor parte en el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos". En la misma línea argumental respecto a las potestades del individuo declara que ese derecho fundamental a la protección de datos "garantiza a los individuos un poder de disposición sobre esos datos…y que nada vale si el afectado desconoce qué datos son los que poseen terceros, quiénes los poseen y con qué fin".

Así, del análisis de la sentencia podemos decir que, el objeto de protección del derecho fundamental a la protección de datos, no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que ya estaría protegido por el art. 18.1 CE, sino los datos de carácter personal.

El derecho fundamental a la protección de datos se concreta en un poder de disposición y de control sobre los datos personales. De esta manera, la persona debe quedar facultada para decidir cuáles de sus datos proporcionar a un tercero, sea la Administración o un particular, decidir cuáles puede este tercero recabar, saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso.

El Tribunal Constitucional, por medio de la Sentencia 292/2000, estableció el derecho a la protección de datos como derecho fundamental autónomo e independiente, cuyo contenido está integrado por los principios y derechos que se contemplan en la Ley Orgánica 15/1999. En virtud de este derecho fundamental, el ciudadano, con carácter general, puede decidir sobre sus propios datos.

### 5.5. NUEVO MARCO NORMATIVO EUROPEO EN PROTECCIÓN DE DATOS PERSONALES

La Unión Europea lleva varios años trabajando en una reforma legislativa integral en el ámbito de protección de datos de carácter personal con la finalidad de modificar diferentes cuerpos legislativos en esta materia que se muestran obsoletos respecto a los avances tecnológicos, la nueva Era Digital y la globalización en el tratamiento de la información. Esta reforma se ha materializado en hitos importantes para establecer un marco jurídico uniforme, para todos los Estados miembros.

A finales del año 2015, hemos podido asistir a un acuerdo entre el Parlamento Europeo, el Consejo y la Comisión para que se concluyeran las negociaciones sobre la reforma en materia de protección de datos, culminando en un paquete legislativo que consiste en:

- Reglamento General de Protección de Datos (RGPD)
- Directiva sobre protección de datos de carácter personal, tratados a efectos policiales y judiciales

El Parlamento Europeo y el Consejo han aprobado finalmente el Reglamento General de Protección de Datos con la intención de unificar los regímenes de todos los Estados Miembros sobre la materia, ha entrado en vigor el día 25 de mayo de 2016, si bien su cumplimiento sólo será obligatorio hasta transcurridos dos años desde dicha fecha, el 28 de mayo de 2018.

El RGPD se considera un hito sin precedentes para la protección de datos personales en Europa; modifica el régimen establecido desde la Directiva 95/46/CE sobre protección de datos, que cada Estado miembro ha ido implementado en su derecho interno de una manera diferente. Así, el nuevo Reglamento nos hace ver que su llegada era necesaria y de vital importancia para permitir un cuerpo normativo común en todos los países de la Unión Europea,

estableciendo una mayor seguridad jurídica y una igualdad de condiciones en un mercado único digital europea.

Por eso, la importancia de un Reglamento, y no de cualquier otro instrumento o acto jurídico, para ejercer las competencias legislativas de la Unión Europea en esta materia, siendo un instrumento directamente aplicable a todos los Estados miembros, sin necesidad de una trasposición a nuestro derecho interno, como ocurre con las Directivas.

Sin entrar en el contenido concreto del RGPD, para eso tendremos tiempo próximamente, entendemos que a través de esta reforma se da una respuesta necesaria a los avances tecnológicos y los nuevos modelos de negocio, que permiten en la actualidad hablar de la globalización de la información y tratamientos masivos de datos de carácter personal, de manera que no se debe ver como una regulación que limita el desarrollo económico e imposibilita la actividad empresarial, sino que se trata de una regulación que establece garantías y protección a los ciudadanos preocupados por el tratamiento de su información, generando una mayor confianza al usuario cuando alguna empresa, institución o Administración Pública usa y trata sus datos.

La Directiva sobre protección de datos de carácter personal, tratados a efectos policiales y judiciales, centra su reforma y actualiza la antigua Decisión marco de 2008, sobre protección de datos en la cooperación judicial en materia penal y en la cooperación judicial, que tenía varios vacíos legales que se necesitaban cubrir, siendo una regulación que se quedaba obsoleta.

### 5.6. REGLAMENTO EUROPEO DE PROTECCIÓN DE DATOS: CARACTERÍSTICAS MÁS RELEVANTES (I)

El objetivo del nuevo Reglamento Europeo es dar más control a los ciudadanos sobre su información privada en un mundo donde la información está mucho más globalizada a través de las redes sociales, la banca por internet, productos y servicios on-line, etc., dando lugar a un mercado único digital. Recogeremos a continuación, algunos de sus características más relevantes:

- Se extiende su ámbito de aplicación más allá de las fronteras de la Unión Europea, en la medida en que se aplicará al tratamiento de datos personales en el contexto de las actividades de un establecimiento del responsable o del

encargado en la Unión, independientemente de que el tratamiento tenga lugar en la Unión o no.

• Se aplicará al tratamiento de datos personales de residentes en la Unión por parte de un responsable o encargado no establecido en la Unión, cuando las actividades de tratamiento estén relacionadas con:

a. Oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si a estos se les requiere su pago, o

b. Control de su comportamiento, en la medida en que este tenga lugar en la Unión.

• Se mantiene los principios actuales sobre protección de datos, entre los que destacamos: calidad de los datos, derecho de información en la recogida de datos, consentimiento del afectado y seguridad de los datos.

• Se refuerza la importancia del consentimiento, exigiendo que sea "claro y afirmativo" y excluyendo el consentimiento tácito o por inacción. Además, el responsable deberá ser capaz de demostrar que el interesado consintió el tratamiento de sus datos personales.

• Se endurece los deberes de transparencia y se refuerza la información que debe ser facilitada a los titulares de los datos, tanto en el supuesto de que los datos se recaben directamente del interesado como si los datos se obtienen de otra fuente.

• Se introducen derechos nuevos de los interesados como: el derecho a la portabilidad de datos, que consiste en derecho que tiene una persona a trasladar los datos de un proveedor de servicios a otro siempre que sea técnicamente viable, así como a recibir los datos en un formato estructurado y de uso común. Además se introduce el derecho al olvido, que ya había sido reconocido de manera jurisprudencial por el Tribunal de Justicia de la Unión Europea en 2014

• Se establecen cuestiones más detalladas que se deben contemplar en el contrato que se formalice entre el responsable y el encargado del tratamiento.

• Se introduce el principio de ventanilla única. Así, en los casos transfronterizos en que estén implicadas varias autoridades nacionales de supervisión se adoptará una única decisión. Es decir, una empresa con

varias filiales en diferentes Estados miembros únicamente deberá tratar con la autoridad de protección de datos del Estado miembro de su establecimiento principal.

Siguiendo con más características relevantes del nuevo Reglamento nos encontramos con:

• Se crea un Consejo Europeo de Protección de Datos, que estará formado por los representantes de cada una de las autoridades de control independientes, y sustituirá al actual Grupo de Trabajo del Artículo 29.

• Se encomienda a la Comisión respecto a las transferencias internacionales de datos, la evaluación del nivel de protección de los terceros países. También se podrán hacer transferencias internacionales cuando se considere que existen garantías apropiadas (tales como cláusulas contractuales de protección de datos o normas corporativas vinculantes).

• Se establecen una serie de principios nuevos: los principios de protección de datos desde el diseño y por defecto, que implican que quien trata datos personales ha de hacerlo considerando este derecho fundamental ya desde las primeras fases de, por ejemplo, el desarrollo de una aplicación, un servicio, etc.

• También se introduce como un principio nuevo el principio de responsabilidad (accountability por su término en inglés), por el que los responsables del tratamiento deben poner en práctica una serie de medidas de seguridad, según consideren que han hecho lo suficiente para preservar la seguridad, ya no hay medidas técnicas concretas y tasadas.

• Se introduce la figura del Delegado de Protección de Datos (DPO, por sus siglas en inglés), de forma que se impone la obligación de nombrar un DPO en determinados casos.

• Se establece la obligación de realizar una evaluación de impacto sobre la protección de datos (PIA, por sus siglas en inglés) para el caso en que sea probable que el tratamiento de datos, suponga un riesgo elevado para los derechos de las personas.

• Se establece la obligación de comunicar a los afectados y al órgano de control las "Brechas de Seguridad " de datos de carácter personal, en un

plazo de 48 horas, así como las medidas correctoras que se hayan adoptado para mitigar el incidente.

• Se amplían los datos sensibles o categorías de datos personales especiales: se suman otros nuevos como los datos genéticos o datos biométricos.

• Se establecen sanciones económicas muy elevadas, de hasta el 4% de la facturación total anual de las empresas ó 20 millones de euros en caso de infracción, que serán impuestas por las autoridades nacionales de protección de datos.

### 5.7. SITUACIÓN DEL NUEVO REGLAMENTO EUROPEO RESPECTO A LA VIGENTE LOPD

La Unión Europea ha optado por llevar a cabo la más importante reforma de la protección de datos de las últimas décadas mediante un Reglamento, siguiendo la necesidad de crear un marco más sólido y coherente, tal y como especifica el Considerando 7 RGPD, evitando de esta manera una aplicación fragmentada, la inseguridad jurídica y las diferencias en la protección de los derechos y libertades de los Estados miembros, esperando de esta manera garantizar un nivel uniforme de protección. Nos encontramos, por primera vez, con una situación compleja en la que la regulación de un derecho fundamental, que de acuerdo al art. 81 CE requiere Ley Orgánica, va a estar contenido en un Reglamento Europeo.

En aras de aclarar esta situación compleja es necesario precisar si el Reglamento General de Protección de Datos desplazará o no a la LOPD, porque nos encontramos con que mantenemos una legislación nacional en la materia que en algunos casos choca con la regulación establecida en el RGPD. Atendiendo a esta situación no debemos olvidar que el Considerando 8 del propio RGPD permite que los Estados miembros incorporen a su derecho nacional elementos de este, en la medida en que sea necesario por razones de coherencia y para que las disposiciones nacionales sean comprensibles para su destinario.

Por otro lado, es necesario indicar que la Sección de Derecho Público de la Comisión General de Codificación ha estado realizando junto con la Agencia Española de Protección de datos un análisis de las implicaciones que el Reglamento deberá tener en la LOPD y como resultado de este trabajo, se decidió

la necesidad de derogar la LOPD y crear una nueva Ley Orgánica de Protección de Datos de Carácter personal.

Se ha considerado que nuestra legislación debe adaptarse a la nueva regulación comunitaria y, por ello, el Gobierno ha impulsado el Anteproyecto de Ley Orgánica, que sustituirá a la actual LOPD y adaptará nuestro sistema al de los países del entorno. El 23 de junio del 2017, se dio a conocer el anteproyecto de Ley y ya en agosto de 2016 el Consejo General del Poder Judicial (CGPJ) ha criticado algunos aspectos del Anteproyecto de Ley por falta de coherencia. Este hecho, junto con la falta de tiempo, va a retrasar la aprobación de una nueva Ley Orgánica de Protección de Datos en España, antes del plazo de aplicación del nuevo Reglamento General de Protección de Datos fijado el 25 de mayo de 2018. Lo que crea cierta inseguridad jurídica a las empresas privadas y organismos públicos que se deben adaptar al Reglamento Europeo antes de dicha fecha.

### 5.7.1. Objeto, ámbito de aplicación y definiciones en el RGPD

El mercado interior seña de identidad de la Unión Europea, necesita de la protección de datos y de la libre circulación de estos datos en base a un régimen uniforme en todos los Estados Miembros, lo que se pretende conseguir a través del nuevo Reglamento, intentando superar las divergencias que trajo consigo la Directiva 95/46/CE.

El objetivo del Reglamento que pasaremos a analizar es doble: regular el derecho fundamental a la protección de datos que reconoce el art. 8 de la Carta Europea de Derechos Humanos y garantizar la libre circulación de dichos datos dentro de la Unión Europea. Pero siempre partiendo de la base de que esa libre circulación en ningún caso puede justificar una reducción en el nivel de protección.

Así, el doble objeto del Reglamento, su ámbito de aplicación, diferenciando entre el ámbito material y territorial, para terminar repasando una serie de definiciones y conceptos que son fundamentales para después entender otros conceptos más complejos de la materia de protección de datos de carácter personal.

El Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de

los datos personales y la libre circulación de estos datos (en adelante RGPD), ya recoge en su denominación cual va a ser el objeto del mismo, así el RGPD, en el art. 1.1 determina que "el presente Reglamento establece las normas relativas a la protección de datos de las personas físicas en lo que respecta al tratamiento de datos personales y las normas relativas a la libre circulación de tales datos".

En el RGPD se entiende que existe un doble objeto, al igual que existía en la Directiva 95/46/CE, ya que hace referencia a dos elementos:

1. Regular el derecho a la protección de datos personales

2. Regular la libre circulación de tales datos

Respecto a la libre circulación de los datos, tanto la Directiva 95/46/CE como el RGPD no sólo mantienen una protección de la intimidad, si no que van más allá y determinan la libre circulación de datos entre los Estados miembros, en este sentido no podrá ser restringida, ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales.

Uno de los motivos de regular la libre circulación de los datos personales en el objeto del RGPD, es consecuencia de la integración económica y social que resulta de la creación y puesta en funcionamiento del mercado interior, por los que se aumentan los flujos transfronterizos de datos que afectan tanto al sector privado, como al sector público. Por otro lado, se requiere una regulación que establezca un nivel de protección coherente y equiparable para todos los Estados miembros, ya que la Directiva no lo había conseguido esto.

Por otro lado, resulta evidente que la innovación tecnológica permite una mayor magnitud en la recogida, tratamiento y comunicación de datos personales, permitiendo igualmente la circulación de datos personales tanto en la Unión Europea como a terceros países, que pueden y deben realizarse sin menoscabar el nivel de protección de los datos personales.

Con respecto al derecho a la protección de datos como parte del objeto, señalar que en el considerando 1 RGPD, se determina claramente que se trata de un derecho fundamental, recogido en el art. 8, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea y en el art. 16, apartado 1 del Tratado de Funcionamiento de la Unión Europea, a través de dichos textos el derecho a la protección de datos se consagró como un derecho autónomo,

independiente del derecho a la intimidad que se regula en otro artículo separado de la Carta Europea de Protección de datos.

Sin embargo, no debemos olvidar que el tratamiento de datos de carácter personal, tiene incidencia con muchos otros derechos fundamentales y no se trata de un derecho absoluto, debe mantener el equilibrio, atendiendo al principio de proporcionalidad tal y como manifiesta el considerando 4 RGPD.

### 5.7.2. Ámbito de aplicación material: norma general

En el art. 2 RGPD, se determina el ámbito de aplicación material y lo hace estableciendo una definición de carácter general, para luego establecer una serie de excepciones a la norma. Así, en el art. 2.1 RGPD estipula que "El presente Reglamento se aplica al tratamiento total o parcialmente automatizado de datos personales, así como el tratamiento no automatizado de datos personales contenidos o destinados en un fichero".

Así, con carácter general determina que es de aplicación a:

- Tratamientos total o parcialmente automatizados y a
- Tratamientos no automatizados o también denominados tratamientos manuales.

De datos personales que ya existan en un fichero o que vayan a ser incluidos en un futuro.

Esta parte coincide con la definición de ámbito de aplicación material que ya existía en la Directiva 95/46/CE y en el art. 2.1 LOPD, que determina su ámbito de aplicación a los datos de carácter personal registrados en soporte físico susceptibles de tratamiento, y a cualquier modalidad de uso posterior de estos datos por los sectores público y privado.

Por otro lado, es interesante definir en este punto que se entiende por: datos personales, tratamiento y fichero.

### 5.7.3. Ámbito de aplicación material: Excepciones I

El apartado segundo del art. 2 RGPD determina las exclusiones del ámbito material a través de un numerus clausus:

A. Actividades fuera del ámbito de aplicación del Derecho de la Unión

El art. 2.2 a) RGPD determina "En el ejercicio de una actividad no comprendida en el ámbito de aplicación del Derecho de la Unión". Es decir, que el RGPD no podrá ser de aplicación a los tratamientos de datos que se desarrollen en función de una materia determinada, para la que la UE no tiene competencia (de acuerdo a los tratados constitutivos). Así, en el considerando 16 del RGPD cita a modo de ejemplo como actividad excluida, la relativa a la seguridad nacional.

B. Actividades de política exterior y de seguridad común realizadas por los Estados miembros

El art. 2.2 b) RGPD indica que "Por parte de los Estados miembros cuando lleven a cabo actividades comprendidas en el ámbito de aplicación del capítulo 2 del Título V del TUE". En esta exclusión, se determinan los tratamientos de datos realizados por los Estados miembros cuando realicen actividades de política exterior y de seguridad común (lo que se ha denominado como PESC), los tratamientos de datos que se pudieran realizar en el desarrollo de esta actividad quedarían excluidos.

C. Actividades personales o domésticas

La tercera de las exclusiones se determina en el art. 2.2 c) RGPD: "El Presente Reglamento no se aplica al tratamiento de datos realizado por las personas físicas en el ejercicio de actividades únicamente personales o domésticas". Esta exclusión también se reflejaba en la Directiva 95/46/CE y en la normativa interna española, tanto en la LOPD como en el RLOPD que ampliaba la excepción a los tratamientos de datos realizados en el marco de la vida familiar, no sólo personal de una persona física.

Por otro lado, el considerando 18 RGPD matiza un poco más la exclusión, ya que se trata de conceptos que con anterioridad habían suscitado jurisprudencia a nivel nacional, así como del Tribunal de Justicia de la Unión Europea (TJUE) y determina que los tratamientos que se realicen en el marco de esta exclusión no deben tener conexión alguna con una actividad profesional o comercial. Además, establece ejemplos en los que no es aplicable el RGPD como son la correspondencia, la llevanza de repertorios de direcciones, la actividad en redes sociales y la actividad online que se realice en el contacto de las actividades personales o domésticas.

Por último, el considerando 18 RGPD, también determina que aunque se considere que los tratamientos de datos en el ejercicio de actividades domésticas o personales están fuera del ámbito de aplicación del RGPD, éste si debe aplicarse a los encargados o responsables de tratamiento que proporcionen los medios para tratar los daos personales relacionados con tales actividades personales o domésticas.

### 5.7.4. Ámbito de aplicación material: Excepciones II

Continuando con las exclusiones del ámbito material mencionaremos:

D. Actividades de persecución de Infracciones penales

La cuarta de las excepciones se refiere al tratamiento de datos que realizan las autoridades competentes bajo la finalidad de actividades de persecución de infracciones penales. Así, queda recogido en el art. 2.2 d) que dice

> "Por parte de 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 amenazas a la seguridad pública y su prevención".

Esta exclusión está alineada con lo establecido en la Directiva 2016/680 del Parlamento y del Consejo de 27 de abril de 2016, que determina que dichos tratamientos de datos si estarán sometidos a esta Directiva 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 la libre circulación de dichos datos.

Se debe tener en cuenta que los Estados pueden encomendar a las autoridades competentes funciones que no tiene que ver con los anteriores fines de persecución de infracciones penales y, en estos casos, el tratamiento de datos personales si entra en el ámbito de aplicación del Reglamento. Esto ocurre en España con el tratamiento de datos que realiza la Policía Nacional para la expedición del DNI. Se faculta a los Estados para determinar disposiciones específicas para adaptar la aplicación de las normas del presente RGPD.

Además, en el considerando 19 RGPD, también determina que los Estados pueden limitar los tratamientos de datos que realicen las empresas privadas y

puede imponer obligaciones y derechos, siempre que dicha limitación sea una medida necesaria y proporcionada en una sociedad democrática para proteger intereses importantes, como la seguridad pública y la persecución de infracciones penales o la ejecución de sanciones penales, como por ejemplo, en el marco de la lucha contra el blanqueo de capitales, de las actividades de los laboratorios de policía científica o de ciberataques.

Por último es necesario tener en cuenta que el Reglamento, en el considerando 20, establece de forma expresa, que el RGPD se aplica a las actividades de los tribunales y otras autoridades judiciales, pero también determina que con el fin de preservar la independencia del poder judicial en el desempeño de sus funciones, la competencia de las autoridades de control no debe abarcar el tratamiento de datos personales cuando los tribunales actúen en el ejercicio de su función judicial y especifica que el control de dichos tratamientos debe realizarse por los mismos órganos de control establecidos dentro del sistema judicial del Estado, siendo en España este control encomendado al Consejo General del Poder Judicial a través de la Ley Orgánica 6/1985 de 1 de julio del Poder Judicial (art. 230).

### 5.7.5. Ámbito de aplicación material: Tratamiento de datos realizados por Instituciones y Organismos Europeos

El párrafo tercero del art. 2 RGPD atiende los tratamientos de datos realizados por las propias instituciones y organismos europeos y determina lo siguiente: Art. 2.3

> "El Reglamento (CE) no 45/2001 es de aplicación al tratamiento de datos de carácter personal por parte de las instituciones, órganos y organismos de la Unión. El Reglamento (CE) n 45/2001 y otros actos jurídicos de la Unión aplicables a dicho tratamiento de datos de carácter personal se adaptarán a los principios y normas del presente Reglamento de conformidad con su art. 98".

Aunque en las primeras propuestas del texto del Reglamento no se consideró así, posteriormente y para garantizar una protección uniforme y coherente, se decidió incluir en el texto aprobado que el RGPD debía ser de aplicación a los tratamientos de datos realizados por las instituciones y

organismos europeos. Incluso estableció en el art. 98 RGPD la previsión de obligar a la Comisión a presentar si procede, propuestas legislativas para modificar los actos jurídicos de la Unión en materia de protección de datos personales.

> F. Por último, en el apartado cuarto del art. 2 RGPD, se determina: "El presente Reglamento se entenderá sin perjuicio de la aplicación de la Directiva 2000/31/CE, en particular sus normas relativas a la responsabilidad de los prestadores de servicios de intermediarios establecidos en sus arts. 12 a 15".

La Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 200, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la Información, en particular, el comercio electrónico en el mercado interior (más conocida como Directiva sobre comercio Electrónico), regula dos cuestiones que guardan especial relación con la normativa de protección de datos de carácter personal y son:

- Envío de comunicaciones electrónicas
- Uso de los dispositivos de almacenamiento y recuperación de los datos en los equipos terminales de los usuarios

Así, en el propio considerando 14 de la Directiva 2000/31/CE, se hace remisión a normativa de protección de datos y reconoce que la aplicación y ejecución de la presente Directiva debe respetar plenamente los principios relativos a la protección de datos personales, en particular en lo que se refiere a las comunicaciones comerciales no solicitadas y a la responsabilidad de los intermediarios, la presente Directiva no puede evitar el uso anónimo de redes abiertas como Internet.

### 5.7.6. Ámbito de aplicación material en la LOPD y en el RLOPD

No hay que olvidar que hasta que el RGPD sea plenamente aplicable el 25 de mayo del 2018 y a la espera de que se apruebe una nueva Ley Orgánica de Protección de datos en España, también deberemos tener en cuenta la LOPD y su Reglamento, que respecto al ámbito de aplicación material determina algunas cuestiones que se deben tener en cuenta y que el RGPD no entra tan al detalle.

Así, atendiendo a materias excluidas que no han sido comprendidas en el RGPD, y sí en la LOPD y el RLOPD concretan que no será aplicable la normativa de protección de datos a las siguientes materias:

- Tratamientos de datos referidos a personas jurídicas (art. 2.2. RLOPD).
- Tratamientos de datos que se limiten a incorporar los datos de personas físicas que prestan sus servicios en personas jurídicas y que sólo contengan el nombre y apellidos, las funciones o puestos desempeñados, así como la dirección postal o electrónica, teléfono y número de fax profesionales (art. 2.2 RLOPD).
- Tratamientos de datos relativos a los empresarios individuales cuando hagan referencia a ellos en su calidad de comerciantes, industriales o navieros (art. 2.3 RLOPD).
- Tratamientos de datos referidos a personas fallecidas, si bien se reconoce el derecho de cancelación, cuando hubiere lugar a ello, a los familiares u otras personas vinculadas al fallecido por razones análogas, previa notificación del óbito al responsable del fichero, aportando acreditación suficiente del fallecimiento (art. 2.4 RLOPD).
- Ficheros sometidos a la normativa de protección de datos de materia clasificados (asuntos, actos, documentos, informaciones, datos y objetos) cuyo conocimiento por personas no autorizadas puedan dañar o poner en riesgo la seguridad y defensa del Estado (art. 2 LOPD y art. 4 RLOPD).
- Ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada, pero se le impone al responsable del fichero el deber de comunicar previamente su existencia, características generales y finalidad a la AEPD (art. 2 LOPD y art. 4 RLOPD).

Por último, tener en cuenta las materias que se determinan en la LOPD y en RLOPD que se rigen por su normativa específica:

- Tratamientos que sirven a fines exclusivamente estadísticos y ésten amparados por la legislación estatal o autonómica sobre función estadística pública (art. 2.3b) LOPD).
- Tratamientos que tengan por objeto el almacenamiento de datos contenidos en los informes personales de calificación a que se refiere la

legislación sobre régimen del personal de las Fuerzas Armadas (art. 2.3c) LOPD).

• Tratamientos derivados del Registro Civil y del Registro Central de penados y rebeldes (art. 2.3d) LOPD).

• Tratamientos procedentes de imágenes y sonidos obtenidos mediante la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad de conformidad con la legislación sobre la materia (art. 2.3e) LOPD).

### 5.7.7. Ámbito de aplicación territorial del RGPD I

El art. 3 RGPD sustituye el art. 4 de la Directiva 95/45/CE (derogada por el RGPD), donde se regula el ámbito de aplicación territorial, materia compleja y que había sido objeto de polémica en diversas sentencias del TJUE. No debemos olvidar que el RGPD tiene como objetivo establecer un nivel de protección de datos equivalente en todos los Estados miembros, así como garantizar una aplicación de estas normas coherente y homogénea, tal y como señala el considerando 10 del RGPD.

Así, se establecen nuevas reglas sobre la aplicación territorial del Derecho de la UE en materia de protección de datos, diferenciando varios supuestos según el tratamiento que se regule en un establecimiento por un responsable o encargado establecido en la Unión o no.

El art. 3.1 RGPD determina. "El presente Reglamento se aplica al tratamiento de datos personales en el contexto de las actividades de un establecimiento del responsable o del encargado en la Unión, independientemente de que el tratamiento tenga lugar en la Unión o no".

Es importante destacar y comprender que se entiende por "establecimiento" señalándose en el considerando 22 RGPD que

> "un establecimiento implica el ejercicio de manera efectiva y real de una actividad a través de modalidades estables. La forma jurídica que revistan tales modalidades ya sea una sucursal o una filial con personalidad jurídica, no es factor determinante al respecto".

Luego para determinar el ámbito de aplicación nos fijamos en dos elementos que el establecimiento este situado en el territorio de un Estado

miembro y si el tratamiento de datos se ha producido en el ámbito de las actividades de dicho establecimiento, no por el establecimiento en cuestión, sino en el marco o conexión de sus actividades, aunque ésta sea mínima.

Esto varía respecto a los criterios establecidos en la LOPD y su reglamento, que seguía las directrices de la Directiva 95/46/CE y atendía a la utilización en el tratamiento de datos de medios situados en territorio español, salvo que tales medios se utilicen con fines de tránsito, aunque el responsable del tratamiento no esté establecido en territorio de la Unión Europea. En este caso, el responsable del fichero deberá designar un representante establecido en el territorio de dicho Estado miembro, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento.

B. Por otro lado, en el art. 3.2 RGPD determina que

> "El presente reglamento se aplica al tratamiento de datos personales de interesados que residan en la Unión por parte de un responsable o encargado no establecido en la Unión, cuando las actividades de tratamiento estén relacionadas con:
>
> a) La oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si a estos se les requiere su pago, o
>
> b) El control de su comportamiento en la medida en que este tenga lugar en la Unión".

Así se prevé que el RGPD podrá ser aplicable, si el tratamiento de datos personales se realiza por un responsable o encargado de tratamiento cuando no esté establecido en la Unión si se dan dos condiciones:

a) Que el objeto del tratamiento sean datos personales de residentes en la Unión, ya que según el considerando 23 RGPD, lo que se pretende es garantizar es que las personas físicas no se vean privadas de la protección a la que tiene derecho en virtud del presente Reglamento.

b) Que las actividades de tratamiento se refieran a un objeto determinado que puede ser:

- Oferta de bienes o servicios a dichos interesados (independientemente de que se requiera su pago). Así, en el considerando 23 RGPD señala que para poder determinar si un responsable o encargado ofrece bienes o

servicios a interesados que residan en la Unión Europea, se debe determinar cómo evidente que proyecta ofrecer servicios en uno o varios Estados miembros de la Unión. Son factores que ayudan a determinar esta intención que el sitio web del responsable o el encargado, o de su intermediario en la UE, use una lengua o una moneda generalmente utilizada en uno o varios Estados miembros, con la posibilidad de poder encargar bienes y servicios en esa otra lengua, además de la lengua generalmente utilizada en el tercer país donde resida. O bien que el sitio web mencione a clientes o usuarios que residen en la Unión.

• Observación del comportamiento de dichos interesados en la medida en que este comportamiento tenga lugar en la Unión. Así, en el considerando 24 RGPD establece que para determinar si se puede considerar que una actividad de tratamiento controla el comportamiento de los interesados, debe evaluarse si las personas físicas son objeto de un seguimiento, en internet, inclusive el potencial uso posterior de técnicas de tratamiento de datos personales que consistan en la elaboración de un perfil de una persona física con el fin, en particular de adoptar decisiones sobre él o de analizar o predecir sus preferencias personales, comportamientos y actitudes.

Por último, el art. 3.3 RGPD determina.

"El presente Reglamento se aplica al tratamiento de datos personales por parte de un responsable que no esté establecido en la Unión sino en un lugar en que el Derecho de los Estados miembros sea de aplicación en virtud del Derecho Internacional Público".

Este supuesto se refiere a los casos de una misión diplomática u oficina consular de un Estado miembro. Igualmente, estos ejemplos quedan reflejados en el considerando 25. Por resumir todos los aspectos que el nuevo RGPD ha introducido más ampliamente para determinar su ámbito territorial establecemos las siguientes conclusiones:

El art. 3 RGPD diferencia dos supuestos esenciales, según el tratamiento se realice en un establecimiento por un responsable o encargado establecido en la Unión o no:

- El RGPD se aplicará en todos los casos en que el tratamiento se realice en el contexto de las actividades del establecimiento, con independencia de donde se realice el tratamiento y donde resida el interesado.
- EL RGPD se aplicará a los responsables del tratamiento de datos establecidos en terceros países cuando el tratamiento (sin importar donde se realice el tratamiento) afecte a residentes de la Unión y siempre que se ofrezcan o bienes o servicios a los interesados de la UE o cuando se realice algún control de su comportamiento.

Las disposiciones sobre aplicación territorial que ha determinado el RGPD, parece que son más claras que las anteriores, así como racionales y simples, lo que siempre permite una mejor defensa de los derechos de los particulares, así como el establecimiento de las condiciones que hagan posible la libre circulación de datos.

### 5.8. PRINCIPIOS DE LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

El derecho fundamental a la protección de datos se desarrolla en la normativa a través de los denominados "Principios de la Protección de datos de carácter Personal" y se consideran como un conjunto de reglas, que en el RGPD, tienen especial importancia, por el carácter de informadores de las instituciones que conforman el ordenamiento jurídico en la materia, han de servir a todos los operadores jurídicos que intervienen, para cumplir de manera satisfactoria las exigencias jurídicas que determinan.

Así, los principios de la protección de datos están constituidos por un conjunto de reglas que determinan cómo se deben recoger, tratar y ceder los datos de carácter personal, a los efectos de garantizar la intimidad y demás derechos fundamentales de los titulares de los datos. Van más allá de meros fundamentos, ya que tienen naturaleza normativa y van a informar y servir para la interpretación de la normativa, estableciendo soluciones concretas, ante supuestos en los que la normativa no establece nada al respecto, por lo que en muchas ocasiones su interpretación permitirá suplir las lagunas legales que puedan existir en la propia normativa, ya que en muchos casos la regulación es mucho más lenta y no prevé los avances tecnológicos que no paran de evolucionar.

Podemos concluir que por todo lo anterior, los principios generales de la protección de datos de carácter personal constituyen una parte esencial del derecho a la protección de datos, y que a través de los mismos, se configura un sistema de tutela que garantiza una utilización más racional y razonable de los datos personales.

En una interpretación diferente de los principios, se puede llegar a decir que también conforman las obligaciones que los operadores jurídicos tienen que cumplir, sobre todo, en el caso del responsable y encargado del tratamiento. Estos principios se traducen en todas las obligaciones que deben seguir para poder cumplir con la regulación, en caso de tratar datos de carácter personal. Por lo tanto, es fundamental que los operadores jurídicos tengan claras las normas y requisitos para que el tratamiento de datos que realicen o se planteen realizar en el futuro, y éste cumpla con todas las garantías de protección respecto al titular o interesado de quien tratan datos.

Los principios en el RGPD se encuentran regulados dentro del Capítulo II, arts. 5 a 11, donde se establecen los siguientes: Principios relativos al tratamiento, licitud del tratamiento, condiciones para el consentimiento, condiciones aplicables al consentimiento del niño en relación con los servicios de la sociedad de la información, tratamientos de categorías especiales de datos personales, tratamientos de datos personales relativos a condenas e infracciones penales, y finalmente, tratamiento que no requieren identificación.

### 5.8.1. Principios relativos al tratamiento I

En el art. 5 RGPD, bajo el Título de los principios relativos al tratamiento, vamos a analizar cada uno de ellos:

1) Principio de licitud, lealtad y transparencia que determina que los datos personales serán tratados de manera lícita, leal y transparente en relación con el interesado:

- En este sentido, el considerando 60 RGPD, aclara que los principios de tratamiento leal y transparente exigen que se informe al interesado de la existencia de la operación de tratamiento y sus fines, estableciendo que el responsable del tratamiento debe facilitar al interesado cuanta

información complementaria sea necesaria para garantizar un tratamiento leal y transparente.

• Se debe informar al interesado de la existencia de elaboración de perfiles y de las consecuencias de dicha elaboración.

• Cuando los datos se recaban directamente del interesado se les debe informar de si están obligados a facilitarlos y de las consecuencias en caso de que no lo hiciera.

• Se recomienda que dicha información se transmita en combinación con unos iconos normalizados que ofrezcan, de forma fácilmente visible, inteligible y claramente legible, una adecuada visión del conjunto del tratamiento de datos previsto.

2) Principio de la limitación de la finalidad recogido en el art. 5.1b) RGPD, y dispone que los datos serán recogidos con fines determinados, explícitos y legítimos y no serán tratados posteriormente de manera incompatible con los fines originarios:

• De acuerdo con el art. 89 RGPD se determina que no se consideran fines incompatibles con la finalidad de origen, si el tratamiento posterior consiste en el archivo en interés público, con fines de investigación científica e histórica o fines estadísticos.

• El principio de limitación responde básicamente a la exigencia de que los datos de carácter personal no pueden ser tratados para otra finalidad, que aquella que expresamente ha sido consentida por parte del titular de los datos.

3) Principio de adecuación de datos o minimización de datos, determinado en el art. 5.1c) RGPD que regula que los datos personales sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados. Así, la minimización de datos requiere que cuando se recaban datos, no se soliciten al titular, más datos que los estrictamente necesarios, para la finalidad para la que van a ser recabados, sólo los imprescindibles para la finalidad que se persigue.

4) Principio de exactitud de los datos, recogido en el art. 4.1d) RGPD, que requiere que los datos sean exactos y si fuera necesario se deben actualizar. Se deben adoptar cuantas medidas sean necesarias para que lo antes posible, se

supriman o se rectifiquen los datos personales que sean inexactos con respecto a los fines para los que son tratados. Se le exige al responsable del tratamiento que se adopten todas las medidas razonables para que además de mantener los datos actualizados, en los casos en que existan datos inexactos, éstos se supriman o se rectifiquen, con los consiguientes problemas de acreditación del consentimiento del titular de los datos, cuando dicha actualización se realiza de oficio.

5) Principio de limitación de la conservación, recogido en el art. 5.1e) RGPD, determina que los datos de carácter personal se deben mantener de forma que se permita la identificación de los interesados, sólo durante el tiempo necesario para los fines del tratamiento:

- Los datos personales podrán conservarse durante periodos más largos siempre que los fines sean de archivo en interés público, fines de investigación científica o histórica, o fines estadísticos de acuerdo con lo establecido en el art. 89.1 RGPD.
- Se deberán aplicar las medidas técnicas, y organizativas apropiadas que establece el Reglamento con el fin de proteger los derechos y libertades del interesado.

6) Principio de integridad y confidencialidad, recogido en el art. 5.1 f) determina que los datos personales serán tratados de tal manera que garanticen una seguridad adecuada, incluida la protección contra el tratamiento no autorizado o ilícito y contra su perdida, destrucción o daño accidental, mediante la aplicación de técnicas organizativas apropiadas. En el principio de limitación de la conservación de los datos de carácter personal como en el de integridad y confidencialidad, se debe tener en cuenta la implementación de las medidas técnicas y organizativas o medidas de seguridad, que con el RGPD descarga toda la responsabilidad en el responsable del tratamiento que ahora debe determinar cuáles son las medidas más idóneas y necesarias que debe adoptar en función de la tipología de los datos, los fines del tratamiento y el resto de circunstancias que rodean al mismo.

7) Principio de responsabilidad proactiva (art. 5.2 RGPD), que determina que el responsable del tratamiento será responsable de todas las exigencias vistas con anterioridad recogidas en el art. 5.1 RGPD y, además, no sólo debe cumplirlas sino demostrar que las ha cumplido.

Estos principios, muestran muchos aspectos del principio de calidad de datos recogido en la Directiva 95/46/CE, donde se afirmaba que sólo estaba permitida la recogida y tratamiento de los datos personales, cuando los mismos eran adecuados pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explicitas y legítimas para las que se habían obtenido los datos, ahora dichos valores se matizan en el sentido de que el tratamiento sea lícito, leal y transparente.

### 5.8.2. Tratamiento de Categorías Especiales de Datos I

El art. 9 RGPD se encuentra dedicado a la regulación del "Tratamiento de las categorías especiales de datos personales" y determina como categorías especiales de datos

> "los 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".

El RGPD, por primera vez, incluye a los datos genéticos y los datos biométricos como categorías especiales de datos, en el art. 4:

- En el considerando 34 RGPD, se establece una definición amplia de que debe entenderse por datos genéticos:

> "Debe entenderse por datos genéticos 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".

- Respecto a los datos biométricos el art. 4.14 RGPD los define como:

> "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".

Es una nueva categoría que se incluye entre las categorías especiales de datos, pero solo cuando están siendo procesados con el fin de identificar de forma única a una persona. Así, en el considerando 51 RGPD determina que:

> "el tratamiento de fotografías no debe considerarse sistemáticamente tratamiento de categorías especiales de datos personales, pues únicamente se encuentran comprendidas en la definición de datos biométricos cuando el hecho de ser tratadas con medios técnicos específicos permita la identificación o la autenticación unívocas de una persona física".

El Reglamento también contiene una definición de que se entiende por datos de salud, en su art. 4.15: "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".

Respecto a los datos sanitarios el considerando 35 RGPD determina "todo número, símbolo o dato asignado a una persona física que la identifique de manera unívoca a efectos sanitarios". Como ejemplo, podemos entender el número de la Seguridad Social. También la información derivada de "una prueba diagnóstica in vitro", lo que incluirá indirectamente, a través de los datos de la gestante, y en ausencia de previsión alguna en el Reglamento, a los datos de los nasciturus.

Una vez que se han aclarado algunos de los conceptos o determinadas categorías de datos especiales, pasamos a analizar cómo han sido regulados en el RGPD. Así, en el art. 9.1 establece la prohibición general del tratamiento de datos especiales, para levantar esa prohibición en determinados casos:

- El tratamiento fue objeto de un consentimiento explícito por el interesado. Aunque el artículo contempla también la posibilidad de que los Estados miembros impidan por Ley que pueda levantarse la prohibición de tratamiento, ni siquiera con consentimiento del interesado.
- El tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos en el ámbito del Derecho laboral y de la seguridad y protección social, también incluye las pensiones según el considerando 52 RGPD.

• El tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento.

• El tratamiento es efectuado, en el ámbito de sus actividades legítimas y con las debidas garantías, por una fundación, una asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera, exclusivamente, a los miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con ellos en relación con sus fines, y siempre que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los interesados.

• El tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicos.

• El tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los Tribunales actúen en ejercicio de su función judicial. El considerando 52 RGPD concreta que esto puede suceder en el marco de un procedimiento judicial o de un procedimiento administrativo o extrajudicial.

• El tratamiento es necesario por razones de un interés público esencial.

• El tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, cuando su tratamiento sea realizado por un profesional sujeto a la obligación de secreto profesional, o bajo su responsabilidad.

• El tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, salvaguardando el secreto profesional.

El RGPD ha contemplado la posibilidad de que los Estados miembros puedan mantener o introducir de manera específica condiciones adicionales, inclusive mediante la formulación de las correspondientes limitaciones, con

relación al tratamiento de los datos genéticos, los datos biométricos, o los datos relativos a la salud en general.

### 5.8.3. Tratamientos de datos personales relativos a condenas e infracciones penales

El art. 10 RGPD restablece la regulación del tratamiento de datos personales relativos a condenas infracciones penales y reproduce de manera prácticamente igual al art. 8.5 de la Directiva 95/46/CE y aunque no se consideran dentro de las categorías especiales de datos, su tratamiento se limita.

Existen dos presupuesto en el precepto:

- Sol podrá llevarse a cabo un registro completo de condenas penales bajo el control de los poderes públicos.
- Los datos penales (condenas, infracciones y medidas de seguridad) deben ser supervisados por las autoridades.

Se establece como regla general que los datos personales sobre comisión de infracciones penales y administrativas comprende todos los datos que revelen la comisión de infracciones sancionadas por la jurisdicción penal, o las autoridades administrativas por personas identificadas o identificables. En principio, las Administraciones públicas son las únicas autorizadas para tratar datos de carácter personal relativos a la comisión de infracciones penales o administrativas dentro de los supuestos previstos en las respectivas normas reguladoras. Por su parte, las empresas privadas y otras entidades que no gocen de la condición de Administración pública no podrán, en ningún caso, tratar este tipo de datos.

Este art. 10 RGPD coincide también con lo dispuesto en el art. 7.5 LOPD donde hay ya una reserva en favor de las Administraciones Públicas competentes con relación al tratamiento de datos de carácter personal respecto a la comisión de infracciones penales o administrativas. En el RGPD, su regulación es algo más permisiva, ya que establece la posibilidad de intervención del sector privado, cuando expresamente lo autorice el Derecho de la Unión o de los Estados miembros que establezca siempre que concurran las garantías adecuadas para preservar los derechos y libertades de los interesados.

### 5.8.4. Tratamiento que no requiere identificación

En el art. 11 del RGPD se regula el tratamiento que no requiere identificación y determina que, si los fines para los cuales un responsable del tratamiento trate datos personales que no requieren o que ya no requieren la 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 dicho Reglamento. Parece que el precepto establece la posibilidad de anonimizar o seudoanonimizar los datos, sin que sea necesario mantenerlos identificados, lo que crea cierto conflicto con la definición estricta de datos de carácter personal.

El Responsable del tratamiento deberá poder demostrar que no es posible realizar la identificación del interesado, y si es posible deberá de informar, en consecuencia ya no estará obligado a atender los derechos de los afectados regulados en el Reglamento (arts. 15 a 20 RGPD): derecho de supresión, derecho al olvido, derecho a limitación del tratamiento, la obligación de notificación relativa a la rectificación o supresión de datos personales o a la limitación del tratamiento y, finalmente, el derecho a la portabilidad de los datos.

En cualquier caso, será necesario determinar que los datos no se encuentran asociados a un sujeto identificable, porque lo que puede ser considerado así en un principio es posible que varíe si existe algún sistema o técnica que aunque sea empleando medios desproporcionados permite identificar al interesado.

### 5.8.5. Transparencia en la Información al Interesado del Tratamiento de sus datos

Vamos a poder profundizar en uno de los principios fundamentales de la protección de datos, recogido por primera vez en el RGPD, que es el principio de transparencia, es evidente que la información es esencial en la vida de las personas y para la marcha de la economía. La unión europea en aras de la confirmación de un espacio único europeo, se propone eliminar los obstáculos de libre circulación de la misma, surgidos de la transposición de la Directiva 95/46/CE mediante prácticas y normas nacionales diversas. El RGPD persigue establecer un régimen único, muy especialmente en cuanto a las garantías que los ciudadanos deben tener para proteger sus datos adecuadamente, reforzando sus

derechos y ampliando los elementos que abarcan el derecho de información y el resto de los derechos, exigiendo que el responsable del tratamiento cumpla estas obligaciones de un modo transparente, es decir, que sea comprensible para el interesado y así aumente su control sobre su información y datos de carácter personal.

Además, las diferentes formas de proporcionar la información al interesado a través del sistema de doble capa, iconos y sistemas de certificación, veremos las obligaciones especiales que el responsable del tratamiento debe prestar cuando traten datos de carácter personal de menores.

### 5.9. PRINCIPIO DE TRANSPARENCIA EN RELACIÓN AL DERECHO DE INFORMACIÓN

Es importante destacar que tanto el principio de transparencia como el principio de información en el RGPD se han regulado en el Capítulo III, denominado "Derechos del Interesado". Sin embargo, el principio de información parece que cambia con respecto a anteriores regulaciones Directiva 95/46/CE, LOPD y RLOPD y deja de considerarse un principio informador de la protección de datos para pasar a considerarse un derecho del interesado.

Respecto al nuevo principio de transparencia, como ya hemos visto, en el art. 5.1.a) RGPD (que regula los principios del tratamiento), introduce el principio de transparencia cuando indica que "los datos personales serán tratados de manera lícita, leal y transparente en relación con el interesado". Sin embargo, se desarrolla y regula dicho principio de transparencia en el art. 12 y dispone, en su apartado primero, que el responsable del tratamiento deberá tomar las medidas oportunas para facilitar a los interesados:

- Información regulada, en los arts. 13 y 14 RGPD, que debe facilitarse al interesado cuando los datos hayan sido obtenidos o no, directamente del interesado.
- Información de las comunicaciones con arreglo a los arts. 15 a 22 y 34 que se refieren a los derechos del interesado (Derecho de acceso, rectificación, supresión, limitación del tratamiento, portabilidad de los datos, derecho de oposición y decisiones individuales automatizadas) y a las comunicaciones relacionadas con violaciones de seguridad.

La justificación de este nuevo principio la podemos encontrar en el Considerando 58 RGPD que determina que este principio de transparencia de información es especialmente importante en

> "situaciones en las que la proliferación de agentes y la complejidad tecnológica de la práctica hagan que sea difícil para el interesado saber y comprender si se están recogiendo, por quién y con qué finalidad, datos personales que le conciernen, como es en el caso de la publicidad en línea. Dado que los niños merecen una protección específica, cualquier información y comunicación cuyo tratamiento les afecte debe facilitarse en un lenguaje claro y sencillo que sea fácil de entender".

Así, el principio de transparencia requiere que la información y las comunicaciones que se realicen por el responsable del fichero sean:

- En forma concisa, transparente, inteligible
- De fácil acceso.
- Con un lenguaje claro y sencillo, debiendo acentuarse estas características cuando esa información va dirigida a un niño.
- Puede ser facilitada por escrito o por otros medios, incluidos los electrónicos.
- Cuando lo solicite el interesado, la información puede facilitarse verbalmente (siempre que se demuestre la identidad del interesado por otros medios).

### 5.9.1. Excepciones

El responsable para cumplir con la información que requiere proporcionar al interesado permite que ésta sea proporcionada mediante el sistema o forma que el responsable elija, siempre que realice su función de garantía de consentimiento informado. Así, el Grupo de trabajo del artículo 29 establece que "suministrarse directamente a las personas. No basta con ponerla a disposición en algún sitio". En este mismo sentido, la AEPD ha declarado lo siguiente:

> "ha venido considerando suficiente el cumplimiento del deber de información, mediante la existencia de un cartel anunciador siempre que el mismo resulte claramente visible por parte del afectado, quedando así

garantizado que el mismo ha podido tener perfecto conocimiento de la información exigible".

Este criterio se considera conforme, si el cartel anunciador señala todos los elementos exigidos por la norma y además reúne los requisitos de visibilidad y legibilidad, que aseguren que el interesado "ha podido tener perfecto conocimiento de la información exigible". Sin embargo, es necesario señalar que hay determinadas finalidades de tratamiento, que no permiten entablar una relación directa con el interesado, cuyos datos son recabados y tratados, como ocurre, por ejemplo, con la grabación de imágenes con fines de videovigilancia, donde las cámaras captan imágenes de un conjunto de personas que incluso en el momento de la recogida de los datos son indeterminadas para el responsable del tratamiento.

Así, la finalidad del tratamiento de vigilancia y los legítimos intereses a que sirve, es en sí misma difícilmente compatible con el suministro directo de información al interesado de la información exigida. En estos casos, se puede valorar el establecer un anuncio de la recogida de datos, que remita a un lugar donde la información exigida esté disponible.

Se ha considerado que esta relajación en el deber de información ha de ir acompañado de un endurecimiento de otros requisitos o exigencias como son:

- El periodo de conservación de los datos
- O la posibilidad de utilizar los datos para otra finalidad diferente.

En el entorno tecnológico de la información acerca del tratamiento tiende a ser compleja y extensa, lo que supone que el interesado no le preste atención y esto puede ser porque no confía en comprender dicha información, o porque no quiere perder el tiempo que requiere leerla. Así, la norma europea ha buscado que la presentación gráfica mediante iconos colabore a una compresión intuitiva de los caracteres del tratamiento.

Sin embargo, hay que tener en cuenta que el Grupo del artículo 29, ya ha advertido, que la información de los iconos por sí sola no es bastante para entender realizado el deber de informar que incumbe al responsable. Se puede considerar que los iconos sirven como complemento de otros medios de informar, o incluso como un recordatorio constante de lo que implica cierto tratamiento.

Este planteamiento es el que ha llevado al art. 12.7 RGPD a que determine que la información que deberá facilitarse al interesado en virtud de los arts. 13 y 14 podrán transmitirse en combinación con iconos normalizados, que permitan proporcionar de forma fácilmente visible, inteligible y claramente legible una adecuada visión del conjunto del tratamiento previsto. Además, que los iconos que se presenten en formato electrónico serán legibles mecánicamente.

La función que se le asigna a los iconos y su eficacia va a depender de su sencillez y de que sean universalmente identificables, por lo que el art. 12.7 RGPD alude a iconos normalizados y el art. 12.8 RGPD remite a actos delegados de la Comisión que deberán especificar la información que se ha de presentar a través de iconos y los procedimientos para presentar iconos normalizados.

En relación con la certificación, he de señalar que el Reglamento incentiva la creación de mecanismos de certificación, mediante los cuales el responsable o el encargado puedan demostrar el cumplimiento de las obligaciones que legalmente le incumben. De este modo, el responsable del tratamiento en relación con la obligación de informar puede acreditar con un sello o marca de protección de datos haber facilitado al interesado las informaciones requeridas por los arts. 13 y 14 RGPD, y según el principio de transparencia.

Hay que entender que la certificación no limita la responsabilidad del responsable, pero si permite al usuario, de un modo sencillo conocer el nivel de protección de datos de los productos o servicios que pretende utilizar. El considerando 100 RGPD afirma que

> "a fin de aumentar la transparencia y el cumplimiento del presente Reglamento, debe fomentarse el establecimiento de mecanismos de certificación y sellos y marcas de protección de datos, que permitan al os interesados evaluar con mayor rapidez el nivel de protección de datos de los productos y servicios correspondientes".

# CAPÍTULO VI.-
# EL ACCESO A LA INFORMACIÓN EN PANAMÁ

# CAPITULO VI.- EL ACCESO A LA INFORMACIÓN EN PANAMÁ

## 6.1. INTRODUCCIÓN

Los países más avanzados y desarrollados del mundo tienen entre otros, el denominador común de haber sido pioneros en el reconocimiento y regulación de la trasparencia[128], y acceso a la información pública[129], por lo que podemos trasladar que el grado de evolución democrática de los países desarrollados puede ser observado entre otros, por los mecanismos y tratamientos que otorga al ciudadano sobre transparencia e información, constituyendo una conquista democrática al servicio del ciudadano, obtener el conocimiento y la vía de acceso a la administración de los recursos públicos, de manera completa, veraz, adecuada y oportuna[130]. En este ensayo, observaremos al respecto, el ordenamiento Jurídico Panameño y el español, para conocer el estado de la cuestión, y cómo se desarrolla su naturaleza, objeto, sujetos obligados, límites, procedimientos y garantías, los mecanismos destinados a garantizar la efectividad del derecho, las obligaciones de publicidad activa en las nuevas tecnologías de la información y finalmente, la que probablemente suscite la gran revolución de la información del siglo xxi en esta materia, encartándose como la destinada a limitar la corrupción.

Entre finales de los años ochenta y principios del siglo XXI, hubo una eclosión de Derechos, generalizándose la aprobación de leyes de transparencia y mecanismos de acceso a la información pública, expandiéndose entre los países

---

[128]Según GICHOT REINA, E., "Transparencia y acceso a la información pública en España: análisis y propuestas legislativas". Documento de trabajo 170/2011. Fundación Alternativas. *En Laboratorio de alternativas* 2011. p. 7. En donde matiza que el reconocimiento y desarrollo legal del derecho de acceso a la información pública están en directa relación con el nivel de democracia de los países,

[129]La aprobación de normas durante el siglo pasado que garantizan el derecho de acceso a la información pública fue liderado por; Suecia desde 1766, Finlandia desde 1951, EEUU desde 1966, Dinamarca y Noruega desde 1970, Francia y Países Bajos desde 1978, Australia y Nueva Zelanda desde 1982, Canadá desde 1983, Austria y Filipinas desde 1987, Italia desde 1990, España desde 1992, e Israel desde 1997.

[130]GUICHOT REINA, E., "Transparencia y acceso a la información…" ob cit. p.10En este sentido abunda Guichot Reina que se presentan diversas excepciones a esta regla, como la tardía apuesta por este género de leyes por grandes potencias europeas como Reino Unido o Alemania, o el caso de Suiza, y restando por incorporarse, en términos generales, donde el sistema político no es exactamente democrático occidental, según el autor, países como Venezuela o Cuba.

latinos[131], leyes reguladoras de las relaciones entre la administración y el ciudadano o leyes sobre el procedimiento administrativo que deberían seguir estos para acceder a información propia o de terceros, posibilitando y afianzando los procesos de democratización que Samuel P. Huntington denomino, la Tercera Ola democratizadora[132], y que por lo general, obedeció como respuesta a una opinión pública especialmente crítica en relación con la opacidad, la corrupción, y el déficit democrático de las instituciones. El acceso a la información es una herramienta definidora de una sociedad democrática, dado que a través del acceso a la información pública se pueden proteger derechos y prevenir abusos, así como luchar contra males como la corrupción. El reconocimiento del derecho de acceso a la información pública como derecho humano ha ido por tanto evolucionando progresivamente en distintos países en el marco de la legalidad y derecho internacional. La regulación del derecho a saber se ha extendido en el mundo y también en América Latina, en donde la región cuenta con una serie de países[133] que han avanzado en el reconocimiento del derecho a acceder a información pública, y enfrentan los desafíos de la implementación de estas nuevas regulaciones. Dada su importancia, la Asamblea General de la OEA ha realizado varios pronunciamientos respecto al derecho de acceso a la información pública, brindando su mandato a la Relatoría Especial para hacer seguimiento al tema, y ha instado a los Estados miembros a que adopten las recomendaciones efectuadas por una Relatoría Especial.[134]

[131]En el ámbito de América central, Sudamérica y Caribe, la legislación y mecanismos de acceso a la información pública fue liderado por Colombia en 1888, Belice desde 1994, Aruba, Antillas Holandesas, Trinidad y Tobago desde 1999, Paraguay desde 2001 (derogada seguidamente), México, Panamá, Perú y Jamaica desde 2002, San Vicente, Las Granadinas y Argentina desde 2003, República Dominicana, Ecuador, Bolivia y Antigua/Barbuda desde 2004, Honduras desde 2006, Nicaragua desde 2007, Uruguay, Islas Caimán, Chile y Guatemala desde 2008, Islas Bermudas desde 2010 y Brasil desde 2011.

[132]HUNTINGTON, S, P., The third wave. Democratization in the late twentieth century, Norman, University of Oklahoma Press, 1991. (La tercera ola), citado en Peschard Mariscal, J., "El derecho de acceso a la información y la universidad pública Universidades" vol. LX, núm. 45, abril-junio, 2010, p. 11, Unión de Universidades de América Latina y el Caribe. *En Red de Revistas Científicas de América Latina, el Caribe, España y Portugal*

[133] Antigua y Barbuda, Brasil, Chile, Colombia, Ecuador, El Salvador, Guatemala, Jamaica, Honduras, México, Nicaragua, Panama, Perú, República Dominicana y Uruguay.

[134]Los informes de la Relatoría Especial a los que se ha hecho mención, los cuales responden a los mandatos de la Asamblea General, se han concentrado en la fijación de los estándares normativos interamericanos sobre acceso a la información, sistematizando la doctrina y la jurisprudencia interamericana en la materia. Una recopilación actualizada del marco jurídico interamericano en

En el año 2006, la Corte Interamericana de Derechos Humanos, marcó un hito[135] jurisprudencial al determinar cuál es el contenido del derecho de acceso a la información pública y su marco normativo internacional, destacando la importancia de este derecho y estableciendo que cualquier restricción al mismo debe ser necesaria en la sociedad democrática y debe respetar el principio de legalidad. En esta línea, los días 16 y 17 de abril del año 2007, tuvo lugar el I Encuentro Iberoamericano sobre Transparencia y Lucha contra la Corrupción, organizado por Transparencia Internacional-España y celebrado en el Instituto Universitario de Investigación Ortega y Gasset en Madrid[136]. Los capítulos nacionales que participaron en dicho encuentro fueron: Argentina, Chile, Colombia, Ecuador, Guatemala, Honduras, México, Nicaragua, Panamá, Paraguay, Perú, República Dominicana, Uruguay, Venezuela, Banco Mundial y el Banco Interamericano de Desarrollo. En el año 2011 se sostuvo que 90 países del mundo habían adoptado leyes que regulaban el ejercicio del derecho a acceder a

---

materia del derecho al acceso a la información pública fue recientemente publicada por la Relatoría Especial. Véase: Relatoría Especial para la Libertad de Expresión. El Derecho de acceso a la información en el marco jurídico interamericano. 30 diciembre 2009. Documento CIDH/RELE/INF.1/09. Disponible en:
http://www.oas.org/es/cidh/expresion/docs/publicaciones/ACCESO%20A%20LA%20INFORMACION%20FINAL%20CON%20PORTADA.pdf

[135]Corte Interamericana de Derechos Humanos Caso Claude Reyes y otros Vs. Chile Sentencia de 19 de septiembre de 2006 (Fondo, Reparaciones y Costas) *Este caso llega a la Corte Interamericana por la negativa del Estado de brindar al señor Marcel Claude Reyes toda la información que solicitó del Comité de Inversiones Extranjeras, en relación con la empresa forestal Trillium y el Proyecto Río Condor, el cual era un proyecto de deforestación que él consideraba podía ser perjudicial para el medio ambiente e impedir el desarrollo sostenible de Chile. El Estado, en sede internacional, argumenta que no se entregó la información financiera de la empresa porque ésta podría afectar el interés colectivo, inhibir las inversiones y afectar la competencia de la empresa en el mercado, aduciendo además que no era el titular de dicha información y no podía entregar información de terceros que se encontrase en su poder. La Corte Interamericana sanciona al Estado Chileno por la negativa de brindar información, considerando que ésta es de interés público, y por la falta de un recurso judicial efectivo para salvaguardar el derecho de acceso a la información.*
Accesible en *http://www.corteidh.or.cr/docs/casos/articulos/seriec_151_esp.pdf*

[136]Para acceder a la declaración completa del evento de referencia, además de tener acceso a los informes de corrupción en España, recomendamos la visita a la página Web http://www.transparencia.org.es/. En la declaración final conjunta se destaca, entre otros puntos, que se reitera la decisión de impulsar la transparencia en la gestión pública mediante la participación ciudadana, el acceso a la información y la rendición de cuentas sobre todos los actos de la Administración Pública, y de propiciar que la lucha contra la corrupción pase a ser punto central de las agendas políticas a nivel local, regional y nacional. Además de intensificar los esfuerzos de la sociedad civil para promover la aprobación en todos los países de una ley de acceso público a la información.

la información[137] La principal característica de estas normas era la posibilidad de solicitar información pública en forma individual. En medio de este auge tuvo lugar la instauración de la Alianza para el Gobierno Abierto (OGP por sus siglas en inglés —Open Government Partnership)[138] en 2011, que ofrece a los países miembros, la oportunidad de integrar sus estrategias en un marco de políticas de Gobierno Abierto. En el caso de Latinoamérica, si bien no todos los países integran el OGP, 21 de ellos cuentan con una LTAI. Estos son: Argentina, Brasil, Belice, Colombia, Chile, Ecuador, El Salvador, Guyana, Guatemala, Honduras, Jamaica, México, Nicaragua, Panamá, Paraguay, Perú, República Dominicana, Trinidad y Tobago, y Uruguay. En este sentido, actualmente cerca de 90 países, reconocen el derecho del ciudadano al acceso a la información que maneja el Estado, mediante leyes y mecanismos para que este, pueda acceder a la información pública, habiendo sido incorporado en más de 40 países, como derecho constitucional[139].

### 6.2. EL OBJETO DEL DERECHO A LA INFORMACIÓN

En un contexto del Estado Social y Democrático de Derecho la Transparencia Administrativa es una obligación de toda Administración Pública. Tal obligación se traduce en el deber de las Administraciones Públicas de informar a los administrados de los diversos aspectos de la gestión administrativa y en los derechos correlativos de los administrados a ser informados, por parte de las Administraciones Públicas, veraz y objetivamente y a buscar información en

[137]Vleugels, Roger. "Overview of all FOI laws". Fringe Special 9 de Octubre de 2011.

[138]En su presentación en www.opengovpartnership.org se lee: «La Alianza para el Gobierno Abierto busca el establecimiento de compromisos de los gobiernos con la ciudadanía para promover la transparencia, empoderar a los ciudadanos y ciudadanas, combatir la corrupción y utilizar las tecnologías con el fin de mejorar la gobernanza democrática. Ofreciendo un foro internacional para el diálogo y para compartir innovaciones entre todos los actores comprometidos en la consecución del gobierno abierto: gobiernos, sociedad civil y el sector privado». Al ingresar a OGP, cada país se compromete a desarrollar un Plan de Acción acorde con sus políticas.

[139]Open Society Justice Initiative; Transparency & Silence. A Survey of Access to Information Laws and Practices in 14 Countries. Justice in Action Series. New York, 2006, pág. 21, citado en "Estudio Especial sobre el Derecho de acceso a la Información" en Relatoría especial para la libertad de expresión comisión interamericana de derechos humanos organización de los estados americanos. WASHINGTON, D. C. 2006. p.12. Accesible en http://cidh.oas.org/relatoria/section/Estudio%20Especial%20sobre%20el%20derecho%20de%20Acceso%20a%20la%20Informacion.pdf

éstas. La obligación a la Transparencia Administrativa no tiene un contenido homogéneo, unívoco, es un instituto jurídico que al señalar el deber ser o arquetipo de toda Administración Pública aglutina una serie de instituciones, mecanismos e instrumentos para actuarla o concretarla cuyo único fin o propósito es hacer visible el poder administrativo.[140] El objeto de una norma sobre el acceso a la información, incluye la información obrante en bases de datos que por lo general se puedan extraer de modo sencillo, al alcance del ciudadano para que puedan dar respuesta a las solicitudes de información administrativa más demandadas y que se requiere, este relacionada con documentos de carácter oficial, cualquiera que sea su soporte, sobre la actividad pública, privada o legislativa.

Esta acotación supone un amplio espectro de información al servicio del ciudadano contemplándose además los documentos en poder de la autoridad pública o de uso interno de la administración, o documentos de naturaleza privada, que hayan sido elaborados o no por estas y cualquiera otro documento preparatorio que tuviere como hemos avanzado, en su consecución y finalidad, el carácter de oficial en su versión definitiva, dentro del aparato administrativo o legislativo de un país.

La generalidad de países democráticos consideran el objeto de información como el derecho de acceso por el ciudadano a un amplio catálogo de administraciones o documentos como por ejemplo, el caso de EEUU, en donde el derecho del administrado le provee de acceso a "cualquier departamento estatal o municipal, panel, buró, división, comisión, comité, autoridad pública, corporación pública, consejo, oficina u otra instancia gubernamental que lleve a cabo una función pública o de gobierno", eso sí, dejando fuera de su aplicación explícitamente a los poderes judicial y legislativo. "la celebración de contratos inminentes" y protege el interés privado por sobre el público al grado de incluir entre sus excepciones toda la información "cuya divulgación causaría una lesión substancial a la competitividad de las empresas" "técnicas o procedimientos de

[140] JINESTA LOBO, E., Transparencia administrativa y derecho de acceso a la información administrativa. Aletheia, Cuadernos Críticos del Derecho. 2-2015 p 136

investigación criminal" y en general los materiales "interinstitucionales" o "intrainstitucionales[141]".

### 6.3. EL DERECHO DE ACCESO A LA INFORMACIÓN EN PANAMÁ

El derecho de acceso a la información no solo en el área latina, sino de manera generalizada por los estados, carecieron durante décadas, de falta de operatividad y eficacia, debido a difusos conceptos jurídico-paternalistas, que debían ser necesariamente emanados, administrados y a recaudo del Estado y en donde el ciudadano, debía someterse al imperativo administrativo en las relaciones con este. Superados tales constructos jurídicos arcaicos, los distintos países fueron adaptando sus legislaciones a una corriente reformadora donde todos los países considerados democráticos instauraban leyes de acceso a la información o leyes de transparencia. Al objeto de este trabajo observaremos las leyes de acceso a la información y leyes de transparencia en Panamá.

En Panamá la Ley N 6 de 22 de enero de 2002[142] dicta normas para la transparencia en la gestión pública y establece la acción de Habeas Data[143] en

[141]Párrafo 2 de la Sección 87 de la Public Officers Law, Artículo 6. Citado en Sandoval, I, E., "Transparencia y Control Ciudadano: Comparativo de Grandes Ciudades". Instituto de Investigaciones Sociales de la Universidad Nacional Autónoma de México. 2007. pp 19 y ss

[142]En Panamá, la Ley N° 6 de 22 de enero de 2002 reconoce este derecho en el numeral 2 del artículo 1 al establecer que este consiste en "Aquel que tiene cualquier persona de obtener información sobre asuntos en tramites en curso en archivos en expedientes documentos registros decisión administrativa o constancias de cualquier naturaleza en poder de las instituciones incluidas en la presente Ley." entendiéndose por información según el artículo 1 numeral 4 de la ley citada todo tipo de datos contenidos en cualquier medio documento o registro impreso óptico electrónico químico físico o biológico. De esta disposición resaltan tres aspectos importantes que se derivan del derecho de libertad de información los que tienen que ver con a) lo puede aducir cualquier persona ya sea esta, por tanto natural o jurídica, nacional o extranjera b) el ejercicio del mismo permitirá recabar o requerir información ya sea de casos en trámite o curso o cuando está ya esté en archivos documentos decisiones administrativas o en constancias de cualquier naturaleza,) y se podrá ejercer con respecto a la información que este en poder o custodia de las instituciones incluidas o las que se refiere a la Ley 6 de 2002

[143]Por primera vez y a través de este recurso legal, se establece un procedimiento especial sumario e informal, para controlar las decisiones que sobre esta materia ofrezcan los custodios y responsables de la información a los solicitantes. Control que por competencia les corresponde a los más altos tribunales de justicia, al dirimir las acciones de Habeas Data. En cuanto a la protección de la esfera íntima de la persona dentro del cambio de modelo de la sociedad tradicional a la sociedad de la información que ante el desarrollo de las comunicaciones la informática, y el intercambio casi incontrolado de todo tipo de información que posibilita el acceso remoto a bases y bancos de datos

donde se establecen los medios administrativos a merced del ciudadano para hacer efectivo el derecho a la información que emana con rango constitucional, el cual se materializa mediante el acto legislativo N 1 del 27 de julio del 2004 en los artículos 42 43 y 44 las cuales constituyen una de las principales iniciativas legislativas de reconocimiento de derechos fundamentales al establecer un mecanismo o instrumento claro y breve para lograr el acceso a la información en manos de agentes del Estado[144] y demás instituciones que incluye la Ley [145]. Según Barrios González, [146] el Habeas Data Panameño entendido como enunciado principialista de su ley de trasparencia, este radica en su contexto ideológico y axiológico, cómo límite a los poderes tanto públicos como privados que tienen el deber de adecuar sus actuaciones al contexto normativo de protección a la información personal y pública y al derecho a la intimidad; mientras que el Habeas data como derecho, debemos entenderlo como un derecho subjetivo y por tanto atribuible a la persona que se manifieste afectada por el incumplimiento que

---

que pueden contener información personal surge la acción de Habeas Data como un mecanismo necesario para proveerle a las personas el derecho a la autodeterminación es decir el derecho de poder decidir y controlar el uso de la información que pertenece al usuario privado, ya que con la acción de Habeas Data los particulares se benefician en el sentido de que se les respete sus derechos humanos a la inanidad se les protege de los abusos excesos y arbitrariedades que con el mal uso de la información puedan lesionar los derechos de la personalidad como otros derechos constitucionales motivados por una información tergiversada, falsa o indiscriminada que conste en un banco de datos

[144]En Panamá, el artículo 8° de la Ley para la Transparencia en la Gestión Pública prevé el principio de publicidad y determina: "las instituciones del Estado están obligadas a brindar, a cualquier personal que lo requiera, información sobre el funcionamiento y las actividades que desarrollan, exceptuando únicamente las informaciones de carácter confidencial y de acceso restringido" República de Panamá. Ley de Transparencia en la Gestión Pública. Ley N° 6. 22 de enero de 2002. Disponible en: http://www.presidencia.gob.pa/ley_n6_2002.pdf

[145]El artículo 17 de la Ley para la Transparencia en la Gestión Pública de Panamá dispone que todas las personas están legitimadas para iniciar una acción constitucional de hábeas data cuando la información que solicitaron les ha sido negada o les ha sido proporcionada en forma incompleta o inexacta. La acción se entabla ante los Tribunales Superiores que conocen de la acción de amparo, cuando el funcionario demandado tenga jurisdicción a nivel provincial o municipal, o ante el mismo Pleno de la Corte Suprema de Justicia, cuando su jurisdicción se extienda sobre dos o más provincias o a nivel nacional344. De acuerdo con el artículo 19, el procedimiento es sumario, no requiere del acompañamiento de un abogado y se rige en distintos aspectos por las reglas de la acción de amparo de garantías constitucionales.

[146]Barrios González, B. El derecho de acceso a la información y el hábeas data. Cultural Portobelo, Volumen 229 de Biblioteca de autores panameños. 2014

se prevé, en los artículos 42[147] y 43[148] de la Constitución Panameña, entonces, la persona puede hacer, uso del ejercicio del Habeas Data como garantía jurisdiccional de protección del derecho fundamental. Es por ello que el incumplimiento de protección del derecho a la información y protección de la intimidad que se circunscribe la ley de trasparencia implica un efecto sancionador contra la autoridad.[149]

En la información de carácter público o de acceso libre en panamá, impera el principio de publicidad el cual está reconocido en la Ley 6 de 2002 cuando dispone en el numeral 11 del artículo 1 que "toda información que emana de la administración pública es de carácter público" Al ser una Información en la que va a prevalecer este principio traerá como resultado el que siendo esta la regla se ha de entender que excepcionalmente se podrá negar el acceso a la información que habiendo emanado del Estado y aun estando en bajo su custodia, no sea de acceso libre, por distinguirse algún tipo de restricción.

El numeral 6 del artículo I de la Ley N 22 de enero de 2002 dispone que por información de acceso libre se entiende todo tipo de información en manos de agentes del Estado o de cualquier institución pública que no tenga restricción. La información libre y de carácter público[150] será entonces aquella que "toda persona

[147]Artículo 42. Toda persona tiene derecho a acceder a la información personal contenida en bases de datos o registros públicos y privados, y a requerir su rectificación y protección, así como su supresión, de conformidad con lo previsto en la Ley."

[148]Artículo 43: Toda persona tiene derecho a solicitar información de acceso público o de interés colectivo que repose en bases de datos o registros a cargo de servidores públicos o de personas privadas que presten servicios públicos, siempre que ese acceso no haya sido limitado por disposición escrita y por mandato de la Ley, así como para exigir su tratamiento leal y rectificación.

[149]El texto constitucional Panameño, conforme a la reforma del 2004, artículos 42 y 43 del texto constitucional distinguen entre información personal y pública; y es por ello que el artículo 42 instituye que, cuando se trata de información personal, toda persona tiene derecho a acceder a su información personal contenida en bases de datos o registros públicos y privados, y a requerir su rectificación y protección, así como su supresión, de conformidad con lo previsto en la Ley; mientras que cuando se trata de información pública el artículo 43 establece que toda persona tiene derecho a solicitar información de acceso público o de interés colectivo que repose en bases de datos o registros a cargo de servidores públicos o de personas privadas que presten servicios públicos, siempre que ese acceso no haya sido limitado por disposición escrita y por mandato de la Ley, así como para exigir su tratamiento leal y rectificación.

[150]El artículo 16 de la Ley de Transparencia Panameña, establece que "las instituciones del Estado que nieguen el otorgamiento de una información por considerarla de carácter confidencial o de acceso restringido, deberán hacerlo a través de resolución motivada, estableciendo las razones en que se fundamenta la negación y que se sustenten en esta Ley".

tiene derecho a solicitar por escrito,[151] sin necesidad de sustentar justificación o motivación alguna"[152], por lo que entendemos como titular del derecho al acceso a la información, a toda persona física o jurídica[153].

Aun todo esto, La ley de Trasparencia Panameña, en su artículo 1, contempla una serie de definiciones, y en su numeral 11 contempla el principio de publicidad, de acuerdo con el cual toda información que emana de la administración pública es de carácter público, salvo las excepciones previstas, correspondientes a la información confidencial[154] y a la de acceso restringido[155].

---

[151]La Ley de Transparencia de Panamá establece que las solicitudes de información solamente se pueden presentar por escrito, bien sea en papel o por vía electrónica. La solicitud no requiere de abogado y, aun cuando no se exige demostrar un interés directo en la información solicitada, el peticionario debe identificarse. Artículo 5° de la Ley de Transparencia en la Gestión Pública: "La petición se hará por escrito en papel simple o por medio de correo electrónico, cuando la institución correspondiente disponga del mismo mecanismo para responderlo, sin formalidad alguna, ni necesidad de apoderado legal, detallando en la medida de lo posible la información que se requiere, y se presentará en la oficina asignada por cada institución para el recibo de correspondencia. Recibida la petición, deberá llevarse de inmediato al conocimiento del funcionario a quien se dirige".

[152]La información solicitada deberá ser suministrada por el funcionario obligado a ello en 'treinta días naturales, que comenzaran a correr a partir de la fecha de la presentación de la solicitud aspecto este al que se refiere el artículo 7 de la Ley 6 de 2002 De igual forma que esté ante la petición de una información de manejo complejo o extenso se deberá hacer saber por escrito de esta situación a la persona que formuló dicha solicitud pudiendo así el funcionario de que se trate, extender el termino para recopilar la información solicitada el cual no podrá exceder de otros treinta días naturales adicionales La necesidad de extender el termino original se deberá notificar dentro de los primeros treinta chas en que se presentó la solicitud de la información.

[153]La Ley de Transparencia Panameña, establece que toda persona "tiene derecho a solicitar, sin necesidad de sustentar justificación o motivación alguna, la información de acceso público en poder o en conocimiento de las instituciones indicadas en la presente Ley"

[154]De acuerdo con el numeral 5 del artículo 1 de la Ley de Transparencia en la Gestión Pública de Panamá, es información confidencial toda aquella que se encuentre en posesión de agentes del Estado, o de cualquier institución pública, que tenga relevancia con respecto a los datos íntimos de las personas, tales como los datos médicos y psicológicos, la vida íntima, su historial penal y policivo, su correspondencia y los expedientes de personal de los funcionarios

[155]De acuerdo con el numeral 7 del artículo 1 de la Ley de Transparencia en la Gestión Pública de Panamá, la información de acceso restringido se refiere a los datos en posesión de agentes del Estado, o de cualquier institución pública, cuya divulgación haya sido circunscrita únicamente a los funcionarios que la deben conocer. Así, el artículo 14 establece que se considera de acceso restringido: La información relativa a la seguridad nacional manejada por los estamentos de seguridad; Los secretos comerciales o la información comercial de carácter confidencial, obtenidos por el Estado, producto de la regulación de actividades económicas; Los asuntos relacionados con procesos [disciplinarios] o jurisdiccionales adelantados por el Ministerio Público y el Órgano Judicial, los cuales sólo son accesibles para las partes del proceso, hasta que queden ejecutoriados; La información que versa sobre procesos investigativos realizados por el Ministerio Público, la

### 6.4. TITULARIDAD DEL DERECHO DE ACCESO A LA INFORMACIÓN

La titularidad del acceso a la información se somete generalmente a la acreditación o no del interés en el asunto que se pretenda demandar o si el titular que lo solicita es un agente de la sociedad civil[156], por cualquier nacional o de ámbito de acceso universal. Desde la citada sentencia de Claude Reyes y otros, la Corte Interamericana establece la idea de que este derecho corresponde a toda persona. La información solicitada debe ser entregada sin necesidad de acreditar un interés directo para su obtención o una afectación personal, salvo en los casos en que se aplique una legítima restricción, admitiendo incluso el ejercicio del derecho por cualquier persona independientemente, por ejemplo, de su condición migratoria, y establece expresamente que todas las personas que se encuentren en el territorio de un país, sean o no nacionales de este, deben beneficiarse de este derecho.

---

Fuerza Pública, la Policía Técnica Judicial, la Dirección General de Aduanas, el Consejo Nacional de Seguridad y Defensa, la Dirección de Responsabilidad Patrimonial de la Contraloría General de la República, la Dirección de Análisis Financiero para la Prevención de Blanqueo de Capitales, la Comisión de Libre Competencia y Asuntos del Consumidor y el Ente Regulador de los Servicios Públicos; La información sobre existencia de yacimientos minerales y petrolíferos; Las memorias, notas, correspondencia y los documentos relacionados con negociaciones diplomáticas, comerciales e internacionales de cualquier índole; Los documentos, archivos y transcripciones que naciones amigas proporcionen al país en investigaciones penales, policivas o de otra naturaleza; Las actas, notas, archivos y otros registros o constancias de las discusiones o actividades del Consejo de Gabinete, del Presidente o Vicepresidentes de la República, con excepción de aquellas correspondientes a discusiones o actividades relacionadas con las aprobaciones de los contratos"; y "La transcripción de las reuniones e información obtenida por las Comisiones de la Asamblea Legislativa, cuando se reúnan en el ejercicio de sus funciones fiscalizadoras" para recabar cualquiera de la información anteriormente relacionada.

[156] Siguiendo a Holsen, S., Journalists' Use of the UK Freedom of Information Act, Open Government: a journal on freedom of information, 2007. Citado por Guichot Reina. op cit p.29, denominamos a la llamada "sociedad civil", descartando en este grupo, al ciudadano de a pie., e incluyendo a los académicos, a los representantes de intereses empresariales, a los despachos de abogados, a las asociaciones y organizaciones no gubernamentales y a los periodistas de investigación, y en donde estos, representan el grupo que mayor demanda de información solicitan de las bases de datos de información.

## 6.5. SUJETOS OBLIGADOS DEL DERECHO A LA INFORMACIÓN

Entre los sujetos obligados encontramos principalmente a las autoridades públicas [157], y al poder ejecutivo, refiriéndonos con esto al gobierno y las administraciones que de este dependan,[158] desempeñando servicios públicos o bien servicios que se financien con fondos públicos.[159] La sentencia en el caso Claude Reyes y otros, también supuso la asunción positiva de obligaciones para los Estados de promover una cultura de transparencia en la sociedad y en el sector público, de actuar con la debida diligencia en la promoción del acceso a la información, por quien solicite esta, suministrándole la información solicitada, o dando respuesta fundamentada, en caso de que proceda la negativa de entrega por encontrarse la información solicitada dentro de las excepciones previstas legalmente.[160] La conducta de funcionarios que nieguen el acceso a la información o la existencia de legislaciones contrarias a la misma, vulneraran este derecho.[161]

---

[157] El artículo 7 de la Ley de Transparencia Panameña, dispone que los empleados de las entidades obligadas deben asistir y orientar a los solicitantes de información.

[158] Así, el artículo 10 de la Ley de Acceso a la Información Pública de Panamá dispone como objeto del derecho las informaciones sobre el funcionamiento, las decisiones adoptadas y los proyectos que se manejan en las instituciones; la estructura y ejecución presupuestaria, estadística y cualquier otra información relativa al presupuesto institucional; los programas desarrollados por la institución y los actos públicos relativos a las contrataciones públicas desarrolladas por la institución. Asimismo, en la Ley se establece que el Ministerio de Economía y Finanzas, y la Contraloría General de la República presentarán y publicarán trimestralmente un informe sobre la ejecución presupuestaria del Estado, en el cual se informará por lo menos sobre el desenvolvimiento del Producto Interno Bruto por sector y sobre el comportamiento de las actividades más relevantes por sector.

[159] La Ley de Transparencia de Panamá establece, en el numeral 8 del artículo 1º, que por institución obligada por las normas de la ley se entiende "Toda agencia o dependencia del Estado, incluyendo las pertenecientes a los Órganos Ejecutivo, Legislativo y Judicial, el Ministerio Público, las entidades descentralizadas, autónomas y semiautónomas, la Autoridad del Canal de Panamá, los municipios, los gobiernos locales, las juntas comunales, las empresas de capital mixto, las cooperativas, las fundaciones, los patronatos y los organismos no gubernamentales que hayan recibido o reciban fondos, capital o bienes del Estado"

[160] Cuando una institución estatal de Panamá niegue el acceso a la información por considerarla reservada deberá hacerlo a través de resolución motivada en la que se establecerá, con base en la Ley, cuál es el fundamento de la negación Ley N° 6. 22 de enero de 2002. Art. 16.

[161] El Capítulo VI de La Ley para la Transparencia de Panamá trata sobre las sanciones y responsabilidades de los funcionarios. Allí se establece, en el artículo 20, que el funcionario que incumple con la obligación de suministrar información después de ser requerido por un Tribunal incurre en desacato y será sancionado con "multa mínima equivalente al doble del salario mensual que devenga" y que la reincidencia será castigada con la destitución. El artículo 22 dispone que también será sancionado con multa el funcionario que obstaculice el acceso a la información y/o destruya o altere algún documento. Estas multas operan sin perjuicio de las responsabilidades penal

## 6.6. PRESUPUESTOS DE LAS LEYES DE TRASPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA EN PANAMÁ

Podemos establecer un paralelismo legista como punto de partida al derecho de acceso a la información pública, entendiendo este derecho como extensión del Derecho a la Información consagrado en la Declaración Universal de Derechos Humanos de 1948, fuente inspiradora y vinculante del ordenamiento jurídico panameño, y que en su artículo XIX establece

> "Todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión."

También en 1948 los Estados Americanos adoptaron la Declaración Americana de los Derechos y Deberes del Hombre, cuyo artículo IV establece que:

"Toda persona tiene derecho a la libertad de investigación, opinión, expresión y difusión del pensamiento por cualquier medio."

En 1966 el Pacto Internacional de los Derechos Civiles y Políticos, firmado en Nueva York, consagra en su artículo 19, lo siguiente:

> "El ejercicio del derecho de investigar y recibir informaciones y opiniones y el de difundirlas, entraña deberes y responsabilidades especiales; y que, por consiguiente, puede estar sujeto a ciertas restricciones, que deberán, sin embargo, estar expresamente fijadas por la ley y ser necesarias para asegurar el respeto a los derechos o a la reputación de los demás y la protección de la seguridad nacional, el orden público o la salud o la moral públicas".

En 1969 se suscribió la Convención Americana sobre Derechos Humanos. En donde el numeral 1 del artículo 13 expresa que:

> "Toda persona tiene derecho a la libertad de pensamiento y de expresión. Este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea

---

y administrativa que se puedan derivar del hecho. Además, la persona afectada por esta negación del acceso a la información podrá demandar al servidor público por los daños y perjuicios que se le hayan generado.

> oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección."

En Panamá, La Constitución Política de la República de Panamá de 1972, Reformada por los Actos Reformatorios de 1978. Por el Acto Constitucional de 1983 y pos los Actos Legislativos N°1 de 1993 y N°2 de 1994 y por El Acto Legislativo de 2004; establece en su Título III, Capitulo 1° "Garantías Fundamentales" en sus artículos 42, 43 y 44, el derecho a la información. Dicha excerta constitucional establece lo siguiente:

> "Artículo 42. Toda persona tiene derecho a acceder a la información personal contenida en base a datos o registros públicos y privados, y a requerir su certificación y protección, así como su supresión, de conformidad con lo previsto en la ley.
>
> Esta información solo podrá ser recogida para fines específicos mediante consentimiento de su titular o por disposición de autoridad competente con fundamento en lo previsto en la le.
>
> Articulo 43 Toda Persona tiene derecho a solicitar información de acceso público o de interés colectivo que repose en base de datos o registros a cago de servidores públicos o de personas privadas que presten servicios públicos siempre que ese acceso no haya sido limitado por disposiciones escrita y por mandato de la Ley, así como para exigir su tratamiento leal y rectificación.
>
> Artículo 44. Toda Persona podrá promover acción de hábeas data con miras a garantizar el derecho de acceso a su información personal recabada en bancos de datos o registros oficiales o particulares, cuando estos últimos traten de empresas que prestan un servicio al público o se dediquen a suministrar información.
>
> Esta acción se podrá interponer de igual forma para hacer valer el derecho de acceso a la información pública o de acceso libre, de conformidad con lo establecido en esta Constitución.
>
> Mediante la Acción de Habeas Data se podrá solicitar que se corrija, actualice, rectifique, suprima o se mantenga en confidencialidad la información o datos que tengan carácter personal. …."

En 1997 la Comisión Interamericana de Derechos Humanos creó la Relatoría Especial para la Libertad de Expresión y en el año 2000 aprobó la Declaración de Principios sobre la Libertad de Expresión elaborada por la Relatoría Especial, cuyo Principio 4 reconoce que:

"El acceso a la información en poder del Estado es un derecho fundamental de los individuos. Los Estados están obligados a garantizar el ejercicio de este derecho."

En 2002 la Comisión Interamericana de Derechos Humanos resaltó que todas las personas tienen el derecho de solicitar, entre otros, documentación e información mantenida en los archivos públicos o procesados por el Estado y, en general, cualquier tipo de información que se considera que es de fuente pública o que proviene de documentación gubernamental oficial. Desde el año 2003 la Asamblea General de la Organización de los Estados Americanos dicta resoluciones específicas sobre el acceso a la información, resaltando su estrecha relación con el derecho a la libertad de pensamiento y de expresión, instando a los Estados a que respeten y hagan respetar el acceso a la información pública a todas las personas, promoviendo la adopción de disposiciones legislativas o de otro carácter que fueran necesarias para asegurar su reconocimiento y aplicación efectiva.

Como combate a la corrupción República de Panamá cuenta con el Consejo Nacional de Transparencia contra la Corrupción (CNTCC), organismo consultivo y asesor del Órgano Ejecutivo para el diseño e implantación de una política pública de transparencia y prevención de la corrupción. Cuenta con una Secretaría Ejecutiva adscrita al Ministerio de la Presidencia, con competencia operativa a nivel nacional.

En 2007, la Secretaría Ejecutiva del Consejo Nacional de Transparencia contra la Corrupción presentó la Guía para la Incorporación de las Instituciones Públicas al Sistema de Buenas Prácticas de Integridad de Panamá (SIBUPRAIP), de conformidad con los lineamientos metodológicos desarrollado por el Proyecto Lecciones Aprendidas y Mejores Prácticas para la Integridad en la Gestión Panameña, auspiciado por el Banco Interamericano de Desarrollo. El SIBUPRAIP está dirigido a promover, identificar, y difundir buenas prácticas de gestión en materia de integridad de la Administración Pública panameña. Para que una

institución gubernamental forme parte del SIBUPRAIP, debe cumplir con una serie de requisitos mínimos de selección, además de ejecutar diversas actividades bajo la asesoría y apoyo técnico del CNTCC.

Otro proyecto ejecutado por el CNTCC es la Academia Regional Anticorrupción para Centroamérica y El Caribe, logro derivado de la participación de la Secretaría Ejecutiva del CNTCC en la Primera Reunión de Grupo sobre el Examen de Aplicación de la Convención de las Naciones Unidas Contra la Corrupción, celebrada en Viena, Austria, del 28 de junio al 2 de julio de 2010, donde se propuso a la República de Panamá como sede de una extensión de la Academia Internacional Anticorrupción de la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODD).

La Academia Regional quedó establecida el 30 de junio de 2011, mediante la firma de un acuerdo entre el Director Ejecutivo de UNODD, Yury Fedotov; el Vicepresidente y Ministro de Asuntos Exteriores de Panamá, Juan Carlos Varela y el Zar Anticorrupción de Panamá, Abigail Benzadón Cohen. La Academia ofrecerá cursos especializados para proporcionar a los fiscales, jueces, oficiales de policía y otros funcionarios públicos habilidades para prevenir, detectar y procesar la corrupción en las oficinas públicas; inicialmente se enfocará en capacitar a los funcionarios públicos de Panamá, para luego expandir sus cursos progresivamente a participantes de Centroamérica y El Caribe.

La Autoridad nacional de transparencia y acceso a la información, (A.N.T.A.I) cuyo rol principal y fundamental es como lo señala su nombre propiciar el acceso a la información y coadyuvar en que la misma bajo los nodos de transparencia sea pública, real, oportuna e íntegra, creada bajo la ley 33 del 25 de abril de 2013, desarrolla de manera profunda el acceso ciudadano y la obligación del Estado en otorgar la información. Entre sus preceptos más definitorios, encontramos en el Artículo 2 que señala "La Autoridad velará por el cumplimiento de los derechos consagrados en la Constitución Política de la República de Panamá en el tema de Derecho constitucional de petición y acceso a la información…".

Es claro entonces que el Estado Panameño en búsqueda no solo de cumplir con mantener una normativa sino de hacerla cumplir, crea una institución cuyo rol principal es permitir acceso a la información de carácter público, que la misma consta en las páginas web de cada institución y que el acceso debe ser amigable y

libre a todo público, esto se ha visto demostrado en las diferentes investigaciones periodísticas y por particulares donde actos de nepotismo, traslados millonarios de fondos y otras acciones de parte de algunos funcionarios han podido ser sancionadas o detenidas en su debido momento.

Del mismo modo ex oficio la Autoridad podrá solicitar información, elaborar investigaciones cuando considere que se están efectuando acciones que atentan contra la ley o reglamentos de la República de Panamá.

### 6.7. LIMITACIONES DEL CONTROL DEL DERECHO A LA INFORMACIÓN. EL CASO DE LOS PAPELES DE PANAMÁ

En la generalidad de las leyes de acceso a la información, los límites impuestos, deben estar enunciados en la propia norma, de modo claro, y si bien, generalmente, estarán relacionados con intereses públicos como los que se refieren a la seguridad exterior e interior, secretos de estado, la prevención y seguimiento de investigaciones criminales, la economía y las finanzas públicas, a la instrucción judicial y el correcto funcionamiento de la justicia, además de la efectividad de las actividades públicas de policía como la vigilancia y el control, datos personales de un tercero, la vida privada, en especial en lo tocante a la salud, la religión y seguridad de las personas; los intereses comerciales y económicos como la propiedad intelectual e industrial.

Es obvio y somos conscientes de que el terrorismo, la delincuencia organizada y la corrupción entre otras acciones no legítimas han utilizado las protecciones que la ley otorga para poder ocultar los beneficios de sus acciones, o el financiamiento de sus campañas cualquiera que sea el caso, del mismo modo la vulneración de las garantías fundamentales por parte de los Estados. En medio de estos se dan situaciones donde la información nace de la posible comisión de un hecho ilícito que es el robo o hurto de información, la violación a la intimidad y la protección del secreto societario. El caso de las infiltraciones que dieron pie a los mal llamados "Papeles de Panamá", adquirió mayor importancia, dado que la información vertida, provocaba acciones por parte de la OCDE contra la república de Panamá, y trastocaba principios fundamentales como el "Parem parem no archí imperium" o entre pares no hay imperio y apresuraba el debate sobre qué derecho prevalece entre el derecho a la información versus el derecho a la

intimidad. Lo que genera entonces el interés de establecer hasta qué punto el Estado puede y tiene la obligación de brindar protección a los datos[162] e información de sus ciudadanos y residentes. Los Estados, no totalitarios, que respetan el derecho a la intimidad de sus ciudadanos encuentran escoyos legales, para garantizar dicha protección, esto afecta de manera directa dado que mucha de esa información es vital para el desarrollo económico, comercial e industrial de algunos Estados.

Del mismo modo que esta salvaguarda, no se convierta en una excusa o razón, para negar el acceso a la información a los ciudadanos[163], el mayor problema se constituye, en la limitada capacidad que en virtud del derecho a la privacidad tiene los Estados para proteger la información lo que provoca la colisión de la obligación versus el derecho, la colectividad versus la individualidad, y la regularización en contradicción con la liberación del ciberespacio, estableciendo mecanismos que procuren la rápida adecuación y adaptación de la normativa de transparencia, a los agiles cambios de la tecnología, que lo que a su vez se traduce en prevención dado que muchas veces el Estado solo actúa de manera reactiva frente a las acciones de la tecnología.

El caso de los mal llamados "Papeles de Panamá", es una muestra de cómo la información privada pudo ser sustraída y difundida; dejando el velo corporativo y las garantías del derecho a la intimidad sin ninguna protección. Es pertinente poner un alto en este punto y por la trascendencia del tema establecer algunos aportes, para mayor claridad.

---

[162]De modo general establece que la información relativa a la seguridad nacional, manejada por los estamentos de seguridad; los secretos comerciales de carácter confidencial, producto de la regulación de la actividad económica, asuntos relacionados a procesos judiciales adelantados por el Ministerio Público y el Órgano Judicial, los procesos investigativos de las autoridades de seguridad del Estado, la unidad de análisis financiero, la información sobre yacimientos minerales y petrolíferos, las memorias, notas y correspondencia relacionadas a negociaciones diplomáticas los documentos enviados por otros países por motivos de investigaciones penales, las actas, notas, archivos, constancias de las discusiones o actividades del Consejo de Gabinete, el Presidente o vicepresidente de la república. Este grupo de documentos mencionados no es cerrado, dado que, si existiera otra información que el órgano judicial, el legislativo o ejecutivo consideren que debe ser confidencial deberá estar motivado dentro de la ley, una información restringida no podrá permanecer por más de 20 años y podrá prorrogarse por resolución por 10 años más.

[163]La realidad actual al 2017, es que si bien existe clasificación de información restringida vivimos en un mundo de la Información, donde las redes sociales, y equipos móviles han permitido que sea de conocimiento público información privada, lo que ha propiciado que información pública de contratos, concesiones, compras etc. salte a la vista y se ponga en la primera plana de los tabloides

Lo primero que cabe señalar es el origen o antecedente histórico, dado que la Ley de Sociedades Anónimas (Ley N 32 del 26 de febrero de 1927) como vemos al momento del escándalo es una normativa con casi cien años de vigencia. Su espíritu no es el de esconder o ser utilizadas para transgredir evadir u ocultar, era en su momento para lograr mayor agilidad comercial, de su artículo primero se desprende tales motivos.

> Artículo 1. Dos o más personas mayores de edad, de cualquier nacionalidad, aun cuando no estén domiciliadas en la República, podrán constituir una sociedad anónima para cualquier objeto lícito, de acuerdo con las formalidades prescritas en la presente ley.

Hasta el 2015, Panamá era uno de los sistemas societarios más utilizados, lo que le ha dado lugar a ser uno de los sistemas de conveniencia para la creación de personas jurídicas además por las facilidades, ventajas y eficacia que ofrece para la creación no solo empresas con fines legales sino aquellas constituidas para llevar acabo transacciones financieras y comerciales tendientes a propiciar la fase intermedia entre la colocación y diversificación de activos provenientes de actividades ilícitas, y así incorporarlos al mercado financiero como dinero lícitamente obtenido.

Analizaremos aquellos artículos que hacen flexible esta ley para los efectos de la filtración de este dinero sucio.

Desde el inicio se plantea en su Artículo 1 que cualquier persona de cualquier nacionalidad residentes o no en la República de Panamá podrá solicitar el registro de una Sociedad, solo cumpliendo con el requisito de que en su protocolo notarial manifiesta las actividades licitas y que no contravengan la legislación panameña, que llevará a cabo dicha persona jurídica una vez constituida. Esto es sumamente peligroso en el ámbito del blanqueo de capitales porque permite que cualquier persona u organizaciones delincuenciales puedan tener control y manejo de la empresa desde cualquier parte del mundo sin verificación alguna de las actividades por parte de la jurisdicción registral.

Del mismo modo esta ley contiene en su segundo artículo situaciones como en el primer numeral, que señala la figura del suscriptor, que viene a ser una de las pocas personas que figura en el registro de la sociedad, esta figura en la práctica corresponde a sujetos que no guardan la más mínima relación con la

operación, control y en fin la función de la sociedad, ni si quiera llegan a saber quiénes son los propietarios de la sociedad, casi siempre se busca a secretarios de la misma notaria, o funcionarios de las oficinas de abogados o personas que por un precio mínimo prestan su nombre para este fin, lo que propicia aún más la inacción de las leyes para frenar el blanqueo de capitales.

Continuando con el mismo artículo se establece la necesidad de establecer el domicilio de la sociedad que en casi todas las escrituras corresponde a la República de Panamá, sin necesidad de establecer un domicilio real y fijo donde ser notificado, esto se suple entonces con la figura del agente residente que será un abogado quien tendrá que especificar su nombre y domicilio.

Como respuesta a una posible instrumentalización criminal [164] de las posibilidades bancarias de la República de Panamá, esta acoge la Ley 23 de 27 de abril de 2015, publicada mediante Gaceta Oficial N° 27768-B del 27 de abril de 2015. Donde se establece

> "Que adopta medidas para prevenir el blanqueo de capitales, el financiamiento del terrorismo y el financiamiento de la proliferación de armas de destrucción masiva. Y dicta otras disposiciones".

Esta ley establece o ratifica la obligación del agente residente en conocer al cliente y la naturaleza de su negocio, además de efectuar la debida diligencia que produzca conocer la proveniencia de los fondos y el destinatario final de los mismos, esto y otra serie de medidas como la creación de la Intendencia de sujetos no regulados, y la desmovilización de las acciones al portador,

[164] Panama forma parte del Convenio Centroamericano para la Prevención y la Represión de los Delitos de Lavado de Dinero y Activos relacionados con el Tráfico Ilícito de Drogas y Delitos Conexos Fue suscrito en Panamá, el 11 de julio de 1997. Este convenio tiene una naturaleza regional limitada originalmente a los siguientes países centroamericanos: Costa Rica, El Salvador, Guatemala, Nicaragua, y Panamá. El contenido de este convenio es prácticamente exacto al Reglamento Modelo elaborado por los expertos del Comité de Lavado de Activos de la Comisión Interamericana para el Control del Abuso de Drogas (CICAD), órgano de la Organización de Estados Americanos, en la versión vigente a la fecha en que se suscribió, que limitaba el lavado de activos a los recursos provenientes del tráfico de drogas, versión que fue abandonada posteriormente conforme se indicará más adelante cuando se trate lo relativo a las propuestas normativas.

estableciendo la figura del custodio autorizado, que es quien deberá mantener posesión del libro de registro de acciones.[165].

Volviendo a la Ley bancaria como ejemplo esta vez de denegación de la información, cabe señalar que no le es dado a las instituciones públicas negar la información de manera antojadiza, como bien señala el artículo 16 de la ley 6, dicha negación tendrá que darse por resolución motivada, estableciendo las razones por la cual no se otorga la información.

1. del Decreto Ejecutivo Nº 52 del 30 de abril de 2008 que regula el Régimen Bancario en la República de Panamá:

> "Artículo 194: Derecho de los clientes bancarios. Los clientes bancarios tendrán entre otros, los siguientes derechos básicos e irrenunciables:

[165]Para el tema que nos ocupa dicha ley establece en su título VIII la "Confidencialidad" citamos: Artículo 55. Confidencialidad y reserva de la información. La información por un organismo de supervisión y la Unidad de Análisis Financiero para la Prevención del Delito de Blanqueo de Capitales y financiamiento del Terrorismo en el ejercicio de sus funciones deberá mantener bajo estricta confidencialidad y solo podrá ser revelada al Ministerio Público, a los agentes con funciones de investigación y a las autoridades jurisdiccionales conforme a las disposiciones legales vigentes. Los funcionarios de los organismos de supervisión y de la Unidad de Análisis Financiero para la Prevención del Delito de Blanqueo de Capitales y Financiamiento del Terrorismo que reciban y requieran por escrito a los sujetos obligados financieros, sujetos obligados no financieros y actividades realizadas por profesionales sujetas a supervisión, o tengan conocimiento de información por razón de lo establecido en esta Ley, deberán mantenerla en estricta reserva, confidencialidad y solamente podre ser revelada al Ministerio Público, a los agentes con funciones de investigación penal y a las autoridades jurisdiccionales conforme a las disposiciones legales vigentes. Los funcionarios de los organismos de supervisión y de la Unidad de Análisis Financiero que, directa o indirectamente, revelen, divulguen, o hagan uso personal indebido a través de cualquier medio o forma de la información confidencial incumpliendo con su deber, responsabilidad y obligaciones de reserva y estricta confidencialidad, sin perjuicio de la responsabilidad civil y administrativa, serán sancionados según lo dispuesto en el Código Penal. Los funcionarios públicos que, con motivos de los cargos que desempeñan, tengan acceso a la información de que trata este artículo quedaran obligados a guardar la debida confidencialidad, aun cuando cesen en sus funciones. Todo funcionario público está en la obligación de denunciar a las autoridades competentes cualquier contravención y/o desviación a la disposición contenida en el presente artículo. En el presente artículo es basto y amplio buscando que no exista la más mínima posibilidad de interpretar de forma contraria la obligación que tienen los servidores públicos que tengan acceso a información clasificada, en mantener estricta reserva y clasifica quienes en virtud de su accionar pueden tener dicha información, lo cual permite una protección a la persona investigada en virtud de las operaciones comerciales, financieras o legales que lleve a cabo, buscando siempre la protección de las garantías fundamentales, la presunción de inocencia además de la no afectación de la reputación comercial, para que no se vea afectado por el simple hecho de ser investigado.

> 1- Conocer antes, durante y después toda la información de manera clara, veraz y sin costo alguno, respecto de un producto o servicio bancario.
>
> 2- Desistir en cualquier momento de continuar la relación con el banco sin menoscabo del cumplimiento de sus obligaciones, ni de los cargos previamente pactados y aplicables al desistimiento prematuro de la relación.
>
> 3- Confidencialidad en lo que respecta a su relación con el banco frente a terceros, así como su privacidad.
>
> 4- Recibir un servicio diligente y eficiente por parte del banco, particularmente en lo que respecta a consultas y peticiones para conocer el estado de las obligaciones o derechos dimanantes de las mismas."

Quedando claramente establecido, que la información Bancaria de los cuentaavientes ya sean personas naturales o personas jurídicas debe mantener protección frente a terceros.

Esto tiene algunas excepciones, la clásica que es la solicitud por parte de autoridad competente cuando se trate de persecución o investigación de hechos punibles, tendrá la entidad bancaria que brindar toda la información requerida.

## 6.8. CONCLUSIONES

El derecho de acceder a la información pública, se ha generalizado en una conquista globalizada como consecuencia de los mecanismos de participación ciudadana y control de las democracias representativas, bajo la necesidad y conveniencia, de aprobar normas que garanticen y regulen el acceso a la información pública, que se mostraba especialmente crítica en relación con el oscurantismo, los casos de corrupción o el déficit democrático de las instituciones, creando una cultura de gestión racional y honesta de la información, previniendo casos de corrupción.

Hasta hace 10 años atrás el mayor de los problemas del Estado, era posibilitar el acceso a la información ciudadana, hoy día es el mismo con la arista de mantener el control de la información que si amerita mantenerse clasificada o de acceso restringido, pero al encontrarse los sujetos en la posibilidad de conocer absolutamente todo por medios lícitos o en ocasiones ilícitos de acceso a la información en el ciberespacio, los Estados se encuentran más vulnerables y al

mismo tiempo más fiscalizados. Cabe destacar en este sentido, que en el mes de enero de 2017, se ha presentado por parte del Ministerio de la Presidencia de Panamá, autorizado por el Gabinete de ministros, un proyecto de ley que busca establecer un marco regulatorio para la protección de datos contenida en archivos, bases de datos físicas o tecnológicas. El proyecto de ley presentado, busca propiciar que esa big data de los ciudadanos contenida en archivos o bases de datos, en instituciones públicas o empresas privadas, mantengan una serie de controles para que no pueda ser vulnerada y obtenida para fines ajenos a los que fue entregada en su momento.

La Republica de Panamá no ha sido ajena a la necesidad y demanda de información y control de sus administraciones y ha implementado un ambicioso modelo de participación ciudadana, que abandona el oscurantismo legista y administrativo de anteriores regímenes, reticentes a someter su gestión a la sanción del debate público, distanciándose la legislación actual, como una ventana abierta y en constante interacción que debe servir para que los ciudadanos incidan en la vida social, compatibilizando la transparencia y la protección de los intereses públicos y privados. Pero aun así, hemos de observar que la transparencia diseñada a través del acceso a la información, no se puede mostrar suficiente, únicamente mediante la observancia de la administración de los servicios públicos, se muestra necesario la exigencia que los servidores público informen, demuestren y expliquen sus acciones, mediante un lenguaje claro y accesible al público, y a los actores sociales, para que pueda realmente consolidarse como herramienta efectiva para la transparencia y el mejoramiento de la rendición de cuentas gubernamental que demanda el ciudadano.

# VII.-
# CONCLUSIONES

## VII.- CONCLUSIONES GENERALES

**PRIMERA.** La naturaleza multidimensional de la globalización y la pluralidad de contextos sobre los que recae su marco teórico, complica la descripción y concreción del repertorio de factores que se producen como consecuencia de los distintos ámbitos relacionados en este artículo, si bien, resultó oportuno ponerla en relación con el binomio Estado-sociedad, figuras preponderantes en el mundo de hoy, convino ilustrar el cambio sufrido del modelo de Estado-nación el cual se encuentra en fase de transformación profunda para adaptarse a un modelo más horizontal y moldeable. Así, el mapa político actual es difícil de describir y analizar, dado que es reflejo de tendencias e impulsos complejos y contradictorios entrelazados, a falta de regulación internacional que permita solucionar los problemas de aplicación estatal, provocada por los propios límites que le impone el principio de legalidad al que se encuentran sometidos los sistemas penales tradicionales derivados la concepción clásica de soberanía de Estado-nación, se generan crisis de legitimidad institucional ante la falta de acción estatal por hechos de esta relevancia, y de la que se hacen eco los medios de comunicación. De hecho, los cambios sociopolíticos acaecidos durante el transcurso del estado moderno y posmoderno, se han caracterizado por ser rápidos y profundos, además de constantes. Así, pues, y en el marco de nuevas entidades espaciales y territoriales, surgen otras formas de poder y de ejercicio de poder" y organizaciones tales como el Consejo Europa, Naciones Unidas, Tribunales Internacionales, Organismos Intergubernamentales, Organismos no Gubernamentales, etc., se han convertido en actores imprescindibles en la gestión de lo público, formando parte de la nueva forma de gobernar, la gobernanza.

**SEGUNDA.** La *política de Seguridad Nacional* en España se perfila como una política pública de Estado que implica a todo el sector público y a la sociedad en pleno. La *Seguridad Nacional* es, por tanto, un proyecto compartido, *de todos y para todos*, que tiene como marco regulador La *Estrategia de Seguridad Nacional 2013* y la novedosa *Estrategia de Seguridad Nacional 2017*, recientemente publicada, así como lo establecido en la Ley 36/2015, de Seguridad Nacional que establecen, entre otros, una dimensión orgánica a través del *Sistema de Seguridad Nacional*. La

concepción estratégica de *Seguridad Nacional* va más allá de una novación de la arquitectura securitaria del Estado y de establecer nuevos marcos competenciales; en realidad, se concibe como la acción del Estado dirigida a proteger la libertad y el bienestar de la población, a garantizar la defensa de España y sus principios y valores constitucionales, en el marco de una acción conjunta con nuestros aliados. En la actualidad, la importancia de los espacios comunes globales, como el ciberespacio, el espacio marítimo y el espacio aéreo y ultraterrestre han sido tensionados, al tiempo que se ha dado gran valor a las infraestructuras críticas, por su provisión de servicios esenciales a la sociedad. Esta tesitura obliga a potenciar un modelo integral de seguridad y a impulsar una *Cultura de seguridad nacional* en el que sea partícipe la sociedad en su conjunto.

**TERCERA.** En este nuevo proyecto de *Seguridad Integral* se puede desdibujar la línea roja entre seguridad y libertad, así como ser un ejemplo de cómo la seguridad ha calado tanto en el imaginario colectivo a proteger. La seguridad, la democracia y la libertad representan los tres pilares vertebradores de la sociedad para su desarrollo. Si uno de ellos es vulnerado, el Estado se muestra fallido. Frente a las multifacéticas amenazas y desafíos en las que el mundo global se enfrenta, el Estado debería poder ir a la avanzada. La política organiza la sociedad y el Derecho la regula. La gobernanza de la seguridad no es sólo sobrevivir y resistir frente a una tesitura compleja, sino demostrar la capacidad para mantener la resiliencia social e institucional. Los riesgos globales enfrentan a los Estados a un nuevo entorno estratégico cada vez más abierto e incierto, que genera una sensación de inseguridad. Las medidas a adoptar pueden ser de distinta naturaleza, pero casi todas ellas han venido auspiciadas por la necesidad de garantizar la seguridad nacional, constituyendo esta situación el caldo de cultivo para legislar de forma excepcional, produciéndose, así, un verdadero proceso de marginalización y desamparo en perjuicio de las garantías constitucionales. La actividad desplegada por algunas agencias de inteligencia pareciera que se ha desarrollado con base en una cuestionable legislación adoptada ante la urgencia y necesidad de combatir actos terroristas, lo que ha permitido el acceso a las comunicaciones y los documentos privados de las personas con el objetivo de proteger la seguridad interna de las naciones. Los gobiernos también se han beneficiado con la utilización de estas tecnologías,

permitiendo una mejora considerable en la atención de sus fines y objetivos. Es así como, a pesar de las considerables ventajas que representan estas nuevas tecnologías, también han aparecido nuevos problemas y desafíos que causan preocupación en la población. De esta manera, los derechos y libertades fundamentales se han visto afectados de forma positiva y negativa. La vigilancia electrónica indiscriminada y arbitraria, tema de reciente data, inició un gran debate en la academia y diversos sectores de la sociedad.

**CUARTA.** Uno de los derechos más afectados por el uso de las tecnologías de información y comunicación, ha sido el derecho de intimidad de las personas. Este derecho se ha visto vulnerado por diversas conductas de los gobiernos, las empresas y por los propios particulares. La sensación de inseguridad ha venido para quedarse. En esta nueva dimensión, el Estado deberá de ser permeable y sensible a las transformaciones profundas que la sociedad necesita para proteger el gran valor de la Libertad, núcleo de todos los Derechos Humanos. Es, en este sentido, la seguridad un valor prioritario, siendo en muchos casos, el motivo central del pacto que justifica la aparición de la sociedad en el mundo moderno y el instrumento necesario para que otros valores menos accesorios, como por ejemplo la libertad, sean posibles, siendo aquí donde establecemos la conexión entre el valor principal de la seguridad y el valor accesorio de la libertad. No es posible el desarrollo seguro de la comunidad sin la existencia de condiciones seguras y eso sitúa a la seguridad en el núcleo duro de los derechos fundamentales, como exigencia mínima para que una sociedad sea viable y condición sine quan non para que la libertad sea viable.

**QUINTA**. Se ha mencionado a lo largo del trabajo la importancia que tiene la legislación nacional en la protección de la Información Clasificada de las organizaciones internacionales y sus programas, y desafortunadamente hay que decir que siendo la pieza clave del engranaje de protección encontramos deficiencias y carencias en dicha legislación. Está desajustado el esquema legislativo español necesario para dar respuesta a las exigencias actuales en materia de protección de la Información Clasificada de cualquier tipo y grado, nacional o internacional, el cual debería basarse en tres niveles de desarrollo:

1. La ley de Secretos Oficiales que dé cobertura legal al máximo nivel a lo previsto en el artículo 105b de la Constitución incorporando el

nombramiento de la Autoridad Nacional de Seguridad.

2. Un Real Decreto que establezca las funciones de la Autoridad Nacional de Seguridad, incluyendo la posibilidad de delegar estas funciones en una Autoridad Delegada.

3. Cinco disposiciones de rango de instrucción de Secretario de Estado elaboradas por la Autoridad Delegada designada al efecto, en las que se incluyan instrucciones para la protección y el tratamiento de la Información Clasificada en soporte físico, en las personas, en las instalaciones, en los sistemas de información y telecomunicación y en la industria.

En cuanto al primer nivel, es necesario abordar una actualización de la Ley de Secretos Oficiales que se alinee de forma clara con los estándares internacionales de las organizaciones de las que España forma parte. En particular es necesario que vengan reflejados los cuatro niveles de clasificación que contemplan las normativas internacionales, a la vez que se proceda al nombramiento de una Autoridad Nacional para la Protección de la Información Clasificada que solvente la situación actual de que exista dicha autoridad para la protección de la Información Clasificada de "otros" gracias a los sucesivos nombramientos por acuerdo de Consejo de Ministros, mientras que no existe de manera explícita para la protección de la Información Clasificada propia. En esta reforma se debería nombrar de manera explícita al Consejo de Ministros como Autoridad Nacional de Seguridad con capacidad de delegar sus funciones en una Autoridad Delegada, tal y como se ha venido haciendo hasta ahora para el ámbito internacional. Dicha autoridad Nacional de Seguridad debe serlo para cualquier tipo de Información Clasificada, nacional e internacional, de la que España tenga que responsabilizarse de su protección por encontrarse en su territorio de soberanía, en virtud de la legislación nacional y los acuerdos internacionales firmados por España. La autoridad Nacional de Seguridad, es decir el Consejo de Ministros, solo se debería reservar en exclusiva la clasificación en el máximo grado de SECRETO pudiendo delegar las funciones de autoridad de clasificación para el grado de reservado. Es necesario incorporar a la ley cobertura para desarrollos legislativos en los siguientes niveles en cuanto a la protección de la Información Clasificada en los sistemas de información y

comunicación y en la industria, puesto que estos dos ámbitos están ausentes en la actual ley. En cuanto al segundo nivel es necesario abordar un nuevo desarrollo de la Ley que incorpore lo que es práctica habitual a día de hoy a través de las normas de Autoridad Nacional de Seguridad y exija su cumplimiento para el conjunto de las administraciones españolas con capacidad de acceder y generar Información Clasificada. Es decir, se necesita derogar el decreto actual (no se trata de un Real Decreto pues, como ya se ha dicho, es anterior a la actual monarquía parlamentaria consagrada en la Constitución de 1978) y elaborar un Real Decreto en el que se definan las funciones de la Autoridad Nacional de Seguridad, y cuáles de ellas se delegan en la Autoridad Delegada. Se deberían establecer las autoridades de clasificación para los dos niveles inferiores de clasificación y su capacidad para delegar estas funciones. El tercer nivel de desarrollo se encuentra a día de hoy vigente y con el rango que se propone, es decir como instrucción del Secretario de Estado Director del CNI, en calidad de Autoridad Nacional de Seguridad Delegada, si bien dado que carece de la cobertura legal necesaria, estrictamente hablando, solo son de aplicación para la protección de la Información Clasificada internacional de la OTAN, la UE y la ESA, y de terceros estados con los que se tiene firmado un acuerdo bilateral de protección de Información Clasificada, pero no para la protección de la Información Clasificada nacional, ni para la de otras organizaciones internacionales que carecen de nombramiento expreso.

**SEXTA** Es necesaria continuar la divulgación y concienciación en el mundo empresarial de las oportunidades que ha supuesto la apertura del mercado europeo en lo relativo a programas y contratos clasificados, de forma que se genere un tejido industrial preparado para poder competir internacionalmente en las oportunidades de negocio que se presentan fuera de España. Resulta de especial importancia los programas de la Unión Europea H2020 (Horizon 2020) dotados de un presupuesto astronómico, y en los que una parte de los proyectos vinculados a los mismos son clasificados. La capacidad de proteger adecuadamente Información Clasificada de cualquier tipo, nacional o internacional, se ha convertido en un activo para las empresas, especialmente las de los sectores de defensa y aeroespacial, que si bien se puede acreditar únicamente con ocasión de participar en un contrato en el que se maneje y/o genere información clasificada, disponer de esta capacidad sitúa a las empresas

en una categoría superior.

**SEPTIMA.** En Panamá, derecho de acceder a la información pública, se ha generalizado en una conquista globalizada como consecuencia de los mecanismos de participación ciudadana y control de las democracias representativas, bajo la necesidad y conveniencia, de aprobar normas que garanticen y regulen el acceso a la información pública, que se mostraba especialmente crítica en relación con el oscurantismo, los casos de corrupción o el déficit democrático de las instituciones, creando una cultura de gestión racional y honesta de la información, previniendo casos de corrupción. Hasta hace 10 años atrás el mayor de los problemas del Estado, era posibilitar el acceso a la información ciudadana, hoy día es el mismo con la arista de mantener el control de la información que si amerita mantenerse clasificada o de acceso restringido, pero al encontrarse los sujetos en la posibilidad de conocer absolutamente todo por medios lícitos o en ocasiones ilícitos de acceso a la información en el ciberespacio, los Estados se encuentran más vulnerables y al mismo tiempo más fiscalizados. Cabe destacar en este sentido, que en el mes de enero de 2017, se ha presentado por parte del Ministerio de la Presidencia de Panamá, autorizado por el Gabinete de ministros, un proyecto de ley que busca establecer un marco regulatorio para la protección de datos contenida en archivos, bases de datos físicas o tecnológicas. El proyecto de ley presentado, busca propiciar que esa big data de los ciudadanos contenida en archivos o bases de datos, en instituciones públicas o empresas privadas, mantengan una serie de controles para que no pueda ser vulnerada y obtenida para fines ajenos a los que fue entregada en su momento.

**OCTAVA.** La República de Panamá no ha sido ajena a la necesidad y demanda de información y control de sus administraciones y ha implementado un ambicioso modelo de participación ciudadana, que abandona el oscurantismo legista y administrativo de anteriores regímenes, reticentes a someter su gestión a la sanción del debate público, distanciándose la legislación actual, como una ventana abierta y en constante interacción que debe servir para que los ciudadanos incidan en la vida social, compatibilizando la transparencia y la protección de los intereses públicos y privados. Pero aun así, hemos de observar que la transparencia diseñada a través del acceso a la información, no

se puede mostrar suficiente, únicamente mediante la observancia de la administración de los servicios públicos, se muestra necesario la exigencia que los servidores público informen, demuestren y expliquen sus acciones, mediante un lenguaje claro y accesible al público, y a los actores sociales, para que pueda realmente consolidarse como herramienta efectiva para la transparencia y el mejoramiento de la rendición de cuentas gubernamental que demanda el ciudadano.

# VIII.-
# REFERENCIAS

## VIII.- REFERENCIAS


AA, VV. Reglamento General de Protección de datos, Madrid, 2016.

ACKERMAN, J, M., Social Accountability in the Public Sector: a conceptual discusión, Cuaderno de Trabajo No. 82, de la Colección Partcipation and Civic Engagement, Banco Mundial.2007.

ACKERMAN, J,M y SANDOVAL, I,E., Leyes de acceso a la información en el mundo. México, D.F.: Instituto de Investigaciones Jurídicas de la Universidad Nacional Autónoma de México, 2007.

ALVAREZ ALVAREZ, L,A Y PERDOMO CORDERO,C. (2015) "Inteligencia, Cibereguridad y Ciberdefensa; nuevas implicaciones conceptuales en las Estrategias de Seguridad Nacional." ULPGC 2012

ARTEAGA, F. (2011). "Propuesta para la implantación de una Estrategia de Seguridad en España". DT 19/2011, Real Instituto Elcano, Madrid.

ARTEAGA, F. & FOJÓN, E. (2007). *El Planeamiento de la Política de Defensa y Seguridad en España*. Instituto Universitario General Gutiérrez Mellado. Madrid: UNEDAKERMAN, B. (2007). *Antes que nos ataquen de nuevo.* La defensa de las libertades en tiempos de terrorismo, Barcelona, Península,

ALVAREZ CONDE, E y GONZALEZ, H. (2006*), Legislación terrorista comparada después de los atentados del 11 de septiembre y su incidencia en el ejercicio de los derechos fundamentales,* Real Instituto Elcano, Área Terrorismo Internacional, *ARI* n. 7

APARICIO SALOM, J., Estudio sobre la Protección de Datos, 4.ª ed., Pamplona, 2013.

APARICIO VAQUERO, J, P. Y BATUECAS CALETRIO, A., En torno a la privacidad y la protección de datos en la sociedad de la información, Granada, 2015.

ARBELÁEZ HERRERA, Á. M. (2009). La Noción de Seguridad en Thomas Hobbes. Revista de la Facultad de Derecho y Ciencias Políticas, (110).

BALLESTEROS MARTÍN, M Á (2016) *En busca de una Estrategia de Seguridad Nacional*, Madrid. Ministerio de Defensa

BALLESTEROS MARTÍN, M Á (2017). "Las novedades de la Estrategia de Seguridad Nacional 2017", *Revista del Instituto Español de Estudios Estratégicos*, núm. 74. [En línea 28.02.2018] http://www.ieee.es/Galerias/fichero/docs_analisis/2017/DIEEEA74-2017_Novedades_ESN2017_MABM.pdf

BAUMAN, ZYGMUNT (2017): *Retrotopía*, Barcelona. Paidós.

BLANCO NAVARRO, J, Mª Y DÍAZ MATEY, G. (20159. Presente y futuro de los estudios de inteligencia en España. Documento marco IEEE.

BOBIO, N., El futuro de la democracia, Plaza y Janes.1985. p.107

BROOKS, D.J. (2010).What is security: Definition through knowledge categorization. *Security Journal*, *23*(3), 225-239.

CARRILLO RUIZ, J,A et al.(2013) "Big data en los entornos de defensa y seguridad" documento resultado del grupo de trabajo sobre big data, de la comisión de investigación de nuevas tecnologías del centro superior de estudios de la defensa nacional. (CESEDEN) Documento de Investigación del Instituto Español de Estudios Estratégicos (IEEE) 03/2013

CURBET, J. (2007). Temeraris atemorits. L'obsessió contemporània per la seguretat, Girona, CCG Edicions.

DABAT, A. (2000). Globalización: Capitalismo informático-Global y nueva configuración espacial del mundo. *México: Universidad Nacional Autónoma de México*.

DÍAZ, A. (2006) «*La adaptación de los servicios de inteligencia al terrorismo internacional* « *ARI Nº 52-2006.*

DÍEZ-PICAZO, L.M., La criminalidad de los gobernantes, Ed. Crítica, Barcelona, 2000.

"Estudio Especial sobre el Derecho de acceso a la Información" en Relatoría especial para la libertad de expresión comisión interamericana de derechos humanos organización de los estados americanos. Washington, D. C. 2006.

FROWEIN, J. A., EN Pettiti, Louis-Edmond, Decaux, Emmanuel et Inbert, Pierre-Heri. *La Convention Européenne des Droits de L'Homme: Comentaire article par article,* 2da Edition, parís, Ed. Económica 1999.

GARAY MALDONADO. D., Seguridad Pública y Gobernabilidad. En estado Constitucional, Derechos Humanos, Justicia y vida universitaria. Instituto de investigaciones jurídicas. Estudios en homenaj a Jorge Carpizo. UNAM. 2015.

GARCÍA MAHAMUT, R. Y RALLO LOMBARTE, A., Hacia un nuevo derecho de protección de datos, Valencia, 2015.

GARRIDO ROBRES, J,A. (2016). *¿Sería conveniente una especialidad fundamental de inteligencia para las Fuerzas Armadas Españolas? Estudio de esta especialidad en otras Fuerzas Armadas*. Madrid, ESFAS, 2006.

GARRIGA DOMÍNGUEZ, A., Nuevos retos para la protección de datos personales, Madrid, 2016.

GALLOWAY, D. Classifying Secrets in the EU. (General Secretariat of the Council of the European Union). Journal of Common Market Studies (JCMS 2014 pp. 1–16)

GIL GONZÁLEZ, E., Big data, privacidad y protección de datos, Madrid, 2016 Guide for handling classified information in the context of framework programme cooperative research projects (European Comission).

GICHOT REINA, E., "Transparencia y acceso a la información pública en España: análisis y propuestas legislativas". Documento de trabajo 170/2011. Fundación Alternativas. *En Laboratorio de alternativas* 2011.

GIRÓN TOMÁS, M. (2018). "La Ley de Seguridad Nacional en España: La seguridad de los países en clave internacional. Análisis de la Ley de Seguridad Nacional en España como Ley de Seguridad Integral". *Revista del Instituto Español de Estudios Estratégicos*, núm.10. [En línea, 2.03.2018] http://revista.ieee.es/index.php/ieee/article/view/313/571

GONZALEZ MONTENEGRO; Rigoberto. EL HABEAS DATA; IEPI Instituto de Estudios Políticos Internacionales de Panamá; Editorial Chen, Panamá 1999; pág 27.

GUDIN, F. (2006). *La lucha contra el terrorismo en la sociedad de la información*, Madrid: Edisofer.

HERNÁNDEZ LÓPEZ, J. M., El derecho a la protección de datos personales en la doctrina del Tribunal Constitucional, Pamplona, 2013.

HOBBES, T. Leviatán ó la Materia, Forma y Poder de una Republica Eclesiástica y Civil, trad. esp. Manuel Sánchez Sarto; México, 1940.

HOLSEN, S., Journalists' Use of the UK Freedom of Information Act, Open Government: a journal on freedom of information, 2007.

HUNTINGTON, S, P., The third wave. Democratization in the late twentieth century, Norman, University of Oklahoma Press, 1991. (La tercera ola)

I CATALÁ, J. P. (2010). Políticas de buena administración para la Administración General del Estado en España. Un enfoque de Gobernanza Democrática. In Gobernanza democrática y fiscalidad (pp. 25-55). Tecnos.

INTELLIGENCE INFORMATION: Need-to-Know vs. Need-to-Share Richard A. Best Jr. Specialist in National Defense June 6, 2011

IRAVEDRA, J. C. (2011). «Inteligencia de fuentes abiertas en la Unión Europea (proyecto Virtuoso)», Jornadas de Estudios de Seguridad, 17, 18 y 19 mayo de 2011

JINESTA LOBO, E., Transparencia administrativa y derecho de acceso a la información administrativa. Aletheia, Cuadernos Críticos del Derecho. 2-2015

KAPLAN, M. (1994). La soberanía estatal-nacional: retos e interrogantes. Problemas actuales del derecho constitucional. Estudios en homenaje a Jorge Carpizo, 225-234.

KIRCHNER, E. J. (2006). The Challenge of European Union Security Governance*. *JCMS: Journal of common market studies*, *44*(5), 947-968.

KRAHMANN, E. (2003). Conceptualizing security governance. Cooperation and conflict, 38(1), 5-26.

LASCOUMES, P., Corrupciones, El poder frente a la ética, Ediciones, Bellaterra, Barcelona, 2000.

LIND, W,S. (2004). Internet World Stats: Usage and Population Statistics. Antiwar..

LÓPEZ ÁLVAREZ, L., Protección de datos personales, Madrid, 2017.

MARTÍNEZ MARTÍNEZ, R., (2005): Una aproximación crítica a la autodeterminación informativa, Madrid, Civitas.

MARTÍN DE SANTOS, I. Y VEGA, A. M. (2010). «Las fuentes abiertas de información: un sistema de competencia perfecta», en Inteligencia y Seguridad: revista de análisis y prospectiva, número 8, pp. 91-112, junio-noviembre.

MARTÍNEZ, GILBERTO L. (2011). "Minería de datos: Cómo hallar una aguja en un pajar", Ingenierías, 53. págs. 55-63.

MATTELART, A y VITALIS.A., (2015). De Orwell al cibercontrol. Gedisa.

MALEM SEÑA, J., La corrupción. Aspectos éticos, económicos, políticos y jurídicos, Gedisa Editorial, Barcelona, 2002.

MORERA DE LA VALL. Secretos de Estado y Estado de Derecho: régimen jurídico de los secretos oficiales en España. Helen Wilkinson (Atelier Libros Jurídicos).

NAVARRO, D. (2004). El ciclo de inteligencia y sus límites. *Cuadernos Constitucionales de la Catedra Fadrique Furió Ceriol, Vol. 48*.

OPEN SOCIETY JUSTICE INITIATIVE; TRANSPARENCY & SILENCE. A Survey of Access to Information Laws and Practices in 14 Countries. Justice in Action Series. New York, 2006.

PASCUAL ESTEVE, J M. (2010) «El buen gobierno 2.0: La gobernanza democrática territorial». Ed. Tirant Lo Blanch, Valencia,

PALIWODA, S. J., &SLATER, S. (2009). Globalisation through the kaleidoscope. *International Marketing Review*, *26*(4/5), 373-383.

PESCHARD MARISCAL, J. "El derecho de acceso a la información y la universidad pública Universidades" vol. LX, núm. 45, abril-junio, 2010,

PERALES, J. A. S. (2008). ¿Un mundo unipolar, multipolar, o apolar? la naturaleza y la distribución del poder en la sociedad internacional contemporánea. In *Cursos de Derecho internacional y Relaciones internacionales de Vitoria-Gazteiz, 2007: Vitoria-Gasteizkonazioartekozuzenbide eta nazioartekoharremanenikastaroak, 2007*(pp. 297-384).

PIÑAR MAÑAS, J. L., Transparencia, acceso a la información y protección de datos, Madrid, 2015.

RAWLS, J (1996): Sobre las libertades, Barcelona, Paidós.

Relatoría especial para la libertad de expresión comisión interamericana de derechos humanos organización de los estados americanos. "Estudio Especial sobre el Derecho de acceso a la Información" WASHINGTON, D. C. 2006. p.12.

REVENGA SANCHEZ, M. (2006*), Garantizando la libertad y la seguridad de los ciudadanos en Europa: Nobles sueños y pesadillas en la lucha contra el terrorismo*, Parlamento y Constitución, n. 20.

REVENGA SÁNCHEZ, M (2007) (Director), Terrorismo y Derecho bajo la estela del 11 de septiembre, Valencia, Tirant lo BlanchRECIO GAYO, M., Protección de datos personales e innovación, Madrid, 2016.

ROSE-ACKERMAN, S., La Corrupción y los gobiernos, Siglo XXI de España Editores, S.A., Madrid, 2001.

RUIZ MIGUEL, C (2003): «El derecho a la protección de los datos personales en la Carta de derechos fundamentales de la Unión Europea», Revista de Derecho Comunitario, n.º 14.

RUIZ, J. C., &VANDERSCHUEREN, F. (2007). Base conceptual de la seguridad. Consolidación de los gobiernos locales en seguridad ciudadana. Red, 14, 10-34.

SANDOVAL, I,E., "Transparencia y Control Ciudadano: Comparativo de Grandes Ciudades". Instituto de Investigaciones Sociales de la Universidad Nacional Autónoma de México. 2007.

SERRA CRISTÓBAL, R., (2015) "La opinión pública ante la vigilancia masiva de datos. El difícil equilibrio entre acceso a la información y seguridad nacional". En *Revista de Derecho Político* N.º 92, enero-abril

SILVA SANCHEZ, J M., (2001) La expansión del Derecho penal. Aspectos de la política-criminal de las sociedades postindustriales, 2ª ed., Madrid 2001

SUSTENTIA & OPEN SOCIETY JUSTICE INITIATIVE. *Transparencia y silencio. Estudio sobre el acceso a la información en España*. Madrid, octubre de 2005.

UMPHRESS, D,A. (2006). "Naufragando en el contenedor digital: el impacto que tiene la Internet en la recopilación de inteligencia de fuentes abiertas (OSINT)", Air and Space Power Journal en español, 4., pp. 6-16.

VALERO TORRIJOS, J., La protección de datos personales en Internet ante la innovación tecnológica, Pamplona, 2014.

VELÁSQUEZ, E. (2007b) "Gobernabilidad de la seguridad ciudadana en Bogotá 1992-2007: Una primera lectura". En: Velásquez, E. & Godard, H.(eds). Gobernabilidad territorial en las ciudades andinas. Organización y recomposiciones territoriales y socio-políticas. Bogotá: IFEA-U. Externado.

VERVALE J (2006), *La legislación antiterrorista en Estados Unidos, ¿Inter arma silent leges?*, Buenos Aires: Ediciones del Puerto.

VERGOTTINI, D (2004). *Guerra e costituzione. Nuovi conflictti e sfide alla democrazia*, Bologna:Il Mulino.

VILLORIA, M., La corrupción política, Síntesis, Madrid, 2006.

VIRTA, S. (2002). Local security management: Policing through networks. *Policing: An International Journal of Police Strategies& Management*, *25*(1), 190-200.

VLEUGELS, R. "Overview of all FOI laws". Fringe Special 9 de Octubre de 2011.

WALTER, M. (2006). *Terrorismo y guerra justa*, Barcelona:Centre de Cultura Contemporanea de Barcelona.

WEBBER, M., CROFT, S., HOWORTH, J., TERRIFF, T., &KRAHMANN, E. (2004). The governance of European security. Review of international studies, 30(01), 3-26.

WHITAKER, R. (1999), *El fin de la privacidad: cómo la vigilancia total se está convirtiendo en realidad*, Barcelona: Paidós

WITT, E., *La suprema Corte de Justicia y los Derechos Individuale*s, Traducción de Ana Isabel Stellino, 2da Edición, Ed. Gernika, México, 1995.

## REFERENCIAS NORMATIVAS

Constitución Española de 1978.

Ley 9/1968, de 5 de abril de Secretos Oficiales publicada en el BOE número 84 de 6 de Abril de 1968, modificada por la Ley 48/78 de 7 de octubre de 1978 publicada en el BOE número 243 de 1978.

Real Decreto 242/1969 de 20 de febrero, por el que se desarrollan las disposiciones de la Ley 9/1968 sobre secretos oficiales.

Normas de la Autoridad Nacional de Seguridad (www.cni.es/es/ONS).

Orden Ministerial 76/2006 de 19 de mayo, por la que se aprueba la política de Seguridad de la información del Ministerio de Defensa.

Orden IET/2377/2015, de 5 de noviembre, por la que se regula la protección de la información clasificada en el Ministerio de Industria, Energía y Turismo.

COMMISSION DECISION (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information.

COUNCIL DECISION of 23 September 2013 on the security rules for protecting EU classified information.

C-M(2002)49 Security within the north Atlantic Treaty Organization (NATO).

C-M(2007) 0118 North Atlantic Council. The NATO Information Management Policy.

AC/35-D/2000-REV7 Directive on Personal Security.

AC/35-D/2001-REV2 Directive on Physical Security.

AC/35-D/2002-REV4 Directive on Security of Informtion.

AC/35-D/2003-REV5 Directive on Classified Project and Industrial Security.

AC/35-D/2004-REV3 Primary Directive on CIS Security.

Acuerdo De Consejo De Ministros de fecha 25 De Junio De 1982. Creación de la Autoridad Nacional de Seguridad para la protección de la Información Clasificada de la OTAN.

Orden comunicada de la Presidencia del Gobierno de 11 de agosto de 1982. Designación de la Autoridad Delegada para la Seguridad de la Información Clasificada de la OTAN.

Acuerdo del Consejo de Ministros de fecha 19 de abril de 2002. Creación de la Autoridad Nacional de Seguridad para la seguridad de la Información Clasificada de la Unión Europea y la Unión Europea Occidental.

Orden Comunicada de 24 de mayo de 2002 por la que se designa la autoridad delegada para la seguridad de la Información Clasificada para la Unión Europea y Unión Europea Occidental.

BOE Nº 53 de 3 de marzo de 2005. Instrumento de Ratificación del Acuerdo entre los Estados parte en el Convenio para el establecimiento de una Agencia Espacial Europea y la Agencia Espacial Europea para la protección y el intercambio de información clasificada, hecho en París el 19 de agosto de 2002.

Acuerdo de Consejo de Ministros de fecha 18 de noviembre de 2005. Creación de la Autoridad Nacional de Seguridad para la seguridad de la Información Clasificada de la Agencia Espacial Europea.

BOE Nº 257 de 27 de octubre de 2006. ORDEN PRE/3289/2006, de 23 de octubre, por la que se designa la Autoridad Delegada para la seguridad de la información clasificada de la Agencia Espacial Europea y se crea el Registro Central de información clasificada de la Agencia Espacial Europea.

Orden PRE/2130/2009, de 31 de julio, por la que se designa la Autoridad Delegada para la Seguridad de la Información Clasificada originada por las partes del Tratado del Atlántico Norte, por la Unión Europea y por la Unión Europea Occidental.

Acuerdo de Consejo de Ministros de fecha 11 de mayo de 2012, por el que se modifican los acuerdos de creación de la Autoridad Nacional de Seguridad de la Información Clasificada originada por las partes del tratado del Atlántico Norte, la Autoridad Nacional de Seguridad para la seguridad de la Información Clasificada para la Unión Europea y la Unión Europea Occidental, y la autoridad Nacional de Seguridad de la Información Clasificada de la Agencia Espacial Europea.

Acuerdos del Consejo de Ministros de 28 de noviembre de 1986 por el que se clasifican determinados documentos, asuntos y materias con arreglo a la Ley de Secretos Oficiales (2 acuerdos).

Acuerdo del Consejo de Ministros de 29 de marzo de 1994 por el que se amplía el acuerdo del 28 de noviembre de 1986.

Directive 2009/81/EC of the European Parliament and of the Council of 13 July 2009 on the coordination of procedures for the award of certain works contracts, supply contracts and service contracts by contracting authorities or entities in the fields of defence and security.

Ley 24/2011, de 1 de agosto, de contratos del sector público en los ámbitos de la defensa y de la seguridad, publicada en el BOE número 184 el 2 de agosto de 2011.

Real Decreto Legislativo 3/2011, de 14 de noviembre, por el que se aprueba el texto refundido de la Ley de Contratos del Sector Público, publicado en el BOE número 276 el 16 de noviembre de 2011.

Ley 11/2002 de 6 de mayo reguladora del Centro Nacional de Inteligencia.

Naciones Unidas. *Informe del Programa de Desarrollo Humano* (PNUD) (1994). Publicado para el Programa de las Naciones Unidas para el desarrollo. Fondo de Cultura Económica, S.A. de C.V. [en línea, 11.03.2018] https://derechoalaconsulta.files.wordpress.com/2012/02/pnud-informe-1994-versic3b3n-integral.pdf

Cortes Generales. *Constitución Española*. BOE núm. 311, Publicada el 29 de diciembre de 1978. Referencia: BOE-A-1978-31229. Revisión vigente desde el 27 de septiembre de 2011. https://www.boe.es/buscar/doc.php?id=BOE-A-1978-31229

Presidencia del Gobierno (2011), *Estrategia Española de Seguridad. Una responsabilidad de todos* (2011), Madrid, Secretaria General Técnica. [En línea, 15.02.2018] http://www.realinstitutoelcano.org/wps/wcm/connect/c06cac0047612e998806cb6dc6329423/EstrategiaEspanolaDeSeguridad.pdf?MOD=AJPERES&CACHEID=c06cac0047612e998806cb6dc6329423

Presidencia del Gobierno (2013), *Estrategia de Seguridad Nacional. Un proyecto compartido* (2013), Madrid, Secretaría General Técnica. BOE núm. 131. Publicada. 1.06.2013. Referencia: BOE-A-2013.5771. [En línea, 15.02.2018] https://www.boe.es/diario_boe/txt.php?id=BOE-A-2013-5771

Presidencia del Gobierno. *Informe Anual de Seguridad Nacional 2016*, aprobado por el Consejo de Seguridad Nacional en su reunión de 20 de enero de 2016 [En línea, 2.03.2018] http://www.dsn.gob.es/es/documento/informe-anual-seguridad-nacional-2016

Presidencia del Gobierno (2017), *Estrategia de Seguridad Nacional. Un proyecto compartido de todos y para todos* (2017), Madrid, Secretaria General Técnica. BOE núm. 309. Publicada el 21 de diciembre de 2017. Referencia: BOE-A-2017-15181. [En línea, 20.02.2018] https://www.boe.es/boe/dias/2017/.../BOE-A-2017-15181.pdf

Tribunal Constitucional. *Sentencia del Pleno del Tribunal Constitucional 184/2016 dictada en el Recurso 7330/2015 contra los artículos 4.3. 15.c) y 24 de la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional.* BOE núm. 299, Publicado el 12 de diciembre de 2016. Referencia: BOE-A-2016-11817. [en línea, 28.02,2018] http://hj.tribunalconstitucional.es/es/Resolucion/Show/25150

Consejo de Estado. *Dictamen Anteproyecto de Ley de Seguridad Nacional*. Núm. de expediente referencia: 405/2015. Presidencia. Documento CE-D-2015-405. Fecha de aprobación: 13.05.2015. BOE núm. 233, Publicado el 29 de septiembre de 2015. Referencia: BOE-A-2015-10389. [ En línea, 27.02.2018] http://www.boe.es/buscar/doc.php?id=CE-D-2015-405

Jefatura del Estado. Ley Orgánica 5/2005, de 17 de noviembre, de la Defensa Nacional. BOE núm. 276, Publicada el 18 de noviembre de 2005. Referencia: BOE-A-2005-18933. https://www.boe.es/buscar/pdf/2005/BOE-A-2005-18933-consolidado.pdf

Jefatura del Estado. Ley 50/1997, de 27 de noviembre, del Gobierno. BOE núm. 285, Publicada el 28 de noviembre de 1997. Referencia: BOE-A-1997-25336. https://boe.es/buscar/pdf/1997/BOE-A-1997-25336-consolidado.pdf

Jefatura del Estado. Ley 11/2002, de 8 de mayo, reguladora del Centro Nacional de Inteligencia. BOE núm. 109. Publicada el 7 de mayo de 2002. Referencia: BOE-A-2002-8628. https://www.boe.es/buscar/pdf/2002/BOE-A-2002-8628-consolidado.pdf

Jefatura del Estado. Ley 36/2015, de 28 de septiembre, de Seguridad Nacional. BOE núm. 233. Publicada el 29 de septiembre de 2015. Referencia: BOE-A-2015-10389. https://www.boe.es/buscar/act.php?id=BOE-A-2015-10389

Presidencia del Gobierno. Real Decreto 1886/2011, de 30 de diciembre, por el que se establecen las Comisiones Delegadas del Gobierno. BOE núm. 315. Publicado el 31 de diciembre de 2011. Referencia: BOE-A-2011-20640. https://www.boe.es/buscar/pdf/2011/BOE-A-2011-20640-consolidado.pdf

Presidencia del Gobierno. Real Decreto 1119/2012, de 20 de julio, de modificación del Real Decreto 83/2012, de 13 de enero, por el que se reestructura la Presidencia del Gobierno. BOE núm. 175. Publicado el 23 de julio de 2012. Referencia: BOE-A-2012-9816. https://www.boe.es/boe/dias/2012/07/23/pdfs/BOE-A-2012-9816.pdf

Presidencia del Gobierno. Real Decreto 571/2013, de 26 de julio, de modificación del Real Decreto 83/2012, de 13 de enero, por el que se reestructura la Presidencia del Gobierno. BOE núm. 184, Publicada el 2 de agosto de 2013. Referencia: BOE-A-2013-8506 [en línea, 13.03.2017] https://www.boe.es/boe/dias/2013/08/02/pdfs/BOE-A-2013-8506.pdf.

Presidencia del Gobierno. Real Decreto 571/2013, de 26 de julio, de modificación del Real Decreto 83/2012, de 13 de enero, por el que se reestructura la Presidencia del Gobierno. BOE núm. 184, Publicada el 2 de agosto de 2013.

Referencia: BOE-A-2013-8506 [en línea, 13.03.2017] https://www.boe.es/boe/dias/2013/08/02/pdfs/BOE-A-2013-8506.pdf.

Presidencia del Gobierno. Real Decreto 770/2017, de 28 de julio, por el que se desarrolla la estructura orgánica básica del Ministerio de Interior. BOE núm. 180. Publicado el 29 de julio de 2017. Referencia: BOE-A-2017-9013. https://www.boe.es/buscar/doc.php?id=BOE-A-2017-9013

Presidencia del Gobierno. Real Decreto 1008/2017, de 1 de diciembre, por el que se aprueba la Estrategia de Seguridad Nacional 2017. BOE núm. 309. Publicado el 21 de diciembre de 2017. Referencia: BOE-A-2017-15181. https://www.boe.es/diario_boe/txt.php?id=BOE-A-2017-15181

Presidencia del Gobierno. Real Decreto 766/2017, de 28 de julio, por el que se reestructura la Presidencia del Gobierno . BOE núm. 180. Publicado el 29 de julio de 2017. Referencia: BOE-A-2017-9007. https://www.boe.es/diario_boe/txt.php?id=BOE-A-2017-9007

Ministerio de la Presidencia y para las Administraciones Territoriales. Orden PRA/115/2017, de 9 de febrero, por la que se publica el Acuerdo del Consejo de Seguridad Nacional, por el que se aprueba el procedimiento para la elaboración de la Estrategia de Seguridad Nacional. BOE núm. 38. Publicado el 14 de febrero de 2017. Referencia: BOE-A-2017-1459. https://www.boe.es/diario_boe/txt.php?id=BOE-A-2017-1459

Ministerio de la Presidencia y para las Administraciones Territoriales. Orden PRA/116/2017, de 9 de febrero, por la que se publica el Acuerdo del Consejo de Seguridad Nacional de Implementación de los mecanismos para garantizar el funcionamiento integrado del Sistema de Seguridad Nacional. Ministerio de la Presidencia y para las Administraciones Territoriales. BOE núm. 38. Publicado el 14 de febrero de 2017. Referencia: BOE-A-2017-1460. https://www.boe.es/diario_boe/txt.php?id=BOE-A-2017-1460