LA DEFINICIÓN DE LAS MATERIAS CLASIFICADAS: UNA VISIÓN DESDE LOS ESTÁNDARES INTERNACIONALES Y EL DERECHO COMPARADO[1]

SUSANA SANCHEZ FERRO
Profesora Titular de Derecho Constitucional
Universidad Autónoma de Madrid

TRC, nº 55, 2025, pp. 207-260
ISSN 1139-5583

Sumario

I. INTRODUCCIÓN

La reforma de la Ley de Secretos Oficiales de 1968, de 5 de abril, sobre secretos oficiales (Ley 9/1968) es una de las propuestas del Plan de Acción por la Democracia presentado por el Gobierno socialista en la XV legislatura. El Gobierno señala en dicha propuesta de reforma que «[e]s necesario un marco avanzado y garantista que sustituya [a la] ley preconstitucional, vigente desde 1968, para actualizarla y adaptarla a los mejores estándares de las legislaciones de los países democráticos de nuestro entorno» (Gobierno de España, 2024:19). En este artículo hemos querido, precisamente, volver nuestra mirada a dichos estándares, pero,

1 Esta publicación es parte del proyecto de I+D+i «Una Aproximacion Holistica al Regimen Juridico de la Informacion Clasificada en la Era Digital» (PID2021-123563NB-I00), financiado por MICIU/AEI/10.13039/501100011033/ y «FEDER/UE».

también, a los estándares internacionales que se derivan de algunos instrumentos normativos internacionales y al *soft law* existente en la materia, para luego analizar la definición de materias clasificadas contenida en el Anteproyecto de Ley de Información Clasificada que el Gobierno elaboró en la XIV legislatura.

A nadie se le oculta que hace ya mucho tiempo que debería haberse reformado la Ley de Secretos Oficiales, una ley aprobada hace ya más de 50 años en un contexto muy diferente al actual. Esta Ley, modificada en el año 1978 por Ley 48/1978, de 7 de octubre y desarrollada por el Real Decreto 242/1969, de 20 de febrero, indica en su preámbulo que su punto de partida es el principio de publicidad «porque las cosas públicas que a todos interesan pueden y deben ser conocidas de todos», si bien nos advierte de la «innegable [...] necesidad de imponer limitaciones» al principio de publicidad, «cuando precisamente de esa publicidad puede derivarse perjuicio para la causa pública, la seguridad del mismo Estado o los intereses de la colectividad nacional». Al avanzar en la lectura del preámbulo nos topamos con el fin último de la ley: la ley pretende proteger, incrementando las garantías contra su revelación, la información relativa a la seguridad y defensa del Estado. En efecto, subraya el preámbulo de la ley que «al contrario de lo que [ocurría] en los Estados caracterizados por la mayor libertad de información», España no contaba con una regulación de medidas protectoras de los secretos oficiales más allá de lo dispuesto en la legislación penal, que protegía con sanciones penales, tanto en el Código Penal Común como en el de Justicia Militar, la revelación de secretos oficiales con penas que alcanzaban «la máxima severidad». Para el legislador la sanción penal, especialmente represiva, solo servía para proteger de una manera indirecta, por medio de la intimidación, el descubrimiento o revelación de secretos oficiales; las medidas de protección eficaces serían aquellas que la propia Administración estableciera para garantizar que los documentos o materiales en que físicamente se reflejasen los secretos no pudieran ser conocidos más que por aquellas personas que, por razón de su cometido, estuvieran autorizadas para ello. Por ello, la ley estableció «un conjunto de medidas positivas» para evitar que trascendiera el conocimiento de lo que debía permanecer secreto, «señalando normas severas que [impidieran] la generalización de calificaciones que tienen carácter excepcional». La finalidad de la ley era, pues, proteger la información clasificada *ad intra* de la administración, finalidad totalmente legítima. Otra cosa es cómo se configure dicha protección y, sobre todo, con qué alcance. Proteger la seguridad del Estado es legítimo, pero la misma debe protegerse en su justa medida, ni más, ni tampoco menos, precisamente por la relevancia que tiene el principio de publicidad en un Estado democrático de Derecho[2].

2 El verdadero problema es el balance que la LSO realiza de dicho principio de publicidad en relación con las necesidades de protección de la seguridad del Estado. La ley no establece, por ejemplo, ningún sistema de desclasificación automática de la información clasificada.

II. LA CONSTITUCIONALIZACIÓN DEL PRINCIPIO DE PUBLICIDAD Y EL SECRETO DE ESTADO COMO EXCEPCIÓN

El principio de publicidad fue institucionalizado mínimamente por primera vez en la época de la ilustración (De Lucas: 1990, 133). En época liberal dicho principio se conectaba con la idea de racionalización de la política y con la necesidad de alcanzar la verdad mediante el debate en el Parlamento, dando lugar así a la formación de una opinión pública libre (Habermas, 1999: 133-135)[3]. El principio de publicidad se aplicaba entonces en exclusiva a la actividad parlamentaria y judicial (Vega García, 1995: 5404 y 1998: 806; Fernández Ramos, 1997: 22); se creía que el sometimiento a la ley sería suficiente garantía del control del poder ejecutivo, siendo la ulterior garantía jurisdiccional la que aseguraría el control de dicho poder para mantenerlo dentro de los márgenes de lo legal, sin que fuera necesario proyectar sobre el ejecutivo dicho principio de publicidad. En el Estado Constitucional los asuntos de gobierno dejan de concebirse como asuntos privados del monarca o de los aristócratas gobernantes y comienza la lucha por el sufragio, por la libertad de prensa y por ampliar la publicidad en el ámbito de gobierno (Shils, 1956: 23).

A partir de mediados del siglo XX se institucionaliza en Europa el derecho de acceso a los documentos administrativos como un primer paso en pos de la publicidad en el seno de la Administración[4]. Con la aprobación de las Constituciones contemporáneas y su atribución de la soberanía al pueblo se hace evidente la necesidad de que el pueblo, referente último del poder, cuente con toda la información necesaria para ser verdaderamente soberano[5]. Decía Norberto Bobbio que la democracia es el gobierno del poder visible (Bobbio, 36-37). Si a esto unimos la limitación del poder que introducen las constituciones modernas como garantía de que el pueblo soberano seguirá siéndolo, la conclusión no puede ser otra que la de que el secreto se debe regular de forma restrictiva. Como decía Friedrich, la historia del Constitucionalismo es, desde sus comienzos la historia de la lucha por someter el poder político a reglas que conduzcan al imperio de la razón (bajo la ilustración encarnada por la Ley) y no al simple *imperium* de los gobernantes o «razón de Estado» (Friedrich, 1964: 412). La razón de Estado constitucional es en último término «cosa de ordenación cada vez más eficaz de un gobierno con arreglo a Derecho» (*idem*). En este sentido, «donde hay secreto falta el control, y sin controles no hay garantías para la efectividad de los

3 Dice Habermas que en el Estado liberal-burgués la publicidad política se manifiesta en la categoría central de la norma legal (Habermas, 1999: 91).

4 Suecia contaba ya desde el siglo XVIII con algunas normas que aplicaban el principio de publicidad a los documentos administrativos.

5 La constatación de que el pueblo, como titular de la soberanía, debe ser el referente último que legitime la actuación del poder público conlleva la exigencia jurídica de que se mantenga un flujo constante de información entre las instituciones gobernantes y el pueblo soberano (Pitruzzella, 1992: 2-3).

límites». Por ello «en el constitucionalismo, la publicidad es la norma [y] el secreto lo excepcional» (Revenga Sánchez, 1995: 34)[6].

Que el secreto deba ser lo excepcional[7] no significa que no puedan existir secretos en el Estado constitucional. Ciertamente, su ámbito ha quedado muy reducido en lo que a la esfera pública se refiere, y de ahí la necesidad perentoria de revisar la obsoleta LSO. Como advertía Pendás hace no muchos años, las actuales democracias transitan ahora por el camino del «Gobierno abierto»; sin ir más lejos, fruto de esta tendencia, el legislador aprobó en el año 2013 la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno (LTAIBG). El Gobierno Abierto forma parte «de la agenda pública en las democracias contemporáneas» y se concibe como la superación de los *arcana* de la razón de Estado, según los planteamientos del Estado absolutista. Se trata de un paso «en la buena dirección para actualizar y completar la democracia representativa, seña de identidad de una sociedad abierta y pluralista» (Pendás, 2015: 48). Siendo esto así, lo cierto es que el secreto de Estado sigue teniendo aun cabida dentro del Estado Constitucional, si bien de una forma limitada, dado el contexto en el que se inserta.

También es verdad que el secreto debe despojarse de connotaciones negativas, pues como bien dice la filósofa Sissela Bok, «debemos mantener una definición neutral del secreto, en lugar de una que asuma desde el principio que los secretos son condenables o peligrosos o, por el contrario, maravillosos y dignos de respeto. Un cierto grado de ocultación o de transparencia acompaña a todo lo que hacen o dicen los seres humanos. Debemos determinar qué es y qué no es censurable examinando prácticas concretas de secretismo, en lugar de asumir una postura valorativa inicial» (Bok, 1989: 20-21). «Si consideramos que el secreto es intrínsecamente engañoso o que oculta principalmente lo que es vergonzoso o censurable, estaremos utilizando conceptos preconcebidos antes incluso de examinar las prácticas que nos obligan a tomar una decisión; de este modo sólo confundiremos o desviaremos las cuestiones morales que se plantean. Es casi como si el esfuerzo por definir el *secreto* reflejara los deseos contradictorios que suscita a muchos el acercamiento al auténtico *secreto*: la cautelosa preocupación de dejarlo cuidadosamente sellado [para algunos] o, por el contrario, la determinación de abrirlo, restringirlo, ver sólo uno de sus aspectos, apresurarse a resolver su enigma...» (Bok, 1989: 25-26)[8]. El secreto, verdaderamente, no es más que una

6 En el mismo sentido, De Lucas, 1990:135 y 1999: 22; Fernandez Ramos, 1997: 447.

7 El secreto es, ante todo, un saber, un conocimiento intencionadamente separado: esto quiere decir, sencillamente, que se trata de un conocimiento que discrimina a favor de unos pocos, que se reserva a ellos y excluye a los demás; lo decisivo, pues, es la derogación del principio general del conocimiento, una derogación que se advierte a sí misma como excepcional. Excepcionalidad y restricción de los titulares son características propias de la noción de secreto. Sobre la etimología y las características del secreto vid. Bok, 1989: 6; Lucas, 1999: 24; Pitruzzella, 1992: 1; Sánchez Ferro, 2006: 4-5.

8 Traducción nuestra. Bok propone definir el secreto simplemente como ocultación intencionada, despojándolo de su carga moral.

herramienta, un instrumento, para proteger un bien jurídico; en el caso del secreto de Estado un bien jurídico importantísimo, la seguridad del Estado. El secreto, en definitiva, es en sí mismo instrumental (Sánchez Ferro, 2006: 5). Y no nos engañemos, el secreto de Estado es necesario porque los ciudadanos vivimos en un mundo de Estados nación repleto de conflictos[9]. Como bien señala Díez-Picazo en su libro *Sobre secretos oficiales*, un debate político fructífero sobre los secretos de Estado, «más que sobre la propia existencia de éstos [debería] girar en torno cuál pueda ser su regulación más adecuada» [Díez-Picazo, 1998: 37]. No cabe duda de que el principio de publicidad deberá colocarse en el epicentro de dicha regulación. Cualquier normativa que se quiera aprobar en la actualidad deberá partir de dicho principio, en tanto que principio central que se deriva de nuestra normativa constitucional[10]. Ciertamente, este principio de publicidad no se aplica de manera uniforme con respecto a los diferentes poderes del Estado (Díez-Picazo, 1998: 81, Sánchez Ferro, 2006: 36), pero de lo que no cabe duda es de que estamos ante un principio constitucional que debe informar la normativa sobre secretos de Estado y de que hoy en día este principio es, también, aplicable a la actividad del poder ejecutivo (véase el art. 105 b) CE). Es preciso garantizar al máximo la publicidad de la actuación de los poderes públicos, siendo dicho principio parámetro de la constitucionalidad de las normas.

Los secretos de Estado no solo interfieren con el principio de publicidad, sino que interfieren con diversos principios constitucionales y derechos fundamentales —la *Corte Costituzionale* italiana ponía como ejemplo los principios que regulan la función jurisdiccional—; por ello, en su sentencia núm. 86 del año 1977, de 24 de mayo, en línea con lo dicho en la sentencia núm. 82, del 14 de abril de 1976, la *Corte Costituzionale* estableció que era preciso encontrar un fundamento constitucional a la existencia de los secretos de Estado (conocidos en Italia por aquel entonces como secretos político-militares). Para la *Corte Costituzionale* al

9 «Sartre sostenía que «la transparencia debe sustituir en todo momento al secreto», pero que esto sólo será posible cuando se haya suprimido su necesidad material. En ese estadio, la relación entre los hombres dejará de ser antagónica» (Bok, 1989: 29) [traducción propia].

10 Nuestra Constitución se refiere a la publicidad en varias de sus disposiciones. En relación con los poderes públicos, el art. 9 CE impone la publicidad de las normas; el art. 80 CE se refiere a la publicidad de las sesiones plenarias del Congreso y del Senado, «salvo acuerdo en contrario de cada Cámara, adoptado por mayoría absoluta o con arreglo al Reglamento [de cada una de las Cámaras]»; el art. 120.3 CE exige que las sentencias sean motivadas y se pronuncien en audiencia pública; el art. 164 CE, por su parte, determina que las sentencias del Tribunal Constitucional se publiquen en el boletín oficial del Estado con los votos particulares, si los hubiere. El art. 120.1 CE recoge el principio de publicidad de las actuaciones judiciales «con las excepciones que prevean las leyes de procedimiento», mientras que el art. 24.2 CE reconoce el correlativo derecho de toda persona a un proceso público. En fin, el art. 105 b) CE incorpora el derecho de acceso de los ciudadanos a los archivos y registros administrativos, «salvo en lo que afecte a la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de las personas». Es claro que el principio de publicidad informa la labor de los poderes públicos. Por lo demás, en muchos casos el principio de publicidad se entiende que es un corolario necesario de la calificación de nuestro Estado como un Estado social y democrático de Derecho (art. 1 CE), así como de la atribución al pueblo de la soberanía y su papel como referente último del poder (art.1.2 CE).

proteger el secreto de Estado la fuerza, la preparación y la defensa militar del Estado (entonces la seguridad se enfocaba mucho más hacia la defensa), el interés protegido por el secreto político-militar sería el interés supremo de la seguridad del Estado referido al plano internacional del mismo, esto es, el interés del Estado-comunidad en su integridad territorial, su independencia y su propia supervivencia y tal interés sería objeto de protección en todos los ordenamientos jurídicos. En el caso italiano dicho interés se encontraría protegido en la Constitución, pudiéndose derivarse su fundamento constitucional de lo dicho por el artículo 52 de la Constitución italiana (CI), según el cual la defensa de la patria es un deber sagrado del ciudadano. En este sentido, la seguridad del Estado como bien constitucionalmente protegido constituiría un límite legítimo a esos otros principios constitucionales que mencionaba la *Corte* en las susodichas sentencias.

En España la seguridad del Estado también es un bien constitucionalmente protegido. El art. 105 b) CE limita el acceso a los archivos y registros administrativos en lo que afecte a la seguridad y defensa del Estado; el art. 2 CE establece la indisoluble unidad de la nación española, mientras que el art. 8 CE encarga a las Fuerzas Armadas la misión de «garantizar la soberanía e independencia del España, defender su integridad territorial y el ordenamiento constitucional». El art. 97 CE, por su parte, encarga al Gobierno la dirección de la administración militar y la defensa del Estado, y el preámbulo de la Constitución, aunque sin valor normativo, pero sí con un importante valor interpretativo, incluye entre los deseos del constituyente el de establecer la seguridad del Estado. En definitiva, los secretos de Estado protegen un bien jurídico constitucional y su existencia es perfectamente legítima[11]. Ahora bien, al constituir un límite, entre otros, al principio de publicidad, principio que debe ser la norma, y no la excepción en un Estado democrático de Derecho, su configuración debe ser lo más restrictiva posible, respetando eso sí, la necesidad de que el bien jurídico de la seguridad del Estado se vea también protegido (aplicando en la medida de lo posible el principio de concordancia práctica).

Los instrumentos internacionales también reconocen la legitimidad de la existencia del secreto para proteger la seguridad de los Estados[12]. Ahora bien,

11 El secreto de Estado es un secreto *ratione materiae*, más que *ratione personae*, dado que «las medidas de restricción de su difusión y empleo tienen su fundamento en las particularidades del objeto o materia sobre la que versan y, en concreto, en los daños que tales difusión y empleo incontrolados podría causar [a la seguridad del Estado]» (Santamaría Pastor, 1995: 6089).

12 Resolución 1838 (2011), de la Asamblea del Consejo de Europa *sobre el abuso del secreto de estado y seguridad nacional*, párr. 5; Resolución 1954 (2013), de la Asamblea del Consejo de Europa *sobre seguridad nacional y acceso a la información* (párr.3); Preámbulo de los *Principios globales sobre seguridad nacional y el derecho a la información*, de 12 de junio de 2013 («Principios de Tshwane»), que reconocen que, para poder preservar el ejercicio pleno de los derechos humanos, en ciertas circunstancias es preciso mantener cierta información en secreto para proteger los intereses de la seguridad nacional.

Los Principios de Tshwane han sido avalados por el Informe del Relator Especial para la promoción y protección a la libertad de opinión y expresión sobre derecho de acceso a la información, A/68/362, 4 septiembre 2013, párr. 64, 65, 66 y 67 y recomendados por la Asamblea Parlamentaria del Consejo de Europa a sus

remarcan que dado que el abuso del secreto puede tener un impacto negativo en el ejercicio de la jurisdicción, en el imperio de la ley, en el control parlamentario, en la libertad de prensa o en el gobierno abierto, o impedir que la ciudadanía participe en la determinación de determinadas políticas del Estado, es preciso encontrar un justo equilibrio entre secreto y divulgación en este campo[13].

III. EL CONCEPTO DE SECRETO DE ESTADO Y LA INFORMACIÓN CLASIFICADA ¿REALIDADES COINCIDENTES?

Llegados a este punto conviene posar la mirada en una distinción terminológica relevante, la referida a los secretos de Estado y a la información clasificada. No siempre ambos términos son coincidentes o abarcan una misma realidad.

En Alemania, por ejemplo, el Código penal (*Strafgesetzbuch* o StGB) es el único que se refiere en su texto literalmente al secreto de Estado, si bien el concepto se usa también en otros ámbitos del Derecho. El Código penal alemán parte de un concepto material del secreto de Estado (Sánchez Ferro, 2006: 118 y ss). En efecto, según el art. 93 StGB, titulado *Begriff des Staatsgeheimnisses* (concepto de secreto de Estado), «[l]os secretos de Estado son hechos, objetos o conocimientos que sólo son accesibles a un círculo limitado de personas y que deben mantenerse en secreto frente a una potencia extranjera para evitar el peligro de que se produzcan daños graves para la seguridad exterior de la República Federal de Alemania» [art. 93 (1) StGB[14]]. El propósito de la normativa penal es sancionar la traición y otros delitos que ponen en peligro la seguridad exterior (Stemmler, 2025: I.1 y bibliografía allí citada). Por ello, en Alemania no toda la información clasificada se considera secreto de Estado a efectos de su protección penal. Solo lo es aquella información cuya divulgación a una potencia extranjera produzca un daño grave a la seguridad exterior de la República Federal de Alemania. Así pues, la clasificación de una información u objeto por la Administración no es suficiente para que se considere que estamos ante un secreto de Estado a efectos penales, es más, para determinar si entra en juego la protección penal es indiferente que la información esté o no clasificada (Träger: 1988: 141). No hace falta que intervenga un poder del Estado identificando formalmente la información como secreta, esto es, clasificando la información, para que la información sea tratada y protegida como un secreto de Estado por el Código penal (Stree: 1997: 977; Träger, 1988: 133-134).

En el proceso contencioso-administrativo se maneja un concepto de secreto de Estado de contenido más amplio y distinto al concepto penal, y es que la finalidad

Estados miembros para guiar la clasificación de información en la ley y en la práctica en la Resolución 1954, de 2 de octubre 2013 (párr. 8).

13 Preámbulo de los Principios de Tshwane.

14 El art. 94 del Código penal alemán, por su parte, regula el delito de traición relacionado con la revelación de secretos de Estado.

que persigue la normativa es diferente, como lo son también los intereses que entran en conflicto. El concepto de secreto de Estado en el marco del proceso contencioso-administrativo abarca no solo cuestiones relativas a la seguridad exterior de Alemania, sino también cuestiones relativas a la seguridad interior (Stemmler, 2025: II. 2.1. a)). El precepto clave es el art. 99 del Código alemán de Procedimiento Contencioso-Administrativo (§ 99 Verwaltungsgerichtsordnung, VwGO). En este contexto el secreto busca evitar «perjuicios para el bienestar de la Federación o de un estado federado» o «amenazas para la seguridad nacional»[15]. Además, hay que tener en cuenta que no toda información que afecte al bienestar de la Federación o de un estado federado es objeto de protección en el marco del proceso contencioso-administrativo: las autoridades pueden negarse a aportar ciertos documentos o informaciones al proceso contencioso-administrativo por entender que ello sería perjudicial para el bienestar de la Federación o de un Estado federado, pero en tal caso, «[p]ara que se admita la solicitud de que cierta información se mantenga en secreto, la jurisprudencia del Tribunal Contencioso-administrativo Federal exige «razones de peso» y que exista un «perjuicio para intereses federales esenciales» (vid. por ejemplo, BVerwG, de 23.06.2011, 20 F 21/10, no. 19; BVerwG, de 29.4.2015, 20 F 8/14, nº. 13)» (Stemmler, 2025: II. 2.1 a))[16]. La clasificación de la información no impide la revelación de la información en el marco del proceso contencioso-administrativo, en tanto que puede determinarse que dicha información no protege un interés de entidad suficiente como para evitar su divulgación en el proceso, en vista, además, de los demás intereses en juego (desde la tutela judicial efectiva a la búsqueda de la verdad procesal etc.). De nuevo nos encontramos con un concepto material del secreto de Estado.

En definitiva, la protección administrativa de la información mediante el sistema de clasificación, que limita la difusión de la información a determinadas personas, no coincide por entero con la protección otorgada al secreto de Estado por el código penal o por la normativa que regula el proceso contencioso-administrativo.

15 Sobre las diferentes interpretaciones que se han dado del contenido del secreto de Estado en la jurisdicción contencioso-administrativa vid. Stemmler, 2025: II.2.

16 Cuando la Administración se niega a aportar cierta documentación al proceso contencioso-administrativo por considerarla secreto de Estado, el art. 99 del Código alemán de Procedimiento Contencioso-Administrativo prevé que el tribunal encargado de resolver la causa principal remita la cuestión al Tribunal competente para decidir sobre la incorporación o no de la información secreta al proceso. Este revisará a puerta cerrada (*in camera*) los documentos o la información y decidirá si pueden incorporarse al proceso principal. En principio, el tribunal contencioso-administrativo superior es el competente para llevar a cabo la revisión, decidiendo mediante auto. Si la decisión denegatoria procede de una autoridad federal superior que consideró que la divulgación sería perjudicial para el bienestar de la Federación, el procedimiento tendrá lugar ante el Tribunal Contencioso-Administrativo Federal. Si es el Tribunal Contencioso-Administrativo Federal el que actúa como tribunal de primera y última instancia en relación con el proceso principal, será él el que revise la documentación (Stemmler, 2025: V. 3.1 c)). La necesidad de secreto es solo uno de los factores a tener en cuenta —un factor relativo, por tanto—a la hora de decidir si se deniega el acceso a los documentos; se toman en cuenta también la implicación de otros intereses en juego (Stemmler, 2025: V. 3.1 b)).

La información se clasifica normalmente en distintos niveles en función de la necesidad de protección que requiere la información en cuestión. En Alemania, la Ley sobre los requisitos y el procedimiento para las habilitaciones federales de seguridad y protección de la información clasificada [*Gesetz über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Bundes und den Schutz von Verschlusssachen*. - (*Sicherheitsüberprüfungsgesetz* - SÜG)], que se ve desarrollada a nivel federal por el Reglamento administrativo general sobre la protección material de la información clasificada de 13 de marzo de 2023 (Instrucción de Información Clasificada - VSA) [*Allgemeine Verwaltungsvorschrift zum materiellen Geheimschutz* (*Verschlusssachenanweisung* - VSA)], establece en su art. 4 (1) SÜG que son informaciones clasificadas aquellos «hechos, objetos o conocimientos que requieren permanecer en secreto en interés público, en particular para proteger el bienestar de la Federación o de un estado federado, independientemente de su forma de presentación. [Se pueden, por ejemplo, clasificar] productos y los documentos asociados a los mismos, así como las claves para cifrar, descifrar y transmitir información (medios criptográficos)». Ese mismo artículo dispone que «los secretos comerciales, de empresa, de invención, fiscales u otros secretos privados o circunstancias de la esfera personal también pueden requerir mantenerse en secreto en interés público». Por su parte, el apartado (1a) del art. 4 SÜG señala que «sólo podrán tener conocimiento de la información clasificada las personas que tengan necesidad de conocerla debido al cumplimiento de sus funciones. Ninguna persona podrá ser informada antes de que sea necesario para el cumplimiento de sus funciones sobre la información clasificada, ni más extensamente de lo que sea necesario para el cumplimiento de [estas] funciones».

En cuanto al nivel de protección de la información clasificada, la SÜG clasifica la información en cuatro niveles: 1) *Top Secret* o Alto Secreto, aplicable a aquella información cuyo acceso (conocimiento) por personas no autorizadas puede poner en peligro la existencia o los intereses vitales de la República Federal de Alemania o de uno de sus *Länder*; 2) *Secreto* (*Geheim*), aplicable a aquella información cuyo acceso (conocimiento) por personas no autorizadas puede poner en peligro la seguridad de la República Federal de Alemania o de uno de sus Estados o causar graves daños a sus intereses; 3) *Confidencial (Vs-Vertraulich),* aplicable a aquella información cuyo acceso (conocimiento) por personas no autorizadas pueda resultar perjudicial para los intereses de la República Federal de Alemania o de uno de sus *Länder* y 4*) Solo para uso oficial o reservado (Vs-Nur für den Dienstgebrauch)*, cuando el acceso por personas no autorizadas puede ser desventajoso para los intereses de la República Federal de Alemania o de uno de sus *Länder*[17].

17 También en Italia se reconocen cuatro niveles de clasificación de la información. El art. 39.5 de la ley de 3 agosto 2007, n. 124 del *Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto* (publicada en la G.U. el 13 agosto 2007, n. 187), establece que el Primer Ministro regulará, por medio de reglamento, los criterios para la identificación de la información, los documentos, actos, actividades, cosas y lugares susceptibles de ser secreto de Estado. El Primer Ministro dictó el «Decreto del Presidente del

De acuerdo con el art. 4.4 SÜG, las autoridades y otros órganos públicos de la Federación estarán obligados a proteger la información clasificada mediante medidas de protección del secreto sustantivo de conformidad con el reglamento que desarrolla la ley, que es el *Allgemeine Verwaltungsvorschrift zum materiellen Geheimschutz (Verschlusssachenanweisung - VSA)*. La clasificación de la información tiene consecuencias a nivel interno, dentro de la propia Administración, y a nivel externo también, en cuanto que los terceros, personal de empresas, por ejemplo, que trabajan con la Administración, necesitan de una habilitación especial de seguridad para acceder a dicha información. En efecto, por un lado, la clasificación supone que solo ciertas personas pertenecientes a la Administración, o a entidades externas que trabajan con esta, tienen permitido el acceso a dicha información —aquellas que tienen una habilitación de seguridad en vigor que les permite el acceso a la misma; las habilitaciones de seguridad se confieren en función del nivel de clasificación de la información (cuanto mayor sea el nivel de clasificación de la información, más cerrado será el círculo de personas que tendrán acceso a la misma, con el fin de correr menos riesgos y evitar que la información salga a la luz). Además, se tomarán medidas de seguridad dentro de la Administración para que la información no trascienda. Por otro lado, es posible que se contemplen sanciones administrativas para el personal que revele aquella información clasificada a la que accedió gracias a su habilitación de seguridad a personas sin derecho de acceso a la misma[18]. Los

Consiglio dei ministri n. 7 del 12 giugno 2009» (DPCM 12 giugno 2009, n. 7) y el «Decreto del Presidente del Consiglio dei ministri» «*Disposizioni per la tutela amministrativa del segreto di Stato e delle informazioni classificate e a diffusione esclusiva*» (Decreto n. 5/2015, modificado por el Decreto del 2 ottobre 2017, n. 3). De acuerdo con el art. 39.1 de la Ley de 3 de Agosto de 2007, serán secretos de Estado los actos, los documentos, informaciones, actividades y cualquier otro asunto cuya difusión sea idónea para producir daño a la integridad de la República, incluso en relación con los acuerdos internacionales, a la defensa de las instituciones reguladas en la Constitución como pilares de la misma, a la independencia del Estado con respecto a otros Estados y a las relaciones con ellos y a la preparación y defensa militar del Estado.

Existen 4 niveles de clasificación diferentes en Italia: riservato, riservatissimo, segreto, segretissimo (reservado, confidencial, secreto y alto secreto o top secret), Las clasificaciones se otorgan en función de los criterios normalmente utilizados en las relaciones internacionales (art. 42.3 de la ley de 3 de agosto de 2007). La clasificación de alto secreto o top secret se otorgará a la información, los documentos, los actos, las actividades o los objetos cuya divulgación no autorizada puede (sea idónea para) causar un daño excepcionalmente grave a los intereses esenciales de la República (art. 4.3 del DPCM 12 giugno 2009, n. 7). La clasificación de secreto se atribuye a la información, los documentos, los actos, las actividades o las cosas cuya difusión no autorizada puede (sea idónea para) causar un daño grave a los intereses esenciales de la República (art. 4.4. DPCM 12 giugno 2009, n.7). Se otorgará la clasificación de muy confidencial a las informaciones, documentos, actos, actividades o cosas cuya divulgación no autorizada puede (sea idónea para) causar un perjuicio a los intereses esenciales de la República (art. 4.5 de dicho reglamento). La clasificación de reservado se atribuye a la información, los documentos, los actos, las actividades o las cosas cuya divulgación no autorizada puede (sea idónea para) causar un daño menor a los intereses de la República. Como se puede observar existen grandes paralelismos con la regulación alemana. Ambos ordenamientos jurídicos siguen, en cierta medida, el modelo de clasificación de la OTAN, Melero Alonso, 2025: III.2.

18 La clasificación de la información impacta evidentemente en el derecho de los ciudadanos a acceder a la información administrativa, se constituye en un límite a dicho derecho constitucionalizado (y en este

funcionarios en Alemania están sometidos a sanciones penales, pero también a sanciones administrativas[19].

Por lo que respecta a las sanciones penales, si quien comete el delito del art. 93 StGB es un funcionario se agrava la pena[20]. Además, el art. § 353 (b) StGB recoge el delito de violación del secreto oficial y del deber especial de confidencialidad, que se aplica a quien revele un secreto del que tenga conocimiento como funcionario público o a aquella persona sometida a un deber especial de confidencialidad en el servicio público o a quien desempeñe funciones o ejerza poderes en virtud de la ley de representación del personal o sea funcionario público europeo. El precepto se aplica a todo tipo de información oficial, también a la información no clasificada, lo que significa que la información clasificada entra definitivamente en el ámbito de aplicación de esta disposición[21].

Por lo que respecta a las sanciones disciplinarias administrativas[22], el precepto clave en materia de violación del secreto a nivel federal es el art. 67 de la *Bundesbeamtengesetz* (BBG) (Ley Federal de la Función Pública). Este artículo establece un deber de confidencialidad[23]. Según el Tribunal Contencioso-Administrativo Federal alemán, «[e]l deber de confidencialidad de los funcionarios públicos es uno de los principios tradicionales de la función pública (Art. 33 párrafo 5 GG) y tiene rango constitucional. El deber de los funcionarios públicos de mantener el secreto oficial sirve para mantener y garantizar el buen funcionamiento de una administración pública ordenada, ya que ésta sólo puede funcionar de manera constitucionalmente impecable, fiable e imparcial si se garantiza que los procedimientos oficiales por parte de los funcionarios públicos se mantienen en secreto frente al mundo exterior. Es uno de los deberes más importantes de los funcionarios públicos (véase BVerfG, decisión de 28 de abril de 1970 - 1 BvR 690/65 - BVerfGE 28, 191 <198 f.>; BVerwG, sentencias de 25 de febrero de

ámbito, de nuevo, los intereses en juego son distintos a los que entran en juego en el proceso penal o contencioso-administrativo).

19 Quería agradecer a M. Stemmler su ayuda con este apartado relativo a las sanciones de los funcionarios públicos que revelan información clasificada.

20 Vid. § 94 para 2 no 1 StGB: «si el infractor [...] abusa de un puesto de responsabilidad que le impone la obligación especial de salvaguardar secretos de Estado...» y § 97 para 2 StGB: «Quien revele un secreto de Estado mantenido en secreto por un organismo oficial o a instigación suya y al que haya tenido acceso en virtud de su cargo, de su posición oficial o de una orden emitida por un organismo oficial [...]».

21 La información clasificada puede, aunque es bastante improbable, contener información personal sensible (pensemos por ejemplo en la identidad de los informantes). La divulgación de esta información personal sensible está castigada penalmente (§ 37 SÜG) y puede desencadenar responsabilidad civil.

22 Estas sanciones pueden seguir a una condena penal.

23 Respecto a este deber de confidencialidad el § 67(1) BBG establece que «[l]os funcionarios mantendrán la confidencialidad con respecto a los asuntos oficiales de los que tengan conocimiento durante el ejercicio de sus funciones oficiales o con ocasión de las mismas. Esto también se aplicará más allá del ámbito de un empleador y tras la finalización de la relación funcionarial. Por lo demás, el apartado (2) establece las excepciones a dicho deber, entre las que se incluyen las sospechas de que se haya cometido un delito de corrupción o la comunicación de la información a un órganismo de denuncia competente de conformidad con los requisitos de la Ley de protección de denunciantes.

1971 - 2 C 11.70 - BVerwGE 37, 265 <268 f.> y de 24 de junio de 1982 - 2 C 91.81 - BVerwGE 66, 39 <41 f.>) [BVerwG 2 A 19.21, Sentencia de 2 de marzo de 2023, paras. 46-48][24]. La infracción de este deber de confidencialidad puede dar lugar a un procedimiento disciplinario con arreglo a la Ley disciplinaria federal (*Bundesdisziplinargesetz*, BDG)[25]. La sanción disciplinaria puede tener graves consecuencias para las personas afectadas en función de la gravedad de la falta, una sanción especialmente estricta es la retirada del estatuto de funcionario y, por tanto, del servicio, ya que conlleva la pérdida de los derechos de pensión. El *Bundesverwaltungsgericht* —BVerwG— (Tribunal Contencioso-Administrativo federal) en su sentencia de 2 de marzo de 2023, recaída en un caso en el que un funcionario público que trabajaba para el Servicio Federal de Inteligencia reveló información confidencial, puso de manifiesto que la violación del deber de confidencialidad del § 67 párr. 1 BBG es una falta grave en los ámbitos administrativos en los que el deber de confidencialidad reviste especial importancia -especialmente en el ámbito del servicio de inteligencia exterior-, lo que puede justificar la adopción de medidas disciplinarias que pueden llegar incluso a la separación de la condición de funcionario (principio 1 de la Sentencia de 2 de marzo de 2023). El demandado incumplió un deber primario derivado de la relación funcionarial y perdió definitivamente la confianza de su empleador y del público en general. El Tribunal dejó claro que el deber de secreto oficial afectaba en mayor medida al demandado. Es obvio —señaló el Tribunal Contencioso-Administrativo Federal— que, en particular, las partes de la administración estatal encargadas de garantizar la existencia y la seguridad exterior del Estado dependen especialmente de la confidencialidad de todos sus empleados (véase BVerfG, decisión de 28 de abril de 1970 - 1 BvR 690/65 - BVerfGE 28, 191 <199>). Esto se aplica en particular al trabajo para el servicio de inteligencia exterior. La protección de secretos es un requisito indispensable para las actividades de los servicios de inteligencia. Por ello, el demandado fue instruido en repetidas ocasiones acerca de su deber de confidencialidad, que va más allá del deber de confidencialidad generalmente aplicable, debido al ámbito sensible en el que desempeñaba su trabajo. El manejo fiable de información confidencial y sujeta a secreto forma parte de la esencia del trabajo del BND [el servicio de inteligencia exterior alemán o *Bundesnachrichtendienst*], por lo que la «idoneidad» de sus empleados depende de su capacidad y disposición para cumplir los requisitos resultantes.».

En definitiva, en Alemania la información clasificada se protege solo parcialmente mediante normas penales, reconduciéndose la protección de las materias

24 BVerwG 2 A 19.21, Urteil vom 02.03.2023 [ECLI:DE: BVerwG:2023:020323U2A19.21.0]. Algunas partes de la sentencia no son públicas, por lo que no es seguro que estuviera involucrada información clasificada en el caso, pero es lo más probable. En muchas ocasiones la confidencialidad sirve para asegurar un principio que viene recogido en nuestra propia Constitución, el de eficacia administrativa (art. 103 CE).

25 El § 5 Bundesdisziplinargesetz recoge las posibles sanciones disciplinarias.

clasificadas que no constituyen secreto de Estado a efectos penales al ámbito de las sanciones administrativas.

La situación en Francia es diferente. En el país vecino el concepto de secreto de Estado que maneja el código penal es un concepto formal, no material. El secreto en Francia se conoce como secreto de la defensa nacional (*secret de la défense nationale*). El Código penal francés define en su art. 413-9 el concepto[26]. A efectos penales se considerará «secreto de la defensa nacional» los «procedimientos, objetos, documentos, informaciones, redes informáticas, datos informatizados o ficheros de interés para la defensa nacional que hayan sido objeto de medidas de clasificación destinadas a restringir su difusión o acceso». Como se puede observar, aquí sí existe una coincidencia total entre el secreto de Estado protegido por el Código penal (Cp)y la información clasificada. De acuerdo con este art. 413-9 Cp «los niveles de clasificación de los procesos, objetos, documentos, informaciones, redes informáticas, datos informatizados o ficheros clasificados como secretos de defensa nacional y las autoridades encargadas de definir las modalidades de organización de su protección se determinan por decreto en Consejo de Estado».

Como explica Hubert Alcaraz, el régimen jurídico de la información clasificada sufrió una importante modificación en Francia en los años 2019 y 2021 (Alcaraz, 2025). El art. 11 del Decreto n.º 2019-1271, de 2 de diciembre de 2019, relativo a los procedimientos de clasificación y protección de los secretos de defensa nacional, sustituyó los tres niveles de clasificación que existían hasta entonces —Defensa-confidencial, Secreto de la defensa y Alto secreto de la defensa[27]— por dos niveles de clasificación y habilitación[28]: «Secreto» (*Secret*), y «Alto secreto» (*Très Secret*)[29]. De acuerdo con el artículo R 2311-3 del Código de defensa (*Code de la défense*, (CD)), que reproduce la Instrucción General Interministerial 1300 sobre la protección de los secretos de la defensa nacional[30], el nivel Secreto protege la información y los medios cuya divulgación o acceso podría perjudicar la defensa y la seguridad nacionales, mientras que el nivel Alto secreto protege la información y los medios cuya divulgación o acceso tendría

26 Este artículo se encuentra ubicado en el Título I del Código penal, dedicado a los delitos «contra *los intereses fundamentales de la nación* (cursiva nuestra), Capítulo III, sobre «Otros atentados contra la defensa nacional, sección 2ª del Libro IV del Código penal, titulado «Crímenes y delitos contra la nación, el Estado y la paz pública». El Código penal, nos dice Hubert Alcaraz, y creo que es relevante, ya no vincula el secreto de la defensa nacional a los «crímenes y delitos contra la seguridad del Estado», como hacía antes de que se aprobara el nuevo Código de 1992 (Alcaraz, 2025).

27 Confidentiel Défense, Secret Défense et Très Secret Défense.

28 La habilitación no es suficiente para acceder a información clasificada. Para acceder a ella es necesario demostrar la necesidad de conocerla [Arrêté du 10 juin 2024 portant approbation de l'instruction ministérielle relative à la protection du secret de la défense nationale au sein des ministères de l'éducation nationale et de la jeunesse, de l'enseignement supérieur et de la recherche et des sports et des jeux Olympiques et Paralympiques].

29 La decisión de clasificación se manifiesta en el sello de clasificación correspondiente.

30 Introducción al Arrêté du 9 août 2021 portant approbation de l'instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale.

consecuencias excepcionalmente graves para la defensa y la seguridad nacionales[31]. El concepto de seguridad nacional no se había utilizado en Francia hasta ese momento (Alcaraz, 2025). Ello da cuenta de los intereses cambiantes y el carácter evolutivo del concepto de la seguridad del Estado, como más adelante veremos. Además, existe cierta información no clasificada que está sujeta a un deber de discreción profesional —reserva— y que se protege mediante la categoría de «difusión restringida» (*diffusion restreinte*)[32]. El incumplimiento de la obligación de discreción profesional puede dar lugar a sanciones administrativas y disciplinarias. El Código penal castiga únicamente la violación del secreto de defensa que se identifica en este caso con la información clasificada, no con la categoría de difusión restringida[33].

La reforma del sistema de clasificación obedeció, según la Instrucción General Interministerial 1300 sobre la protección de los secretos de la defensa nacional a una doble preocupación: por un lado, evitar la tendencia a hacer un uso poco razonable del nivel más bajo de clasificación y, en consecuencia, tratar de frenar la proliferación de información y soportes clasificados; y, por otro, reajustar las normas de protección de los niveles de clasificación franceses a las normas de protección de los niveles de clasificación de los socios internacionales, con el fin de proteger mejor la información y los soportes clasificados intercambiados con estos últimos. Se dice, con razón, que tan malo es sobreclasificar la información como infraclasificarla: «La decisión de clasificar una información o un soporte es importante, tanto por las medidas restrictivas de protección que conlleva como por las consecuencias jurídicas que puede acarrear. Por lo tanto, la decisión de clasificar debe tratarse con cuidado»; una utilización abusiva iría en detrimento de la necesidad de reactividad y agilidad de la acción pública debido a las medidas de

31 La información y los medios clasificados como Alto secreto que conciernen a las prioridades gubernamentales en materia de defensa y seguridad nacional están sujetos a clasificaciones especiales definidas por el Primer Ministro [Código de defensa, art. R 2311-3].

32 https://www.defense.gouv.fr/sga/au-service-armees/droit-defense/informations-classifiees#:~:text=Les%20modalit%C3%A9s%20de%20classification,-Il%20existe%20plusieurs&text=Secret%20%3A%20ce%20niveau%20prot%C3%A8ge%20les,niveau%20%C2%AB%20Confidentiel%2DD%C3%A9fense%20%C2%BB. Diffusion Restreinte (Difusión Restringida) no es un nivel de clasificación sino un nivel de protección con sus propias normas [Arrêté du 9 août 2021 portant approbation de l'instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale].

33 El art. 413-10 Cp castiga con una pena de siete años y multa económica, a quien custodiando o estando en posesión, bien en virtud de su condición o profesión, bien en virtud de una función o encargo temporal o permanente, de un proceso, objeto, documento, información, red informática, datos informatizados o fichero que sea secreto de defensa nacional, lo destruya, sustraiga, reproduzca o dé acceso a él a una persona no habilitada o lo ponga en conocimiento del público o de una persona no habilitada. Cuando el depositario haya actuado con imprudencia temeraria o negligencia, el delito se castigará con tres años de prisión y multa. El hecho de obtener la posesión, acceder o tener conocimiento de un procedimiento, objeto, documento, información, red informática, datos informatizados o fichero que constituya un secreto de defensa nacional, destruirlo, sustraerlo o reproducirlo, en cualquier forma, o ponerlo en conocimiento del público o de una persona no cualificada siempre que la persona no entre dentro de las categorías definidas en el art. 413-10 se castiga con una pena de cinco años (art. 410-11 Cp).

protección que rodean a la información clasificada. La sobreclasificación provocaría una devaluación del secreto de defensa nacional y una erosión gradual del respeto de las normas asociadas a la clasificación. La infrautilización de la potestad de clasificación facilita el acceso de servicios de inteligencia extranjeros, grupos hostiles o individuos que buscan desestabilizar el Estado o la sociedad, a informaciones y medios cuya divulgación puede perjudicar los intereses fundamentales de la Nación[34].

En este punto debe llamarse la atención sobre algo que no se identifica como preocupación en esta norma interministerial: las consecuencias que el concepto formal de secreto de la defensa que adopta el Código penal pueden tener para el justiciable. Recordemos que la sanción penal debe ser siempre la última *ratio* ¿Cómo puede conciliarse el principio de intervención mínima del Derecho penal con este carácter formal del secreto? Es verdad, como señala Hubert Alcaraz, que el establecimiento de un concepto formal de secreto de la defensa parece garantizar una mayor seguridad jurídica por su previsibilidad (Alcaraz, 2025). Ahora bien, en un sistema penal donde la información clasificada integra el tipo penal correspondiente la clasificación debe restringirse al máximo. Sin embargo, vemos que ello no es así en Francia. El Código penal incluye el delito de violación del secreto de defensa nacional en aquellos delitos que tienen como fin salvaguardar los intereses fundamentales de la nación. Estos intereses van más allá del tradicional ámbito cubierto por la defensa del Estado (Alcaraz, 2025)[35]. Según explica el profesor Alcaraz, el campo de la seguridad nacional se amplía constantemente y algunos autores lo extienden a todos los intereses de la Nación (Alcaraz, 2025). De hecho, el objetivo de la estrategia de la seguridad nacional es, según el art. L. 1111-1 CD «identificar todas las amenazas y riesgos susceptibles de afectar a la vida de la Nación». Se trata de un concepto transversal. «La mención de los «riesgos» junto a las amenazas» y al mismo nivel que éstas añade claramente una dimensión preventiva a la seguridad nacional: «la prevención y la gestión de crisis, incluso las vinculadas a una causa accidental (como la crisis sanitaria del Covid-19), forman parte del perímetro de la seguridad nacional»», concepto que ««trasciende» la «distinción trandicional entre seguridad interior y exterior (Warusfel, 2021: 26)]»» (Alcaraz, 2025). Esta noción de seguridad nacional es «más adecuada a la variedad de amenazas contemporáneas» (Warusfel, 2021: 20). El problema es que «casi cualquier acción de clasificación puede justificarse sobre la base de una concepción tan amplia» (Fonbaustier, 2012: 6) [Alcaraz,

34 Introducción al *Arrêté du 9 août 2021 portant approbation de l'instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale.*

35 A los efectos del presente Título, dice el art. 410-1 del Código penal, «se entenderá por intereses fundamentales de la Nación su independencia, la integridad de su territorio, su seguridad, la forma republicana de sus instituciones, los medios de su defensa y de su diplomacia, la protección de su población en Francia y en el extranjero, el equilibrio de su medio natural y los elementos esenciales de su potencial científico y económico y de su patrimonio cultural».

2025]. Esto se convierte en un problema desde el punto de vista del alcance que deben tener las disposiciones penales, según el principio de intervención mínima, si bien es cierto que el criterio del daño mitiga en cierta medida el círculo de informaciones que pueden verse protegidas (recordemos que para clasificar una información, objeto, fichero, etc. como secreto es preciso que se produzca un perjuicio para la defensa o la seguridad nacionales y para clasificar una información, objeto, fichero, etc. como alto secreto se requiere que se produzca un perjuicio excepcionalmente grave para la defensa o la seguridad nacionales). Si los niveles de clasificación se desvinculan de la protección penal podría admitirse, en principio, una mayor amplitud en el ámbito protegido por los diversos niveles de clasificación, aunque habría que analizar en qué medida deberían ajustarse estos en función de otros derechos o intereses, como el derecho de acceso a la información o el principio de publicidad.

En todo caso, después de este análisis queda claro que el alcance de la clasificación de la información no puede ser igual en un ordenamiento jurídico donde la protección penal del secreto de Estado sea material que en un ordenamiento jurídico donde la protección del secreto de Estado sea formal. En este último caso solo deben clasificarse —en terminología francesa— aquellos procesos, objetos, documentos, informaciones, redes informáticas, datos informatizados o ficheros especialmente necesitados de protección, puesto que se está utilizando la herramienta de protección más fuerte con la que cuenta el Estado, el código penal (tiene sentido que la información sometida a difusión restringida, que tiene que ver con el deber de reserva dentro de la Administración, no se proteja penalmente). Por otro lado, es verdad que el gran reto de un sistema penal que utilice un concepto material del secreto es el de cómo reducir la inseguridad jurídica[36].

¿Qué sistema de protección del secreto de Estado es el que tenemos en España? Nuestro sistema de protección penal del secreto de Estado sigue un modelo formal. El Código Penal, en el Título XXIII, dedicado a «los delitos de traición y contra la paz o la independencia del Estado y relativos a la Defensa Nacional», establece sanciones basadas en la clasificación de la información como reservada o secreta diferenciando entre aquellas acciones que favorecen a potencias extranjeras y las que, sin dicha intención, afectan a la seguridad nacional o a

36 Una definición excesivamente vaga o amplia del secreto de Estado en las leyes que penalizan el espionaje o castigan la violación del secreto de Estado supone un peligro para la libertad y permite toda clase de abusos, decía Dick Marty en su informe al Comité de Asuntos Jurídicos y Derechos Humanos de la Asamblea del Consejo de Europa titulado *Abuse of state secrecy and national security: obstacles to parliamentary and judicial scrutiny of human rights violations*, Documento 12714 de 16 de septiembre de 2011. Tal y como recoge el informe de Amnistía Internacional **¿Abrimos ya el candado de la ley de secretos oficiales?**, ya en 2007 la Asamblea Parlamentaria del Consejo de Europa urgía a los estados miembros a «examinar su legislación vigente sobre secretos oficiales y reformarla de modo que sustituya las disposiciones vagas y demasiado amplias por otras específicas y claras, eliminando así todo riesgo de abuso o de enjuiciamiento injustificado» [Asamblea Parlamentaria del Consejo de Europa. Recomendación 1792 (2007), *Fair Trial issues in criminal cases concerning espionage or divulging state secrets*, en cumplimiento de la Resolución 1551 (2006)].

la defensa del Estado. Se castiga el procurarse dicha información, la revelación, el falseamiento, la inutilización o la sustracción de la información clasificada que pueda comprometer la seguridad o la defensa nacionales. Específicamente, el art. 584 CP castiga el delito de traición y los arts. 598 a 603, tipifican distintos comportamientos relacionados con el uso y revelación de la información reservada o secreta. Las sanciones varían desde los seis meses hasta los doce años de prisión, dependiendo de la gravedad de la conducta y su impacto en la seguridad del Estado. Dado que el sistema penal español vincula la sanción exclusivamente a la clasificación de la información, se subraya la importancia de restringir la clasificación a aquellos documentos que realmente requieran protección penal, evitando así un uso indiscriminado de esta herramienta.

IV. ALGUNOS ESTÁNDARES INTERNACIONALES RELEVANTES EN MATERIA DE LIBERTAD DE EXPRESIÓN E INFORMACIÓN E INFORMACIÓN CLASIFICADA

No cabe duda de que la clasificación de cierta información supone un obstáculo a la libertad de información y afecta, por tanto, al normal, desenvolvimiento de la democracia, que se nutre del conocimiento de los asuntos públicos, que a todo el mundo interesan, y del debate público. Recordemos que la información clasificada queda excluida de la circulación pública y su conocimiento queda reservado únicamente a un círculo limitado de personas, estando su divulgación a personas no autorizadas prohibida, y pudiendo acarrear la misma sanciones administrativas o penales[37]. Por ello, no es de extrañar que organismos internacionales que se ocupan de la libertad de expresión e información y otros actores de la esfera internacional se hayan manifestado sobre este tema.

Frank La Rue, Relator especial de las Naciones Unidas sobre la promoción y protección del derecho a la libertad de opinión y expresión señala que «[e]l principio general es que tanto las limitaciones como las restricciones [a la libertad de expresión e información] permisibles constituyen la excepción a la norma, y deben reducirse al mínimo necesario buscando un objetivo legítimo»[38]. Un objetivo legítimo, según los estándares internacionales, sería el de la seguridad del Estado. Ahora bien, «un estado no podrá denegar acceso de modo terminante a toda la información relativa a la seguridad nacional, sino que deberá designar por

37 Señala el preámbulo de los Principios de Tshwane que «[e]l acceso a la información, al permitir el escrutinio público de la acción del Estado, no sólo salvaguarda contra los abusos de los funcionarios públicos, sino que también permite al público desempeñar un papel en la determinación de las políticas del Estado y, por lo tanto, constituye un componente crucial de la auténtica seguridad nacional, la participación democrática y la formulación de políticas sólidas» (traducción propia de la versión inglesa de los principios).

38 Informe del Relator Especial para la promoción y protección a la libertad de opinión y expresión sobre derecho de acceso a la información, de 20 de abril, 2010, A/HRC/14/23, párr. 77.

ley sólo aquellas categorías específicas y estrictas de información que sea necesario no revelar para proteger un interés legítimo de seguridad nacional» (Principio 12 de los Principios de Johannesburgo sobre la Seguridad Nacional, la Libertad de Expresión y el Acceso a la Información)[39]. Obsérvese la referencia a la legitimidad del interés de seguridad.

En esta misma línea, los Principios de Tshwane señalan que «[n]o se podrá imponer ninguna restricción al derecho a la información por motivos de seguridad nacional a menos que el gobierno pueda demostrar que (1) la restricción (a) está prescrita por la ley y (b) es necesaria en una sociedad democrática (c) para proteger un interés legítimo de seguridad nacional» (Principio número 3). Estos principios aluden a la necesidad de que la información represente «un **riesgo real e identificable de perjuicio significativo** para un interés **legítimo** de seguridad nacional» (negrita nuestra) (Principio 3 (b) (i) Tshwane). Los principios Tshwane definen, en su glosario, el interés legítimo de seguridad nacional como aquel que se refiere a un interés cuya finalidad genuina y principal efecto es proteger la seguridad nacional, en consonancia con la legislación internacional y el Derecho nacional.

Una restricción que se quisiera justificar por motivos de seguridad —indican, por su parte, los Principios de Johannesburgo— «no sería legítima si su propósito genuino o su efecto demostrable fuera «el de proteger intereses inconexos con la seguridad nacional, incluso, por ejemplo, el de proteger a un gobierno en una situación embarazosa o de la revelación de algún delito, o el de ocultar información sobre el funcionamiento de sus instituciones públicas, o el de afianzar una ideología en particular, o el de suprimir la conflictividad industrial» . Por su parte, el Comité de Derechos Humanos indica que «[n]o es compatible con el párrafo 3, [del art. 19 PIDCP] por ejemplo, hacer valer [las leyes sobre secretos de Estado o sobre sedición] para suprimir información de interés público legítimo que no perjudica a la seguridad nacional, o impedir al público el acceso a esta información, o para procesar a periodistas, investigadores, ecologistas, defensores de los derechos humanos u otros por haber difundido esa información. Tampoco procede, en general, incluir en el ámbito de estas leyes categorías de información tales como las que se refieren al sector comercial, la banca y el progreso científico»[40].

Los Principios de Siracusa inciden en la idea de que la seguridad nacional no puede servir como pretexto para imponer limitaciones a los derechos humanos vagas o arbitrarias[41] y añaden que «[l]a seguridad nacional no puede

39 Principios de Johannesburgo sobre la Seguridad Nacional, la Libertad de Expresión y el Acceso a la Información, Art. 19, noviembre de 1996, Principio, 12. Los Principios de Johannesburgo han sido avalados por el Informe del Relator Especial para la promoción y protección de la libertad de opinión y expresión, E/CN.4/1996/39, 22 marzo 1996, párrs. 4 y 154.

40 Observación Nº 34 sobre el art. 19 del Pacto Internacional de Derechos Civiles y Políticos.

41 Principios de Siracusa sobre las disposiciones de limitación y derogación del Pacto Internacional de Derechos Civiles y Políticos. Anexo, E/CN.4/1984/4 (1984), Principio 31.

invocarse como motivo para imponer limitaciones destinadas a prevenir amenazas meramente locales o relativamente aisladas contra el orden público» (principio 30).

Por lo demás, más allá de proteger un interés legítimo de seguridad, la ley que restrinja la libertad de expresión o información «deberá ser accesible, inequívoca, redactada estrictamente y con precisión para permitir que los individuos prevean si una acción en particular fuera ilícita» (principio de Johannesburgo 1.1. (a))[42]. Los principios Tshwane señalan que la ley debe recoger de forma clara las categorías de información que pueden clasificarse con base en argumentos relativos a la seguridad nacional (principio 3 c))[43] y consideran como una «buena práctica que la legislación nacional establezca una lista exclusiva de categorías de información limitadas» (Principio 9 (a)) de los Principios Tshwane)[44]. En relación con estas categorías, el Relator Especial para la promoción y protección del derecho a la libertad de opinión y expresión considera que la «inaplicabilidad de las normas generales a la seguridad nacional ha estado relacionada tradicionalmente con la información sobre los planes de defensa que se estén llevando a cabo, los sistemas de armamentos y comunicaciones, la infraestructura crítica y las operaciones, fuentes y métodos de inteligencia» y que los Estados «también protegen desde hace mucho tiempo las actividades diplomáticas sensibles relacionadas con la seguridad»[45].

La lista de categorías que recoge los Principios Twshane es sumamente interesante: el primer apartado del principio 9 (a) se refiere a la información sobre «planes, operaciones y capacidades de defensa en curso durante el tiempo que la

42 En este sentido, una definición excesivamente vaga o amplia del secreto de Estado en las leyes que penalizan el espionaje o castigan la violación del secreto de Estado supone un peligro para la libertad y permite toda clase de abusos, señalaba D. Marty en su informe al Comité de Asuntos Jurídicos y Derechos Humanos de la Asamblea del Consejo de Europa titulado *Abuse of state secrecy and national security: obstacles to parliamentary and judicial scrutiny of human rights violations*, Documento 12714 de 16 de septiembre de 2011. Tal y como recoge Amnistía Internacional en su informe ¿Abrimos ya el candado de la ley de secretos oficiales? (2020), ya en 2007, la Asamblea Parlamentaria del Consejo de Europa, urgía a los estados miembros a «examinar su legislación vigente sobre secretos oficiales y reformarla de modo que sustituya las disposiciones vagas y demasiado amplias por otras específicas y claras, eliminando así todo riesgo de abuso o de enjuiciamiento injustificado» [Asamblea Parlamentaria del Consejo de Europa. Recomendación 1792 (2007), *Fair Trial issues in criminal cases concerning espionage or divulging state secrets*, en cumplimiento de la Resolución 1551 (2006)].

43 Por su parte, el principio 2 c) Tshwane establece que «se considera buena práctica para la seguridad nacional, cuando la misma es empleada para limitar el derecho a la información, que [s]e defina con precisión en el ordenamiento jurídico de un país de forma consistente con una sociedad democrática».

44 Según el Principio 11 d) Tshwane, cuando se clasifica la información, «(i) una marca protectora debe incorporarse al documento indicando el nivel, si procede, y la duración máxima de la clasificación, y (ii) debe incluirse una declaración en la que se justifique la necesidad de clasificar la información a ese nivel y por ese período», práctica que no siempre se sigue y que debería seguirse. Además, solo debe clasificarse aquella parte del documento que contenga información sensible, no todo el documento si no es necesario (Principio 22).

45 *Informe del Relator Especial para la Promoción y protección del derecho a la libertad de opinión y de expresión sobre la protección de las fuentes de información y los denunciantes de irregularidades,* de 8 de septiembre de 2015*,* A/70/361, párr. 47.

información sea de utilidad operativa» (Principio de Tshwane 9 (a) (i)). Se aclara en nota adjunta que «la frase «durante el período en que la información resulte de utilidad operativa» exige divulgar la información una vez que esta ya no suponga revelar datos que podrían ser aprovechados por enemigos para conocer la capacidad de reacción del Estado, su capacidad, sus planes, etc». El apartado (ii) del Principio 9 (a) señala que las autoridades podrán restringir el acceso a la información «sobre la producción, capacidades, o uso de los sistemas de armamentos y otros sistemas militares, incluidos los sistemas de comunicaciones» y aclara en nota posterior que «d[i]cha información incluye datos e inventos tecnológicos, e información sobre su producción, capacidad o uso». De esta categoría se excluye específicamente «[l]a información sobre partidas presupuestarias relativas a armamento y otros sistemas militares», que deberían encontrarse disponibles para el público. Se considera una buena práctica «que los Estados mantengan y publiquen una lista de control de armamento» (alentada por el Tratado sobre el Comercio de Armas en lo que concierne a armas convencionales) así como «[l]a publicación de información relativa a armas, equipos y números de tropas» (Nota al Principio 9 (a) (ii))[46]. Se admite la restricción de la «[i]nformación sobre medidas específicas destinadas a resguardar el territorio del Estado, infraestructura crítica o instituciones nacionales fundamentales (*institutions essentielles*) contra amenazas, uso de la fuerza o sabotaje, cuya efectividad depende de su confidencialidad» (Principio Tshwane 9 (a) (iii))[47]. La lista de categorías objeto de clasificación se cierra con la «[i]nformación perteneciente a, o derivada de, operaciones, fuentes y métodos de los servicios de inteligencia, siempre que conciernan a asuntos relativos a la seguridad nacional» (Principio 9 (a) (iv)) y la «[i]nformación relativa a asuntos de seguridad nacional suministrada por un Estado extranjero u organismo intergubernamental con una expectativa expresa de confidencialidad, y otras comunicaciones diplomáticas en tanto tengan que ver con asuntos relativos a la seguridad nacional» (Principio 9 (a) (v))[48]. Los principios de Tshwane admiten que se puedan añadir nuevas categorías a la lista, pero «únicamente si dicha categoría está específicamente identificada y definida de forma limitada y la preservación de la confidencialidad de la información es necesaria para proteger un interés legítimo de seguridad nacional establecido por ley, tal y cómo se sugiere en el Principio 2(c)» (Principio 9 (c)). Además, se añade que, al proponer una nueva categoría, «el Estado debería explicar que la divulgación de la

46 Además, estos principios consideran que la información sobre la adquisición de armas nucleares u otras armas de destrucción masiva por parte del Estado no podrá ser clasificada porque es una información que tiene un interés público predominante lo que no afectará a los detalles de manufactura o capacidades operacionales (Principio de Tshwane 10 D (2)).

47 Se aclara que la ««**[i]**nfraestructura crítica» hace referencia a recursos estratégicos, activos y sistemas, ya sean físicos o virtuales, de tal importancia para el Estado que su destrucción o incapacidad tendría un impacto debilitador en la seguridad nacional».

48 La nota aclaratoria del Principio de Tshwane 9 (a) (v) deja de manifiesto que se considera buena práctica consignar por escrito dichas expectativas.

información contenida en la misma supondría una amenaza para la seguridad nacional» (*idem*)[49].

El principio 10 de los Principios Tshwane establece una presunción de publicidad para ciertas categorías de información, pues considera que las mismas revisten «un interés público especialmente significativo o preponderante por su relevancia extraordinaria para el proceso de control democrático y el Estado de derecho»; estas categorías son: «[v]iolaciones de los derechos humanos internacionales y del derecho internacional humanitario», «[g]arantías relativas al derecho a la libertad y seguridad de la persona, la prevención de la tortura y otros abusos y el derecho a la vida», «[e]structuras y poderes de gobierno», «[d]ecisiones relativas al uso de la fuerza militar o a la adquisición de armas de destrucción masiva», el marco jurídico general en materia de vigilancia de todo tipo, así como los procedimientos a seguir para su autorización, la selección de los objetivos y el uso, intercambio, almacenamiento y destrucción del material interceptado, las entidades autorizadas para llevar a cabo dichas acciones de vigilancia, y las estadísticas relativas al uso de dichas acciones, así como las vigilancias ilegales que se hayan producido[50]; «información suficiente para permitir que el público entienda las finanzas del sector de la seguridad, así como las reglas que las rigen», «r]esponsabilidad relativa a violaciones constitucionales y estatutarias y otros abusos de poder» por parte de autoridades y personal público, toda la información que permita que el público entienda o tome las medidas pertinentes para evitar o mitigar el daño procedente de una amenaza inminente o actual a la salud pública, a la seguridad pública o al medioambiente, «tanto si ésta deriva de causas naturales como de actividades humanas, incluyendo por acciones del Estado o de compañías privadas» y «[c]ualquier otra información, actualizada regularmente, sobre la explotación de recursos naturales, contaminación e inventarios de emisiones, los impactos medioambientales derivados de grandes obras públicas existentes o propuestas, o de la extracción de recursos, y evaluación de riesgos y planes de gestión de las instalaciones especialmente peligrosas». Desarrollaremos algo más alguna de estas presunciones cuando hablemos de la definición negativa de los secretos de Estado[51].

49 Los Principios de Siracusa son más restrictivos y establecen que «la seguridad nacional sólo podrá invocarse para justificar medidas limitativas de determinados derechos cuando se adopten para proteger la existencia de la nación o su integridad territorial o independencia política contra la fuerza o la amenaza de la fuerza» (Principio 29), pero hay que tener en cuenta que son mucho más antiguos y que el concepto de seguridad y defensa ha ido evolucionando con el tiempo.

50 Se aclara que «[e]l derecho de la sociedad a ser informada no se extiende, necesariamente, a los detalles fácticos u operativos de las vigilancias efectuadas con arreglo a la ley y en consonancia con las obligaciones relativas a los derechos humanos. Dicha información podría ser clasificada, tanto para el público como para aquellos que se encuentran sujetos a vigilancia, al menos hasta que el período de vigilancia haya concluido». (Nota Principio de Tshwane 10 E (2)). Se excluye también la vigilancia a Gobiernos extranjeros (Principio Tshwane 10 E 5).

51 El Relator Especial para la Promoción y protección del derecho a la libertad de opinión y de expresión también sostiene que cabe «presumir que algunas cuestiones deben considerarse de interés público, como las infracciones penales y las violaciones de los derechos humanos o del derecho internacional humanitario, la

En fin, al limitar el derecho a obtener información debe tomarse particularmente en cuenta el interés público en conocer la información[52]. D. Kaye, Relator Especial para la Promoción y protección del derecho a la libertad de opinión y de expresión, recuerda que «a fin de satisfacer el principio de proporcionalidad, la institución pertinente también debería estar dispuesta a mostrar que el daño a un interés legítimo concreto de seguridad nacional es superior al interés público que existe en que se produzca esa divulgación»[53].

Tomando en cuenta todos estos estándares analicemos cómo ha definido el legislador la información clasificada en España, así como la propuesta de modificación de la LSO que presentó el PSOE en la XIV legislatura, esto es, el Anteproyecto de Ley de Información Clasificada de agosto de 2022.

V. LA DEFINICIÓN DE LAS MATERIAS CLASIFICADAS, LA LEY DE SECRETOS OFICIALES DEL 68 Y EL ANTEPROYECTO DE LEY DE INFORMACIÓN CLASIFICADA DE LA XIV LEGISLATURA

1. La definición de las materias clasificadas

El abuso del secreto de Estado puede socavar los fundamentos democráticos. En lugar de proteger la seguridad, podría servir de cobertura para encubrir violaciones de derechos humanos, evitar el escrutinio público o proteger intereses gubernamentales que no están relacionados con la seguridad del Estado. En el caso de España el riesgo existe, en cuanto que la LSO no prevé mecanismos de desclasificación automática de la documentación clasificada ni mecanismos efectivos de revisión sistemática de dicha documentación, más allá de la propia revisión interna que pueda llevarse a cabo por la propia Administración. En este epígrafe vamos a analizar la definición que se ha dado de las materias clasificadas en nuestro ordenamiento jurídico, así como la propuesta planteada por el Anteproyecto de Ley de Información Clasificada de 2022 (ALIC). Un buen control de la documentación clasificada comienza por establecer una definición acotada de lo que pueda constituir materia clasificada.

corrupción, la seguridad pública y los daños ambientales, y el abuso de los cargos públicos» [Informe de 8 de septiembre de 2015, A/70/361, párr. 10].

52 Principios de Johannesburgo sobre la Seguridad Nacional, la Libertad de Expresión y el Acceso a la Información, artículo 19, noviembre de 1996 (Principio 13).

El Convenio del Consejo de Europa sobre el acceso a documentos públicos, también conocido como el Convenio de Tromsø (Council of Europe Convention on Access to Official Documents. Tromsø, 18 de junio de 2009 (CETS no. 205)), ratificado por España en septiembre del 2023 y que entró en vigor el 1 de enero de 2024, reconoce un derecho de acceso a los documentos oficiales que puede verse limitado si el acceso pudiera o sería probable que dañara la defensa, la seguridad nacional o las relaciones internacionales a no ser que exista un interés público superior en su divulgación (art. 3.2 Convenio de Tromsø).

53 Informe de 8 de septiembre de 2015, A/70/361, párr. 48. Vid. también Principio 3 (b) (ii) Tshwane.

1.1. *La definición positiva de las materias clasificadas*

La LSO, recurre a la utilización de conceptos jurídicos indeterminados para establecer qué materias pueden ser clasificadas[54]. De acuerdo con el art. 2 LSO «podrán ser declaradas «materias clasificadas» los asuntos, actos, documentos, informaciones, datos y objetos cuyo conocimiento por personas no autorizadas pueda dañar o poner en riesgo la seguridad y defensa del Estado»[55]. Se requiere de una declaración de clasificación por parte del Gobierno, que es quien ostenta la potestad de dirección política[56], para que los documentos, datos y objetos queden clasificados, siempre respetando lo que dice la ley. En el marco de esta definición el Gobierno, mediante Acuerdos del Consejo de ministros[57], ha ido estableciendo qué categorías de información deberían considerarse clasificadas, sin ningún control a la hora de establecer dichas categorías, lo que le ha llevado en ocasiones a extender el halo del secreto más allá de lo razonable sin mayores consecuencias[58]. El control más incisivo de la declaración de materias clasificadas se produce en nuestro país principalmente a raíz de la necesidad de incorporar ciertos documentos clasificados a un proceso[59].

54 En concreto se recurre a los conceptos de seguridad y defensa del Estado, conceptos que son «innegablemente flexibles» y que cuentan con una muy baja «densidad normativa», como señala Puente Rodríguez reproduciendo lo dicho por Díez-Picazo Giménez y Bacigalupo Sagesse (Puente Rodríguez, 2022: ep. II).

55 La redacción del art. 2 LSO es mejorable en tanto en cuanto que se incluye como materias clasificadas no solo documentos y objetos, sino informaciones, asuntos o datos (no los ficheros o soportes en los que se incluyen esos datos). Lo que debería entenderse como clasificable sería el soporte de la información, pero la información por sí misma es inaprensible (Sánchez Ferro, 2006: 30).

56 Recordemos que el Gobierno es quien dirige la política de defensa, exterior e interior del Estado y la Administración civil y militar (art. 97 CE).

57 Acuerdo del Consejo de Ministros de 28 de Noviembre de 1986: Acuerdo por el que se clasifican determinados asuntos y materias con arreglo a la Ley de Secretos Oficiales; Acuerdo de 12 de marzo de 1987 que clasifica como secretas las actas de la Junta Interministerial Reguladora del Comercio Exterior de Material de Defensa y de Material de Doble Uso (JIMDDU); Acuerdo del Consejo de Ministros de febrero de 1996; Acuerdo del Consejo de Ministros de 15 de octubre de 2010; Acuerdo del Consejo de Ministros, de 6 de junio de 2014.

58 Antes de la entrada en vigor de la Constitución, el año 1974 el Consejo de Ministros decidió desclasificar muchas de las materias que en aquellos momentos estaban sustraídas del conocimiento general. El problema no fue tanto la redacción del supuesto de hecho del art. 2 LSO como la interpretación antidemocrática que se hizo del mismo y la utilización de dicha herramienta por el Gobierno para proteger sus propios intereses. Se trató de escamotear del debate público lo relacionado con la Ley Sindical, por ejemplo, u ocultar a la opinión pública uno de los escándalos políticos-financieros más importantes de la época, el caso MATESA [Gómez-Reino y Carnota, 1976: 131]. Después de la entrada en vigor de la Constitución, el Gobierno decidió en un Acuerdo secreto ¡sí, secreto! — Acuerdo del Consejo de Ministros de 15 de octubre de 2010— clasificar hasta 17 materias vinculadas con las relaciones exteriores que incluían, entre otras, la protección de los derechos humanos, cuestiones de asilo y refugio, entrevistas con mandatarios o diplomáticos extranjeros o candidaturas españolas a puestos en organismos internacionales (vid. González, M. Exteriores blinda todos sus documentos, *Diario El País* de 3 de junio de 2012). Para conocer el perjuicio que dicho Acuerdo de clasificación, claramente *ultra vires* en algunas de sus categorías, produjo en relación con la investigación de los historiadores, vid. Pereira y Sanz Díaz, 2015.

59 El Tribunal Supremo, en sus sentencias de cuatro de 4 abril de 1997 de la Sala de lo Contencioso-Administrativo sobre «los papeles del Cesid» señaló que el derecho fundamental de todas las personas a

Los conceptos de seguridad y defensa del Estado son, según la tesis del Tribunal Supremo, conceptos jurídicamente asequibles[60]. Estos conceptos se constituyen en el límite material de la actividad de clasificación de acuerdo con el art. 2 LSO, pero el legislador, además, limita el poder de clasificación del Gobierno a través de la exigencia de que para que una materia pueda ser clasificada, el conocimiento de la información clasificada por persona no autorizada pueda dañar o poner en riesgo dicha seguridad o defensa del Estado (art. 2 LSO)[61]. Analicemos ambos límites.

1.1.1. El límite material

El Relator Especial de Naciones Unidas, Frank La Rue nos ponía sobre aviso sobre el posible uso de «un concepto impreciso de seguridad nacional para justificar limitaciones invasivas del goce de los derechos humanos». Señalaba La Rue que dicho uso «plantea serias preocupaciones. Este concepto tiene una definición amplia y, por consiguiente, es vulnerable a la manipulación del Estado como medio de justificar medidas dirigidas a grupos vulnerables como defensores de los derechos humanos, periodistas o activistas. También permite justificar el secreto a menudo innecesario en torno a investigaciones o actividades de las fuerzas del orden, socavando los principios de la transparencia y la rendición de cuentas»[62]. Lo cierto es que es difícil definir tales conceptos desde un punto de vista abstracto[63].

obtener una tutela judicial efectiva del artículo 24.1 CE parecería incompatible con la existencia de una parte de la actividad del Gobierno exenta de control jurisdiccional (aludió además al art. 9 CE). Cuando el legislador ha definido mediante «conceptos judicialmente asequibles» los límites o requisitos previos a los que deben sujetarse los actos de dirección política, los Tribunales deben aceptar el examen de las eventuales extralimitaciones o incumplimiento de los requisitos previos en que el Gobierno hubiera podido incurrir al tomar la decisión. Ante una negativa de desclasificación de documentos por parte del Gobierno para ser incorporados al proceso, el Tribunal Supremo, Sala de lo Contencioso-administrativo, se declaró competente para determinar la vinculación entre los documentos clasificados como secretos y la seguridad del Estado y consideró, además, que le era asequible determinar negativamente la concurrencia de elementos que o bien eliminaran totalmente la afección a dicha seguridad o bien la aminorasen en términos que —ponderando los intereses jurídicos en juego— le permitieran dar prevalencia, en su caso, al derecho constitucional a la tutela judicial efectiva (STS de 4 de abril de 1997 (rec. 726/1996), Fto Jco 7º).

60 Vid. nota previa.

61 La Ley de Secretos Oficiales establece, además, que «[t]endrán carácter secreto, sin necesidad de previa clasificación, las materias así declaradas por Ley» (Art. Primero Dos).

62 Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión, Frank La Rue sobre las consecuencias de la vigilancia de las comunicaciones por los Estados en el ejercicio de los derechos humanos a la intimidad, de 17 de abril de 2013. A/HRC/23/40, párr. 60.

63 Decían Lustgarten y Leigh en su libro *In from the Cold* que «pocos conceptos son más complejos, más discutidos y tienen tal importancia para el ejercicio del poder político como lo tiene el concepto de seguridad nacional. Este concepto no admite definiciones o discusiones abstractas. La posición que cada cual ocupa o es capaz de ocupar [en el panorama internacional] es un elemento crítico de éste. Nuestro mundo es todavía un mundo de Estados-nación en el que coexiste la cooperación con la rivalidad, la ley y el Derecho con la anarquía.

El legislador español ha abordado la tarea de definición de la defensa y seguridad nacionales en la Ley Orgánica 5/2005, de 17 de noviembre, de la Defensa Nacional (LODN) y la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional (LSN).

La LODN señala que la política de defensa tiene como finalidad «la protección del conjunto de la sociedad española, de su Constitución, de los valores superiores, principios e instituciones que en ésta se consagran, del Estado social y democrático de derecho, del pleno ejercicio de los derechos y libertades, y de la garantía, independencia e integridad territorial de España. Asimismo, tiene por objetivo contribuir a la preservación de la paz y seguridad internacionales, en el marco de los compromisos contraídos por el Reino de España» (art. 2 LODN). Además, se indica que las Cortes Generales deberán aprobar las leyes relativas a la defensa y los créditos presupuestarios correspondientes, debatir las líneas generales de la política de defensa y controlar al Gobierno en este ámbito (art. 4 LODN). Por su parte, la LSN establece en su art. 3 que «a los efectos de esta ley se entenderá por Seguridad Nacional la acción del Estado dirigida a proteger la libertad, los derechos y 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 el cumplimiento de los compromisos asumidos»; como se puede observar, la definición es muy amplia, sobre todo en lo que respecta al bienestar de los ciudadanos; si esta es la referencia a la que debe vincularse la potestad clasificatoria, parece que la discrecionalidad de la que pueda gozar el Gobierno será también bastante amplia.

Cabe preguntarse si sería posible dotar de una mayor densidad normativa al límite material de la información clasificada. Sin embargo, antes de abordar esta cuestión es necesario comprender cómo funciona verdaderamente la actividad clasificatoria.

En términos generales, el Gobierno no clasifica cada documento de forma individual, sino que establece una serie de categorías materiales que pueden ser objeto de clasificación bajo el marco de lo establecido legalmente (vid. los Acuerdos del Consejo de Ministros mencionados en la nota 57) ¿podría/debería el legislador establecer ese elenco de categorías materiales clasificadas en lugar de hacerlo el Gobierno, en línea con lo sugerido por los estándares/buenas prácticas internacionales que hemos analizado? Establecer categorías de información clasificada por ley, en la línea de lo dispuesto por los estándares internacionales, es lo que intentó precisamente el ALIC; en principio, parecería lógico seguir esta vía —sin entrar ahora en el análisis de la corrección de las categorías concretas que se establecieron en el ALIC—. El legislador, en un régimen parlamentario, debe establecer el marco en el que debe moverse la dirección política del Gobierno,

Cada Estado tiene su propio carácter, intereses y vulnerabilidades. Por consiguiente, el significado práctico de la seguridad nacional varía de un Estado a otro» [traducción propia] (Leigh y Lustgarten, 1994: 3].

también en materia de seguridad, por supuesto sin sustituir al Gobierno en su tarea de dirección política. Al fin y al cabo, el Gobierno no hace sino establecer categorías en abstracto de la información que debe permanecer clasificada conforme a la LSO, cosa que podría y debería hacer el Parlamento. Ciertamente, hay un problema, más allá del estado de nuestro parlamentarismo, en el que aquí no voy a entrar, que se vincula directamente con el propio concepto de seguridad del Estado. El concepto de seguridad del Estado es cambiante y evoluciona con el tiempo (véase Sánchez Ferro, 2006: 221 y ss], por lo que parece imposible establecer una lista de categorías totalmente cerrada (a pesar de lo que se dice en los Principios de Tshwane) [64]. El legislador va a tener que dejar, inevitablemente, una puerta abierta a que el Gobierno incluya alguna categoría adicional. La válvula de escape que deje el legislador para que el Gobierno pueda incluir alguna otra categoría en un momento dado debe, eso sí, establecerse como algo muy excepcional[65].

Ya decía Arnold Wolfers[66] allá por los años cincuenta del siglo pasado que el de seguridad nacional es un concepto ambiguo y que, además, no es uniforme para todos los Estados. «Sabemos —decía Wolfers— más o menos lo que la gente tiene en mente cuando se queja de que su gobierno descuida la seguridad nacional o exige sacrificios excesivos para mejorarla» (Wolfers, 1952: 483); «La seguridad —decía Wolfers— apunta a un mayor grado de protección de valores previamente adquiridos: valores fundamentales, siguiendo a Lippmann» (*idem*). «De hecho, basta con echar un vistazo a la historia para darse cuenta de que la supervivencia ha estado en juego sólo excepcionalmente, sobre todo para las grandes potencias. Si las naciones no estuvieran preocupadas por la protección de valores distintos de su supervivencia como Estados independientes, la mayoría de ellas, la mayor parte del tiempo, no habrían tenido que preocuparse seriamente por su seguridad» (Wolfers, 1952: 488-489). Pero el concepto de seguridad no

64 Tratar de hacer una foto fija de las defensa y seguridad del Estado es prácticamente imposible, aunque recordemos que aquí estamos hablando de establecer categorías en abstracto y que luego el Gobierno y la administración encajen los documentos o soportes cuya revelación pueda dañar la seguridad del Estado dentro de esas categorías. Para Hubert Alcaraz una de las principales dificultades de la noción de secreto es la determinación de lo que debe ser clasificado y lo que no: «se trata de una dificultad ineludible y recurrente, que el Legislador se confiesa impotente para resolver». Para el autor «es dudoso que pueda resolverse esta dificultad de definir lo que es secreto, es decir, de identificar una materia que es por naturaleza secreta y que agota todo el universo de posibilidades». Finaliza con una sentencia: «El secreto es una forma, pero más improbablemente una sustancia» (Alcaraz, 2025).

65 Es verdad que en Estados Unidos se establecen mediante Orden Ejecutiva del Presidente las categorías que pueden ser objeto de clasificación de forma cerrada (vid. Orden Ejecutiva 13526, de 29 de diciembre de 2009), pero también es cierto que el Presidente puede cambiar dicha Orden ejecutiva con rapidez y agilidad e incluir nuevas categorías de forma inmediata, cosa que un Parlamento no puede hacer (carece de esa agilidad que puede ser necesaria en un momento dado); en nuestro país, el Gobierno, como director de la política de seguridad y defensa puede reaccionar con rapidez a la necesidad de incorporar una nueva categoría a la lista (categoría residual), siempre, como se ha dicho, de forma excepcional y respetando los límites que imponga el legislador en la ley a esa facultad.

66 La traducción de los pasajes del artículo de Wolfers es nuestra.

es igual en toda sociedad: La seguridad es un valor del que una nación puede tener más o menos y al que puede aspirar a tener en mayor o menor medida (Wolfers, 1952: 484). Además, no es lo mismo la seguridad en sentido objetivo que la seguridad en sentido subjetivo: «la seguridad, en un sentido objetivo, mide la ausencia de amenazas a los valores adquiridos, en sentido subjetivo, la ausencia de temor a que dichos valores sean atacados». En ambos sentidos, nos movemos de la inseguridad o sensación de inseguridad en un polo, a la seguridad casi total o ausencia de miedo en el otro, dice el autor. «La posible discrepancia entre lo objetivo y lo subjetivo es significativa en las relaciones internacionales» (Wolfers, 1952: 485). Otra razón aún más poderosa —dice Wolfers— por la que hay que esperar que las naciones no actúen de manera uniforme es que no todas ellas, o no de forma constante, se enfrentan al mismo grado de peligro (Wolfers, 1952: 486). Ahora bien, aunque los esfuerzos de seguridad de un Estado tiendan a variar, lo que sí parece ser igual es la gama de valores o intereses para los que se busca protección: con respecto a esta gama —dice Wolfers— puede parecer que existe un grado considerable de uniformidad (Wolfers, 1952: 489). «En todo el mundo los pueblos se sacrifican para proteger y preservar lo que les parece que constituyen los valores nucleares mínimos del Estado, la independencia nacional y la integridad territorial, si bien hay naciones que buscan también la protección de valores más marginales» (Wolfers, 1952: 489). En este sentido es interesante que el legislador haga un esfuerzo por concretar cuáles son los valores e intereses que en nuestro Estado deben quedar protegidos mediante esa herramienta tan específica que es el secreto de Estado, que funcione como marco en el que deba moverse el Gobierno en su política de clasificación. De hecho, como ya habíamos mencionado, en nuestro país existen ya algunas materias que no requieren de clasificación por parte del Gobierno —no es preciso que el Gobierno mediante Acuerdo decida sobre su carácter clasificado— porque ya han sido declaradas secretas por parte del legislador. Es el caso de «las actividades del Centro Nacional de Inteligencia, así como su organización y estructura interna, medios y procedimientos, personal, instalaciones, bases y centros de datos, fuentes de información y las informaciones o datos que puedan conducir al conocimiento de las anteriores materias», clasificadas con el grado de secreto por el legislador en el art. 5 de la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia; lo es también de la Directiva de Inteligencia, que la misma ley clasifica como secreta en su art. 3[67]. Asimismo se clasifican por ley las actuaciones del Magistrado que controla de forma previa la entrada en domicilio y la afectación del secreto de las comunicaciones por parte de los servicios de inteligencia (art. Único, apartado 3º de la Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia), que tienen también la

67 La Directiva de Inteligencia es el instrumento mediante el cual el Gobierno determina y aprueba anualmente los objetivos a perseguir por el Centro Nacional de Inteligencia.

consideración de secretas, o la información relativa a los créditos destinados a los gastos reservados, así como la correspondiente a su utilización efectiva, clasificados por la Ley 11/1995, de 11 de mayo reguladora de la utilización y control de los créditos destinados a los gastos reservados, y, en fin, del Plan Nacional de Protección de Infraestructuras Críticas, los Planes Estratégicos Sectoriales, los Planes de Seguridad del Operador, los Planes de Protección Específicos y los Planes de Apoyo Operativo (Disposición adicional segunda de la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas)[68].

En este punto, resulta interesante hacer una referencia a las categorías de información clasificadas como Alto Secreto (*Top Secret*) o Secreto (*Secret*) en el Reino Unido. En primer lugar, porque se demuestra la viabilidad de establecer categorías que definan con precisión los intereses fundamentales que una sociedad quiere proteger. Aunque en el Reino Unido estas clasificaciones son establecidas por el *Cabinet Office* y no por el Parlamento, cabría considerar que este último podría realizar un ejercicio análogo para definir los intereses esenciales de seguridad y defensa. En segundo lugar, el sistema británico prevé una categoría residual bien definida, que restringe la posibilidad de clasificar información adicional únicamente en casos excepcionales y cuando la materia sea de igual relevancia y riesgo que las categorías predefinidas.

Si comparamos la lista de categorías clasificadas en el Reino Unido con las establecidas en el ALIC o en la LSO observaremos cómo las mismas delimitan de una forma mucho más estricta el daño a la seguridad y defensa del Estado que es preciso que concurra para que una materia sea clasificada[69]. Alto secreto y secreto en el Reino Unido equivaldrían a nuestras categorías de secreto y reservado. La información se clasifica en dichas categorías cuando su descubrimiento accidental o deliberado puede dar lugar a daños graves o muy graves a la seguridad del Estado —nuestra LSO, en su art. 2 se contenta con que la divulgación no autorizada de la materia clasificada pueda «dañar o poner en riesgo la seguridad y defensa del Estado»—; es verdad que en el Reino Unido se establece una tercera categoría, que es la de oficial, que precisamente correspondería con la necesidad que tiene la administración de mantener determinadas cuestiones reservadas[70]. El

68 En Suecia existe una práctica que nos parece bastante acertada. De acuerdo con la Ley de Libertad de Prensa (Freedom of the Press Act) las restricciones del derecho de acceso a la información deben ser especificadas con detalle en la Ley de Acceso a la Información y del Secreto (Public Access to Information and Secrecy) y si bien es posible incluir preceptos restringiendo este derecho en otras leyes, siempre debe hacerse referencia a dichos preceptos en la propia Ley de Acceso a la Información y del Secreto [Sobre la regulación Sueca del Derecho a la Información y del Secreto vid. Cameron, 2025].

69 Es interesante que el lector contraste estas categorías con las que ha ido estableciendo el Gobierno en España mediante Acuerdo del Consejo de Ministros, algunas de ellas sumamente amplias (esto debiera corregirse).

70 La información oficial se definía en el sistema de clasificación británico anterior a 2023 como la información que no suponía una amenaza elevada pero que, de ser difundida, podría tener consecuencias

ALIC, como veremos, llega a clasificar incluso aquella información que perjudica levemente a la seguridad y defensa del Estado o simplemente la contraría.

El Government Security Classifications Policy de 2024 en Reino Unido define la información Secreta como aquella «[i]nformación muy sensible que requiere controles de protección reforzados, (...) adecuados para defenderse de agentes altamente capacitados y decididos y cuya divulgación podría poner en peligro la vida de un individuo o grupo, dañar gravemente la seguridad y/o las relaciones internacionales del Reino Unido, su seguridad/estabilidad financiera o impedir su capacidad para investigar la delincuencia grave y organizada». Esta categoría incluye aquella información cuya filtración accidental o deliberada probablemente[71] resultaría en: a) una amenaza directa para la vida, la libertad o la seguridad de una persona (por parte de agentes capaces de amenazar); b) un perjuicio importante a la capacidad del Reino Unido para planificar eficazmente posibles emergencias o incidentes graves en el futuro; c) impedir la respuesta del Reino Unido a emergencias o incidentes graves; d) graves daños a la eficacia operativa o a la seguridad de las fuerzas del Reino Unido o de sus aliados, de modo que resulte imposible llevar a cabo tareas militares o que las capacidades actuales o futuras, o las instalaciones, queden inutilizadas; e) un daño grave a la reputación internacional del Reino Unido o de un país amigo; f) un daño grave a las relaciones con países amigos, que dé lugar a una protesta o sanción formal; g) daños graves a la seguridad, la protección o la prosperidad del Reino Unido o de naciones amigas al afectar a sus intereses comerciales, económicos y financieros; h) graves daños a la eficacia operativa de operaciones de seguridad o inteligencia de gran valor; i) un perjuicio importante a la capacidad de investigar o perseguir la delincuencia organizada grave; j) un menoscabo grave a la capacidad de combatir (es decir, disuadir, responder, investigar o perseguir) el terrorismo, el espionaje u otras actividades que socaven la seguridad nacional o la democracia parlamentaria del Reino Unido; k) daños graves a la seguridad y resistencia de los

perjudiciales; no era necesario introducir explícitamente una marca en la información oficial (*Government Security Classifications* de mayo de 2018). Esto podríamos pensar que hiciera referencia, entre otros aspectos, al interés de la Administración en actuar conforme al principio de eficacia, que en nuestro sistema se recoge a nivel constitucional en el art. 103 CE. Como reflexión general, no limitada al sistema británico, recordemos que los funcionarios tienen normalmente un deber de confidencialidad, y habría que estudiar cuál es el alcance de dicho deber en comparación con el régimen jurídico aplicable a la información clasificada. Ahora la nueva política clasificatoria británica estima que la información confidencial es «la mayor parte de la información que se crea, procesa, envía o recibe en el sector público y las organizaciones asociadas, que podría causar un daño moderado si se ve comprometida y debe defenderse contra una amplia gama de agentes amenazantes con distintas capacidades mediante controles de protección matizados». Dentro de esta categoría de información oficial en el Reino Unido existe la categoría de información oficial sensible, que debe se etiquetada como oficial-sensible. La nueva política de clasificación establece que la marca sensible debe aplicarse a aquella información OFICIAL «que no está destinada a ser divulgada al público y que es de interés para los actores amenazantes (internos o externos), activistas o medios de comunicación» cuya divulgación «puede causar un daño moderado al trabajo o a la reputación de la organización y/o el Gobierno de Su Majestad».

71 Subrayado nuestro.

activos/recursos de las Infraestructuras Críticas y l) la causación de otro modo de un grave perjuicio a la seguridad nacional del Reino Unido. El interés que se quiera proteger a través de esta categoría residual debería equipararse en cuanto a importancia al resto de los intereses protegidos en la categoría de secreto, como también el nivel de daño causado, que es, como se puede ver, elevado.

La *Government Security Classifications Policy* de 2024 establece, además, una especificación sobre el perfil de amenaza ante la que es preciso defenderse. En el caso de la información Secreta esta debe protegerse frente a amenazas de agentes altamente sofisticados, bien financiados y decididos, más capacitados que los contemplados en el nivel OFICIAL. Entre los posibles actores hostiles se incluyen agentes estatales, ciberdelincuentes patrocinados por gobiernos, grupos de delincuencia organizada y personal que suponga una amenaza interna. Para mitigar estos riesgos, se implementarán controles de seguridad, tecnologías avanzadas y estrategias de defensa contra ataques específicos y dirigidos.

En cuanto a la categoría de Alto Secreto, comprende información excepcionalmente sensible que sustenta directamente la seguridad nacional del Reino Unido y de sus aliados. Su protección requiere medidas de seguridad extremas, dado que actores estatales hostiles pueden intentar comprometerla con recursos avanzados y prolongados en el tiempo. Respecto al perfil de amenaza, en este caso refleja el máximo nivel de capacidad desplegado para intentar comprometerla. Se supone que los actores estatales hostiles darán prioridad a comprometer esta información, utilizando importantes recursos técnicos, financieros y humanos durante largos periodos de tiempo. Pueden desplegarse ataques altamente personalizados y selectivos, combinando fuentes y acciones humanas con ataques técnicos. En fin, el análisis de riesgo señala que se puede tolerar muy poco riesgo para este tipo de información. La *Government Security Classifications Policy* de 2024 indica que se trata de información que, de verse comprometida, accidental o deliberadamente, <u>sería probable</u> que produjera el siguiente resultado (subrayado nuestro): m) provocar la pérdida de vidas humanas; n) un deterioro excepcionalmente grave, a largo plazo o sistémico de la capacidad del Reino Unido para planificar eficazmente posibles emergencias o incidentes graves futuros; o) una amenaza directa a la capacidad del Reino Unido para responder a una emergencia en curso; p) daños excepcionalmente graves a la eficacia o la seguridad del Reino Unido o de las fuerzas aliadas, lo que conduce a la incapacidad de cumplir cualquiera de los Resultados de Defensa del Reino Unido (*UK Defence Outcomes*); q) un aumento de la tensión internacional; r) un daño excepcionalmente grave a las relaciones con naciones amigas o con las que cooperan estrechamente; s) un daño a largo plazo a la economía del Reino Unido; t) una amenaza directa a la seguridad nacional o la estabilidad interna del Reino Unido o de naciones amigas; u) un daño excepcionalmente grave a la eficacia continuada de operaciones de seguridad o inteligencia extremadamente valiosas; v) un perjuicio importante y duradero a la capacidad de investigar o perseguir la delincuencia organizada grave; w) un perjuicio grave y duradero a la capacidad de hacer frente (es decir, disuadir,

responder, investigar o perseguir) al terrorismo, el espionaje u otras actividades que socaven la seguridad nacional o la democracia parlamentaria del Reino Unido y x) la causación de otro modo de un *perjuicio importante y a largo plazo* a la seguridad nacional del Reino Unido (cursiva nuestra). Posteriormente analizaremos el ALIC y veremos que establece categorías mucho más amplias, que no se hace referencia a daños sistemáticos o que duren en el tiempo y que el criterio del daño deja bastante que desear en las categorías más bajas.

1.1.2. El perjuicio a la seguridad o defensa del Estado

Para que una información sea clasificada, debe existir un perjuicio real para la seguridad y defensa del Estado en caso de divulgación no autorizada. En el Reino Unido, el nivel de daño exigido es elevado, mientras que en España, la LSO requiere únicamente que la información pueda *dañar o poner en riesgo* la seguridad del Estado. El riesgo es la contingencia o proximidad del daño (cursiva nuestra)[72]. La regulación de los países de nuestro entorno contrasta con la española. Hay países que exigen criterios más estrictos.

Es preciso puntualizar primero que debe existir una conexión entre la clasificación y un *riesgo real e identificable* de daño a la seguridad del Estado. En Chile, el Consejo de Transparencia, en el ámbito del derecho de acceso a la información, ha señalado que no basta con que la información se relacione con el bien jurídico protegido, sino que es preciso que la divulgación vaya a ocasionar un *daño cierto, probable y especifico* a dicho bien (cursiva nuestra), y que exista proporcionalidad entre los daños que la publicidad provoca a los bienes establecidos en la Ley de Transparencia y el perjuicio que el secreto causa al libre acceso a la información y al principio de publicidad[73]. En Estados Unidos la Orden Ejecutiva 13526, de 29 de diciembre de 2009 establece, en su sección 1.4, que una información no se considerará para su clasificación a menos que pueda esperarse razonablemente que su divulgación no autorizada cause *daños identificables o descriptibles* a la seguridad nacional de conformidad con la sección 1.2 de esta orden[74], y se refiera a alguna de las categorías de información que se mencionan en la Orden[75].

72 Diccionario de la Lengua Española de la R.A.E.: «riesgo», primera acepción.

73 Recogido por el Relator Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos en su informe *Derecho a la información y seguridad nacional* [OEA/Ser.L/V/II; CIDH/RELE/INF.24/2020].

74 La sección 1.2 de dicha Orden establece que la información podrá clasificarse en tres niveles diferentes en función del daño que la divulgación no autorizada pueda causar a la seguridad nacional (*Top Secret* o Alto secreto, Secreto y Confidencial).

75 Estas categorías son las siguientes: (a) planes, sistemas de armas u operaciones militares; (b) información de gobiernos extranjeros; c) actividades de inteligencia (incluida acciones encubiertas), fuentes o métodos de inteligencia o criptología; (d) relaciones exteriores o actividades extranjeras de los Estados Unidos, incluidas fuentes confidenciales; (e) asuntos científicos, tecnológicos o económicos relacionados con la

La exigencia de que exista una conexión entre la clasificación y un riesgo real e identificable de daño a la seguridad del Estado se encuentra también en los textos internacionales. La Observación número 34 del Comité de Derechos Humanos, en este caso en relación con las restricciones a la libertad de expresión, señala que cuando un Estado «haga valer» una razón legítima para restringir la libertad de expresión, deberá demostrar de forma concreta e individualizada la naturaleza precisa de la amenaza y la necesidad y proporcionalidad de la medida concreta que se haya adoptado, en particular estableciendo una conexión directa e inmediata entre la expresión y la amenaza[76]. Por su parte, los Principios de Tshwane, refiriéndose a las restricciones del derecho a la información, indican que para que una restricción pueda considerarse necesaria en una sociedad democrática es preciso, entre otros elementos, que la divulgación de la información represente «*un riesgo real e identificable de perjuicio significativo* para un interés legítimo de seguridad nacional» (cursiva nuestra) (Principio 3 (b) (i)). El riesgo de perjuicio que supondría la divulgación debería superar al interés público de difundir la información (Principio 3 (b) (ii)), debiendo buscarse siempre el medio menos restrictivo disponible para evitar el perjuicio (Principio 3 (b) (iii)).

En cuanto al nivel de daño o perjuicio necesario para poder clasificar una información, veamos qué se dice en algunos ordenamientos de nuestro entorno.

En el Reino Unido las materias secretas cubren aquella información que, de verse comprometida, sería probable que pusiera en peligro la vida (de un individuo o grupo) o *dañara gravemente* la seguridad y/o las relaciones internacionales del Reino Unido, su seguridad/estabilidad financiera o impidiera su capacidad para investigar la delincuencia grave y organizada. Por su parte, el Alto Secreto se aplica a aquella información que probablemente causaría un *daño excepcionalmente grave* a ciertos intereses fundamentales enumerados en una lista que ya conocemos (cursiva nuestra). La distancia entre la existencia de un riesgo o daño para la seguridad del Estado, que es lo que exige la normativa española, y el nivel de daño exigido en Reino Unido es grande; en España no se establece con qué probabilidad se estima que el riesgo desembocará en lo que la técnica aseguradora denomina siniestro, que es cuando el daño materializa[77], ni tampoco se exige que el daño sea de cierta intensidad.

La legislación croata, por su parte, establece que el grado de Alto secreto (*Top Secret*) se utilizará para clasificar la información cuya divulgación no autorizada

seguridad nacional; f) Programas del Gobierno de los Estados Unidos para salvaguardar los materiales o instalaciones nucleares; (g) vulnerabilidades o capacidades de sistemas, instalaciones, infraestructuras, proyectos, planes o servicios de protección relacionados con la seguridad nacional; o (h) el desarrollo, producción o uso de armas de destrucción masiva [sección 1.4 de la Orden Ejecutiva 13526].

76 Comité de Derechos Humanos, Observación General N°34, sobre el derecho a la libertad de opinión y de expresión garantizado en el art. 19 del Pacto Internacional de Derechos Civiles y Políticos, CCPR/C/GC/34, 12 septiembre 2011, Párr. 35.

77 Sobre esta cuestión vid. Sánchez Ferro, 2006: 270-274.

supondría un daño excepcionalmente grave para la seguridad nacional y los intereses vitales del país, y especialmente a los siguientes bienes: base de la estructura de la República establecida por la Constitución, independencia, integridad y seguridad, relaciones internacionales, capacidad de defensa y sistema de inteligencia, seguridad pública, bases del sistema económico y financiero, descubrimientos científicos, inventos y tecnologías de gran importancia para la seguridad nacional (art. 6 del *Data Secrecy Act* de 13 de julio de 2007[78]). El grado de secreto (*Secret*) se utilizará para clasificar la información cuya divulgación no autorizada resultaría en un daño grave a los bienes mencionados en el art. 6 de la Ley. De nuevo nos encontramos con un ordenamiento jurídico que requiere un grado de daño grave o excepcionalmente grave para clasificar una materia como Alto secreto o Secreto. Es verdad que la ley croata añade dos categorías más, confidencial y restringido, y que, en ese sentido, protege cierta información que causa un daño de menor intensidad al daño grave o excepcionalmente grave. Confidencial se utiliza para clasificar la información cuya divulgación no autorizada resulte perjudicial para los bienes a los que se refiere el art. 6 de la Ley y restringido para clasificar la información cuya divulgación no autorizada sea perjudicial para el funcionamiento de las autoridades estatales y las tareas de ejecución de la actividad de las autoridades estatales en materia de defensa, sistema de inteligencia de seguridad, asuntos exteriores, seguridad pública, procedimientos penales y ciencia, tecnología, hacienda pública y economía.

Por su parte en Francia, como ya explicamos, dados los vínculos entre la sanción penal y el sistema de clasificación, los niveles de clasificación se redujeron a dos: la categoría de secreto, aplicable a la información y los medios/objetos cuya divulgación o acceso produzca un daño a la seguridad nacional (aquí no se hace referencia a daño grave) y la categoría de Alto secreto, reservada a la información y los medios u objetos cuya divulgación o acceso tenga consecuencias excepcionalmente graves para la defensa y la seguridad nacional (el único problema es que el Gobierno francés puede cambiar esta regulación cuando quiera, como hemos visto, en tanto que el Código penal refiere la definición del secreto al Consejo de ministros, que aprobará la misma por decreto en Consejo de Estado, así que en el fondo el sistema es menos garantista).

En nuestra opinión, si bien es fundamental resguardar la seguridad del Estado en asuntos sensibles, la clasificación de información, dado el impacto que para una democracia tiene extraer información del debate público, debe justificarse mediante la demostración de que concurre un daño significativo para la seguridad del Estado y un riesgo real e identificable, como dicen los principios de

78 Es el legislador y no el Gobierno el que ha establecido las categorías de clasificación de la información de forma detallada. Vid. https://www.zsis.hr/UserDocsImages/Sigurnost/Security/Data%20Secrecy%20Act.pdf [consultado el 20.12.2024]. *Zakon o tajnosti podataka*, Official Gazette nos.79/2007 and 86/2012, de acuerdo con la información extraída de la sentencia del TEDH Sĕks v. Croatia, sección primera *(Application no. 39325/20)*, sentencia de 3 de mayo de 2022

Tshwane. Esto es especialmente relevante cuando la divulgación no autorizada conlleva sanciones penales, como en nuestro país. En este contexto, resulta adecuado limitar la sanción penal a daños graves o excepcionalmente graves a la seguridad del Estado, siguiendo un enfoque similar al británico[79].

1.1.3. La definición de las materias clasificadas en el Anteproyecto de Ley de Información Clasificada presentado en la XIV Legislatura

El Anteproyecto de Ley de Información Clasificada presentado en la XIV Legislatura intenta detallar las categorías que podrán constituir materia clasificada, en línea con lo que desde el ámbito internacional se dice que constituye una buena práctica en este campo. Sin embargo, al analizar dichas categorías, surge la preocupación de que no siempre se proteja información relacionada con la seguridad y defensa del Estado[80] o verdaderamente sensible para dicha seguridad y defensa del Estado[81]. Por lo demás, el Anteproyecto elimina la referencia al riesgo, aunque incorpora el concepto de peligro, además del de daño a la seguridad o defensa nacionales (vid. art. 1 ALIC). Es preciso acudir a la categorización concreta de los diferentes niveles de clasificación para encontrar el nivel de daño que

79 Otra cuestión, como ya se dijo antes, es la del deber de reserva de los funcionarios, que no se protege necesariamente por sanciones penales y que puede proteger intereses diversos, como la actuación eficaz de la Administración o cuestiones relacionadas con la seguridad del Estado de menor entidad [Vid. sobre el deber de reserva, Sainz Moreno, 1991: 2864; sobre el secreto en el ámbito de la actividad burocrática, vid. Weber, 1977: 92 y Weber: 1984: 179, 717, 744-745]. Habría que estudiar cómo sería el régimen de protección de materias relacionadas con la seguridad del Estado sobre las que existiera un deber de reserva y cuál sería el régimen de acceso de dichas materias desde el punto de vista del derecho de acceso a la información. Quizás en algunos casos podrían recogerse como excepciones al derecho de acceso a la información en la *Ley 9/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno* (LTAIBG), pero no asimilarse a la información clasificada, que tiene sus propios contornos y su sistema de protección.

80 L. Puente manifiesta dicha preocupación, al señalar que no está claro que la «seguridad pública» (concebida como algo distinto de la «seguridad del Estado» y de la «seguridad nacional») quepa en el art. 105 b CE), que dispone 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, la averiguación de los delitos y la intimidad de las personas»). Otro tanto —dice el autor— pasaría, por ejemplo, con aquello que afecte a la «efectividad (…) de los servicios de inteligencia» o a los «intereses económicos o industriales de carácter estratégico». Insiste el autor en que no le cabe duda de que esta información es importante para «los intereses de España». Lo que debe quedar claro es que, en el marco de la información clasificada, «la Constitución no habilita a declarar secreta «información importante para los intereses de España», sino solo aquella que afecte a la seguridad y defensa del Estado» (Puente Rodríguez, 2022: ep. III). Mostraremos nuestra posición en el análisis de cada categoría.

81 Recordemos las palabras del Supremo en las sentencias de los papeles del CESID: «una excepción de la trascendencia de la que hemos descrito [lo que afecte a la seguridad y defensa del Estado] solamente puede moverse en las zonas más altas y sensibles, atinentes a la permanencia del orden constitucional, entendida como un todo regulador y definidor de las sustanciales formas políticas y jurídicas de convivencia ciudadana en el ámbito nacional español, frente a quienes, por medios violentos pretenden atentar contra su subsistencia, mediante ataques a su seguridad interior o exterior» [Vid. por todas, STS de la Sala Tercera de 4 de abril de 1997 (Rec. Núm. 726/1996), Fto. Jco. 7)].

debe sufrir «la seguridad o defensa nacional» o el peligro que debe acechar para activar la protección ofrecida por el sistema. Veamos cuáles son esas categorías recogidas por el ALIC.

El art. 3 (1) ALIC señala que la información podrá clasificarse como Alto secreto, Secreto, Confidencial y Restringido. El art. 3 (2) ALIC establece que la clasificación de «Alto secreto» «se aplicará a la información que precise del más alto grado de protección, toda vez que su revelación no autorizada o utilización indebida pueda dar lugar a una amenaza o perjuicio extremadamente grave para los intereses de España en los siguientes ámbitos: a) La soberanía e integridad territorial; b) El orden constitucional y la seguridad del Estado; c) La seguridad nacional; d) La defensa nacional; e) La seguridad pública y la vida de los ciudadanos; f) La capacidad o la seguridad de las Fuerzas Armadas de España o de sus aliados, o de las Fuerzas y Cuerpos de Seguridad; g) La efectividad o seguridad de las misiones y operaciones de los servicios de inteligencia o de información de España o de sus aliados, o de las Fuerzas y Cuerpos de Seguridad; h) Las relaciones exteriores de España o situaciones de tensión internacional; i) Los intereses económicos o industriales de carácter estratégico; j) Cualquier otro ámbito cuya salvaguarda requiera de la más alta protección». Por su parte el art. 3 (3) ALIC establece que «[l]a clasificación de «Secreto» se aplicará a la información que precise de un alto grado de protección, toda vez que su revelación no autorizada o utilización indebida pueda dar lugar a una amenaza o perjuicio grave para los intereses de España en los mismos ámbitos que los recogidos en el apartado (1), incluyendo también una categoría residual en el apartado j) que reza así: «[c]ualquier otro ámbito cuya salvaguarda requiera de un alto grado de protección». El art. 3 (4) ALIC, por su parte, define la categoría de «Confidencial»: «La clasificación de «Confidencial» se aplicará a la información cuya revelación no autorizada o utilización indebida pueda causar una amenaza o perjuicio leve para los intereses de España en los siguientes ámbitos: a) El efectivo desarrollo de las políticas del Estado o del funcionamiento del sector público; b) Negociaciones políticas o comerciales de España con otros Estados; c) Los intereses económicos o industriales; d) Funcionamiento de los servicios públicos; e) La prevención, detección e investigación de delitos y f) Cualquier otro ámbito que pueda causar una amenaza o perjuicio leve para los intereses de España. Finalmente, la categoría de «Restringido» se aplica «a la información cuya revelación no autorizada o utilización indebida pueda ser contraria a los intereses de España en cualquiera de los ámbitos relacionados en los apartados anteriores» (art. 3 (4) ALIC).

En este punto surge ya una primera preocupación, que tiene que ver con la conexión que existe entre las categorías de clasificación y los tipos penales relativos a la información clasificada. Para empezar, la denominación de dichas categorías cambia, y ello tiene un impacto en los tipos penales. El Anteproyecto establece sanciones administrativas, por cierto, en algunos casos de importe muy elevado, pero no se acuerda de las sanciones penales, salvo para establecer el carácter subsidiario del procedimiento administrativo sancionador respecto del penal

(art. 46 ALIC). El Código Penal, como ya vimos, sanciona con penas de prisión la obtención, falsificación, inutilización o revelación de información clasificada como reservada o secreta, distinguiendo entre actos con o sin intención de favorecer a una potencia extranjera. El ALIC amplía las categorías de clasificación de dos a cuatro, generando incertidumbre sobre su correspondencia con las disposiciones penales vigentes ¿Debería haberse entendido, de haber llegado a término el Anteproyecto y haberse convertido en ley, que el Código penal solo haría referencia a la información secreta y reservada? Es cierto que el ALIC establece en la Disposición Adicional 2ª un cuadro de correspondencias entre las calificaciones del Anteproyecto y las de la LSO, así como otras normas administrativas: Secreto equivaldría en el ALIC a Alto secreto, Reservado a Secreto, Confidencial a Confidencial y Difusión limitada a Restringido[82]. Si la sanción penal se limitara a castigar las conductas que supusieran «una amenaza o perjuicio extremadamente grave a los intereses de España» (relacionados con la seguridad o defensa nacional) —Alto secreto—, o «una amenaza o perjuicio grave para los intereses de España» (relacionados con la seguridad o defensa nacional) —Secreto—, ello se correspondería más con la finalidad última que deben cumplir las normas penales[83]. Si el Código penal protegiera toda la información clasificada por el ALIC se estaría protegiendo información cuya revelación no autorizada o utilización indebida pudiera causar una amenaza o perjuicio leve para los intereses de España (art. 3 (3) ALIC) o la información cuya revelación no autorizada o utilización indebida pudiera ser contraria a los intereses de España, lo que es contrario, valga la redundancia, a la idea de que el código penal debe ser un instrumento de *ultima ratio*[84].

Además, la clasificación de información impacta no solo en el ámbito penal, sino también en el derecho de acceso a la información pública. La LTAIBG prevé un régimen jurídico específico para las materias clasificadas, excluyéndolas de su aplicación[85]. Es lógico que ello sea así en lo que se refiere a las materias

82 Los grados confidencial y difusión limitada no están definidos en la LSO; sí lo están en la norma «NS-04 Seguridad de la Información», de la Autoridad Delegada para la Seguridad de la Información Clasificada, así como en Políticas de Seguridad de Organizaciones Internacionales y Acuerdos para Protección de la Información Clasificada.

83 Puente Rodríguez señala que la pena «puede» resultar excesiva para la revelación de determinadas informaciones que con el Anteproyecto podrían ser clasificadas como «confidencial» o «restringido». Yo creo que no es que pueda resultar excesiva, sino que sencillamente es excesiva. Por lo demás, este autor señala que «[s]i se va a hacer una cuatripartición como la que figura en el Anteproyecto lo adecuado sería (…) que tal división tuviera su reflejo en la regulación penal, castigando únicamente la revelación de informaciones clasificadas como «alto secreto» y «secreto» y no simplemente, como dice hoy el Código penal, «información clasificada» (que comprendería también a la «confidencial» y «restringida»)» (Puente 2022, III); no podemos estar más de acuerdo, como ya hemos puesto de manifiesto en este trabajo.

84 El código penal incluye la referencia a que debe tratarse de información relacionada con la seguridad y defensa del Estado, con lo que algunas de las categorías recogidas en el ALIC no se protegerían por no tener relación alguna con estas.

85 Dice la D.A. 1ª, ap. 2º LTAIBG que «[s]e regirán por su normativa específica, y por esta Ley con carácter supletorio, aquellas materias que tengan previsto un régimen jurídico específico de acceso a la información».

clasificadas como Alto secreto o Secreto, porque se refieren a materias que suponen una amenaza o perjuicio extremadamente grave o grave a los intereses de España, pero no parece lógico excluir las materias Confidenciales y Reservadas de la LTAIBG, en tanto que la revelación no autorizada o utilización indebida de ambas queda limitada a los casos en los que se pueda causar una amenaza o perjuicio leve para los intereses de España o, más genérico aún, ser contraria a los intereses de España. Como ya vimos, el Tribunal Supremo entiende que la potestad del Gobierno para clasificar información, como actividad política, «solamente puede moverse en las zonas más altas y sensibles, atinentes a la permanencia del orden constitucional frente a quienes por medios violentos pretenden atentar contra su subsistencia, mediante ataques a su seguridad interior o exterior» [STS de 4 de abril de 1997 (rec. 726/1996), FJ 7º]. La información clasificada debería responder a estos parámetros. No parece que lo hagan las categorías de información Confidencial o Restringida. Tampoco parece que estemos ante actos políticos o de dirección política, sino más bien ante actos de naturaleza administrativa que deberían sujetarse al régimen de acceso de la LTAIBG y verse sometidos a un control de proporcionalidad como el que se establece en la ley en relación con el derecho de acceso de los ciudadanos a la información administrativa[86].

En fin, volviendo a las materias que el Anteproyecto establece como materias clasificadas, parece que ordenamientos jurídicos como el del Reino Unido, en lo que se refiere a la información clasificada como Alto Secreto o Secreto, o el de EEUU[87] ajustan mejor las categorías materiales que pueden ser objeto de

86 Si la afectación a la seguridad y defensa es leve, como en el caso de la clasificación de confidencial, o simplemente se contrarían esos intereses, como en el caso de la información restringida, nos encontramos ante supuestos que pueden subsumirse tranquilamente en los recogidos en la LTAIBG. El art. 14 LTAIBG ya limita el acceso a la información cuando dicho acceso suponga un perjuicio, lo que incluye, desde luego, un perjuicio leve o el ser contrario a esos intereses —no se sabe, por cierto, en qué consiste esto del ser contrario si ni siquiera produce un perjuicio leve—, para: a) La seguridad nacional, b) La defensa, c) Las relaciones exteriores, d) La seguridad pública, e) La prevención, investigación y sanción de los ilícitos penales, administrativos o disciplinarios, f) La igualdad de las partes en los procesos judiciales y la tutela judicial efectiva, g) Las funciones administrativas de vigilancia, inspección y control, h) Los intereses económicos y comerciales, i) La política económica y monetaria, j) El secreto profesional y la propiedad intelectual e industrial, k) La garantía de la confidencialidad o el secreto requerido en procesos de toma de decisión y l) La protección del medio ambiente. Esta Ley, en línea con lo que establecían los instrumentos internacionales de *soft law*, permite ponderar si concurre un interés público o privado superior que justifique el acceso de los ciudadanos a la información. En efecto, según el art. 14.2 LTAIBG, «[l]a aplicación de los límites será justificada y proporcionada a su objeto y finalidad de protección y atenderá a las circunstancias del caso concreto, especialmente a la concurrencia de un interés público o privado superior que justifique el acceso».

87 La Orden Ejecutiva 13526 de 29 de diciembre de 2009, recordemos, clasifica la información en tres niveles diferentes en función del daño que la divulgación no autorizada pueda causar a la seguridad nacional (Alto secreto, Secreto y Confidencial) La sección 1.4 de dicha Orden establece que la información no se considerará para su clasificación a menos que pueda esperarse razonablemente que su divulgación no autorizada cause daños identificables o descriptibles a la seguridad nacional de conformidad con la sección 1.2 de esta orden, y se refiera a uno o más de las siguientes categorías: (a) planes, sistemas de armas u operaciones militares; (b) información de gobiernos extranjeros; c) actividades de inteligencia (incluida acciones encubiertas), fuentes o métodos de inteligencia o criptología; (d) relaciones exteriores o actividades extranjeras de los

clasificación, siendo menos generosos que el legislador español, lo cual es bueno, si con ello se protege de forma suficiente la seguridad del Estado, dadas las implicaciones que tiene la clasificación en todos los ámbitos (los ya mencionados del Derecho penal o del derecho de acceso a la información pública, pero también en el ejercicio de la jurisdicción, la libertad de información etc.).

Analicemos las categorías de información que pueden ser objeto de clasificación según el ALIC de 2022. El Anteproyecto clasifica aquella información que precise del más alto grado de protección, «toda vez que su revelación no autorizada o utilización indebida dé lugar a una amenaza o perjuicio extremadamente grave para la seguridad y la defensa nacional» (Alto secreto) o aquella información que precise «de un alto grado de protección, toda vez que su revelación no autorizada o utilización indebida dé lugar a una amenaza o perjuicio grave para la seguridad y defensa nacional» (secreto) en los siguientes ámbitos:

1) La soberanía nacional y la integridad territorial (arts. 3.2 a) y 3.3 a) ALIC), así como la protección del orden constitucional (art. 3.2 b) y 3.3 b) ALIC). Estas materias se relacionan con la seguridad y defensa del Estado, aunque la última de las categoría podría, quizás, delimitarse mejor, en línea con lo que señalaba la sentencia del Tribunal Supremo de los «papeles del CESID», limitándola a la protección de la permanencia del orden constitucional;

2) La seguridad del Estado, la seguridad y la defensa nacionales (arts. 3.2 b), c) y d) y 3.3 b), c) y d) ALIC). Estas categorías resultan curiosas, son categorías genéricas que luego parecen desarrollarse en detalle a través de los apartados posteriores, lo cual carece de lógica, dado que la referencia general abarca otras categorías dentro de las ya definidas. Además, los conceptos de seguridad del Estado y seguridad nacional se solapan[88].

3) La «seguridad pública y la vida de los ciudadanos» (arts. 3.2 e) ALIC y 3.3 e) ALIC)[89]. En nuestra opinión, esta categoría debería limitarse a los asuntos relacionados con la seguridad y defensa del Estado y no extenderse a toda la seguridad

Estados Unidos, incluidas fuentes confidenciales; (e) asuntos científicos, tecnológicos o económicos *relacionados con la seguridad nacional* (cursiva nuestra; nos parece esencial que se haga esta referencia a la seguridad nacional en estos ámbitos); f) Programas del Gobierno de los Estados Unidos para salvaguardar los materiales o instalaciones nucleares; (g) vulnerabilidades o capacidades de sistemas, instalaciones, infraestructuras, proyectos, planes o servicios de protección relacionados con la seguridad nacional; o (h) el desarrollo, producción o uso de armas de destrucción masiva.

88 Mientras que anteriormente se hablaba de seguridad del Estado, la influencia de Estados Unidos ha llevado a adoptar el término de seguridad nacional [Vid. Sánchez Ferro, 2006: 221-229]. Hoy en día en la legislación española las únicas categorías definidas por el legislador son las de defensa y seguridad nacionales.

89 Podría considerarse una redacción similar a la del Reino Unido, en donde se protege aquella información cuya revelación no autorizada o uso indebido amenace o dañe de forma extremadamente grave (o grave) y *directa* la vida, libertad o seguridad de un individuo (por parte de actores que tengan una alta capacidad de amenazar dichos intereses) o que tengan relación con la seguridad del Estado y requieran una garantía extremadamente alta de protección porque su revelación accidental o deliberada podría provocar directamente la pérdida generalizada de vidas humanas [cursiva uestra].

pública[90]. Es verdad que la revelación de ciertos datos relacionados con operaciones de lucha contra el terrorismo de origen interno (ej. individuos nacidos en España radicalizados) o externo (ej. terrorismo yihaidista internacional) podrían afectar a la seguridad nacional (vid., entre otras, Estrategia de Seguridad Nacional 2021 (ESN 2021) donde se mencionan estos peligros[91]). El Consejo de Ministros ha clasificado a lo largo de estos años en relación con la seguridad pública únicamente ciertos aspectos destinados a la lucha contra el crimen organizado y el terrorismo, que son los que verdaderamente se relacionan con la preservación de la seguridad nacional. El *Acuerdo de 16 de febrero de 1996* clasificó como secreto la estructura, organización, medios y técnicas operativas utilizadas en la lucha antiterrorista por las Fuerzas y Cuerpos de Seguridad del Estado, así como sus fuentes y cuantas informaciones o datos pudieran revelarlas. El Acuerdo del Consejo de Ministros, de 6 de junio de 2014, hizo lo mismo en relación con el crimen organizado[92].

4) La capacidad o la seguridad de las Fuerzas Armadas de España o de sus Aliados, o de las Fuerzas y Cuerpos de Seguridad (art. 3.2.f) y 3.3.f) ALIC). Estamos, de nuevo, ante una categoría redactada en términos demasiado amplios. Compárese con lo dicho en determinados instrumentos internacionales o en el Derecho comparado:

Los principios de Tshwane contemplan como posible categoría, dentro de las categorías de materias que pueden ser legítimamente clasificadas, la de «los planes, operaciones y capacidades de defensa en curso, durante el tiempo en que la información [sea] de utilidad operativa»; quizás tenga más sentido esta redacción (al proteger esta información se protege ya «la seguridad» de las Fuerzas Armadas o de sus Aliados). En el caso de la Fuerzas y Cuerpos de Seguridad del Estado podrían clasificarse las capacidades que se refieran a la lucha contra el terrorismo o el crimen organizado, durante el tiempo en que la información sea de utilidad operativa, que es lo que se relaciona directamente con la seguridad del Estado.

La Orden Ejecutiva 13526, de 29 de diciembre de 2009, de los Estados Unidos, en su art. 1.4 establece que puede clasificarse la información sobre

90 La seguridad pública se dirige a la protección de las personas individualmente consideradas, al mantenimiento del orden público y de la tranquilidad ciudadana. Conforme al art. 104 CE «[l]as Fuerzas y Cuerpos de seguridad, bajo la dependencia del Gobierno, tendrán como misión proteger el libre ejercicio de los derechos y libertades y garantizar la seguridad ciudadana. Los principios de Siracusa señalan que «[l]a seguridad nacional no puede invocarse como motivo para imponer limitaciones destinadas a prevenir amenazas meramente locales o relativamente aisladas contra el orden público» [Principio 30 de Siracusa].

91 Estrategia de Seguridad Nacional 2021 | DSN (presidencia del Gobierno).

92 El Acuerdo no se había publicado, algo que es absolutamente reprobable porque los ciudadanos tienen derecho a conocer qué materias están excluidas del conocimiento público, como tampoco lo había sido el Acuerdo de 2010. Fue a raíz de la Resolución de 30 de octubre de 2017, del Consejo de Transparencia y Buen Gobierno (núm. de expediente 001-016224) ante una solicitud de acceso a la información cuando el Ministerio del Interior facilitó el texto completo del Acuerdo que dice así: «Se otorga, con carácter genérico, la clasificación de secreto a la estructura, organización, medios y técnicas operativas utilizados en la lucha contra la delincuencia organizada por las Fuerzas y Cuerpos de Seguridad del Estado, así como sus fuentes y cuantas informaciones o datos puedan revelarlas».

«vulnerabilidades o capacidades de sistemas, instalaciones, infraestructuras, proyectos, planes o servicios de protección relacionados con la seguridad nacional», siempre que pueda esperarse razonablemente que su divulgación no autorizada cause daños identificables o descriptibles a la seguridad nacional (añadiríamos nosotros que el grado del daño debiera ser grave o excepcionalmente grave).

La normativa del Reino Unido hace referencia a la eficacia operativa (más que a las capacidades) y a la seguridad de las fuerzas del Reino Unido o de sus aliados, pero de forma más restrictiva que el ALIC y, por tanto, más adecuada. Se clasifica en la categoría de Secreto la información que si se viera comprometida accidental o deliberadamente probablemente resultaría en graves daños a la eficacia operativa o a la seguridad de las fuerzas del Reino Unido o de sus aliados, de modo que en el desempeño de las tareas militares: i. La capacidad actual o futura quedaría inutilizada; ii. Se perderían vidas o iii. Se causarían daños a las instalaciones que quedarían inutilizadas; y en la de Alto secreto la que probablemente resultaría en daños excepcionalmente graves a la eficacia o la seguridad del Reino Unido o de las fuerzas aliadas, lo que conduciría a la incapacidad de cumplir cualquiera de los Resultados de Defensa del Reino Unido.

5) La efectividad o seguridad de las misiones y operaciones de los servicios de inteligencia o de información de España o de sus aliados, o de las Fuerzas y Cuerpos de Seguridad (arts. 3.2.g) y 3.3.g) ALIC)[93]. Esta categoría también es demasiado amplia; piénsese en las numerosas misiones y operaciones que pueden llevar a cabo las Fuerzas y Cuerpos de Seguridad. Creo que es mucho más ajustada la regulación británica, que clasifica como *Secreto* la información que si se viera comprometida accidental o deliberadamente probablemente resultaría en 1) graves daños a la eficacia operativa de operaciones de seguridad o inteligencia de gran valor, 2) un perjuicio importante a la capacidad de investigar o perseguir la delincuencia organizada grave o 3) un menoscabo grave de la capacidad de combatir (es decir, disuadir, responder, investigar o perseguir) el terrorismo, el espionaje u otras actividades que socaven la seguridad nacional o la democracia parlamentaria del Reino Unido y como *Alto secreto* la información que si se viera comprometida accidental o deliberadamente probablemente resultaría en 1) un daño excepcionalmente grave a la eficacia continuada de operaciones de seguridad o inteligencia extremadamente valiosas; 2) un perjuicio importante y duradero a la capacidad de investigar o perseguir la delincuencia organizada grave o 3) un perjuicio grave y duradero a la capacidad de hacer frente (es decir, disuadir,

93 Recordemos que la L*ey 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia* clasifica en su art. 5.1 las «actividades del Centro Nacional de Inteligencia, así como su organización y estructura interna, medios y procedimientos, personal, instalaciones, bases y centros de datos, fuentes de información y las informaciones o datos que puedan conducir al conocimiento de las anteriores materias» y lo hace con la calificación de secreto y que el *Acuerdo de 28 de noviembre de 1986* clasificó como secreto la estructura, organización, medios y procedimientos operativos específicos de los servicios de información, así como sus fuentes y cuantas informaciones o datos pudieran revelarlos.

responder, investigar o perseguir) al terrorismo, el espionaje u otras actividades que socaven la seguridad nacional o la democracia parlamentaria del Reino Unido (vid epígrafe V, apdo. 1.1.1 de este trabajo)[94].

6) Las relaciones exteriores de España o situaciones de tensión internacional (3.2.h) y 3.3 h) ALIC). La redacción no es muy afortunada en lo que se refiere a que se dé un perjuicio grave o extremadamente grave para las situaciones de tensión internacional. Comparemos con la regulación británica. En el Reino Unido lo que se dice es que se podrá clasificar como Alto secreto la información que, si se viera comprometida de forma accidental o deliberada, probablemente resultaría en un incremento de la tensión internacional [*Government Security Classifications Policy,* 2024, Alto secreto, categoría q)]. Esta redacción parece tener más sentido. En lo que respecta a las relaciones internacionales, el ALIC establece que se protegerá la información sobre las relaciones exteriores de España cuando su divulgación o uso indebido suponga una amenaza grave o extremadamente grave a las mismas. Parece que el grado de daño que se requiere podría dar lugar, efectivamente, a un grave daño a la seguridad del Estado al poder quedar comprometidas las relaciones exteriores y, por lo tanto, la cooperación con otros países en materia de seguridad, tan necesaria en un mundo globalizado. Lo que no cabría en un Estado democrático es una exclusión redactada en unos términos tan amplios como la recogida en el Acuerdo del Consejo de Ministros de 15 de octubre de 2010, sobre la política de seguridad del Ministerio de Asuntos Exteriores. No puede excluirse del conocimiento público todo lo que pueda dañar de alguna manera las relaciones exteriores de España porque ello sería contrario al derecho de acceso a la información, ya que convertiría la excepción en la regla, y a otros derechos, como el derecho a la investigación científica.

La regulación británica es, de nuevo, algo más concreta a la hora de regular esta categoría. En dicha regulación se dice que se considerará Alto secreto la información que, si se viera comprometida de forma accidental o deliberada, probablemente resultaría en un daño excepcionalmente grave a las relaciones con naciones amigas o con las que cooperan estrechamente. La información que, si se viera comprometida de forma accidental o deliberada, probablemente resultaría en un daño grave a la reputación internacional del Reino Unido o de un país amigo o en un perjuicio grave a las relaciones con países amigos, que dé lugar a una protesta formal o sanción, se califica como secreta. En relación con esto último, parece mejor opción que la reputación del país o de un país amigo o las relaciones con estos se protejan a través de la ley que regula el derecho de acceso a la información, como nuestra LTAIBG, en lugar de a través del régimen

94 Los estándares internacionales a los que hicimos referencia *supra* entienden que no debería clasificarse el número de solicitudes de vigilancia aprobadas y rechazadas, los proveedores de servicios que colaboran con las autoridades en la vigilancia, el tipo de investigación y sus propósitos, la información disponible sobre el número de individuos y el número de comunicaciones intervenidas, además de si se ha llevado a cabo alguna monitorización sin autorización o de forma ilegal.

jurídico de las materias clasificadas. Recordemos que esta ley, en su art. 14, limita el acceso de los ciudadanos a la información que suponga un perjuicio para las relaciones exteriores. Esta ley permite a las autoridades administrativas independientes y a los jueces evaluar ese perjuicio ponderándolo con el interés público y del público a saber, y creo que esa es la vía correcta a seguir en estos casos.

7) Los intereses económicos o industriales de carácter estratégico (art. 3.2 (i) y 3.3 (i) ALIC). Creemos que aquí debiera haberse añadido una coletilla: intereses económicos o industriales de carácter estratégico cuya revelación suponga un daño grave o extremadamente grave a la seguridad del Estado[95]. Y es que no toda perturbación de un sector estratégico necesariamente producirá un perjuicio a la seguridad nacional; pensemos en el turismo[96]. En países de nuestro entorno encontramos regulaciones que sí hacen referencia a la seguridad y defensa del Estado en este campo. En Croacia, por ejemplo, el art. 6 del *Data Secrecy Act* dispone que tendrá la clasificación de alto secreto aquella información cuya divulgación no autorizada pueda resultar en un daño irreparable a la seguridad nacional y a los intereses vitales de la República de Croacia, y en especial, entre otros bienes, a los fundamentos del sistema económico y financiero de la República de Croacia. Además, esta norma incluye también un apartado relativo a los descubrimientos científicos, invenciones y tecnologías que son de gran importancia para la seguridad nacional de la República de Croacia. En México se protege la información cuya revelación o uso indebido pueda suponer un daño grave o extremadamente grave a la política monetaria, cambiaria o del sistema financiero del país o pueda poner en riesgo grave o muy grave la estabilidad de las instituciones financieras susceptibles de causar un riesgo sistémico o del sistema financiero del país. Como se puede observar, se circunscribe mucho más la información que puede ser clasificada.

El art. 3.4 c) ALIC, por su parte, hace referencia a los intereses económicos e industriales, sin siquiera hacer referencia a que sean sectores estratégicos —este artículo señala que la clasificación de «Confidencial» se aplicará a la información cuya revelación no autorizada o utilización indebida pueda causar una amenaza o perjuicio leve para los intereses económicos e industriales—. Pues bien, si esos intereses no están relacionados con el sector de la seguridad y defensa no deberían incluirse en un sistema como el que los británicos llaman *Security Classifications*

95 La Orden Ejecutiva 13526 de EEUU hace referencia a los asuntos científicos, tecnológicos o económicos *relacionados con la seguridad nacional* (cursiva nuestra). La conexión con la seguridad nacional es imprescindible. Por lo demás, es importante, desde el punto de vista de la seguridad, como se indica, por ejemplo, en la ESN 2021, protegerse frente a posibles injerencias de terceros en el dominio de las infraestructuras digitales, como los centros de procesamiento de datos o los cables submarinos, o los activos que sustentan la propiedad intelectual e industrial del sector empresarial, pues determinados ataques a estos centros de procesamiento etc. podrían dañar la seguridad del Estado [Estrategia de Seguridad Nacional 2021 | DSN (presidencia del Gobierno)].

96 Diferente sería el caso de otros sectores estratégicos como el financiero, las telecomunicaciones, la energía, o los carburantes.

Policy, no debería formar parte del sistema de información clasificada y, menos aun, siendo el daño que se espera leve; otra cosa, como decíamos, es que exista un deber de reserva sobre determinados aspectos de la política industrial y económica, que se proteja **vía deber de reserva,** al que se aplicará, en todo caso, un régimen jurídico diferente (para empezar tal información no estaría sometida a períodos de clasificación tan largos como en el ALIC).

Además, el ALIC clasifica como Confidencial «la información cuya revelación no autorizada o utilización indebida pueda causar una amenaza o perjuicio leve para los intereses de España en los siguientes ámbitos» (art. 3.4 ALIC): a) El efectivo desarrollo de las políticas del Estado o del funcionamiento del sector público; b) Negociaciones políticas o comerciales de España con otros Estados; c) Los intereses económicos o industriales ya mencionados d) Funcionamiento de los servicios públicos. e) La prevención, detección e investigación de delitos. f) Cualquier otro ámbito que pueda causar una amenaza o perjuicio leve para los intereses de España. Esta categoría de información —Confidencial— debería, en nuestra opinión, desaparecer del sistema de clasificación relacionado con la seguridad del Estado, siendo la regulación aplicable en estos casos la contenida en la LTAIBG, que es verdad que no contempla todos estos intereses, pero porque algunos no se consideran dignos de constituirse en límite al acceso de los ciudadanos a la información administrativa[97].

En fin, en relación con el art. 5 ALIC, coincido con lo dicho en el *Informe del Consejo de Transparencia y Buen Gobierno*. Dice el Consejo de Transparencia en su informe que «en relación con los supuestos en los que la información se puede clasificar en la categoría de «Restringido», [es en el que se alcanza un mayor grado de amplitud e indeterminación, pues] además de prever [el Anteproyecto] un presupuesto habilitante muy genérico (que la revelación no autorizada o utilización indebida de la información «pueda ser contraria» a los intereses de España), su aplicación se extiende a «cualquiera de los ámbitos relacionados en los apartados anteriores», los cuales, como hemos expuesto, no sólo abarcan áreas

97 El art. 14 LTAIBG limita el derecho de acceso a la información cuando dicho acceso suponga un perjuicio para la garantía de confidencialidad o el secreto requerido en procesos de toma de decisión (art. 14 h), los intereses económicos y comerciales (art. 14 h), la política económica y monetaria (art. 14 i), la prevención, investigación y sanción de los ilícitos penales, administrativos o disciplinarios (art. 14 e) y, por lo que se refiere al funcionamiento de los servicios públicos, se limita el derecho de acceso respecto de las funciones administrativas de vigilancia, inspección y control (art. 14 g) o la seguridad pública (art. 14 d). La protección a través de la LTAIBG implica que cualquiera persona podrá solicitar el acceso a dicha información (art. 12 LTAIBG), que su aplicación como límites al derecho de acceso a la información deberá ser «justificada y proporcionada a su objeto y finalidad de protección y atenderá a las circunstancias del caso concreto, especialmente a la concurrencia de un interés público o privado superior que justifique el acceso» (art. 14 2 LTAIBG) y que, tras una resolución motivada por parte del sujeto competente, la resolución podrá ser impugnada ante el Consejo de Transparencia y Buen Gobierno con carácter potestativo (art. 24 LTAIBG), antes de tener que acudir a la jurisdicción contencioso-administrativa. Consideramos que este régimen de protección es suficiente No vamos a entrar a analizar la LTAIBG y los supuestos que se incorporan como límites porque no es el objeto de este trabajo.

ajenas a la seguridad y la defensa nacional, sino que contienen cláusulas generales de apertura indeterminada» [Consejo de Transparencia y Buen Gobierno, 2022]. Para clasificar una información como Restringida basta con que el uso indebido o el acceso no autorizado sea «contrario» a dichos intereses tan ampliamente definidos; este «contrario», ligado a que ya hay una categoría que se refiere a los daños leves -la categoría de confidencial-, conduce a entender que la difusión en el caso de reservado ni siquiera produce un daño leve a la seguridad y defensa del Estado, lo que implica una sobreprotección de la información que va más allá de lo deseable en un Estado democrático de Derecho, en el que la publicidad debe ser la norma y el secreto la excepción[98].

Por lo demás, el ALIC no incluye ninguna salvaguarda que requiera que el daño sea identificable y descriptible, algo que es, sin duda, criticable.

1.2. *La definición negativa de las materias clasificadas*

La seguridad y defensa del Estado es un concepto intrínsecamente vinculado al ordenamiento jurídico y a la protección de los valores fundacionales de la comunidad. En un Estado democrático de Derecho, los derechos fundamentales son esenciales, y los poderes públicos están sometidos a la legalidad (art. 9 CE)[99]. La seguridad del Estado no debe oponerse a estos derechos, sino garantizar su protección (vid. Sánchez Ferro, 2006: XXXIV-XXXVI). Ben Emmerson, Relator Especial sobre la promoción y protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo de Naciones Unidas, manifestaba en su Informe de abril de 2017 que «entre las consideraciones de seguridad nacional legítimas no figuran las actividades y los intereses del gobierno que constituyan delitos graves conforme al derecho internacional de los derechos humanos, y mucho menos las políticas cuyo fin sea precisamente eludir el cumplimiento de dicho derecho»[100]. Además, Emerson ponía de manifiesto en su informe que

98 Dice L. Puente que «se puede afirmar sin temor a equivocación que solo una parte de lo que con el Anteproyecto podría ser considerado «alto secreto» o «secreto» podría merecer un tratamiento análogo con la legislación hoy vigente. En las dos categorías siguientes, sin embargo, la cosa es distinta: nada de lo que con el Anteproyecto podría clasificarse como «confidencial» o «restringido» puede ser sustraído a la opinión pública con la Ley 9/1968» (Puente Rodríguez, 2022: ep. III).

99 En el caso del Centro Nacional de Inteligencia, el art. 2 de la Ley 11/2002, de 7 de mayo, reguladora del CNI, dispone que este organismo se regirá por el principio de sometimiento al ordenamiento jurídico.

100 Ben Emerson proseguía diciendo que «[e]n el asunto El-Masri, el Tribunal Europeo de Derechos Humanos señaló que el Gobierno de los Estados Unidos de América había reivindicado una interpretación injustificadamente amplia de la noción de secreto de Estado en los procesos judiciales celebrados en su territorio en relación con este asunto, y que ese mismo enfoque había llevado a las autoridades de la ex República Yugoslava de Macedonia a ocultar la verdad». «En el contexto del programa de detenciones secretas, entregas y torturas operado por la CIA de la era Bush, el Tribunal concluyó, de manera acertada —prosigue Emerson—, que la noción de «secreto de Estado» a menudo se esgrime para impedir la búsqueda de la verdad»

«América del Sur tiene un largo historial de este tipo de fenómenos, que constituyen un grave abuso de poder público. Allí se han esgrimido con frecuencia consideraciones de seguridad nacional para tratar de impedir el control judicial de violaciones sistemáticas de los derechos humanos. Gracias a su amplia experiencia en este tipo de casos, la Corte Interamericana de Derechos Humanos —proseguía Emerson— ha desarrollado una sólida respuesta, en la que sostiene que los poderes públicos «no pueden escudarse tras el manto protector del secreto de Estado para evitar o dificultar la investigación de [actos] ilícitos atribuidos a los miembros de sus propios órganos»[101]. La Corte —prosigue Emerson—, ha sostenido que, en esos casos, el intento de impedir la revelación de información alegando motivos de seguridad nacional «puede ser considerado (...) un intento de privilegiar la «clandestinidad del Ejecutivo» y perpetuar la impunidad»[102]. En este sentido, no son pocos los instrumentos internacionales u ordenamientos extranjeros que prohíben la clasificación de determinada información relativa a la violación de los derechos humanos. Comencemos nuestro análisis por el Derecho comparado.

Tanto Italia como Alemania han incluido en su ordenamiento jurídico una definición negativa del secreto de Estado. En Italia, el art. 39.11 de la Ley 124/2007, de 13 agosto 2007 —*Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto*— impide ocultar bajo el manto del secreto de Estado delitos de terrorismo, de subversión del orden constitucional, y otros delitos graves (como devastación, asociación mafiosa, etc.) (Vedaschi, 2025)[103]. En el ordenamiento alemán no se consideran secretos de Estado las informaciones sobre hechos contrarios a los fundamentos del Estado libre y democrático (§ 93 Código penal) [Sánchez Ferro, 2006: 274 y ss].

Al otro lado del Atlántico, Uruguay establece que no pueden oponerse los límites aplicables al derecho de acceso a la información, entre los que se

[Informe del Relator Especial sobre la promoción y protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo, Ben Emerson. Principios marco para garantizar la rendición de cuentas de los funcionarios públicos por las violaciones manifiestas o sistemáticas de los derechos humanos cometidas en el transcurso de iniciativas de lucha contra el terrorismo respaldadas por los Estados [A/HRC/22/52, 23 de abril de 2017], párr. 39].

101 *Ibidem,* párr. 40. Las sentencias más relevantes de la Corte Iberoamericana de Derechos Humanos en este punto son el caso Myrna Mack Chang vs. Guatemala, Sentencia de 25 de noviembre de 2003 y el caso Gomes Lund y otros («Guerrilha do Araguaia») vs. Brasil, de 24 de noviembre de 2010. En el caso Gomes Lund y otros contra Brasil, la Corte afirmó que «en casos de violaciones de derechos humanos, las autoridades estatales no se pueden amparar en mecanismos como el secreto de Estado o la confidencialidad de la información, o en razones de interés público o seguridad nacional, para dejar de aportar la información requerida por las autoridades judiciales o administrativas encargadas de la investigación o proceso pendientes» (caso Gomes Lund y otros («Guerrilha do Araguaia») vs. Brasil, de 24 de noviembre de 2010, párr. 202; en el mismo sentido, caso Myrna Mack Chang vs. Guatemala, Sentencia de 25 de noviembre de 2003, párr. 180.

102 A/HRC/22/52, 23 de abril de 2017, párr. 40.

103 La ley anterior a esta, la Ley de 24 de octubre de 1977, n. 801 (*Istituzione e ordinamento dei servizi per le informazioni e la sicurezza e disciplina del segreto di Stato*) ya excluía del ámbito protegido por el secreto de Estado aquellas informaciones sobre actos de destrucción del orden constitucional (*fatti eversivi dell'ordine costituzionale*) [Sánchez Ferro, 2006: 274].

encuentra la seguridad nacional, en los casos de información relativa a violaciones de derechos humanos o información relevante para investigar, prevenir o evitar violaciones de los mismos (art. 12 de la Ley N° 18381, Ley de Derecho de Acceso a la Información Pública). Argentina, por su parte, en la Ley 27275, Ley de Derecho de Acceso a la Información Pública, de 29 de septiembre de 2016, dispone que las excepciones al derecho de acceso, entre las que se encuentra la información expresamente clasificada como reservada, confidencial o secreta por razones de defensa o política exterior (art. 8 a)), no serán aplicables en caso de graves violaciones de derechos humanos, genocidio, crímenes de guerra o delitos de lesa humanidad (art. 8 Ley 27275). Colombia, en su Ley 1712, de 2014, de Transparencia y del Derecho a la Información Pública Nacional, señala que las excepciones que la ley establece respecto del acceso a la información, «no aplican en caso de violación de derechos humanos o delitos de lesa humanidad» y que en todo caso deben protegerse los derechos de las víctimas de dichas violaciones (art. 21). Por lo que atañe a México, el art. 115 de su Ley General de Transparencia y Acceso a la Información Pública, de 4 de mayo de 2015, establece que no podrá invocarse el carácter reservado cuando (I) Se trate de violaciones graves de derechos humanos o delitos de lesa humanidad, o (II) Se trate de información relacionada con actos de corrupción de acuerdo con las leyes aplicables[104]. El art. 112 de la Ley Federal de Transparencia y Acceso a la Información Pública de 9 de mayo de 2016 establece exactamente lo mismo. La justicia mejicana, sobre la base del mencionado art. 115 (II) de la Ley General de Transparencia y Acceso a la Información Pública, otorgó a un ciudadano el derecho a acceder a la información sobre la adquisición y características del software *Pegasus* El Juez del Octavo Distrito en Materia Administrativa en la Ciudad de México mantuvo en su sentencia que existían indicios que permitían inferir actos de corrupción porque se podía establecer «*prima facie* que el software Pegasus no se utilizó de forma primordial para salvaguardar la «seguridad nacional» sino que también fue utilizada como un arma política en contra de periodistas, políticos y ciudadanos comunes, es decir, en forma preliminar como un desvío de poder en la actuación del Estado»[105].

A través de la Plataforma Nacional de Transparencia, la organización R3D (Red en Defensa de los Derechos Digitales) solicitó la versión pública de «cualquier documento relacionado con la contratación de cualquier software, licencia o herramienta tecnológica desarrollada por la firma NSO Group o por alguna de sus filiales y/o subsidiarias incluyendo versión publica de los contratos

104 Sobre el derecho de acceso a la información en México y el sistema de clasificación mexicano, puede consultarse Carranza Galaico, 2024.

105 Juez del Octavo de Distrito en Materia Administrativa en la Ciudad de México. Sentencia en el juicio de amparo 592/2018 de 13 de diciembre de 2018. Disponible para consulta en: https://es.scribd.com/document/395959163/Sentencia-Pegasus [Informe CIDH/RELE/INF.24/20, ap. 125].

correspondientes»[106]. El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) «ordenó a la Procuraduría General (PGR) entregar una versión pública de un contrato celebrado en 2014» y «consideró que las especificaciones técnicas del software y los métodos de operatividad debían ser clasificados como reservados» y que «se debían proteger los «[n]ombres, cargos y firmas de aquellas personas físicas que participaron en la contratación y que [tenían] conocimiento privilegiado, concreto y específico sobre [los] procedimientos relacionados, métodos especificaciones técnicas, tecnología y equipo que se utilizan para la generación de inteligencia»»[107]. El juez del Octavo Distrito en Materia Administrativa de Ciudad de México invalidó la resolución de la INAI y -según resumen de la resolución hecho por la Relatoría Especial para la Libertad de Expresión de dicha sentencia- «estableció que «[l]a resolución del INAI que determinó reservar con base en el argumento de «seguridad nacional» las especificaciones técnicas y los métodos de operatividad del software Pegasus [era] inconstitucional, toda vez que el INAI pasó inadvertido que la información relacionada con violaciones graves a derechos humanos y con actos de corrupción no debe clasificarse como información reservada» [pues la herramienta se había utilizado para espiar a periodistas, defensores de los derechos humanos, abogados y políticos, según consta en la página 21 del informe del Relator Especial]. Asimismo, indicó que «[l]a relevancia de la información solicitada permitiría contar con mayores elementos para saber si las instituciones, los recursos públicos y el aparato estatal en general se [utilizaban] para fines claramente ilegítimos como lo es hackear a ciudadanos comunes para obtener toda su información privada sin autorización judicial». Por otro lado, subrayó que «en un Estado constitucional el concepto de seguridad nacional equivale a seguridad de los integrantes de la sociedad y protección legítima de las instituciones democráticas». [Juez Octavo de Distrito en Materia Administrativa en la Ciudad de México. Sentencia en el juicio de amparo 592/2018 de 13 de diciembre de 2018].

No cabe duda de que la decisión del juez mejicano es de gran interés.

En lo relativo a los instrumentos internacionales, la Asamblea Parlamentaria del Consejo de Europa considera la lucha contra la impunidad de los autores de graves violaciones de derechos humanos una prioridad del Consejo de Europa (Resolución 1675 (2009) *State of human rights in Europe: the need to eradicate impunity*, párr.6)[108]. La mencionada Asamblea Parlamentaria entiende que una forma de luchar contra la impunidad es garantizar que el secreto de Estado y las inmunidades no impidan «investigaciones efectivas, independientes e imparciales

106 Derecho a la información y seguridad nacional : El acceso a la información de interés público frente a la excepción de seguridad nacional / Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos, OEA/Ser.L/V/II CIDH/RELE/INF.24/20, p. 21 y nota 116.

107 OEA/Ser.L/V/II CIDH/RELE/INF.24/20, p.22.

108 En el mismo sentido, Recomendacion 1876 (2009) de la Asamblea del Consejo de Europa: State of human rights in Europe: the need to eradicate impunity*, 24 de junio de 2009 (22nd Sitting)*, párr. 1.

sobre graves violaciones de derechos humanos, -incluidas las relacionadas con detenciones secretas y traslados interestatales ilegales de personas que han tenido lugar en Europa y que los responsables rindan cuentas-» (Resolución 1675, 2009: párr.9.2)[109]. Por lo demás, la Asamblea considera que la responsabilidad de los agentes estatales que hayan cometido graves violaciones de derechos humanos, como asesinatos, desapariciones forzadas, tortura o secuestros, no merece ser protegida por el secreto de Estado[110]. Esto no es de extrañar; la Asamblea, recordando los Principios de Siracusa sobre las Disposiciones de Limitación y Derogación del Pacto Internacional de Derechos Civiles y Políticos, «confirma firmemente que la violación sistemática de los derechos humanos socava la seguridad nacional y puede poner en peligro la paz y la seguridad internacionales», y que el «Estado responsable de dicha violación no podrá invocar la seguridad nacional como justificación» (Resolución 1954 (2013), *National security and access to information*, párr. 4). En definitiva, las vulneraciones graves de derechos humanos no merecen la protección del secreto (*idem*, párr. 5).

Según el Comité de Ministros del Consejo de Europa, ««violaciones graves de los derechos humanos» se refiere a aquellos actos respecto de los cuales los Estados tienen la obligación, en virtud del Convenio y a la luz de la jurisprudencia del Tribunal, de promulgar disposiciones de Derecho penal. Tales obligaciones surgen en el contexto del derecho a la vida (art. 2 del Convenio), la prohibición de la tortura y las penas o tratos inhumanos o degradantes (art. 3 del Convenio), la prohibición del trabajo forzoso y la esclavitud (art. 4 del Convenio) y en relación con determinados aspectos del derecho a la libertad y la seguridad (art. 5, apartado 1, del Convenio) y del derecho al respeto de la vida privada y familiar (art. 8 del Convenio). No todas las violaciones de estos artículos alcanzarán necesariamente este umbral»[111].

Los principios de Tshwane[112] inciden en que en ninguna circunstancia pueden protegerse las violaciones graves de los derechos humanos o las violaciones serias de Derecho internacional humanitario[113], incluyendo los delitos de Derecho internacional y aquellas vulneraciones sistemáticas o extendidas del derecho

109 En el mismo sentido, Recomendacion 1876, 2009: párr. 2.2.

110 Asamblea Parlamentaria del Consejo de Europa. Resolución 1838 (2011), Abuse of state secrecy and national security: obstacles to parliamentary and judicial scrutiny of human rights violations, párr. 4. Sobre este tema de la responsabilidad de los agentes que han cometido graves violaciones de derechos humanos en el particular contexto italiano vid. Vedaschi, 2025.

111 Vid, *Guidelines of the Committee of Ministers of the Council of Europe on eradicating impunity for serious human rights violations (Adopted by the Committee of Ministers on 30 March 2011 at the 1110th meeting of the Ministers' Deputies),* párr. II. ap. 3.

112 Precisamente la ya mencionada Resolución 1954 (2013), en su párrafo 7, hace una mención a los principios de Tshwane, dando la bienvenida a su adopción.

113 Sobre esto, el Principio 10 (6) establece que no puede quedar cubierto por el secreto la descripción completa de los actos u omisiones que constituyen las violaciones graves del derecho internacional humanitario o de los derechos humanos, así como las fechas y circunstancias en que ocurrieron y la ubicación de cualquier persona desaparecida o de sus restos mortales, ni las identidades de las víctimas, si es compatible con el

a la seguridad y libertad[114], alegando razones de seguridad nacional, dado que, en estos casos, se dice, el interés público en el acceso a la información es predominante (Principio 10 A (1) Tshwane). Además, estos principios establecen una fuerte presunción (*high presumption*) a favor de la divulgación de la información que esté relacionada con otras vulneraciones de derechos humanos o del Derecho humanitario (Principio 10 A (2)).

Ciertamente, la prohibición de excluir del secreto determinada información sobre vulneraciones de derechos humanos no es exactamente igual en todos los ordenamientos jurídicos, pero en todos ellos existe al menos un núcleo excluido coincidente, las violaciones graves de derechos humanos. Creo que la ley española debería considerar seriamente, como algo imperativo, incluir una definición negativa del secreto de Estado que evitara que el secreto se utilizara para cubrir determinados hechos contrarios al ordenamiento jurídico excepcionalmente graves (entre ellos dicha vulneración grave de derechos humanos). Decía Dick Marty, relator de la Asamblea del Consejo de Europa, que en el marco del Consejo de Europa, más allá de llegar a un consenso sobre lo que pudiera ser calificado como secreto de Estado, era importante acordar una definición de lo que no podía constituir un secreto de Estado legítimo, esto es, introducir una definición negativa del secreto de Estado (Marty, 2011: Párr. 5). Pues bien, coincidimos en que la definición negativa del secreto de Estado es algo que no debemos pasar por alto, y ni la LSO ni el ALIC contienen una definición en este sentido.

VI. CONCLUSIÓN

La protección de la información clasificada en el ordenamiento jurídico español plantea, como hemos visto, importantes desafíos. Por un lado, resulta imperativo actualizar una normativa obsoleta, como la Ley de Secretos Oficiales de 1968, que fue concebida en un contexto preconstitucional y que no satisface las exigencias de transparencia propias de una sociedad avanzada. Por otro lado, el proceso de reforma debe garantizar un equilibrio adecuado entre la necesaria protección de la seguridad del Estado y el principio constitucional de publicidad,

derecho a la privacidad y otros derechos de las víctimas, sus familiares y testigos. Se considera buena práctica en este caso publicar los datos desagregados o anonimizados.

114 En relación con el derecho a la seguridad y libertad, el Principio 10 B Tshwane establece que no debería constituir un secreto «[l]a ubicación de todos los sitios donde se mantiene a personas privadas de su libertad y que sean administrados por el Estado o en representación de éste, así como la identidad de todas las personas privadas de su libertad, los motivos de su detención y los cargos en su contra, incluso durante conflictos armados» (Principio 10 B (2)); «Información sobre el fallecimiento de detenidos, e información sobre cualquier privación de la vida de la que sea responsable un Estado, incluyendo la identidad de la persona/s fallecidas, las circunstancias de su muerte y la ubicación de sus restos mortales» (Principio 10 B (3)). Vid. también la muy interesante nota aclaratoria de este Principio y su referencia a los problemas relacionados con la privacidad en estos casos.

que informa la actuación de los poderes públicos, así como asegurar el derecho ciudadano de acceso a la información.

El Derecho comparado y los estándares internacionales, como los Principios de Johannesburgo y de Tshwane, resaltan la importancia de definir de manera precisa las materias clasificadas, limitando el recurso al secreto de Estado a situaciones estrictamente justificadas y necesarias para la protección de intereses legítimos de seguridad nacional. En este sentido, el Anteproyecto de Ley de Información Clasificada de 2022 representa un avance al incorporar categorías específicas de información clasificable, pero su propuesta adolece, como ha quedado de manifiesto, de carencias importantes que comprometen su adecuación a los principios esenciales de nuestro ordenamiento jurídico. Entre los aspectos más preocupantes destaca la falta de precisión en la definición de algunas categorías de información clasificable, lo que abre la puerta a interpretaciones discrecionales y potencialmente abusivas por parte del Gobierno o de la Administración y a una restricción excesiva de la información disponible para el conjunto de los ciudadanos.

El análisis comparado revela, por otro lado, una tensión entre los modelos de protección formal y material del secreto de Estado. La protección formal, aunque ofrece mayor seguridad jurídica al delimitar de manera objetiva qué constituye un secreto, corre el riesgo de sobreproteger información que no merecería protección penal alguna. En el caso español, la dependencia de un sistema formal exige reforzar el cuidado a la hora de determinar qué información debe ser clasificada, así como establecer mecanismos de supervisión eficaces para evitar abusos, asegurando que solo la información esencial para la seguridad del Estado reciba la protección más severa.

En fin, la experiencia comparada pone de relieve que la regulación del secreto de Estado debe garantizar tanto la protección de la seguridad del Estado como la preservación de los derechos fundamentales. En este marco, el legislador español tiene la oportunidad y la responsabilidad de adoptar un modelo normativo en el que la protección de la información clasificada no descuide el fortalecimiento de los principios democráticos o la necesidad de favorecer la confianza de la ciudadanía en sus instituciones.

BIBLIOGRAFÍA CITADA

Alcaraz, H. (2025). Sobre una especificidad francesa: el secreto de la defensa nacional. *El régimen jurídico de la información clasificada: una visión global. s.* Zaragoza. Fundación Manuel Giménez Abad (en prensa).

Álvarez Conde, E. (2000). Secretos de Estado y Constitución. *Regap*, 25, vol.1, 27-52.

Amnistía Internacional (2020). ¿Abrimos ya el candado de la ley de secretos oficiales? preocupaciones y recomendaciones de amnistía internacional para la tramitación de la reforma de la ley 9/1968, de 5 de abril, sobre secretos oficiales, Amnistía Internacional, septiembre de 2020.

Asamblea Parlamentaria del Consejo de Europa. Recomendación 1792 (2007), *Fair Trial issues in criminal cases concerning espionage or divulging state secrets.*

Asamblea Parlamentaria del Consejo de Europa. Resolución 1838 (2011). Abuse of state secrecy and national security: obstacles to parliamentary and judicial scrutiny of human rights violations.

Asamblea Parlamentaria del Consejo de Europa. Resolución 1954 (2013). National security and access to information.

Bobbio, N. (1992). *Estado, Gobierno y Sociedad. Por una teoría general de la política*. 1ª ed. (2ª reimpresión), México: Fondo de Cultura Económica.

Bok, S. (1989). *Secrets. On the ethics of concealment and revelation.* New York: Vintage Books, Random House.

Cano Bueso, J. (1997). Información parlamentaria y secretos oficiales. *Revista De Las Cortes Generales*, (42), 7-34.

Cameron, I. (2025). Secreto y divulgación de información en Suecia. *El régimen jurídico de la información clasificada: una visión global.*. Zaragoza: Fundación Manuel Giménez Abad, (en prensa).

Carranza Galaico, G. (2024). Entre la máxima publicidad y la reserva: análisis del sistema de información clasificada en México desde la perspectiva del sistema español. Revista de Estudios Políticos, 206, 195-228.

Comité de Derechos Humanos (2011). Observación general Nº 34. Art. 19. Libertad de opinión y libertad de expresión. CCPR/C/GC/34. 12 de septiembre de 2011.

Consejo de Transparencia y Buen Gobierno (2022): Informe sobre el Anteproyecto de Ley de Información Clasificada.

De Lucas, J. (1990). Democracia y transparencia. Sobre poder, secreto y publicidad, *Anuario de Filosofía del 2*

De Lucas, J. (1999). De Secretos, mentiras y razones de Estado. *Claves de Razón Práctica*, 52, 22-30.

Díez-Picazo, L.M. (1998). *Sobre secretos oficiales*. Madrid: Cuadernos civitas.

Fernández Ramos, S. (1997). *El Derecho de acceso a los documentos administrativos*, Madrid: Marcial Pons.

Fonbaustier, L. (2012). Le côte obscur de la Charte de l'environment? A propos d'un incise dans la décision du Conseil constitutionnel nº 2011-192 QPC du 10 novembre 2011. *Environment*, 2, Etude 3.

Friedrich, C.J. (1964). *La filosofía del Derecho*, México, Buenos Aires: Fondo de Cultura Económica.

Gobierno de España (2024). *Plan de Acción Por la Democracia.*

Gómez-Reino y Carnota, E. (1976). El principio de publicidad de la acción del Estado y la técnica de los secretos oficiales, *REDA*, 8, 115-133.

González, M. Exteriores blinda todos sus documentos, *Diario El País* de 3 de junio de 2012

Habermas, J. (1999). *Historia y Crítica de la Opinión Pública*, 6ª ed., México: G.Gili.

Informe del Relator Especial para la promoción y protección a la libertad de opinión y expresión sobre derecho de acceso a la información (2010), de 20 de abril de 2010, A/HRC/14/23.

Informe del Relator Especial para la promoción y protección a la libertad de opinión y expresión sobre derecho de acceso a la información (2013), A/68/362, de 4 septiembre 2013.

Informe del Relator Especial sobre la promoción y protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo, Ben Emerson (2017). Principios marco para garantizar la rendición de cuentas de los funcionarios públicos por las violaciones manifiestas o sistemáticas de los derechos humanos cometidas en el transcurso de iniciativas de lucha contra el terrorismo respaldadas por los Estados [A/HRC/22/52, 23 de abril de 2017].

Lustgarten, L. y Leigh, I. (1994). *In from the Cold. National security and parliamentary democracy.* Oxford. Clarendon Press.

Marty, D. (2011). *Abuse of state secrecy and national security: obstacles to parliamentary and judicial scrutiny of human rights violations*, Documento 12714 de 16 de septiembre de 2011

Melero Alonso, E (2025). La información clasificada en el ámbito de la OTAN. *El régimen jurídico de la información clasificada: una visión global.* Zaragoza: Fundación Manuel Giménez Abad (en prensa).

Pendás, B. (2015). Regeneración democrática. Reflexiones y propuestas. En Enrique Arnaldo Alcubilla y Pedro González-Trevijano (dirs.), *En pro de la regeneración política en España*, 1ª ed. Madrid: Thomson Reuters Aranzadi.

Pereira, J.C. y Sanz Díaz, C. (2015). «Todo secreto». Acuerdos secretos, transparencia y acceso a los documentos históricos de Asuntos Exteriores y Defensa. *Ayer 97/2105* (1): 243-257.

Principios de Siracusa sobre las disposiciones de limitación y derogación del Pacto Internacional de Derechos Civiles y Políticos (1984). Anexo, E/CN.4/1984/4.

Principios globales sobre seguridad nacional y el derecho a la información (2013), de 12 de junio de 2013 («Principios de Tshwane»).

Pitruzzella, G. (1992). Segreto. I profili costituzionali. *Enciclopedia Giuridica*, XXVIII: 1-11.

Puente Rodríguez, L. (2022). Comentario urgente al Anteproyecto de Ley de Información Clasificada. *Diario La Ley*, Nº 10130, Sección Doctrina, 14 de septiembre de 2022.

Revenga Sánchez, M. (1995). *El imperio de la política. Seguridad nacional y secreto de Estado en el sistema constitucional norteamericano*. Barcelona: Ariel.

Relator Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos (2020). Informe *Derecho a la información y seguridad nacional* [OEA/Ser.L/V/II; CIDH/RELE/INF.24/2020].

Sainz Moreno, F. (1991). Secreto e información en el Derecho Público. *Estudios sobre la Constitución española en homenaje al Profesor Eduardo García de Enterría,* vol. III (pp. 2863-2981). Madrid: Civitas.

Santamaría Pastor, J.A. (1995). Secreto oficial, *Enciclopedia Jurídica Básica*, vol. IV (pp. 6088-6090). Madrid: Civitas.

Shils, E. A. (1956). *The Torment of Secrecy*, Glencoe, Illinois: The Free Press.

Sánchez Ferro, S. (2006). *El secreto de Estado.* Madrid. Centro de Estudios Políticos y Constitucionales.

Stemmler, M. (2025). El control judicial de los secretos de Estado en Alemania. El ejemplo de los tribunales de lo contencioso-administrativo. *El régimen jurídico de la información clasificada: una visión global.* Zaragoza: Fundación Manuel Giménez Abad (en prensa).

Stree (1997). § 93. Begriff des Staatsgeheimnisses. En Schönke y Schröder, *Strafgesetzbuch Kommentar,* 25 Auflage, München: C.H.Beck.

Träger (1988). § 93. En *Strafgesetzbuch. Leipziger Kommentar. Großkommentar*. 10 Auflage. 4 Band, §§ 80 bis 184 c. En Jescheck, Rub y Willms (editores), (pp. 120-158) Berlin-New York: Walter de Gruyter.

Vedaschi, A. (2005). *El régimen jurídico de la información clasificada: una visión global.* Zaragoza: Fundación Manuel Giménez Abad (en prensa).

Vega García, P. de (1995). Publicidad Parlamentaria, *Enciclopedia Jurídica Básica*, vol. IV (pp. 5402-5408). Madrid: Civitas.

Vega García, P. de (1998). Art. 80: Las sesiones plenarias de las cámaras. En Oscar Alzaga Villaamil (dir.), *Comentarios a la Constitución española de 1978*, tomo IV (art.s 66-80). Madrid: Cortes Generales y EDERSA.

Warusfel, B. (2021). Construire un droit démocratique de la sécurité nationale. *Les Champs de Mars : revue d'études sur la guerre et la paix*, 2022, 2021/1 (36), pp.19-41.

Weber, M. (1977) *¿Qué es la burocracia?*, Buenos Aires. La Pléyade.

Weber, M. (1984) *Economía y Sociedad*, 2ª ed. 7ª reimpresión, México. Fondo de Cultura Económica.

Wolfers, A. (1952). «National Security» as an Ambiguous Symbol. *Political Science Quarterly*, Vol. 67, No. 4., 481-502.

***

TITLE: *The definition of classified information: An international and comparative law analysis*

ABSTRACT: *This article analyzes the international standards and comparative law in relation to the definition of classified information, with a particular emphasis on ensuring a balance between the protection of national security and the principle of publicity inherent to any democracy and essential for preserving the rule of law. The article highlights the importance of defining classified matters in such a way as to protect only legitimate national security interests and to do it in a restrictive manner, so as to safeguard the principle of publicity, essential in our constitutional system. The article delves, then, into the analysis of the Preliminary Draft of the Classified Information Law of 2022, presented in the XIV Legislature, as a key initiative to replace the obsolete Official Secrets Law of 1968. Although the Preliminary Draft takes a step in the right direction, by trying to define the different classification categories by law, it raises problems of overclassification and lack of clarity in the regulation of some essential aspects. These shortcomings could compromise its objective of aligning Spanish legislation with international standards and the best practices of comparative law, and of guaranteeing an adequate balance between security and transparency, pillars of the Spanish democratic order.*

RESUMEN: *Este artículo analiza los estándares internacionales y el Derecho comparado en relación con la definición de las materias clasificadas, con particular énfasis en el aseguramiento del equilibrio entre la protección de la seguridad nacional y el principio de publicidad inherente a todo Estado democrático de Derecho. En el artículo se pone de manifiesto la importancia de definir estrictamente las materias clasificadas de forma que se protejan exclusivamente intereses legítimos de seguridad nacional. Sobre esta base, el art. profundiza en el análisis del Anteproyecto de Ley de Información Clasificada de 2022, presentado en la XIV Legislatura, como una iniciativa clave para sustituir la obsoleta Ley de Secretos Oficiales de 1968. Aunque el Anteproyecto, da un paso en la buena dirección, al tratar de establecer las materias clasificadas por ley,*

plantea problemas de sobreclasificación y falta de claridad en la regulación de algunos aspectos esenciales. Estas carencias podrían comprometer su objetivo de alinear la legislación española con los estándares internacionales y las mejores prácticas del Derecho comparado y de garantizar un adecuado equilibrio entre seguridad y transparencia, pilares de nuestro Estado democrático de derecho.

KEYWORDS: *State Secrets, Official Secrets, Classified information, Principle of publicity, right of access to information, Official Secrets Act, Draft Bill on Classified Information (XIV Legislature), Comparative law, international standards.*

PALABRAS CLAVE: *Secreto de Estado, Información clasificada, Principio de publicidad, derecho de acceso a la información, Ley de Secretos Oficiales, Anteproyecto de Ley de Información Clasificada (XIV legislatura), Derecho comparado, estándares internacionales.*

FECHA DE RECEPCIÓN: *03.01.2025* FECHA DE ACEPTACIÓN: 20.02.2025

CÓMO CITAR/ CITATION: Sánchez Ferro (2025) La definición de las materias clasificadas: Una visión desde los estándares internacionales y el Derecho comparado. *Teoría y Realidad Constitucional* 55, 207-260.