GUÍAS SOBRE BUENA GOBERNANZA

No. 06

El equilibrio entre apertura y confidencialidad en el sector de defensa: enseñanzas a partir de las buenas prácticas internacionales

Centre for Integrity in the Defence Sector

Norwegian Ministry of Defence

CENTRO DE INTEGRIDAD EN EL SECTOR DE DEFENSA

El Centro de Integridad en el Sector de Defensa (CIDS, por sus siglas en inglés) trabaja para promover la integridad, las medidas anticorrupción y la buena gobernanza en el sector de defensa. En colaboración con socios noruegos e internacionales, el centro tiene como objetivo el desarrollo de competencias, el fomento de la concienciación y la oferta de medios concretos para reducir las posibilidades de que se produzcan casos de corrupción. El CIDS fue fundado en 2012 por el Ministerio de Defensa de Noruega.

SOBRE EL AUTOR

Francisco Cardona es un experto internacional asociado del CIDS. Cardona es un profesional de reconocido prestigio cuyo trabajo se centra en el diseño y evaluación de reformas en el ámbito de la función y administración públicas, la justicia y el derecho administrativos, las políticas anticorrupción y el desarrollo institucional. Su experiencia incluye tanto el trabajo que ha realizado en España (su país de origen), donde desarrolló su carrera en la función pública, hasta su labor en organizaciones internacionales como la OCDE (el programa SIGMA), en las que ha trabajado durante 15 años como analista superior de políticas en el ámbito de la gobernanza pública. En el marco de este programa, ha asesorado a unos 25 países en transición y en desarrollo en Europa Oriental, África y la región de América Latina y el Caribe. Es abogado de formación (Universidad de Valencia, 1976) y cuenta con varios másteres en administración pública.

PRÓLOGO

El objetivo principal de las *Guías sobre buena gobernanza* del CIDS consiste en presentar aspectos claves del ámbito de la "buena gobernanza". La intención es que sean documentos concisos, pero que no simplifiquen en exceso dichas cuestiones.

El presente folleto es el sexto de la serie; en él, el autor pretende poner en tela de juicio el concepto de confidencialidad en el sector de defensa. Con tal propósito, se pregunta cuál debería ser el término medio entre el libre acceso a la información y una cierta restricción de dicho acceso en una sociedad democrática con un "gobierno abierto", y lo que es más: ¿en qué casos resulta indispensable limitar la información por motivos de seguridad nacional? Véase el derecho de la ciudadanía a la protección del Estado.

El autor de esta guía es Francisco Cardona, uno de los expertos internacionales superiores del CIDS. Desde aquí agradezco su contribución a un tema tan importante en el campo de la buena gobernanza que ha ocupado un lugar de rabiosa actualidad en los debates públicos de los últimos años y que probablemente seguirá siendo pertinente en el futuro.

También me gustaría reconocer las aportaciones de Bård Bredrup Knudsen (editor del centro) y Åse Marie Fossum (coordinadora de publicaciones) al presente trabajo.

Esperamos que este recurso sea de utilidad a una audiencia amplia tanto en el sector público (que abarca la defensa) como en otras esferas. Alcanzar el equilibrio entre la apertura y la confidencialidad resulta indispensable para el correcto funcionamiento de las sociedades democráticas.

El CIDS está abierto a recibir cualquier comentario sobre esta guía.

Oslo, 24 de abril de 2018

Per Christensen
Director

ÍNDICE

Introducción

La presente *Guía sobre buena gobernanza* ofrece un breve resumen de las buenas prácticas que se siguen en países de la Unión Europea y de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) con el propósito de mantener el carácter confidencial de la información pública en el campo de la defensa y la seguridad nacional y, a la vez, fomentar el derecho general de la población a acceder a los datos en poder de las instituciones estatales. El documento tiene por objeto proponer políticas que impulsen el gobierno abierto, el acceso a la información y la capacidad de la ciudadanía para tomar decisiones con conocimiento de causa sobre la actuación de las autoridades. De forma paralela, deben establecerse límites que permitan proteger sin fisuras los secretos de Estado relativos a cuestiones que exigen discreción absoluta por razones de seguridad nacional, defensa, inteligencia y lucha contra la corrupción y la delincuencia.

La transparencia y la publicidad son medidas preventivas excelentes frente a la corrupción, las irregularidades administrativas y la mala gobernanza. La buena salud democrática es incompatible con el predominio del secretismo, ya que, en tales circunstancias, los regímenes sencillamente dejan de ser democracias al impedir la participación ciudadana en el proceso político. Esto conllevaría la posibilidad de que el ejercicio de la autoridad escapara a todo control, así como la ausencia de responsabilidad democrática. No obstante, también puede resultar indispensable limitar el acceso público a la información con miras a sostener el correcto funcionamiento de la democracia en un Estado regido de una manera eficiente. Así pues, tanto la divulgación de información pública como la imposición de determinadas restricciones a esa comunicación deben redundar por igual en el interés general.

El marco conceptual: la seguridad nacional como justificación de la confidencialidad

Desde el punto de vista conceptual, se parte del supuesto de que el gobierno abierto y el libre acceso a la información, por un lado, y una cierta restricción de tal acceso, por otro, favorecen el interés público. El principio general reconocido a nivel internacional dispone que los Gobiernos han de promover el "derecho a saber" y, a la vez, acotarlo con límites razonables para mantener la confidencialidad de determinada información pública. Se trata de limitaciones imprescindibles para abordar con eficacia las actividades del Estado en algunas esferas, sobre todo aquellas relacionadas con la seguridad nacional y la defensa.

En lo que se refiere al secreto, el mayor problema estriba en definir en qué casos y de qué modo es válido coartar el acceso público a la información. Una de las aspiraciones de las democracias sanas consiste en garantizar el debido acceso público a la información sin dejar de ponerle coto mediante ciertas salvedades legítimas. El procedimiento para llegar a un término medio entre ambos aspectos depende en gran medida de la historia, los valores sociales y demás factores culturales del país en cuestión; he aquí uno de los motivos por los que resulta difícil constatar si hay pautas internacionales que faciliten alcanzar ese justo equilibrio (Transparency International UK, 2014). En la práctica, no existen normas precisas de esta clase, si bien los últimos años han sido testigo de numerosos debates intelectuales y tentativas encaminadas a fijar algunos principios generales.[1]

El ejercicio de garantizar el secreto y la confidencialidad debe someterse a controles; en caso contrario, se convierte con facilidad en una práctica frecuente y exhaustiva. En determinados servicios públicos que se ocupan de la seguridad nacional, la defensa, las investigaciones judiciales, la recopilación de información o la lucha antiterrorista existe la tendencia a que todas las actividades permanezcan bajo secreto, incluso cuando esto supone un obstáculo para que la ciudadanía ejerza su derecho a saber lo que hace la Administración. Al margen del gran gasto que comporta mantener el "aparato del secretismo" operativo, recurrir a la confidencialidad en abundancia y de forma generalizada suele minar la confianza de la población en las instituciones estatales y, a la larga, debilitar la legitimidad democrática. Además, hacer un uso excesivo del secreto acarrea por lo general más errores e infracciones que la transparencia y el control público, ya que la falta de transparencia dificulta el escrutinio por parte de la sociedad y la rectificación de las malas prácticas. En consecuencia, la opacidad podría constituir a largo plazo un peligro mayor para la seguridad nacional que la apertura.

1 Véanse los Principios de Tshwane (2013): https://www.justiceinitiative.org/publications/global-principles-national-security-and-freedom-information-tshwane-principles/es

Tal y como opinan algunos cargos públicos (en los Estados Unidos, por ejemplo), llevar el secreto demasiado lejos "se ha convertido en un escollo injustificado para la difusión de información dentro y fuera de la Administración, lo cual va en detrimento de las políticas públicas" (Aftergood, 2008, pág. 400). Esto señala el problema de la sobreclasificación; o lo que es lo mismo, que a la hora de clasificar la información en su poder, las instituciones van casi siempre mucho más allá de las necesidades reales.

La finalidad de cualquier sistema de clasificación consiste en evitar que se divulgue información susceptible de poner en peligro la seguridad nacional, pero la definición de conceptos como "seguridad nacional" y "amenazas para la seguridad" es difusa e imprecisa, algo que abre la puerta a que se abuse del secreto. No es fácil diferenciar entre datos objetivos y subjetivos, lo que complica que se fijen criterios bien delimitados para una clasificación adecuada de la información.

Clasificar información de manera adecuada es una idea problemática de por sí, pero en lo que al concepto se refiere, podemos coincidir en que la clasificación "adecuada" es aquella que se aplica con sensatez y se desvía lo menos posible de los valores democráticos de apertura, transparencia y libre acceso a la información. Dicho de otro modo, podríamos convenir en que, para considerarse fundada, la limitación de la transparencia debe a) tener carácter excepcional y b) proteger intereses destacados en materia de seguridad nacional. Esta conclusión reconoce que, en el campo de la seguridad nacional y la defensa, se dispone de información que *no* es imprescindible ocultar en aras de la seguridad del Estado y, por consiguiente, puede revelarse total o parcialmente sin ningún problema.

En algunos países democráticos predomina aún la concepción tradicional que contempla la transparencia únicamente como la exigencia de un particular mientras considera que el secreto encarna el interés común, por el bien de la seguridad nacional. A modo de ejemplo, podemos citar las palabras de Jean-Marc Sauvé, vicepresidente del Consejo de Estado francés, en un discurso pronunciado ante la Asamblea Nacional de Francia (la Cámara Baja del Parlamento galo) el 5 de julio de 2011: "Es el camino que hemos de seguir para trazar la línea divisoria entre el legítimo interés general que requiere mantener el secreto y la transparencia que exige la ciudadanía" (Sauvé, 2011, pág. 6). Tal declaración parte del supuesto de que la confidencialidad preserva el interés general y la transparencia no redunda en beneficio de este, sino que se trata de una mera petición que responde a la curiosidad de la población general y los periodistas. Estamos ante una hipótesis muy discutible: la experiencia nos ha demostrado que una de las mejores formas de proteger el interés común es fomentar la transparencia, puesto que contribuye a que los poderes públicos rindan cuentas ante los ciudadanos y otros mecanismos de control democrático. Por tanto, cabe interpretar la transparencia (y no el secreto) como una herramienta para *salvar* "la distancia que surge por naturaleza entre el Estado y el pueblo" (Fenster, 2010, pág. 619).

En lo que respecta a las actuaciones y políticas de las instituciones públicas, existe un amplio consenso internacional en torno a primar la transparencia como norma general y recurrir al secreto como excepción. Es más, dichas excepciones deberán fundamentarse y solo se considerarán justificables si su validez queda patente. A su vez, la validez está condicionada a que se demuestre que las excepciones se han producido con tal de defender unos intereses legítimos en materia de seguridad nacional.

La necesidad de diferenciar el secreto lícito del ilícito precisa de un cierto control por parte de autoridades que no se supediten a quien clasifica la información. Dichos mecanismos de control independientes pueden estar en manos de tribunales o de organizaciones gubernamen-

tales más especializadas y su misión consiste en determinar si los intereses de seguridad nacional esgrimidos para clasificar información son auténticos y lo bastante importantes. A falta de mecanismos externos de control, las decisiones sobre la clasificación de la información se vuelven puramente facultativas y, casi con total probabilidad, arbitrarias. No obstante, como veremos más adelante, los tribunales han actuado a lo largo de la historia con demasiada deferencia hacia la ocultación de información por parte de organismos de seguridad e inteligencia (y todavía conservan esa inclinación).

Desde el punto de vista conceptual y como ya se ha mencionado, la transparencia absoluta no es conveniente y seguramente tampoco resultaría viable. Asimismo, los Estados siempre realizarán actividades en algunas esferas ambiguas o abstrusas. Tal y como señala Fenster (2010, pág. 623), a menudo hay un punto intermedio entre el secreto y la transparencia, lo que implica que no tienen por qué ser polos opuestos. En la práctica, estas dos nociones no conforman una realidad antagónica e inequívoca, pues ambas exigen sus propias bases institucionales, que presentan diferencias de estructura (Riese, 2014, pág. 14).

Potenciar la transparencia no conlleva por fuerza una merma del secreto, pero mejorar su calidad servirá para proteger la confidencialidad. Lo que sí entraña una mayor transparencia es reservar la protección a los casos en que verdaderamente se precise mantener la confidencialidad. La institucionalización de las políticas de transparencia es un fenómeno relativamente reciente en la mayoría de los países, mientras que la del secretismo proviene de tradiciones muy arraigadas. Los valores e intereses que subyacen a dichas tradiciones siguen siendo heterogéneos y un tanto discordantes. La dificultad radica en armonizar de forma gradual la institucionalización del derecho a saber y de la protección de las necesidades de confidencialidad genuinas en lo que respecta a las estructuras organizativas que las gestionan y las prácticas gubernamentales. Lo ideal sería que la búsqueda de una mayor coherencia entre ambos enfoques propicie la formulación de una única política integral y que la institucionalización de las normas de acceso a la información en las Administraciones centrales sea más congruente, de acuerdo con las necesidades en materia de seguridad nacional.

No obstante, "seguridad nacional" es un concepto sumamente escurridizo cuyo significado puede variar de un contexto a otro, algo que complica todavía más las cosas. En el grueso de los países que analizó Jacobsen (2013), la seguridad nacional abarca también en mayor o menor grado las relaciones internacionales y las amenazas internas para la seguridad. Dicho de otro modo, no siempre hay un límite evidente.

Sin dejar de reconocer que, en lo referente a las políticas públicas, el sempiterno problema reside en marcar la línea que separa el secretismo fundado del infundado y en amparar el uno mientras se arroja luz sobre el otro, Aftergood (2009, págs. 402 y 403) propone encuadrar el secreto en tres categorías prácticas para determinar si el secretismo del Estado está o no justificado:

1. **Secreto legítimo en aras de la seguridad nacional:** protege información que representaría una amenaza discernible para la seguridad del país al poner en peligro su defensa o relaciones exteriores. Ocultar datos de esta naturaleza no suscita polémica porque constituye la base teórica de todos los sistemas de clasificación y no divulgarlos es la opción más beneficiosa para el interés público.

2. **Secreto burocrático:** así se denomina la predisposición de los burócratas a proteger información ya sea por comodidad o porque tengan la leve sospecha de que revelarla podría acarrear más riesgos que mantenerla en secreto. Por lo general, esta tendencia de la burocracia lleva a sobreclasificar información y se traduce en una cantidad ingente de material clasificado sin necesidad. Además, multiplica los costes presupuestarios del secreto y a menudo se aprovecha de la prepotencia en el ámbito administrativo y de la reticencia a dar a conocer los métodos de trabajo de una determinada institución del Estado.

3. **Secreto político:** se trata de la inclinación a valerse de la clasificación para obtener réditos políticos. Estamos ante la modalidad de secreto más reprobable, ya que se aprovecha de la legitimidad reconocida a los verdaderos intereses en materia de seguridad nacional con el fin de impulsar unos objetivos egoístas, sortear una controversia política o poner trabas a la rendición de cuentas pública. En casos extremos, el secreto político encubre incumplimientos de la ley, abusos contra los derechos humanos e incidentes de corrupción o mala gestión, y hace que la integridad de los procesos políticos corra peligro.

LA ESCASA PARTICIPACIÓN DE LA JUDICATURA EN EL CONTROL DE LOS SISTEMAS DE CLASIFICACIÓN

Según lo comentado anteriormente, el trato que la justicia ha dispensado a las autoridades encargadas de la clasificación y su supuesta "prerrogativa del Ejecutivo en cuanto a secretos de Estado" ha sido bastante deferente a lo largo de la historia (y sigue siéndolo hoy en día). Esta suma cortesía de la judicatura ha ayudado a consolidar la idea de que la seguridad nacional es un asunto demasiado delicado como para transmitir la información siquiera a los juzgados. Reynolds contra los Estados Unidos, el caso emblemático de la Guerra Fría, ofrece un claro ejemplo de ello en EE. UU.[2]

La predisposición benévola del poder judicial hacia el ejecutivo se acentuó tras los atentados terroristas perpetrados en dicho país el 11 de septiembre de 2001 (lo que se ha venido a llamar "11-S"). En los tribunales, las alegaciones del Estado acerca de la protección de la seguridad nacional se han impuesto sin cesar a principios como la rendición de cuentas, la transparencia y el gobierno abierto. Los numerosos ejemplos de los Estados Unidos, el Reino Unido, Francia y otros lugares del mundo democrático (por no hablar de los casos en países menos democráticos) ponen de manifiesto que existe una conformidad de base con la interpretación restrictiva del papel de los jueces en el examen de las decisiones ejecutivas relacionadas con la seguridad. Por desgracia, este enfoque podría menoscabar la protección de los derechos fundamentales, el imperio de la ley y el respeto a los auténticos intereses de seguridad.

Las autoridades ejecutivas de clasificación esgrimen con mucha frecuencia lo que se denomina "prerrogativa del Ejecutivo en cuanto a secretos de Estado" *(state secrets executive privilege)* en EE. UU., "certificado de inmunidad especial de la Corona" *(public interest immunity certificate)* en el Reino Unido y "carácter reservado" *(secret-défense)* en Francia. Con ello, su intención es evitar la revisión judicial o reducir su efectividad. Es habitual que la justicia acepte excepciones al principio de apertura que se apoyan en argumentos como las tres fórmulas mencionadas, incluso cuando (en alguna ocasión) los tribunales afirman sin entrar en detalles que tales prerrogativas deben invocarse solo en circunstancias que realmente atañan a la seguridad nacional. Esta postura tan corriente entre los jueces refleja que, en términos generales, existe "una falta de consideración hacia la idea de contrapoderes institucionales, una dejación de las responsabilidades judiciales y una actitud de desprecio por la necesidad estructural de mantener abierta una vía que permita a los demandantes exigir reparaciones si el Gobierno se ha extralimitado" (Setty, 2012, pág. 1573).

2 https://supreme.justia.com/cases/federal/us/345/1/case.html

En un trabajo extraordinario sobre la función de los tribunales, Fuchs (2006, pág. 168) llegó a la conclusión de que "en vista de los valores notables que respalda el derecho a acceder a la información gubernamental, solo cabe sacrificarlo si hay una verdadera necesidad de mantener el secreto… Ni los Parlamentos ni la población se bastan por sí mismos para desafiar el exceso de secretismo. La judicatura tiene la responsabilidad de velar por que las actuaciones gubernamentales cuenten con la debida autorización, y el control independiente forma parte de dicha responsabilidad". Los tribunales son la única entidad que goza de la suficiente independencia como para desafiar el exceso de secretismo; sin embargo, Fuchs observa que, al parecer, se han negado a cumplir ese cometido.

En prácticamente todos los países europeos que analizó Jacobsen (2013), los tribunales tienen la potestad de revisar la información clasificada que el Gobierno pretenda mantener en secreto por motivos de seguridad nacional. No obstante, es digno de mención que, en algunas naciones, el estudio de dicha información está reservado a los juzgados o jueces que hayan obtenido una autorización especial. En Alemania se permite exclusivamente al Tribunal Supremo de lo Contencioso-Administrativo; en España, si bien la Ley sobre Secretos Oficiales no prevé que los jueces tengan acceso a la información clasificada (a diferencia del Congreso de los Diputados y el Senado), el Tribunal Supremo ha resuelto que él, y sólo él, es el único órgano judicial al que compete examinar los documentos clasificados del Ejecutivo. Francia es el único caso en el que los juzgados no tienen autoridad alguna para inspeccionar este tipo de material de forma directa (Sartre y Ferlet, 2010). No parece haber ningún modo de que los jueces galos consulten directamente información clasificada. A fin de limitar el efecto de la prohibición, una ley de 1998 creó la Comisión Consultiva del Secreto de Defensa Nacional (CCSDN, por sus siglas en francés), una comisión independiente con acceso a los documentos clasificados que haya solicitado un juez para valorar si sería sensato desclasificarlos.[3] En la mayoría de los países europeos, y al igual que sucede en los Estados Unidos, lo normal es que los jueces suscriban la evaluación que haya realizado una autoridad pública sobre el daño que las revelaciones ocasionarían a la seguridad nacional (Jacobsen, 2013).

NIVELES Y CRITERIOS DE CLASIFICACIÓN

Los niveles de clasificación se han normalizado de tal modo que numerosos países de la OCDE emplean el mismo sistema para clasificar documentos. De entre los miembros de dicha organización, Nueva Zelanda ofrece un buen ejemplo del procedimiento que se sigue en lo relativo a los secretos de Estado. En esta nación austral, la información oficial se protege conforme a criterios basados en una definición estricta de la necesidad de mantenerla a buen recaudo: la información se protegerá en la medida en que sea compatible con el interés común y el amparo de la privacidad. La clasificación de este tipo de material procura asignarle una categoría en función del perjuicio que causaría revelar los datos sin autorización para ello y detalla las medidas de salvaguardia que deben adoptarse.[4] Según las directrices neozelandesas, las clasificaciones no permiten de por sí que se oculte información oficial, sino que es indispensable analizar las características de los documentos en cuestión a partir de los criterios que establece la legislación.[5] En Australia, el sistema de clasificación de seguridad es interesante porque incluye unas pautas claras sobre cómo clasificar y desclasificar información secreta.[6]

3 http://www.defense.gouv.fr/sga/le-sga-en-action/droit-et-defense/secret-defense/secret-defense

4 Ley de Información Oficial de Nueva Zelanda (Official Information Act, 1982).

5 Directrices sobre la protección de la información oficial en Nueva Zelanda. Véase: https://protectivesecurity.govt.nz/home/information-security-management-protocol/new-zealand-government-security-classification-system/

6 Australia (2014): Pautas para gestionar la seguridad de la información en el marco del sistema de clasificación del Gobierno de Australia. Disponible en: https://www.protectivesecurity.gov.au/informationsecurity/Documents/AustralianGovernmentclassificationsystem.pdf

A continuación se explican los niveles de clasificación de Nueva Zelanda, que se ajustan a una práctica internacional muy común y cuya pertinencia depende del bien público objeto de la protección:

- Relacionado con la seguridad nacional: la divulgación pondría en peligro la seguridad, la defensa o las relaciones exteriores del país o de Gobiernos amigos.

- Relacionado con la política pública o la privacidad: la divulgación pondría en peligro el funcionamiento de la Administración o supondría un perjuicio para un particular.

Seguidamente enumeramos los niveles y criterios de protección del material que concierne a la seguridad nacional:

1. **Secreto:** la divulgación perjudicaría de manera extremadamente grave los intereses nacionales.

   - Supondría una amenaza directa para la estabilidad interna de Nueva Zelanda o de países amigos.
   - Sería la causa directa de un gran número de víctimas mortales.
   - Ocasionaría un perjuicio sumamente grave a la seguridad de las fuerzas militares de Nueva Zelanda o de sus aliados.
   - Ocasionaría un perjuicio sumamente grave a la eficacia de las operaciones de las fuerzas militares de Nueva Zelanda o de fuerzas amigas.
   - Ocasionaría un perjuicio sumamente grave a la continuidad de la eficacia de operaciones muy importantes en materia de seguridad o inteligencia.
   - Ocasionaría un perjuicio sumamente grave a las relaciones con otros Gobiernos.
   - Ocasionaría un perjuicio grave y duradero a infraestructuras nacionales críticas.

2. **Reservado:** la divulgación perjudicaría gravemente los intereses nacionales.

   - Aumentaría las tensiones en el plano internacional.
   - Ocasionaría un perjuicio grave a las relaciones con Gobiernos amigos.
   - Ocasionaría un perjuicio grave a la seguridad de las fuerzas militares de Nueva Zelanda o de fuerzas amigas.
   - Ocasionaría un perjuicio grave a la eficacia de las operaciones de las fuerzas militares de Nueva Zelanda o de fuerzas amigas.
   - Ocasionaría un perjuicio grave a la continuidad de la eficacia de operaciones importantes en materia de seguridad o inteligencia.
   - Ocasionaría un perjuicio grave a la estabilidad interna de Nueva Zelanda o de países amigos.
   - Inutilizaría infraestructuras nacionales críticas o provocaría trastornos considerables en ellas.

3. **Confidencial:** la divulgación perjudicaría de manera importante los intereses nacionales.

   - Ocasionaría un perjuicio sustancial a las relaciones diplomáticas; desencadenaría una protesta formal u otras sanciones.
   - Ocasionaría un perjuicio a la eficacia de las operaciones de las fuerzas militares de Nueva Zelanda o de fuerzas amigas.
   - Ocasionaría un perjuicio a la seguridad de las fuerzas militares de Nueva Zelanda o de fuerzas amigas.
   - Ocasionaría un perjuicio a la continuidad de la eficacia de operaciones importantes en materia de seguridad o inteligencia.
   - Ocasionaría un perjuicio a la estabilidad interna de Nueva Zelanda o de países amigos.
   - Provocaría trastornos en infraestructuras nacionales críticas.

4. **Difusión limitada:** la divulgación podría repercutir negativamente en los intereses nacionales.

    - Afectaría a las relaciones diplomáticas.
    - Interferiría con la eficacia de las operaciones de las fuerzas militares de Nueva Zelanda o de fuerzas amigas.
    - Interferiría con la seguridad de las fuerzas militares de Nueva Zelanda o de fuerzas amigas.
    - Afectaría a la estabilidad interna de Nueva Zelanda o de países amigos.
    - Afectaría al bienestar económico de Nueva Zelanda o de países amigos.

Los niveles y criterios de protección de la política pública y la privacidad de la población son:

1. **Secreto y restringido:** perjudicaría intereses estatales o pondría en peligro a la ciudadanía.

    - Comprometería la seguridad de una persona.
    - Ocasionaría un perjuicio grave a la economía de Nueva Zelanda.
    - Dificultaría las negociaciones del Gobierno.

2. **Confidencial:** menoscabaría el orden público, dificultaría las actividades del Gobierno o vulneraría la privacidad de la ciudadanía.

    - Comprometería el mantenimiento del orden público.
    - Repercutiría negativamente en la privacidad de una persona física.
    - Ocasionaría un perjuicio a la información comercial de la población.
    - Ocasionaría un perjuicio al deber de sigilo.
    - Socavaría las medidas que protegen la salud o la seguridad de la población.
    - Ocasionaría un perjuicio a los intereses económicos de Nueva Zelanda.
    - Socavaría las medidas de prevención o atenuación de daños materiales que afectan a la población.
    - Quebrantaría convenciones constitucionales.
    - Entorpecería la gestión de los asuntos públicos.
    - Vulneraría la prerrogativa de secreto profesional en la abogacía.
    - Dificultaría las actividades comerciales del Gobierno.
    - Revelaría o emplearía información para obtener un beneficio o ventaja indebidos.

Como ya se señaló antes, hallamos marcas y criterios parecidos para clasificar información en un buen número de países de la OCDE. Es sabido que existen ciertos niveles de clasificación incluso en Turquía, que no ha hecho públicas las normas que regulan esta esfera. De todos los países que respondieron a la encuesta objeto del análisis de Jacobsen (2013), Suecia es el único donde la ley no especifica cuáles son los niveles, ya que allí la clasificación cumple una función estrictamente administrativa.

En otros aspectos que rodean a la clasificación de información (por ejemplo, los procedimientos para ello, los requisitos de marcado, las autoridades de clasificación, la obligación de justificar la clasificación, la responsabilidad en caso de que esta sea inadecuada, los órganos de supervisión, etc.), las diferencias a lo largo y ancho de Europa pueden ser muy notables (véanse Jacobsen, 2013 y Transparency International UK, 2014).

CRITERIOS DE DESCLASIFICACIÓN

En el Viejo Continente, la desclasificación de documentos viene marcada por tres criterios básicos: los límites temporales, el desencadenante y la revisión periódica obligatoria. El objetivo fundamental es impedir que la información quede declarada bajo secreto a perpetuidad. Sin embargo, la ausencia de criterios de desclasificación en legislaciones o procedimientos administrativos nacionales no resulta rara. Teniendo en cuenta los plazos máximos para desclasificar información en Europa (que abarcan desde los 10 años en los Países Bajos a los 100 en Rumanía), los cálculos de Jacobsen (2013) indican que la mediana se sitúa en 30 años. Dicha estimación no pasa por alto dos casos singulares en la región: el secreto es eterno en Turquía y España.

Con respecto a las revisiones obligatorias de datos clasificados, lo más habitual es que se produzcan cada cinco años. La normativa sueca no contempla la figura de la revisión forzosa preestablecida, pero sí estipula que, cuando se solicite la revelación de algún dato, la clasificación que se le asignó deberá someterse a examen. La desclasificación automática (el desencadenante) varía de un contexto nacional a otro, pero el rasgo más notorio en la mayoría de ellos es que levantar el secreto que pesa sobre diversos tipos de información queda a discreción del Gobierno. También es posible que se trate de la decisión tomada a raíz del procedimiento iniciado por un particular u organización de la sociedad civil en virtud de una ley de acceso a información pública.

EVALUACIONES PARA CONTROLAR EL SECRETO: EL TEST DE DAÑO Y EL TEST DE INTERÉS PÚBLICO

Según *Right2INFO.org*, una ONG que fomenta la adopción de leyes y prácticas adecuadas, lo que se ha venido en denominar "test de daño" y "test de interés público" surge al exigir que toda restricción al derecho de acceder a la información sea proporcionada y necesaria.[7] SIGMA-OCDE (2010) proporciona un enfoque teórico amplio y minucioso de los conceptos en los que se fundamentan y que se deriva del contraste entre restricciones en términos absolutos y relativos cuando se habla del acceso a la información. Por lo general, las restricciones en términos absolutos engloban aquellas referidas a la defensa y la seguridad nacional.

EL TEST DE DAÑO

Con arreglo al test de daño, las autoridades públicas tienen que demostrar que sacar a la luz determinada información representa una amenaza para un interés protegido y por eso no debe divulgarse. El test obliga al Estado a acreditar el riesgo de que un interés legítimo en particular sufra un perjuicio grave y constatable. Debe quedar probado que hay un vínculo entre la restricción y el interés legítimo en cuestión y, además, que este se vería muy afectado si se revelara la información. Ha de ser un perjuicio lo suficientemente concreto, específico, inminente y directo, y no tratarse de un detrimento improbable o basado en conjeturas.

EL TEST DE INTERÉS PÚBLICO

El test de interés público es una cuestión de proporcionalidad, que requiere un ejercicio de ponderación en el que se compara el perjuicio que acarrearía la revelación y sus posibles beneficios para la ciudadanía. En cada país, la legislación deberá detallar las circunstancias en las que un interés público expreso y riguroso podría primar sobre el argumento en favor del secreto o la confidencialidad. Según muchos modelos nacionales de clasificación (como el interamericano o el africano), el interés general se convierte en un imperativo que prevalece sobre las demás consideraciones si se trata de material referente a abusos contra los derechos humanos o crímenes de lesa humanidad. Este test exige la intervención de una autoridad pública u órgano de supervisión que, ante un determinado interés protegido, pondere las repercusiones negativas

7 http://www.right2info.org/exceptions-to-access/harm-and-public-interest-test

de la divulgación frente a cómo favorecería el interés público.

La definición de "interés público" no es la misma en todos los países y a menudo necesita valorarse caso por caso. Por norma general, los intereses públicos que se inclinan a favor de la divulgación de información suelen tener que ver con cuestiones que suscitan una discusión nacional, la participación de la población en los debates políticos, la rendición de cuentas sobre cómo se asignan y se gastan los fondos del Estado, y la seguridad ciudadana. Normalmente se considera que los temas medioambientales y de seguridad ciudadana, los riesgos considerables para la salud y la información acerca de abusos graves contra los derechos humanos justifican que la publicación de documentos en aras del interés general se imponga como prioridad absoluta e ineludible.

Algunos países han formulado directrices para guiar a los funcionarios a cargo de estos procedimientos administrativos. Por ejemplo, los empleados públicos de Nueva Gales del Sur (Australia) deben aplicar el test de interés público a la hora de adoptar decisiones sobre si divulgar datos; esto es, tienen la obligación de sopesar los factores que avalan la transparencia y los factores que la desaconsejan por motivos de interés común.[8] A tenor de las mencionadas directrices, el test de interés público se divide en tres pasos:

1. Señalar cuáles son los intereses públicos en favor de revelar información.

2. Señalar cuáles son los intereses públicos en contra de revelar información.

3. Establecer la importancia relativa de ambos grupos y encontrar el punto de equilibrio entre ellos.

8 http://www.ipc.nsw.gov.au/fact-sheet-what-public-interest-test

Pese a que la legislación australiana es clara en lo que respecta a su preferencia por la divulgación, las leyes regionales sobre el acceso a la información contemplan varios contextos en los que la presunción se inclina a favor de la ocultación y de proteger el secreto. De entre ellos, el más notable se da cuando el documento en cuestión está sujeto a una ley de confidencialidad de rango superior (se mencionan expresamente 26). Esta situación se corresponde con la tónica general en numerosos miembros de la OCDE: en la práctica, la Ley de Libertad de Información (FOIA, por sus siglas en inglés) carece de importancia frente a la legislación convencional sobre secretos de Estado, que se excluyen por sistema del ámbito de aplicación de las leyes que rigen la libertad de acceso a la información. Asimismo, la mayoría de los países ha puesto poco empeño en conciliar su herencia institucional en materia de seguridad estatal con la nueva legislación sobre el libre acceso a la información pública.

En muchos casos, las FOIA apenas si han hecho mella en el secretismo que rodea a los asuntos de seguridad nacional; esto denota que, hasta la fecha, las leyes y los recursos ante los tribunales han surtido menos efecto como instrumentos para frenar la tendencia unánime de los organismos de seguridad e inteligencia a recurrir cada vez más a la confidencialidad y el secreto en el desempeño de su labor. Para estas entidades, que se mantienen su línea habitual (y a menudo inescrutable) de gestión de documentos confidenciales, las FOIA no han tenido prácticamente ninguna repercusión a pesar de la amplia corriente internacional que aboga por impulsar la transparencia pública y de las exigencias de la sociedad civil en conexión con el "derecho a saber".

Lo anterior pone de manifiesto una realidad tanto en el plano teórico como en el práctico: resulta difícil promulgar leyes de carácter general que logren un equilibrio entre el secreto y la apertura. Una de las razones estriba en que las tareas y las prácticas de los organismos y entidades públicos donde más propensión hay a clasificar material suelen perseguir fines muy dispares y obedecer a motivaciones radicalmente distintas. De este modo se contribuye a que las culturas administrativas en torno a la seguridad no coincidan. Por ejemplo, los órganos militares tienden a concentrar esfuerzos en la seguridad de las tecnologías armamentísticas y los planes de operaciones, los organismos de inteligencia se ocupan prioritariamente de mantener a buen recaudo las fuentes y los procedimientos operativos, el foco de interés del cuerpo diplomático está en las repercusiones globales que se derivan de clasificar y desclasificar información sobre esta materia y la Policía se afana en proteger a sus informantes y planes de operaciones. Así, cada institución diseña sus propios protocolos, directrices y mecanismos, que por lo general siguen vigentes durante años sin que se sometan a escrutinio ni se repasen a fondo. Por otra parte, es comprensible que quienes trabajan para esa clase de autoridades tengan tendencia a pecar de precavidos a fin de evitar problemas innecesarios, algo que con frecuencia lleva a la sobreclasificación (Aftergood, 2009).

Debido a ello, observadores informados y profesionales del ramo proponen que, incluso si la clasificación de un documento se lleva a cabo en el organismo pertinente, la autoridad de desclasificación debe ser ajena a dicho organismo. Esta recomendación constituye el mejor modo de eliminar de la ecuación los intereses particulares del organismo y suprimirlos del proceso de clasificación (Aftergood, 2009, pág. 412). Ya se han producido algunos intentos de implantar este sistema en los Estados Unidos con buenos resultados, como los que se han valido del Panel de Apelaciones sobre la Clasificación de la Seguridad Interinstitucional (ISCAP, por sus siglas en inglés)[9] y el Examen de Políticas Básicas de Clasificación (FCPR, por sus siglas en inglés).[10] Francia y la CCSDN son otro ejemplo (véase la mención anterior). En resumidas cuentas y según narra Aftergood (2009), la experiencia en EE. UU. demuestra que "si un organismo no consigue explicar a un alto cargo o un panel de otra institución los motivos de seguridad nacional que exigen la clasificación de un documento y convencerlos de ello, hay razones para poner en duda que se necesite mantener el secreto".

CONCLUSIONES

1. Las leyes que regulan la confidencialidad de la información en el ámbito de la seguridad y la defensa resultan indispensables y han de ser lo más precisas posible. En ellas se establecerán los criterios de clasificación y desclasificación de la información, sin perder de vista que, por definición, se trata de una legislación de carácter general, por lo que también lo serán los criterios definidos. Las leyes sobre confidencialidad se promulgaron en muchos países antes que las leyes sobre el libre acceso a la información. Es indispensable armonizar ambos tipos para evitar la aparición de contradicciones en el ordenamiento jurídico nacional.

2. Para poder aplicar los criterios legales de clasificación con prudencia y sensatez y así fomentar los valores democráticos y el principio de transparencia pública en la medida de lo posible, no solo se requiere un marco jurídico sólido, sino también que los organismos se gestionen de forma deliberada y competente. Es necesario lograr un equilibrio entre diversas consideraciones; tomar plena consciencia de ello debe formar parte de la cultura institucional. Los directivos de los organismos

9 https://www.archives.gov/declassification/iscap

10 https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/ODNI%20FY2017%20FCGR.pdf. Véase también el examen de 1994 en el Departamento de Energía de EE. UU. que marca la pauta: https://www.osti.gov/opennet/forms.jsp?formurl=od/fcprsum.html

implicados han de contemplar el logro de un equilibrio armonioso entre la legítima confidencialidad y la legítima transparencia como uno de los cometidos de su cargo.

3. Reducir la sobreclasificación improcedente y alcanzar el punto intermedio entre el derecho a saber de la población y las exigencias en materia de seguridad nacional (así como otros motivos válidos para proteger el secreto) son arduas tareas. En la mayoría de los países de la Unión Europea y la OCDE, la transformación de una cultura de secretismo a una de transparencia en el sector de defensa parece una posibilidad muy remota a corto plazo.[11]

4. Cabe esperar que las personas que trabajan en el campo de la seguridad y la defensa (sean o no funcionarios) se comporten con lealtad, discreción y respeto hacia los procedimientos establecidos. Reunir estas cualidades es ciertamente indispensable, pero también se puede y se debe fomentar hasta cierto punto la innovación y el surgimiento de nuevas ideas incluso si hay poco margen de maniobra para introducir cambios. Sea como fuere, tenemos que analizar con ojo crítico los métodos para llegar al equilibrio ideal entre el secreto justificado y el acceso legítimo a la información.

5. Hay que impartir formación especializada a quienes se ocupan de aplicar las leyes sobre secretos y las políticas en materia de confidencialidad para que sepan otorgar la debida importancia a las necesidades democráticas de apertura y transparencia en las instituciones al tiempo que sepan reconocer sin lugar a dudas qué datos no pueden hacerse públicos en virtud de la legislación. Poner fin al uso indiscriminado del secreto no significa abrazar la divulgación sin cortapisas. La calidad y las aptitudes del personal del sector de la seguridad y la defensa revisten una importancia crucial, porque repercuten directamente en las sociedades democráticas y en las relaciones entre los organismos de seguridad y la sociedad civil.

6. Es necesario contar con una entidad independiente cuyas atribuciones vayan más allá de las competencias exclusivas de las autoridades de clasificación más importantes (el Ejército, la Policía y los servicios de inteligencia) y que tenga la potestad de examinar y desclasificar la información secreta en poder de los diversos organismos. Una posible opción sería el establecimiento de una comisión interinstitucional de desclasificación. En general, los tribunales han demostrado ser excesivamente deferentes hacia la prerrogativa del Ejecutivo en cuanto a secretos de Estado y hay pocas razones para creer que la situación vaya a cambiar.

7. Se diría que empieza a surgir una buena práctica con una menor presencia de actuaciones discrecionales, que son el rasgo distintivo de los procedimientos habituales de clasificación. La decisión de clasificar y desclasificar información no debe quedar en manos de una única persona, sino de un comité o comisión independiente capaz de emitir un dictamen imparcial sobre si es necesario clasificar o desclasificar una parte o la totalidad de un documento en concreto. Esta entidad especializada seguirá los criterios que marca la ley para evaluar los posibles perjuicios y llevar a cabo el test de interés público. La composición del comité o comisión ha de limitarse a entre cinco y siete miembros, por ejemplo, y englobaría a expertos del ámbito de la seguridad pertenecientes a los tres poderes del Estado y el Defensor del Pueblo.

11 Aunque se diría que Rumanía lo ha conseguido (Matei, 2007).

REFERENCIAS

Aftergood, Steven (2009): "Reducing Government Secrecy: Finding What Works". *Yale Law & Policy Review*, vol. 27, n.º 2 (primavera de 2009), págs. 399-416. Disponible en: https://www.jstor.org/stable/40239716?seq=1#page_scan_tab_contents

Fenster, Mark (2010): *"Seeing the State:* Transparency as Metaphor". *Administrative Law Review*, págs. 617-672. Disponible en: http://scholarship.law.ufl.edu/cgi/viewcontent.cgi?article=1571&context=facultypub

Fuchs, Meredith (2006): *"Judging Secrets:* The Role Courts Should Play in Preventing Unnecessary Secrecy". *Administrative Law Review*, vol. 58, n.º 1 (invierno de 2006), págs. 131-176.

Jacobsen, Amanda L. (2013): "National Security and the Right to Information in Europe". Disponible en: http://www.right2info.org/resources/publications/national-security-page/national-security-expert-papers/jacobsen_nat-sec-and-rti-in-europe

Matei, Florina Cristiana (2007): *"Reconciling Intelligence Effectiveness and Transparency*: The Case of Romania". *Strategic Insights*, vol. 6, n.º 3 (mayo de 2007). Disponible en: https://calhoun.nps.edu/bitstream/handle/10945/11297/mateiMay07.pdf?sequence=1

OCDE (2010): "The Right to Open Public Administrations in Europe: Emerging Legal Standards". *SIGMA Papers*, n.º 46, OECD Publishing, París. Disponible en: http://dx.doi.org/10.1787/5km4g0zfqt27-en

Riese, Dorothee (2014): "Secrecy and Transparency". Artículo presentado durante la Conferencia General del European Consortium for Political Research (ECPR, por sus siglas en inglés) en Glasgow, del 3 al 6 de septiembre de 2014. Disponible en: https://ecpr.eu/Filestore/PaperProposal/2cedead9-5191-42de-ae36-7d320a28a304.pdf

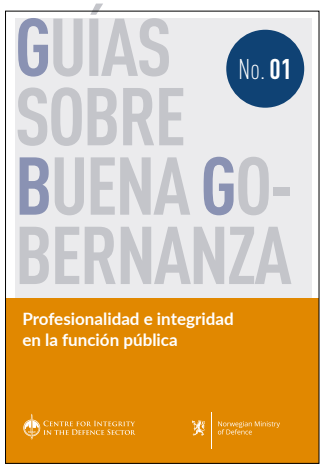
Sartre, Patrice y Ferlet, Philippe (2010): "Le secret de défense en France". *Revue Études*, 2010/2, núm. 412 (febrero), págs. 165-175. Disponible en: https://www.cairn.info/revue-etudes-2010-2-page-165.htm

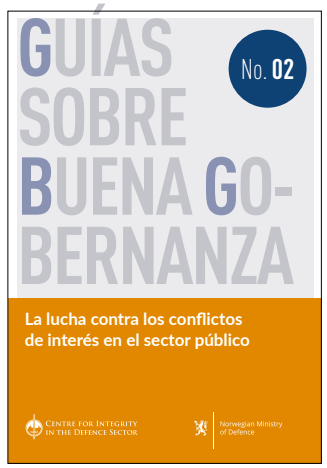
Sauvé, Jean-Marc (2011): *"Culture du secret contre transparence sans limite : quel équilibre pour garantir l'intérêt général ?* Transparence, valeurs de l'action publique et intérêt général". Discurso pronunciado ante la Asamblea Nacional de Francia el martes, 5 de julio de 2011 en un simposio organizado por Transparence Internationale France. Disponible en: http://www.conseil-etat.fr/content/download/2597/7819/version/1/file/discours-transparence-international.pdf

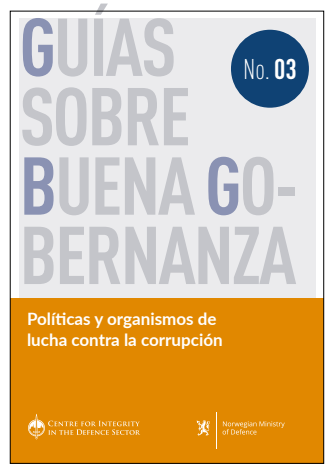
Setty, Sudha (2012): "The Rise of National Security Secrets". *Connecticut Law Review*, vol. 44, n.º 5 (julio de 2012), págs. 1563-1582.

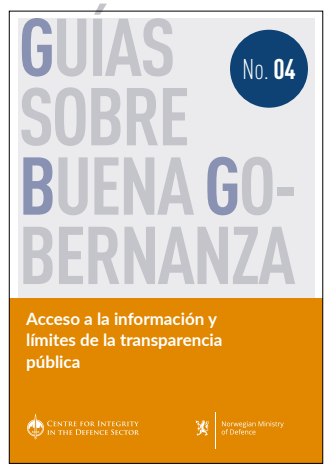
Transparency International UK (2014): *Classified Information: A Review of Current Legislation across 15 Countries & the EU*. Disponible en: http://ti-defence.org/wp-content/uploads/2016/03/140911-Classified-Information.pdf

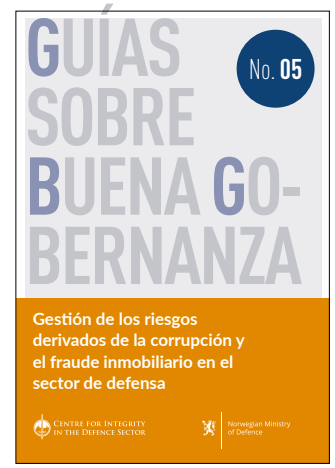
Guías sobre buena gobernanza











Las ***Guías sobre buena gobernanza*** son una serie de folletos breves. Cada uno de ellos trata sobre un tema determinado, importante para la buena gobernanza en el sector de defensa. Estos documentos se dirigen a personas interesadas en saber más sobre uno o varios temas relacionados directamente con la buena gobernanza en el sector de defensa (o, en general, en el sector público). También pueden usarse con fines educativos.

Publicado por: Centro de Integridad en el Sector de Defensa
Diseño: www.melkeveien.no
Impresión: Organización de servicios y de seguridad del Gobierno de Noruega
Mayo/2018 Tirada: 100

CENTRE FOR INTEGRITY IN THE DEFENCE SECTOR

www.cids.no

La traducción al español de la versión original en inglés es cortesía de la Organización del Tratado del Atlántico Norte.