





MIGUEL ÁNGEL ESTEBAN NAVARRO

Documentos secretos y derecho de acceso a la información en el marco del control democrático de los servicios de inteligencia

“La práctica del secreto, para compartimentar información y limitar el acceso a aquellas personas que demuestran una clara necesidad de tener que conocer, dificulta la identificación de las personas responsables y pone en peligro el fundamento de una sociedad democrática y abierta”

(American Civil Liberties Union v. Department of Defense and Central Intelligence Agency, Southern District of New York, 2006-2008. Demanda relacionada con el acceso a documentos clasificados como secretos referentes a los abusos cometidos por el Ejército de Estados Unidos y la CIA en las prisiones de Abu Ghraib en Bagdad y Bagram en Afganistán contra detenidos acusados de terrorismo).

El fin de los servicios de inteligencia de un Estado democrático es garantizar la seguridad colectiva de la nación mediante la estimación y la prevención de riesgos y amenazas procedentes de agentes interiores o exteriores. Pero las actividades que estas instituciones realizan para cumplir con su misión han de ser respetuosas con las normas legales específicas que las regulan y, en general, con los derechos y las libertades constitucionales de los ciudadanos. De lo contrario, la acción de los servicios secretos en lugar de afianzar un ambiente de seguridad que permita un pleno desenvolvimiento de las libertades individuales y colectivas, se puede convertir en una de las más importantes amenazas

Miguel Ángel Esteban Navarro
Departamento de Ciencias de la Documentación, Universidad de Zaragoza
E-mail: mesteban@unizar.es

para ese binomio indisoluble que forman la seguridad y la libertad para el pensamiento democrático. Pero los servicios de inteligencia y sus miembros pueden tener la tentación, al igual que el resto de las instituciones del Estado y de sus empleados, de actuar con arbitrariedad y sin el debido respeto de las normas y los límites legales. Por eso, como un medio a la vez de disuasión para sus directivos y sus oficiales y de garantía para la sociedad, las instituciones de seguridad deben someter su modo de funcionamiento y sus actuaciones, como cualquier otra instancia del poder público, a los principios de la transparencia, del control público y de la rendición periódica de cuentas.

En nuestra opinión, la existencia de tres condiciones relacionadas con la información y con los documentos es indispensable para invitar a las instituciones públicas, con independencia de que pertenezcan o no al ámbito de la seguridad, a ser transparentes en sus actuaciones, para que los órganos de supervisión puedan comprobar la veracidad de sus rendimientos de cuentas y, en definitiva, para que la sociedad pueda realizar un control eficaz de su funcionamiento y de sus actos mediante los procedimientos diseñados para cada caso. Estas tres condiciones son el reconocimiento del derecho de acceso a la información generada y reunida durante el ejercicio de sus funciones por un organismo político o administrativo, la presencia de normas que regulen el ejercicio efectivo de este derecho adecuadas a la diversa casuística y la existencia de recursos e instrumentos que permitan conservar, organizar, buscar y recuperar los documentos administrativos. El acceso a la información concreta para realizar el escrutinio de la Administración puede ser ejercido de modo directo por cualquier ciudadano y por los medios de comunicación o se puede ejercer mediado, según el caso y como garantía de la seguridad nacional o del respeto de otros derechos ciudadanos, como el de la intimidad, a través de los representantes políticos de los ciudadanos o del poder judicial. En cualquier caso, el archivo es un elemento clave del sistema y la libertad de acceso a los documentos de archivo un corolario de la libertad de información consagrada como un derecho humano por la *Declaración Universal de los Derechos del Hombre* de 1948 en su artículo 19.

Los obstáculos y las dificultades de todo tipo y procedencia contra las que se han debido y deben luchar para lograr el reconocimiento, primero, del derecho a la información sobre la acción de los poderes públicos, y para poder ejercerlo en la práctica después, incluso en las democracias, han sido descritas y analizadas recientemente, junto con un análisis de la situación actual, por diversos autores (Guichot, 2009, 2010, 2011b; García, 2010; Organización de los Estados Americanos, 2010; Bishop, 2011). No solo existen barreras doctrinales de tipo ideológico, político y jurídico que se deben vencer, sino que también es determinante, incluso cuando hay normas que reconocen y regulan el acceso, la presencia de contextos sociales y culturales que dificultan e incluso impiden el acceso de los ciudadanos a la información administrativa. A ello hay que sumar la aparición

de limitaciones de origen burocrático como el desconocimiento de las normas de acceso por parte de los funcionarios públicos, la existencia de barreras tecnológicas relacionadas con la información digital, que provocan dificultades para su consulta y la exclusión de amplios colectivos, y el abuso por parte de los responsables de los órganos administrativos del recurso a las excepciones que contemplan las leyes de acceso.

Todos esos frenos están presentes, incluso con mayor virulencia, cuando se trata de la indagación por el público de la acción de los servicios de inteligencia. Pero a ellos se añade uno más, cuya existencia condiciona el modo en que se puede ejercer el derecho de acceso a la información administrativa sobre inteligencia: la necesidad que tienen los servicios de inteligencia de actuar en secreto para poder cumplir su misión con eficacia. La obligación del secreto que impone la lógica del trabajo de inteligencia se ha esgrimido de hecho por todos los Estados sin excepción como la razón, en ningún caso tal vez mejor calificada como razón de Estado, no solo para negar el acceso a esa información, sino incluso para alejar del ojo público cualquier testimonio y documento sobre sus actos y resistirse al establecimiento de mecanismos de rendición de cuentas y de fiscalización de sus actividades. Sin embargo, las demandas de profundización democrática de nuestras sociedades han conducido en los dos últimos decenios en los países donde reina la democracia liberal a dar algunos pasos de índole legal para cambiar esta situación.

La clasificación de los documentos de inteligencia como secretos no afecta únicamente al acceso a la información que estos contienen durante su vida activa. Este hecho también tiene consecuencias en la conservación y el acceso de las series y los fondos que contienen documentos ya sin interés práctico para el ejercicio de sus funciones por el servicio de inteligencia productor o que proceden de agencias ya desaparecidas, pero que son testimonio de sus actividades. La misión de salvaguarda de las memorias institucionales y colectivas encomendada a archivos y archiveros se enfrenta en este ámbito, al menos, con cuatro fenómenos: la política sistemática de muchos Gobiernos de no desclasificar los documentos de inteligencia o de desclasificarlos con importantes restricciones y arbitrariedades; los numerosos sucesos de incautación de fondos por agencias de inteligencia o instituciones represivas de Estados y Gobiernos vencedores de conflictos durante el siglo XX; la destrucción accidental o, de modo más común, intencionada de miles de documentos a lo largo de la historia; y los problemas que plantea la selección y la conservación de millones y millones de datos e informaciones generados por las tecnologías de obtención de imágenes y de interceptación masiva de señales electromagnéticas (por ejemplo, conversaciones telefónicas, emisiones de radio...) y de comunicaciones electrónicas que realizan las agencias de inteligencia desde mediados del siglo XX. Estamos ante unos problemas comunes a todos los países, en menor o mayor medida, a los que se debe intentar dar

una respuesta efectiva y, en lo posible, internacional. Sin su resolución, la indagación de violaciones a los derechos humanos y la depuración de responsabilidades por la comisión de crímenes de Estado son empresas difíciles. Asimismo, la posibilidad de realizar una historia de la inteligencia estará muy comprometida y, además, se perderán documentos esenciales para el estudio de las relaciones internacionales, de las políticas de seguridad interior y exterior de numerosos países, de la actuación de grupos terroristas y de la acción de dictaduras y de Estados represivos en los siglos XX y XXI.

En este sentido, El *Segundo Congreso de Inteligencia*, organizado por el Instituto de Investigación en Inteligencia para la Seguridad y la Defensa de la Universidad Carlos III de Madrid y la Cátedra Servicios de Inteligencia y Sistemas Democráticos de la Universidad Rey Juan Carlos, celebrado del 22 al 24 de noviembre de 2010 en Madrid, con la participación de ponentes de cerca de veinte países, recogía en su quinta conclusión: “El estudio de la historia de la práctica de la inteligencia y de los servicios de inteligencia no se debe considerar únicamente un ejercicio de conocimiento erudito del pasado, sino que debe servir también para conocer el origen y la naturaleza de los actuales servicios de inteligencia, comprender mejor nuestro presente y elaborar un cuerpo de lecciones aprendidas capaz de guiar la práctica y proyectar intervenciones futuras”. Y, por ello, proponía como tarea primera a realizar para alcanzar ese objetivo lo siguiente: “El avance de los estudios históricos exige emprender como una tarea internacional un repertorio sistemático y completo de las múltiples fuentes de interés para el estudio de la historia de la inteligencia” (Segundo Congreso de Inteligencia, 2011). Se trata de un trabajo básico todavía inexistente, que debería inventariar tanto fuentes ya abiertas como tipos y repositorios de documentos todavía cerrados.

Estas acciones son muy necesarias para avanzar tanto en la apertura de archivos no solo de antiguas agencias de seguridad de índole represiva como en el acceso a cualquier documento público secreto con la garantía de un plazo de tiempo prudencial que no suponga riesgos para la seguridad nacional, pero también lo más pronto posible, y sin la realización de expurgos interesados para borrar testimonios. Para ello, la elaboración de esa guía de fuentes debería estar complementada con la redacción por un grupo de trabajo internacional de unas directrices internacionales de desclasificación de la documentación de interés para los estudiosos de la inteligencia, que pudieran servir para inspirar leyes y normas nacionales. La iniciativa de tal trabajo debería recaer, en lo posible, en una organización de prestigio y parte interesada, como el Consejo Internacional de Archivos, y sus conclusiones ser asumidas como recomendaciones a los Estados por alguna organización internacional, especialmente las vinculadas con la defensa de los derechos humanos en general y del derecho a la información en particular o con la transparencia administrativa.

Propuesta y relevancia de un problema de investigación

De acuerdo con el trasfondo descrito, este artículo quiere llamar la atención sobre la existencia y la relevancia social y política de un problema de investigación sobre el que apenas se ha ocupado la bibliografía especializada tanto en Archivística como en Estudios de Inteligencia y en Derecho: el carácter instrumental del acceso a los documentos de inteligencia en fase activa para que los organismos competentes puedan realizar el control democrático de los servicios de inteligencia. Para afrontar esta investigación, sin caer en maniqueísmos doctrinales apriorísticos sobre la superioridad del derecho a la información o de la seguridad nacional, es necesario analizar de modo previo cómo la misión y el modo de trabajo de los servicios de inteligencia determinan el carácter secreto de los documentos que producen y reúnen; y cómo esta necesaria naturaleza secreta en su origen condiciona tanto los modos de uso y de tratamiento por las instituciones productoras como las posibilidades de acceso por los ciudadanos en general, sus representantes políticos, los medios de comunicación y otras instituciones políticas y judiciales. Solo así la Archivística podrá desarrollar propuestas con capacidad para atender e influir sobre un asunto de candente actualidad en los albores del siglo XXI: la necesidad de garantizar y supervisar tanto la efectividad de las actuaciones como el respeto de los principios éticos y legales democráticos por parte de las agencias de inteligencia, especialmente en la lucha contra su principal objetivo durante el último decenio y el presente: el terrorismo.

El escrutinio periódico y normalizado de las acciones de los servicios de inteligencia y de las instituciones policiales en la democracia en este y otros terrenos exige repensar, y adecuar continuamente a la singularidad de los fenómenos y los cambios que se producen en la realidad, por quién, cómo, con qué condiciones y con qué garantías por igual para la libertad y la seguridad se puede acceder a los documentos y los archivos de inteligencia. Por ejemplo, la investigación y la depuración de posibles responsabilidades políticas, morales e incluso penales a la luz de las leyes nacionales y del derecho internacional sobre los actos cometidos en las prisiones de Guantánamo y de Abu Ghraib, los vuelos secretos de aviones de la CIA con detenidos acusados de terrorismo, los interrogatorios a islamistas radicales en cárceles clandestinas repartidas por diversos países, las operaciones encubiertas contra Al-Qaeda y organizaciones y países afines en la Guerra contra el Terror declarada por Estados Unidos bajo la presidencia de George W. Bush, las operaciones de inteligencia de Israel en su lucha contra Hezbo-lá, Hamás y los palestinos en general son asuntos, entre otros, que exigen resolver previamente el acceso a los documentos de inteligencia.

Asimismo, la apertura de procesos de paz en algunos Estados para superar conflictos internos enquistados en el tiempo, donde el recurso a la violencia por organizaciones terroristas y paramilitares y la lucha contra ellos por los servicios

de inteligencia gubernamentales, policiales y militares ha sido la norma (Sudáfrica, Colombia, Irlanda del Norte, España...), también han exigido en su momento o exigen o exigirán, con independencia de que sean procesos más o menos negociados, resolver cuestiones como el acceso a documentos y archivos de organismos de inteligencia involucrados; pero garantizando al mismo tiempo que ni el Estado pierde seguridad ni las agencias de inteligencia ven reducida su capacidad de actuación por el riesgo de que se desvelen algunas fuentes y procedimientos ni la reparación de las víctimas queda en entredicho por la ausencia de testimonios. Y mañana posiblemente serán objeto de procesos de paz y de transiciones a la democracia otros países hoy todavía inmersos en conflictos civiles armados o sufriendo las acciones de grupos terroristas o viviendo bajo la tiranía de dictaduras o de regímenes totalitarios de partido único o recién liberados de esas tiranías.

Y, por último, no se debe olvidar que también es una exigencia irrenunciable poner encima de la mesa la posibilidad de acceder a los documentos y los archivos de inteligencia no solo de instituciones desaparecidas, como recoge toda la doctrina sobre los archivos y los derechos humanos expuesta en el apartado anterior, sino también de aquellos servicios de inteligencia que siguen activos y comprometidos en mayor o menor medida con actividades de represión o de violaciones de derechos humanos -si bien con las cautelas y garantías necesarias para que no pierdan su operatividad en democracia-, si se quiere hacer realmente operativas las Comisiones de Verdad que en los últimos años se están creando o proyectando crear en numerosos países con la democracia recientemente recuperada o con el deseo de construirla. Estos países son en la actualidad Argentina, Brasil, Chile, El Salvador, Guatemala, Haití, Perú, Uruguay, Chad, Ghana, Kenia, Liberia, Marruecos, Nigeria, República de Sudáfrica, Sierra Leona, Togo, Uganda, Islas Mauricio, Islas Salomón, Timor Este e incluso Canadá. Dichas comisiones se consideran necesarias y claves para impulsar verdaderos procesos de reconciliación nacional, la investigación y el recuerdo de las violaciones de los derechos humanos o la finalización de la impunidad, al menos ética y moral, de quienes cometieron abusos y asesinatos, según el caso de cada país.

Archivos, memoria y derechos humanos

El trabajo de investigación que se propone en estas páginas se debe entender como una continuación y una ampliación hacia nuevos terrenos de los trabajos emprendidos en los últimos veinte años sobre la reivindicación del papel crucial de los archivos en las políticas de recuperación de la memoria y de reparación de las víctimas de la represión política. Una reivindicación que está presente en la mayoría de los países que viven procesos de transición democrática desde el inicio de esa transformación de regímenes totalitarios o autoritarios en democracia

o que termina de aparecer con el paso del tiempo y la creación de condiciones sociales y políticas que permiten su expresión y viabilidad. La última década del siglo XX ha sido crucial en su desarrollo y ha merecido una atención creciente por parte de los defensores de los derechos humanos, archiveros y público en general de la mano de las demandas más específicas de conservación y apertura de los archivos de instituciones de inteligencia utilizadas como policías políticas y órganos de represión por las dictaduras latinoamericanas y por los Estados comunistas de Europa durante la Guerra Fría.

El punto de origen doctrinal de la reivindicación de la función especial de los archivos desde esta perspectiva se encuentra en la demanda realizada a las Naciones Unidas por la *Conferencia Mundial sobre los Derechos del Hombre* celebrada en Viena en 1993 sobre la necesidad de intensificar la lucha contra la impunidad de las violaciones de los derechos humanos, que dieron lugar a un informe especial redactado por el jurista Louis Joinet en 1997. Este informe recoge cuarenta principios para la protección y promoción de estos derechos y la lucha contra la impunidad, que funda sobre los tres derechos que tienen todas las víctimas: el derecho de saber, el derecho a la justicia y el derecho de reparación. El derecho de saber implica el derecho inalienable al conocimiento de la verdad sobre su pasado por un pueblo, incluidas historias de opresión, y, en consecuencia, el deber por el Estado de adoptar medidas que permitan la conservación de la memoria, entendida como un patrimonio colectivo. De ahí Joinet dedujo la necesidad de preservar los archivos ligados a las violaciones de derechos humanos y dedicó cinco de sus cuarenta principios a su preservación y acceso. Estos principios fueron adoptados por la *Comisión de Derechos del Hombre de las Naciones Unidas* en 1997 y confirmados en la actualización del informe por Diane Orentlicher en 2005. En junio de 2007 un nuevo informe de esta Comisión volvía a recordar la necesidad de preservar y garantizar el acceso a los archivos que testimonian violaciones de los derechos humanos como un elemento fundamental de los instrumentos y las medidas institucionales que hacen efectivo el derecho a la verdad; al tiempo que recomendaba la realización de un estudio profundo sobre la relación de los archivos y de ese derecho.

De modo paralelo, la UNESCO y el Consejo Internacional de Archivos habían encargado en 1993 a un grupo dirigido por el archivero español Antonio González Quintana (1995) la realización de un informe y unas recomendaciones sobre el tratamiento jurídico y científico de los archivos de los servicios de seguridad de los regímenes represivos desaparecidos en los últimos veinte años. Entre sus recomendaciones figuraban los derechos colectivos de los pueblos a disponer de la integridad de su memoria, acceder a la verdad e identificar a los responsables de los crímenes; y, entre otros, los derechos individuales de las víctimas y de sus familias a conocer el destino de los parientes desaparecidos, los datos referentes a ellos y su rehabilitación. Es interesante reseñar que este informe indicaba

que la reunión y el acceso a los fondos de esos archivos no solo planteaban problemas materiales y científicos, sino que era ante todo una cuestión política y social. Los informes Joinet y González Quintana habían llegado a conclusiones casi idénticas desde perspectivas diferentes.

Un hito clave fue la celebración de la 38 *Conferencia Internacional de la Mesa Redonda de Archivos* (CITRA) el año 2003 en Ciudad del Cabo dedicada a la relación entre los archivos y los derechos humanos, y de la que surgió un grupo de trabajo internacional dentro del Consejo Internacional de Archivos sobre “Archivos y Derechos Humanos”. Allí se llamó la atención sobre la necesidad de preservación tanto de los archivos públicos de las fuerzas de seguridad y de los servicios de inteligencia, denominados del “terror”, como de los archivos privados de las organizaciones de defensa de los derechos humanos, llamados del “dolor”. Detrás de esta conferencia estaba la ejemplar experiencia de la *Comisión sobre la Verdad y la Reconciliación de Sudáfrica* y la transferencia de sus archivos a los Archivos Nacionales sudafricanos. En los últimos años este grupo de trabajo del ICA ha lanzado y apoyado diversas iniciativas en cumplimiento de las resoluciones de la CITRA del Cabo, como coloquios, informes y reuniones con archivistas, diplomáticos, juristas, miembros de organizaciones no gubernamentales... Merece destacarse la publicación de un manual para la gestión de los archivos de las ONG (Le Goff, 2004). Por su parte, la archivera norteamericana Trudy Huskamp Peterson, actual presidenta del citado grupo de trabajo del ICA, ha elaborado una guía para la preservación de la abundante documentación reunida y generada de las Comisiones de Verdad (Huskamp, 2005) y un informe sobre los tribunales penales internacionales (Huskamp, 2008).

Los estudios publicados sobre estos asuntos también han sido muy numerosos en los últimos quince años. La bibliografía en español o de autores españoles destaca en este panorama, con los trabajos pioneros de Antonio González Quintana (1999a, 1999b, 2004 y 2006) proseguidos por otros como los de Da Silva y Jelin (2002) Hernández Olivera (2007) Alberch (2008) o los recogidos en las *Actas del Congreso Internacional de Archivos y Derechos y Humanos* (2008).

Ante las experiencias de tratamiento de documentos de archivos de la represión y del dolor llevadas a cabo en los últimos años en diversos países, la proliferación de publicaciones y los avances doctrinales sobre la materia desde el informe UNESCO/ICA de 1995, González Quintana (2008) procedió a realizar un nuevo informe sobre los archivos policiales y de inteligencia cuyo contenido amplió también a los archivos de las ONG defensoras de los derechos humanos y de las instituciones judiciales y comisiones creadas para la investigación de la represión. El nuevo informe, con el título más ambicioso y más ajustado a la nueva realidad de *Políticas archivísticas para la defensa de los derechos del hombre*, demanda políticas archivísticas globales que comprendan tanto a los archivos públicos

como privados producidos sobre un territorio, y realiza una serie de recomendaciones de tipo operativo para su conservación, gestión y acceso. Otro proyecto en curso promovido por el Consejo Internacional de Archivos a destacar es la identificación y localización de archivos que documentan las violaciones de los derechos humanos, con objeto de realizar una guía internacional de fuentes (accesible en humanrightsarchives.org). Para permitir la gestión de esta guía se ha desarrollado en software libre, con financiación de la UNESCO, una aplicación informática para la organización y descripción de documentos de archivo denominada AtoM (*Access to Memory*, acceso a la memoria) pero cuyo desarrollo todavía no se ha completado y su uso aún no se ha generalizado. Mención destacada en la recuperación y conservación de archivos, sobre todo en América Latina, merecen las actividades emprendidas por la organización de voluntarios *Archiveros sin Fronteras* (www.arxiv.org) cuyo lema es “Conservamos los archivos para garantizar los derechos humanos”.

¿Qué es y cómo se produce la inteligencia?

La función pública de un servicio de inteligencia es conseguir, analizar e interpretar información no alcanzable por otras instituciones sobre los riesgos y las amenazas a la seguridad del país, a la estabilidad del Estado y a los intereses nacionales y sobre las diversas oportunidades de actuación existentes en estos ámbitos. Su acción está orientada principalmente a la prevención de peligros, que acompaña en lo posible de una dimensión proactiva orientada a identificar posibles ventajas frente a los adversarios. Las agencias de inteligencia persiguen despejar el escenario de incertidumbre en el que actúa el Estado al que sirven en los asuntos de seguridad política, económica, de orden público o militar tanto en el orden nacional como en el internacional. Los destinatarios de los informes de inteligencia son las más altas instituciones del Estado y, en particular, el Gobierno; y en el caso de las unidades de inteligencia enclavadas como departamentos subordinados en otras instituciones, como las fuerzas armadas o los cuerpos policiales, a los mandos directivos de esos organismos. En democracia, los servicios de inteligencia gubernamentales no tienen funciones policiales de investigación y represión de delitos o de adversarios políticos ni competencia para decidir por su cuenta medidas de neutralización de las amenazas, ya que tales decisiones conciernen exclusivamente a los gobernantes. No obstante, estas últimas funciones, junto con un mayor grado de autonomía en la acción, suelen estar presentes en los servicios secretos de los regímenes políticos autoritarios y totalitarios. En estos últimos casos, los archivos de los servicios de inteligencia contendrán también documentos que testimonian estas actividades; lo que permite caracterizarlos como archivos de la represión.

Inteligencia es un concepto polifacético dentro de la seguridad del Estado. Al mismo tiempo remite a un proceso, a un producto y a una organización (Lowenthal, 2006). Por inteligencia como proceso se entiende tres realidades complementarias: el método y los medios mediante los que recursos de información son requeridos, buscados, obtenidos, transformados mediante la aplicación de conocimiento y difundidos; la propia protección del proceso y de sus frutos mediante actividades de contrainteligencia y, tercero, las operaciones encubiertas de obtención de información, influencia e intervención sobre la realidad que pueden ser concebidas y ejecutadas por encargo del decisor político o militar. Como producto, la inteligencia es el resultado de llevar a cabo esos procesos, es decir, tanto los informes que recogen la estimación de una situación y de su posible evolución con una orientación a la toma de decisiones, como los efectos de las acciones encubiertas y de contrainteligencia. Y la inteligencia como organización denota a las instituciones o a los organismos del Estado que se encargan de esas funciones.

Las tres facetas del concepto inteligencia (producto, organización y proceso) son totalmente interdependientes. Porque la misión específica encomendada a un servicio de inteligencia concreto por la ley, la estructura de la que este se dota, las normas que regulan su actividad y la relación que mantiene dentro de la comunidad de inteligencia con otras agencias determinan las actividades que puede realizar durante el procedimiento de creación de inteligencia y el carácter de los productos a elaborar. Y, al mismo tiempo, las experiencias acumuladas por una organización de inteligencia durante sus procesos y los resultados que logra influyen en cómo el servicio se organiza, dirige y controla y lleva a cabo nuevos procesos de inteligencia.

Los servicios secretos crean inteligencia mediante una secuencia de actividades complementarias e interrelacionadas de obtención, tratamiento y transformación de la información en un producto de inteligencia ajustado a las necesidades específicas del cliente mediante la integración de información procedente de múltiples fuentes y la aplicación del conocimiento de los analistas. Esas actividades se estructuran en cinco etapas complementarias e ineludibles para su buen éxito: planificación del proceso de creación de inteligencia, obtención de información, producción de inteligencia a partir de la aplicación de conocimiento para el análisis y la interpretación de esa información, comunicación de los resultados y evaluación final. Un proceso habitual de producción y transferencia de inteligencia comienza con una previa identificación por parte del servicio de las necesidades de inteligencia de sus usuarios o la realización de un requerimiento específico por el cliente, continuada en cualquier caso por una planificación de las acciones y de los recursos que se precisan para su consecución. A partir de ahí, se inicia la obtención de datos y de información de fuentes de información muy específicas y mediante instrumentos y técnicas muy peculiares y en su mayoría

reservadas legalmente para su uso por los servicios de inteligencia, que se agrupan tradicionalmente en tres tipos: de procedencia humana (agentes sobre el terreno, informadores, colaboradores, contactos, espías, prisioneros...), de origen técnico con sus diversas subespecies (interceptación de señales y transmisiones de cualquier tipo, captación de emisiones electrónicas, captura de imágenes mediante cámaras y sensores, obtención y decodificación de comunicaciones de radio, video, telefonía, Internet...) y de carácter abierto (todo recurso documental con cualquier tipo de contenido, soporte y forma puesto a disposición pública por su autor). La materia informativa conseguida puede exigir su descriptado, desciframiento y traducción antes de su incorporación en sistemas de información específicos y ultrasecretos para su control, procesamiento, almacenamiento, organización y recuperación mediante técnicas de gestión documental y de información adaptadas a sus características específicas. Los diversos órganos de obtención alimentan con flujos de información continuos los sistemas de información de los servicios secretos. De esos sistemas, los órganos de análisis extraen la información que necesitan para, tras determinar su fiabilidad, credibilidad y pertinencia, proceder a su integración, análisis e interpretación con vistas a resolver las necesidades de inteligencia planteadas durante la fase de planificación. El uso de las tecnologías de la información más avanzadas suele ser habitual, sobre todo durante la colecta de información, para lo que se cuenta con los más modernos instrumentos y sistemas de escucha, de observación geoespacial, de rastreo de comunicaciones y de explotación de grandes almacenes de datos digitales para la captación y el procesamiento de la voz humana, la imagen y la información digital accesible por Internet. El uso de las tecnologías de la información y de las comunicaciones más sofisticadas es vital para un servicio de inteligencia, si quiere alcanzar una superioridad tecnológica respecto al adversario que permita romper los sistemas de protección de sus secretos, realizar análisis y estimaciones más acertadas y rápidas sobre sus intenciones, mejorar los procesos de cooperación y coordinación basados en el intercambio de información y el análisis conjunto con los aliados y preparar y apoyar el despliegue de operaciones encubiertas y de contrainteligencia más efectivas. Finalmente, la dirección del servicio de inteligencia comunica los resultados, normalmente por medio de un informe escrito pero también en ocasiones oral, al cliente final, que tomará de acuerdo con la inteligencia recibida las decisiones que considere oportunas. Por último, se procede a una evaluación periódica de la calidad del producto obtenido y del proceso seguido, para la que se intenta recibir una retroalimentación por parte del cliente.

Cada servicio de inteligencia ajusta este modelo ideal de proceso de producción y transferencia, denominado tradicionalmente ciclo de inteligencia, a sus necesidades, su estructura, sus recursos materiales y humanos y su cultura organizativa. Porque la inteligencia, aunque sea un proceso y un producto de carácter burocrático muy singular y único dentro de los realizados por las instituciones



del Estado, está totalmente mediada, como cualquier otro procedimiento y acción de la Administración, por el contexto sociopolítico que la rodea, la historia de la institución específica que la lleva a cabo y las leyes y normas que la regulan. Por eso, y en este caso exactamente igual que cualquier otra institución, las actividades de los servicios de inteligencia dejan una intensa huella documental: bases de datos relacionales y documentales, grabaciones sonoras, colecciones de imágenes y depósitos de textos de variado contenido y forma, pero con una creciente preponderancia de lo digital, que recogen la información reunida durante las acciones de obtención, los informes internos que se producen con base en esa información, los documentos de comunicación de las estimaciones de inteligencia a los clientes, la documentación de apoyo generada de modo espontáneo durante la planificación y la ejecución de operaciones, las series documentales producidas por las organizaciones de inteligencia como efecto de la administración de sus recursos... En todas las actividades y etapas se crean, reúnen y organizan documentos y se realizan acciones vinculadas con la gestión de información. Esto permite considerar a la inteligencia como un producto de carácter y de origen informacional y entender y analizar, en última instancia, el núcleo de las organizaciones que la producen como sistemas de gestión de la información y del conocimiento (Esteban y Navarro, 2003; Esteban y Carvalho, 2011a). Esta perspectiva informacional para comprender la naturaleza y el funcionamiento de los servicios de inteligencia, que proponemos y que recientemente hemos aplicado con detalle para su caracterización y análisis en otro lugar (Esteban y Carvalho, 2011b), complementa las habituales aproximaciones politológicas, históricas y jurídicas; por lo que contribuye, de este modo, a superar la tradicional mutua ignorancia entre la Ciencia de la Información y el mundo de la inteligencia (Cronin, 2005).

Las actividades más secretas y polémicas: contrainteligencia y operaciones encubiertas

Ayudar al Gobierno de la nación a despejar la incertidumbre y prevenir acciones de terceros que puedan afectar a la seguridad nacional interior y exterior es, sin duda, la misión fundamental de un servicio de inteligencia. Pero para la cuestión que nos ocupa, el derecho de acceso a los documentos secretos y su relación con el control de las agencias de inteligencia, son incluso más relevantes las otras dos funciones de esos servicios complementarias a la de producir conocimiento preventivo sobre la seguridad, y a las que ya se ha hecho referencia: la contrainteligencia y las operaciones encubiertas (Esteban, 2011).

El fin de la contrainteligencia es proteger y preservar la seguridad, la fortaleza política, militar, científica y económica y los secretos de la nación mediante la identificación y la desactivación de operaciones de inteligencia encubiertas

(espionaje, sabotaje, subversión...) llevadas a cabo por poderes exteriores hostiles e incluso a veces amigos. El objetivo es salvaguardar toda información de interés para la seguridad nacional que ha recibido la calificación oficial como reservada o secreta, del acceso por personas no autorizadas. Durante la segunda mitad del siglo XX la mayor parte de la información que entraba en esta categoría era la reunida o producida por organismos estatales y por organismos de investigación y empresas contratistas de programas estatales en la industria militar y la energía nuclear. Pero con la aparición de las amenazas asimétricas, la promoción de la inteligencia económica y la ampliación del concepto de seguridad a otros terrenos que la defensa del territorio, el tipo y el volumen de información de interés público a proteger como secreto se han ampliado, ya que su obtención por terceros puede suponer tanto riesgos para la seguridad general (por ejemplo, los planos y los sistemas de vigilancia y de seguridad de infraestructuras críticas como una central nuclear, un tendido de red eléctrica, una red de metro, un sistema de abastecimiento de agua potable, un puerto...) como pérdida de competitividad de la nación (por ejemplo, patentes, procedimientos industriales complejos, resultados de proyectos de investigación, ofertas económicas en concursos internacionales...). Aunque la eficaz custodia de la información calificada como secreto es una responsabilidad del órgano administrativo productor cuando se trata de documentos de origen público o de las organizaciones que las crean y custodian cuando se trata de documentos privados, los servicios de inteligencia también tienen adscritas funciones de educación del personal en cultura de seguridad, de cooperación en su protección mediante asesorías y auditorías de los sistemas informáticos y de comunicaciones e incluso de vigilancia de su uso (caso del material susceptible de doble uso civil y militar, biotecnologías...).

La contrainteligencia también se ocupa de la seguridad de las instalaciones y los miembros de un servicio de inteligencia frente al espionaje. Dentro de este ámbito se da gran importancia a la relación del personal de las agencias de inteligencia con la información que posee su agencia. Esta relación se rige por dos principios: la compartimentación y la necesidad de saber; por lo que se restringe el acceso a la información secreta únicamente a quienes concurre en ellos la doble condición de disponer de autorización para su conocimiento y de necesitarla para un trabajo específico en curso. Los miembros de un servicio de inteligencia reciben acreditaciones de seguridad, que fijan los sistemas de información y los documentos a los que pueden acceder, con objeto de reducir el daño que pudiera ocasionar una fuga de información. La prohibición de sacar documentación fuera de las instalaciones autorizadas para su uso, incluso por aquellos que tienen derecho a su conocimiento suele ser una disposición complementaria para evitar filtraciones, pérdidas, robos... La educación continua del personal en medidas de seguridad de la información es también una actividad periódica en los servicios de inteligencia.

Otro tipo especial de contrainteligencia es el contraterrorismo cuando se busca prevenir la acción de grupos terroristas y se organizan actividades encubiertas para la obtención de información, la infiltración e incluso la desarticulación por medios más o menos expeditivos. La creciente importancia en las dos últimas décadas de la amenaza terrorista ha llevado también a numerosos países a establecer centros antiterroristas, bien dentro de los servicios de inteligencia, bien comunes a toda la comunidad de inteligencia nacional con la participación de las diversas agencias de inteligencia (interiores y exteriores) y policiales vinculadas con la lucha contra el terrorismo. La complejidad de las actividades de contrainteligencia y el carácter transnacional del terrorismo y del crimen organizado no solo invitan a una sinergia de esfuerzos dentro de una comunidad de inteligencia nacional, sino que demandan incluso una estrecha cooperación internacional entre servicios de inteligencia amigos para hacer frente al adversario común. Una cooperación nacional e internacional que para ser eficaz requiere no solo compartir información con el aliado, sino también colaborar en la realización de algunas de sus actividades e incluso organizar y ejecutar operaciones conjuntas. Esta cooperación plantea nuevos retos para la gestión de los documentos de los servicios de inteligencia; entre los principales, la elaboración de normas de acceso a documentos sensibles por miembros de otras agencias, la creación de bases de datos y repositorios de información digital conjuntos, la reunión y conservación de los documentos generados por estos centros antiterroristas y el acceso por las autoridades nacionales que controlan la actividad de los servicios a archivos en cuya formación participan agencias de otros países.

El hecho de que la contrainteligencia sea ultrasecreta (el corazón de la cebolla, la actividad más secreta entre todas las que llevan a cabo los servicios) y de extrema importancia para la seguridad nacional no se debe esgrimir como impedimento para someter sus actividades a control y rendición de cuentas ni como excusa para espiar a los ciudadanos. Vigilar a personas de modo indiscriminado, sin sospechas fundadas de que supongan una amenaza para la seguridad y sin algún tipo de control exterior al servicio de inteligencia, solo es propio de las agencias con carencias de actuación democrática o de regímenes totalitarios. Ejemplos de estas actividades impropias son las amplias redes de espionaje que organizaron la *Stasi* en la extinta República Democrática de Alemania o la *Securitate* en Rumanía durante la era soviética para vigilar y controlar a sus poblaciones; o en Estados Unidos la investigación a la que el FBI sometió a más de medio millón de ciudadanos norteamericanos durante la Guerra de Vietnam, generalmente pacifistas y activistas de los derechos civiles, sin que ningún caso terminase en una acusación judicial. Cuando se producen estos casos de modo masivo y planificado como una política de Estado, es habitual la generación de enormes volúmenes de documentos como ha puesto de manifiesto la apertura de los archivos de la *Stasi*. La tentación de realizar estas prácticas está siempre presente, sobre todo

cuando el enemigo tiene gran capacidad de ocultación entre la población, como los terroristas y sus redes de apoyo y colaboración.

Por último, la contrainteligencia también se ocupa de proteger las operaciones encubiertas organizadas por el servicio contra la penetración y la interrupción por terceros. Todos los servicios de inteligencia han realizado y realizan operaciones encubiertas; aunque por sistema lo nieguen, ya que la negación forma parte de las reglas del juego. Si se dedicaran únicamente a la creación de conocimiento sobre el entorno de seguridad de un Estado serían simples unidades de análisis. Elaboración de inteligencia, contrainteligencia y operaciones encubiertas son las tres caras de todo servicio de inteligencia. Su reunión en un mismo organismo tiene un efecto sinérgico y aumenta la eficacia y la eficiencia de cada una de ellas. Las operaciones clandestinas son necesarias en muchas ocasiones para obtener información sobre las intenciones ocultas, las actividades secretas y la potencia real del adversario, que de otro modo no se podría conseguir. La defensa del Estado y de la seguridad nacional también exige, tras el descubrimiento y la estimación de la amenaza por el servicio de inteligencia, recurrir en situaciones extremas al desarrollo de actividades de influencia sobre un tercero en pro de los intereses nacionales, al espionaje y la infiltración en el enemigo, a la neutralización de peligros y adversarios mediante acciones de intervención directa sobre la realidad, al contacto con enemigos para negociar fuera del ojo público o a la organización de acciones de ayuda a ciudadanos y empresas que son amenazados o agredidos en el exterior precisamente por ser miembros de un determinado país. La clandestinidad y el encubrimiento de las operaciones son imprescindibles para alcanzar los objetivos pretendidos sin que lo descubra el adversario o porque se tratan de acciones que no se considera conveniente declarar o exigen el anonimato del Gobierno responsable haciendo imposible, o al menos difícil, el establecimiento del origen de la acción. También pesa la necesidad de realizar actividades que es imposible ejecutar de modo abierto o por medio de la diplomacia. La discreción, el silencio y la ocultación, en definitiva el secreto, son en muchas ocasiones necesarios porque las condiciones en las que las operaciones se producen o los medios que se deben emplear impiden que se puedan llevar a cabo de modo abierto con garantías de éxito o exigen actuar en zonas grises de la legalidad, por el hecho de estar poco o nada definidas o sujetas a diversas interpretaciones jurídicas.

Esto no significa que las actividades encubiertas sean por naturaleza ilegales, que deban ser contrarias al Estado de derecho, que deban traspasar unos determinados límites éticos o que no hayan de estar sometidas a controles como el resto de las acciones de un servicio de inteligencia. Para evaluar cualquier acción de inteligencia hay que tener en cuenta, entre otros elementos, sus motivaciones, su contexto, el modo en el que se ha llevado a cabo, sus fundamentos jurídicos y legales, sus implicaciones éticas y morales y sus consecuencias. Pero es evidente

que la obligada necesidad de actuar en la sombra e incluso de poder negar la existencia de una operación exige de los servicios de inteligencia un esfuerzo de protección añadido de la información generada en torno a la operación y también aumenta el riesgo de destrucción de los documentos una vez finalizada la operación. No se escapan las dificultades extras a las que se deben enfrentar los órganos políticos del Estado para acceder a documentos que testimonian esas operaciones durante los procedimientos habituales de control de la actividad de los servicios de inteligencia, e incluso por las autoridades judiciales cuando se emprenden, si ha lugar, investigaciones de carácter penal. Asimismo, el cuándo y el cómo desclasificar los documentos sobre operaciones encubiertas suele generar agudos debates e incluso fricciones entre los servicios de inteligencia y los Gobiernos, por un lado, y los medios de comunicación, los historiadores, las organizaciones de defensa de derechos humanos y el público en general, por otro. Se trata de un asunto todavía no resuelto a satisfacción de todos los interesados, incluso en las actuales democracias; y también se nos antoja de difícil resolución, en especial en todo lo que rodea operaciones que han podido violar derechos humanos o aquellas en las que el Gobierno de un país desea seguir negando su existencia.

La naturaleza secreta de la inteligencia

A la vista de lo anterior, se puede concluir que el trabajo de un servicio de inteligencia está presidido por el secreto: es la barrera a destruir y el objetivo a desvelar del adversario; es la medida de protección de la propia información e inteligencia; y es el modo y el ámbito en el que operan los servicios de inteligencia, ya que romper el secreto del otro exige actuar con sigilo. El secreto afecta a las tres dimensiones de la inteligencia: el proceso de creación está protegido por la reserva, la estructura, los recursos y las actividades puestas en marcha se mantienen ocultos y el producto y la materia con la que se realiza se pretenden inaccesibles. El secreto busca asegurar que determinadas misiones, fuentes, materias, identidades, hechos o decisiones no sean conocidos por quienes podrían valerse de esa información para actuar contra los intereses del país (Esteban y Carvalho, 2011a). Como indica Herman (2001: 5) el secreto es el sello de la inteligencia: la base de su relación con el Gobierno y la sociedad y de su propia autoimagen.

En última instancia, el secreto que rodea a la inteligencia es al mismo tiempo una prerrogativa y un imperativo del poder del Estado para proteger un preciado bien, que se justifican ante la sociedad en democracia apelando a su condición de requerimiento imprescindible para la seguridad nacional. Las filtraciones de información sensible y reservada a los medios de comunicación y el

compartimiento de inteligencia por parte del Gobierno con grupos políticos, incluso de la oposición, o con países amigos no son una ruptura del secreto, siempre que no se comprometan fuentes y métodos de obtención de información. Todo lo contrario, la comunicación de inteligencia se debe entender como un uso de la inteligencia para hacer política. Representa, de modo explícito, una reafirmación por el gobernante de que únicamente él tiene derecho de acceso y libre disposición de la inteligencia. La inteligencia no se puede separar de la política porque la inteligencia es, en sentido estricto, política.

El secreto de las acciones y los productos de un servicio de inteligencia es siempre el resultado de un acto expreso de la autoridad competente, denominado clasificación en el argot de los servicios secretos. Se trata de un acto regulado por una ley mediante el que tras una valoración de la naturaleza de un asunto, este se declara clasificado en nombre de la seguridad del Estado o de la nación; y, por tanto, prohibida su publicidad y restringido el acceso a toda la documentación relacionada durante un período de tiempo. Únicamente tienen conocimiento de las materias clasificadas los órganos y las personas a los que las leyes de cada nación facultan para ello, respetando las formalidades y las limitaciones que se determinen. El acceso a esa información está tan restringido que las normas de todos los países obligan a guardar a los oficiales de inteligencia, como una medida de protección añadida, estricta reserva y secreto sobre sus acciones y sobre todo documento, asunto, identidad u operación que hayan conocido por su condición de miembros del servicio, incluso después de su baja o retiro.

Pero el secreto no es un valor absoluto, sino que es relativo y tiene diversos grados. La protección que se otorga a un asunto puede variar en el tiempo, de acuerdo con la evolución de factores internos y externos a los propios servicios de inteligencia. Las reglas de clasificación también varían de un Estado a otro. Los Estados Unidos de Norteamérica y la OTAN utilizan la siguiente escala de menor a mayor protección: restringido, confidencial, secreto y alto secreto; donde la clasificación se suele acompañar mediante un código que indica a quién se puede distribuir el documento y quién puede acceder a él. En España las materias clasificadas se califican con las categorías de reservado o de secreto. En general, la clasificación más baja se otorga a materias cuya divulgación podría afectar a los intereses fundamentales de la nación y la más alta a aquellas cuyo conocimiento podría comprometer o suponer un alto riesgo para la seguridad. Finalmente, muchos asuntos considerados secretos son desclasificados con el tiempo y se permite el conocimiento por los ciudadanos en la forma que determina la norma reguladora del acceso a los documentos administrativos de cada país. La desclasificación puede tener su origen en el cumplimiento del período de clasificación que marca la ley para cada asunto; en una decisión de la autoridad tras constatar que una materia ha perdido las condiciones necesarias para continuar clasificada

como secreto oficial, ya que su conocimiento público no supone riesgos para la seguridad; y en la apertura de los archivos de los servicios secretos tras el colapso y la desaparición del régimen político al que servían.

El secreto no es contrario al principio general de publicidad de la actuación de los poderes públicos al que obligan las leyes fundamentales de los Estados democráticos. De hecho, esas propias leyes o las que las desarrollan protegen el secreto en ciertos ámbitos y la publicidad en otros, reservando en general la publicidad absoluta exclusivamente para la producción de normas jurídicas y el pronunciamiento de sentencias judiciales. La existencia del secreto es legítima en el Estado de Derecho, máxime cuando se trata de proteger la acción de quienes lo defienden frente a sus enemigos, pero siempre y cuando no sea incondicional y perjudique otros derechos fundamentales, como el derecho a la intimidad (Ruiz, 2007). Pero aun reconociendo esa legitimidad, esto no explica por qué las leyes que regulan los secretos oficiales son tan generosas en permitir la aplicación del carácter de secreto a tantos tipos de información.

Para ello hay que recurrir a la “teoría del mosaico”, ampliamente aplicada en Estados Unidos y otros países tras los atentados terroristas del 11 de septiembre de 2001, cuyo origen se remonta a los años setenta del siglo pasado. Según esta teoría, el Gobierno puede retener por motivos de seguridad nacional información que de modo aislado parece inocua, pero cuya posesión por parte de un actor entendido en la materia, como una agencia de inteligencia hostil, podría ser peligrosa si la combina con otras informaciones. Pequeñas piezas de información, en principio inocentes, cuando se combinan como teselas con otros ítems pueden formar un “mosaico de información” que puede ser muy peligroso para la seguridad nacional (González, 2011). El núcleo de la teoría del mosaico, es decir, el riesgo que plantea la sinergia informativa, puede ser aceptado como válido; lo que ya es más discutible es el abuso en su aplicación, que puede conducir a un gran control y restricción de la información por parte de las autoridades, por ejemplo ampliando la información exenta de publicidad y reteniendo información ya desclasificada por el paso del tiempo, con la excusa de que sigue siendo sensible porque de su combinación con otra pueden resultar riesgos para la seguridad nacional, como hizo la administración Bush con la información relativa a armas de destrucción masiva. Ciertamente, se deniega a posibles adversarios información con un posible valor potencial para estos, pero también se limita gravemente el escrutinio público y la actuación de los tribunales en caso de demandas donde tal información pudiera ser utilizada como prueba judicial. Una aplicación de la doctrina del mosaico más acorde con la transparencia administrativa sería exigir al Gobierno que se acoja a ella para negar el acceso a una información, indicar y explicar de modo específico para qué parte de la seguridad nacional representa una amenaza su divulgación.

La información clasificada en España: la Oficina Nacional de Seguridad

Para terminar, ilustraremos parte de lo expuesto sobre la clasificación de la documentación de inteligencia con la descripción de los procedimientos y las normas sobre protección de información clasificada que rigen en España dependientes de la Oficina Nacional de Seguridad (ONS). Esta oficina fue creada en 1983 como un órgano de trabajo adscrito a la dirección dentro del servicio de inteligencia español, denominado entonces Centro Superior de Información de la Defensa (CESID) y desde el año 2002 Centro Nacional de Inteligencia (CNI). Su misión, según el artículo 4 letra f de la Ley 11/2002, de 6 de mayo, reguladora del CNI, es velar por el cumplimiento de la normativa relativa a la protección de la información clasificada tanto nacional como aquella que es entregada a la Administración o a las empresas en virtud de tratados o acuerdos internacionales suscritos por España. Sus principales funciones son la realización de acuerdos para el intercambio y la protección de información clasificada con un tercer país o una organización internacional, que deberán ser aprobados por las Cortes Generales como establece el artículo 94 de la Constitución; el establecimiento de relaciones con las autoridades nacionales de seguridad de otros países y los departamentos de seguridad encargados de proteger la información clasificada de organizaciones internacionales (Unión Europea, OTAN, Agencia Espacial Europea, la Organización Conjunta de Cooperación en Materia de Armamento...); la participación en foros internacionales donde se traten y establezcan procedimientos de seguridad para la protección de información clasificada, en representación de España; la expedición de habilitaciones personales de seguridad para quien deba acceder por su trabajo a información clasificada; la expedición de habilitaciones de la misma índole para empresas y establecimientos; y la acreditación de órganos, instalaciones y sistemas que manejan información clasificada.

La información clasificada es toda información o material que ha recibido una clasificación de seguridad, de acuerdo con las formalidades y los requisitos previstos en la legislación, con objeto de protegerla contra su divulgación no autorizada. Las materias clasificadas están definidas en España por la Ley 9/68, de 5 de abril, modificada por la Ley 48/78, de 7 de octubre, sobre Secretos Oficiales, como los asuntos, actos, documentos, informaciones, datos y objetos cuyo conocimiento por personas no autorizadas pueda dañar o poner en riesgo la seguridad y la defensa del Estado. Las dos calificaciones previstas son secreto y reservado. La facultad para asignar una de estas calificaciones corresponde al Consejo de Ministros y a la Junta de Jefes de Estado Mayor, y no puede ser transferida ni delegada. Las normativas que desarrollan esa ley también se ocupan de las materias objeto de reserva interna, que se definen como esos asuntos, actos, documentos... cuyo conocimiento por alguien no autorizado puede afectar a la seguridad del

Estado, amenazar sus intereses o dificultar el cumplimiento de su misión; y que, según se reconoce internacionalmente, pueden recibir la calificación de confidencial y difusión limitada, de acuerdo con una normativa específica de cada Ministerio. Las autoridades competentes para ello son los ministros, los secretarios de Estado y los subsecretarios en sus respectivos departamentos y los Jefes de los Estados Mayores de la Defensa, Ejército, Armada y Aire, pudiendo delegar oficialmente dicha atribución.

La responsabilidad de la protección de la información clasificada, tanto de su custodia como de su manejo, recae en el jefe del organismo o entidad que la posee. Para ello deberá disponer la creación de un órgano de control o servicio de protección de materias clasificadas, que se ocupará del registro, control, distribución, custodia, almacenamiento, reproducción y destrucción de la información clasificada; y que actuará bajo el mando y la responsabilidad de un jefe de seguridad. Asimismo, se debe disponer una zona de seguridad, consistente en una instalación con un perímetro definido dentro de la que existe un control y unas condiciones de protección específicas. Los documentos clasificados con un grado de confidencial o superior se almacenan en edificios, locales o habitaciones denominadas zonas de acceso restringido, que disponen de las medidas y los procedimientos de seguridad adecuados para garantizar su protección. Estas zonas cuentan con un plan de protección y un responsable de seguridad y están debidamente acreditadas por la ONS. Por su parte, la información calificada con el grado de difusión limitada se debe manejar en una zona administrativa de protección, que cuenta con un perímetro claramente definido y un control de las personas, el material y los vehículos que ingresan.

El acceso a la información clasificada con un grado de confidencial o superior exige estar en posesión de una habilitación personal de seguridad concedida por la ONS, en nombre del Gobierno, que reconoce la capacidad e idoneidad de esa persona para acceder a la información y su conciencia de la obligación de reserva y de las responsabilidades derivadas de su incumplimiento. También es imprescindible para acceder a esa información tener de modo simultáneo a la habilitación de seguridad la necesidad de conocer, es decir, que la persona habilitada requiera del acceso a esa información para desempeñar sus tareas y cometidos oficiales. La necesidad de conocer de una persona es determinada por su superior jerárquico.

El acceso a la información clasificada implica la prohibición de revelar esa información a terceros no autorizados con un deber de reserva permanente en el tiempo mientras esa información permanezca clasificada. Asimismo, el usuario de esta información es durante su manejo responsable de su protección en todo momento, debiendo evitar formas de acceso no autorizadas, como la lectura en sitios públicos, tener el máximo cuidado a la hora de usar dispositivos como teléfonos y ordenadores y transmitir esa información únicamente a través de sistemas y redes

de comunicación formalmente autorizados. En el caso de que la información clasificada deba salir de las zonas de seguridad por circunstancias tales como transporte autorizado o asistencia a una reunión, los documentos no podrán ser abandonados o perdidos de vista en ningún momento y bajo ninguna circunstancia. La divulgación no autorizada tiene la consideración de delito o falta y lleva consigo unas responsabilidades penales o disciplinarias conforme al Código Penal o el Código Penal Militar, según el caso. Las sanciones pueden ir desde multas hasta penas de prisión, unido a inhabilitación, suspensión de empleo o cargo público, etc.

Por último, es importante reseñar que se tiene plena consciencia de que la seguridad de la información tiene una estrecha dependencia de la seguridad de los documentos que la contienen. La Autoridad Delegada para la Seguridad de la Información Clasificada ha publicado la norma *NS/04 Seguridad de la Información*, cuya segunda edición es de octubre de 2009, donde se especifican los procedimientos a seguir para el correcto manejo de la documentación clasificada, esté en papel o soporte informático, a lo largo de su vida útil. Esta norma trata con gran detalle cómo se deben realizar actividades tales como el transporte, el almacenamiento, el registro, la custodia, la consulta, la distribución, la traducción, la reproducción, la cesión y la destrucción de documentos, con el fin de mantener un nivel de seguridad homogéneo de acuerdo con el grado de clasificación de cada documento. También hay que reseñar la existencia desde 1982 de un Registro Central de la Documentación Clasificada de alto nivel (reservado y secreto o grados equivalentes de otras naciones) encuadrado dentro de la ONS, que tiene por misión realizar el registro, control y distribución de ese tipo de documentación que entra o sale del territorio español perteneciente a organizaciones internacionales o de otros países con los que existe un acuerdo para la protección mutua de información clasificada. La estructura piramidal establecida para la protección de la información clasificada en España se encuentra recogida en la norma *NS/01 Infraestructura Nacional de Protección de la Información Clasificada*, también con una segunda edición del 2009.

Conclusión

Como ya hemos escrito en otro lugar, es un reto de las sociedades democráticas alcanzar un equilibrio entre el necesario carácter reservado y oculto de la función estatal de inteligencia y la consideración de la democracia como un libre espacio público de comunicación basado en el derecho a la información (Esteban y Carvalho, 2011a). Porque no se trata de elegir entre seguridad y libertad, de reforzar una limitando la otra, ya que en democracia la seguridad solo puede existir en un contexto de respeto a los derechos civiles y el imperio de la ley. Está fuera de

discusión que los servicios de inteligencia necesitan guardar secreto sobre sus objetivos, procesos, recursos y fuentes de información para garantizar su efectividad. Pero también es cierto que el secreto a ultranza impide el control de sus actividades y abre la puerta a la tentación de aplicar métodos y emprender acciones no contempladas o incluso no permitidas por la ley. Además, en un Estado democrático los servicios de inteligencia, aunque gocen de la prerrogativa de restringir el conocimiento de su actividad, también tienen, como cualquier otra institución pública, el deber de someter sus actividades a las leyes, a las normas jurídicas y a las reglas éticas de carácter universal, así como de ser controlados por la sociedad a través de los poderes ejecutivo, legislativo y judicial. El secreto es vital para el éxito de las actividades de inteligencia; sin embargo, restricciones excesivamente severas para el acceso a la información de inteligencia tienden a inhibir el debate público y el control de los servicios. Los Gobiernos y las agencias de inteligencia tienden a sobreclasificar la información y a realizar una clasificación indiscriminada. Por ello, es necesario conseguir un punto de encuentro entre el derecho a conocer de los ciudadanos, el derecho de informar de los medios de comunicación y la obligación de reserva de los servicios de inteligencia que se deriva de sus especiales responsabilidades y acciones. La existencia de medidas regulares de desclasificación de información y la contención en la aplicación de la teoría del mosaico para mantener cierta información fuera de circulación son tan importantes como la presencia del secreto.

Lograr ese punto de encuentro exige previamente la realización de estudios doctrinales y la propuesta de directrices y recomendaciones prácticas de carácter internacional, capaces de impulsar la aprobación de leyes y normas nacionales y la implantación de programas de gestión documental que permitan el acceso a los archivos y los documentos de inteligencia en su fase activa por parte de los organismos competentes para llevar a cabo el control democrático de los servicios de inteligencia, con un sistema de garantías que vele por igual por la seguridad nacional y el derecho a la información. Esto se debe realizar con una perspectiva pluridisciplinar que atienda por igual a los principios y los métodos de la Gestión de Documentos, la Archivística, los Estudios sobre Inteligencia y la doctrina sobre los Derechos Humanos. Asimismo, es fundamental proceder a la comparación de diversas realidades nacionales, atendiendo, en particular, a sus específicas legislaciones y normativas sobre secretos oficiales y acceso a la información, sus particulares estructuras y comunidades de inteligencia, sus singulares condiciones sociales y políticas y la especial incidencia de la actividad de grupos terroristas en su territorio. Todo ello con el fin último de poder conciliar el deber de secreto de los servicios de inteligencia con el derecho a conocer de la sociedad.

Bibliografía

- Actas del Congreso Internacional de Archivos y Derechos y Humanos: el acceso y la desclasificación de documentos*. 2008. Sarriá de Ter: Ayuntamiento de Sarriá de Ter; Diputación de Girona; Archiveros sin Fronteras.
- ALBERCH FUGUERAS, Ramón. 2008. *Archivos y derechos humanos*. Gijón: Trea.
- AUTORIDAD DELEGADA PARA LA SEGURIDAD DE LA INFORMACIÓN CLASIFICADA. 2009. *NS/04 Seguridad de la Información*. Disponible en: http://www.cni.es/comun/recursos/descargas/NS-04_Seguridad_de_la_Informacion.pdf
- AUTORIDAD DELEGADA PARA LA SEGURIDAD DE LA INFORMACIÓN CLASIFICADA. 2009. *NS/01 Infraestructura Nacional de Protección de la Información Clasificada*. Disponible en: http://www.cni.es/comun/recursos/descargas/NS-01_Infraestructura_Nacional_de_Proteccion_de_la_IC.pdf
- BISHOP, Cheryl Ann. 2011. *Access to Information As a Human Right*. El Paso: Lfb Scholarly Publishing LLC.
- Conclusiones II Congreso de Inteligencia. 2011. *Inteligencia y Seguridad: Revista de Análisis y Prospectiva*. n, 9, 95-97.
- CRONIN, Blaise. 2005. Intelligence, Terrorism and National Security. *Annual Review of Information Science and Technology*. v. 39, 395-431.
- ESTEBAN NAVARRO, Miguel Ángel; NAVARRO BONILLA, Diego. 2003. Gestión del conocimiento y servicios de inteligencia: la dimensión estratégica de la información. *El profesional de la información*. v. 12, n. 4, 269-281.
- ESTEBAN NAVARRO, Miguel Ángel. 2011. Contrainteligencia y operaciones encubiertas. En: González Cussac, José Luis, ed. *Inteligencia*. Valencia: Tirant lo Blanc, 128-158.
- ESTEBAN NAVARRO, Miguel Ángel; CARVALHO, Andréa V. 2011a. Inteligencia: concepto y práctica. En: González Cussac, José Luis, ed. *Inteligencia*. Valencia: Tirant lo Blanc, 8-36.
- ESTEBAN NAVARRO, Miguel Ángel; CARVALHO, Andréa V. 2011b. Producción y transferencia de Inteligencia. En: González Cussac, José Luis, ed. *Inteligencia*. Valencia: Tirant lo Blanc, 63-124.
- GARCÍA MACHO, Ricardo, ed. 2010. *Derecho administrativo de la información y administración transparente*. Madrid: Marcial Pons.
- GONZALEZ CUSSAC, José Luis. 2011 Servicios de inteligencia y Estado de Derecho. En: González Cussac, José Luis, ed. *Inteligencia*. Valencia: Tirant lo Blanc, 155-190.
- GONZÁLEZ QUINTANA, Antonio. 1995. *Archives of the security services of former repressive regimes: report prepared for UNESCO on behalf of the International Council of Archives*. París: UNESCO.
- GONZÁLEZ QUINTANA, Antonio. 1999a. Archivos y derechos humanos. *Boletín de la ANABAD*. v. XLIX, n. 3-4, 371-389.
- GONZÁLEZ QUINTANA, Antonio. 1999b. Les archives des services de sécurité des anciens régimes répressifs. *Janus*, n 1, 13-31.
- GONZÁLEZ QUINTANA, Antonio. 2004. Los archivos de la represión: balance y perspectivas. *Comma*. n. 2, 59-74.
- GONZÁLEZ QUINTANA, Antonio. 2006. Los archivos de los servicios de seguridad de los Estados. En: d la Calle Velasco, María Dolores; Redero San Román, Manuel, eds. *Guerra Civil, documentos y memoria*. Salamanca: Universidad, 111-130.

- GONZÁLEZ QUINTANA, Antonio. 2008. *Políticas archivísticas para la protección de los derechos humanos actualización y ampliación del informe elaborado para UNESCO y Consejo Internacional de Archivos (1995) sobre gestión de los archivos de los servicios de seguridad del estado de los desaparecidos regímenes represivos*. París: International Council on Archives.
- GUICHOT REINA, Emilio. 2009. *Publicidad y privacidad de la información administrativa*. Cizur Menor: Civitas.
- GUICHOT REINA, Emilio. 2011a. *Transparencia y acceso a la información pública en el Derecho europeo*. Sevilla: Global Law.
- GUICHOT REINA, Emilio. 2011b. *Transparencia y acceso a la información pública en España: análisis y propuestas legislativas*. Madrid: Fundación Alternativas.
- HERMAN, Michael. 2001. *Intelligence Services in the Information Age*. Londres: Frank Cass.
- HERNÁNDEZ OLIVERA, Luis. 2007. Los archivos que surgieron del frío: un repaso a la situación de apertura de los archivos de las policías secretas de los antiguos países comunistas. *Archivamos*. n. 63,16-20.
- HUSKAMP PETERSON, Trudy. 2005. *A Guide to Preserving Records of Truth Commissions*. Baltimore: Johns Hopkins University Press.
- HUSKAMP PETERSON, Trudy. 2008. *Temporary Courts, Permanent Records*. Washington, D.C.: Woodrow Wilson Center for Scholars.
- JELIN, Elisabeth; Ludmila da SILVA CATELA, comps. 2002. *Los archivos de La represión: documentos, memoria y verdad*. Madrid: Siglo XXI.
- JOINET, Louis. 1997. *Question de l'impunité des auteurs des violations des droits de l'homme civils et politiques, Rapport final en application de la décision 1996/119 de la Sous-Commission, Nations Unies, E/CN.4/Sub.2/1997/20 et E/CN.4/Sub.2/1997/20/Rev.1*. Nueva York: United Nations.
- LE GOFF, Armelle. 2004. *Les archives des ONG : Une mémoire à partager. Guide pratique en 60 questions*. París: International Council on Archives.
- LOWENTHAL, Mark M. 2006. *Intelligence: from secrets to policy*. 3ª ed. rev. Whashington, DC: CQ Press.
- ORENTLICHER, Diane. 2005. *Rapport de l'experte indépendante chargée de mettre à jour l'ensemble de principes pour la lutte contre l'impunité, Nations Unies, E/CN.4/2005/102*. Nueva York: United Nations.
- ORGANIZACIÓN DE LOS ESTADOS AMERICANOS. Relatoría Especial para la Libertad de Expresión, Comisión Interamericana de Derechos Humanos. 2010. *El derecho de acceso a la información en el marco jurídico interamericano*. Washington: Organización de los Estados Americanos.
- RUIZ MIGUEL, Carlos. 2007. Problemas actuales del derecho de los servicios de inteligencia. *Inteligencia y Seguridad: Revista de Análisis y Prospectiva*. n, 2, 13-46.