Aspectos críticos de los sistemas de inteligencia. Experiencia internacional

Autores

Juan Pablo Jarufe Bader
Email: jjarufe@bcn.cl
Tel.: (56) 32 226 3173
(56) 22 270 1850

SUP: 138370

Resumen

Mientras en el paradigma alemán, la Sección 3 de la *Informationsfreiheitsgesetz* establece que el derecho de acceso a la información cede su preeminencia, cuando la divulgación de datos pueda tener efectos adversos sobre las relaciones internacionales, los intereses militares o la seguridad interna; en el caso colombiano, el artículo 4° de la Ley 1.621, de 2013, establece como límites el respeto al debido proceso, la Constitución, el Derecho Internacional Humanitario, y la protección de la honra e intimidad de un individuo.

El modelo español gira en torno a la figura del Centro Nacional de Inteligencia, organismo público responsable de facilitar al Presidente los análisis para prevenir peligros contra la integridad territorial del país; en tanto que en Finlandia, el Servicio de Inteligencia y Seguridad es la agencia encargada de enfrentar las amenazas a la seguridad nacional; a la vez que Israel ofrece un modelo de múltiples actores, como la Agencia de Seguridad, el *A'man* y el *Mossad*.

En relación con los datos más confidenciales, la Sección 53 de la *Federal Data Protection Act*, obliga a las personas que trabajan en los servicios de inteligencia alemanes, a mantener la reserva sobre las materias más secretas, aun tras culminar su labor; mientras en EE.UU., la Sección 1.2 de la *President Executive Order No.* 13.526, de 2009, diferencia entre tres niveles de clasificación de datos de inteligencia, a saber, "*Top Secret*", "Secreto" y "Confidencial".

A nivel formativo, Argentina cuenta con una Escuela Nacional de Inteligencia, en tanto que en Costa Rica el personal del rubro debe acreditar cursos impartidos por la Dirección de Inteligencia y Seguridad Nacional, así como por entes afines.

Respecto a la distribución geográfica, el Servicio de Inteligencia y Seguridad finlandés cuenta con ocho departamentos regionales, que operan fuera del Área Metropolitana de Helsinki; mientras en Costa Rica, la Dirección de Inteligencia y Seguridad Nacional divide sus dependencias en oficinas centrales y auxiliares.

Finalmente, en materia de control, en Finlandia actúa el *Ombudsman* de Inteligencia, como órgano autónomo que supervisa la legalidad de las actividades civiles y militares; mientras en Israel el líder del Servicio de Seguridad tiene que emitir al Primer Ministro, al Fiscal General del país y a la Comisión de Asuntos del Servicio, de la *Knesset*, un documento trimestral sobre el modo de utilizar la información sensible.

Introducción

A solicitud de la Comisión de Defensa Nacional de la Cámara de Diputados, el presente documento da cuenta de una serie de elementos propios de los sistemas de inteligencia a nivel internacional, tales como sus niveles de apertura, los actores involucrados, los medios de clasificación de datos sensibles, la formación de los agentes, los niveles de descentralización y los mecanismos de control.

El informe considera la experiencia de países como Alemania, Argentina, Colombia, Costa Rica, España, Estados Unidos (EE.UU.), Finlandia, Francia, Israel, Polonia y Reino Unido, si bien no constituye un examen exhaustivo, dada la limitada disponibilidad pública de información confiable en diversos ítems de la investigación, fundamentalmente en lo referido a la situación de los líderes de agencias de inteligencia tras su retiro.

El trabajo recoge información del informe BCN "Desclasificación de materias de inteligencia: plazos y categorías de seguridad en la experiencia comparada" (Mayo, 2023), de los autores Jana Abujatum, Bárbara Horzella y Juan Pablo Jarufe.

I. Sistemas de inteligencia internacionales

1. Nivel de apertura

En el paradigma alemán, la Sección 3 de la *Informationsfreiheitsgesetz* (IFG) establece que el derecho de acceso a la información cede su preeminencia, cuando la divulgación de datos pueda tener efectos adversos sobre las relaciones internacionales, los intereses militares, la seguridad interna, las tareas de control o supervisión de las autoridades financieras y reguladoras, el comercio exterior, y los procesos judiciales en curso.

También está prohibido divulgar datos cuando la información está sujeta a una obligación de secreto o confidencialidad, como en el caso de la labor de los servicios de inteligencia.

En efecto, la sección siguiente rechaza la solicitud de acceso a la información, cuando esta divulgación pudiera frustrar el éxito de una medida oficial.

Con todo, la Sección 5 admite que el acceso a datos personales puede proceder cuando el interés del solicitante supera el interés legítimo del tercero en excluir el acceso a la información, o cuando este último entrega su consentimiento (IFG, 2020).

En el caso colombiano, en tanto, el artículo 4° de la Ley 1.621, de 2013, establece como límites a la función de inteligencia, el respeto al debido proceso, la Constitución Política, las leyes del país, el Derecho Internacional Humanitario y el Derecho Internacional de los Derechos Humanos, así como la protección de la honra, el buen nombre, la intimidad personal y familiar de un individuo.

Además, ningún dato propio de la inteligencia y contrainteligencia puede ser conseguido con propósitos que atenten contra los fines esenciales del Estado; la normalidad democrática; la integridad territorial; la seguridad y defensa de la Nación; y el derecho a la vida y la integridad de las personas ante amenazas como "el terrorismo, el crimen organizado, el narcotráfico, el secuestro, el tráfico de armas y el lavado de activos".

Tampoco está autorizada la obtención o divulgación de datos en función de criterios de género, raza, origen nacional, lengua, religión, opinión política u organización sindical (Ley 1.621, 2013).

Respecto a España, el artículo 14 de la Ley Nro. 19, de Transparencia, Acceso a la Información Pública y Buen Gobierno, de 2013, limita el derecho de acceso a la información, cuando este pueda entrañar un daño contra la seguridad nacional, la defensa o las relaciones exteriores; la seguridad pública, la prevención, investigación y

sanción de los ilícitos penales, administrativos o disciplinarios; la igualdad de las partes en los procesos judiciales y la tutela judicial efectiva; las funciones administrativas de vigilancia, inspección y control; los intereses comerciales, la política económica y monetaria; el secreto profesional y la propiedad intelectual e industrial; la garantía de la confidencialidad o el secreto requerido en procesos de toma de decisión; y la protección del medio ambiente (Ley Nro. 19, de Transparencia, Acceso a la Información Pública y Buen Gobierno, 2013).

2. Autoridades involucradas

En Alemania, el Servicio Federal de Inteligencia es la autoridad encargada de recopilar y evaluar la información requerida para conseguir datos sobre terceros países, conforme a las necesidades de política exterior y seguridad del país.

De acuerdo a la Sección 2 de la *Gesetz über den Bundesnachrichtendienst* (BNDG), esa orgánica procesa datos personales, siempre que no se produzcan conflictos con las prescripciones de la Ley Federal de Protección de Datos, en el interés de cautelar a sus funcionarios y para monitorear sucesos del exterior, que pudiesen tener impacto en la política exterior y de seguridad germana (BNDG, 2021).

En tanto, el artículo 3° de la Ley 1.621 dispone que los organismos a cargo de la función de inteligencia, son parte de las fuerzas militares y de la Policía Nacional colombiana, así como de la Unidad de Información y Análisis Financiero (Ley 1.621, 2013).

De manera análoga, el artículo 1º del Reglamento de Organización y Funcionamiento, de la Dirección de Inteligencia y Seguridad Nacional, establece que en Costa Rica la Dirección de Inteligencia y Seguridad Nacional es un cuerpo policial que hace las veces de órgano informativo del Presidente de la República, con atribuciones recogidas en el artículo 18 de la misma norma, que tienen relación con la detección e investigación de inteligencia, así como con la coordinación con terceros países en tópicos de seguridad externa (Reglamento de Organización y Funcionamiento, de la Dirección de Inteligencia y Seguridad Nacional, 2005).

El modelo español, por su parte, gira en torno a la figura del Centro Nacional de Inteligencia, que según el artículo 1 de la Ley *Nro.* 11, de 2002, es “el organismo público responsable de facilitar al Presidente del Gobierno y al Gobierno de la Nación, las informaciones, análisis, estudios o propuestas que permitan prevenir y evitar cualquier peligro, amenaza o agresión contra la independencia o integridad territorial de España, los intereses nacionales y la estabilidad del Estado de derecho y sus instituciones” (Ley *Nro.* 11, Reguladora del Centro Nacional de Inteligencia, 2002).

La comunidad de inteligencia en EE.UU., en tanto, está conformada, según la Sección 3 de la *National Security Act*, por agentes como la Oficina del Director de Inteligencia Nacional; la Agencia Central de Inteligencia (CIA); la Agencia de Seguridad Nacional; la Agencia de Inteligencia de Defensa; la Agencia Nacional de Inteligencia Geoespacial; la Oficina Nacional de Exploración; las reparticiones del Departamento de Defensa especializadas en la recolección de información; la Oficina de Inteligencia e Investigación, del Departamento de Estado; la Oficina de Inteligencia y Análisis, del Departamento del Tesoro; la Oficina de Inteligencia y Análisis, del Departamento de Seguridad Interior; y las ramas de inteligencia del Ejército, la Armada, la Fuerza Aérea, los *Marines*, la Guardia Costera, la Oficina Federal de Investigación (FBI), el Departamento de Energía y la *Drug Enforcement Administration*.

De igual forma, la Sección 101 de la *National Security Act* consagra la existencia de un Consejo de Seguridad Nacional, cuya función es asesorar al Primer Mandatario en materia de políticas militares, de seguridad y política exterior, a la vez que estimular que los servicios militares y agencias de gobierno cooperen de manera más efectiva en materias de seguridad nacional.

Otra entidad a destacar en el sistema norteamericano, es el Consejo Comunitario de Inteligencia Conjunta, que de acuerdo a la Sección 101ª del mismo texto legal, tiene como función asistir al Director de Inteligencia Nacional, en el desarrollo e implementación de un concepto unificado de inteligencia a nivel nacional, así como en la determinación de requerimientos presupuestarios y en la evaluación de resultados en materia de inteligencia.

En tanto, la Sección 104ª remite al rol del Director de la CIA, quien es nombrado por el Presidente de la República, con el consentimiento del Senado, encargándose de recoger información a partir de fuentes humanas y otros medios, tanto a nivel nacional como internacional, para contribuir a la seguridad del país (*National Security Act*, 1947).

Respecto a Finlandia, el Servicio de Inteligencia y Seguridad (SUPO) es la agencia del Ministerio del Interior, que se encarga de enfrentar las amenazas a la seguridad del país, aportando con inteligencia para prevenir riesgos.

En concreto, es una entidad que obtiene, analiza y reporta inteligencia a los decisores de gobierno, combate el terrorismo, previene el espionaje y monitorea las amenazas de los extremismos (SUPO, 2023a).

En Francia, en tanto, la Dirección General de la Seguridad Exterior tiene por objeto obtener información protegida, de acceso restringido, para analizar en función de un desarrollo del concepto de inteligencia estratégica, que le permita al gobierno anticipar escenarios y tomar decisiones para proteger la soberanía del país (*Arrêté Portant Organisation de la Direction Générale de la Sécurité Extérieure*, 2015).

Israel, a su turno, ofrece un modelo de múltiples actores involucrados en las tareas de inteligencia, entre los que se encuentran la Agencia de Seguridad (*Shin Bet*), el *A'man* (inteligencia militar) y el *Mossad*.

La primera es el servicio de seguridad interior, que vela por la integridad de las instituciones y el gobierno democrático, frente a amenazas como el terrorismo, la subversión política y el espionaje. Para ello, cuenta con ramas operacionales en ámbitos como el mundo árabe y la cibertecnología (*The Israeli Security Agency (ISA)/Shin Bet/Shabak*, 2023).

El *A'man*, en tanto, tiene por objeto aportar al gobierno y las Fuerzas de Defensa, con una serie de alertas de inteligencia diarias y durante tiempos de guerra, que permitan proteger al país de amenazas externas; y, por último, el *Mossad* es la agencia de inteligencia que utiliza gente para operaciones encubiertas y de contraterrorismo, con foco especial en los países y organizaciones árabes (*Israel Intelligence Agencies*, 2023).

A su vez, los artículos 1 al 6 de la Ley sobre la Agencia de Seguridad Interior y la Agencia de Inteligencia Extranjera, disponen en Polonia la existencia de dos entidades encargadas de las tareas de inteligencia en el país.

La primera es la Agencia de Seguridad Interna, con competencia para la protección de la seguridad interior del Estado y su orden constitucional, a partir de la custodia de información clasificada a nivel nacional e internacional; mientras la segunda es la Agencia de Inteligencia Extranjera, encargada de la protección de la seguridad exterior del Estado, frente al terrorismo internacional, el extremismo y los grupos de delincuencia organizada transnacional (Ley sobre la Agencia de Seguridad Interior y la Agencia de Inteligencia Extranjera, 2002).

Finalmente, en el Reino Unido el Servicio de Inteligencia Secreto está bajo la autoridad del Secretario de Estado, encargándose de obtener información sobre acciones de personas externas al país, efectuando otras misiones alusivas a las acciones o intenciones de tales individuos, de acuerdo a lo que reza el artículo 1 de la *Intelligence Services Act*, de 1994 (*Intelligence Services Act*, 1994).

3. Tratamiento de datos sensibles

En relación con la información más confidencial, la Sección 53 de la *Federal Data Protection Act* obliga a las personas que trabajan en los servicios de inteligencia a mantener la reserva sobre las materias más secretas, aun tras culminar su labor (*Federal Data Protection Act*, 2021).

En esa línea, la Sección 11 de la *Federal Archives Act*, de 2019, estipula que la protección de archivos federales dura treinta años. Cuando la información versa sobre una o más personas naturales, solo puede comenzar a ser utilizada diez años después de la muerte de estos individuos. Si el año del deceso no puede ser establecido, se presume un lapso de cien años tras el nacimiento de la persona. Cuando tampoco se pueda definir esta efeméride, entonces el plazo se calcula en sesenta años.

Con todo, esta regla no aplica para datos sobre autoridades públicas en el ejercicio de sus funciones o sobre personas de la historia contemporánea del país, a menos que su vida privada requiera protección.

Asimismo, la Sección 12 contempla la opción de acortar hasta por un máximo de treinta años este período de protección, previo consentimiento de los involucrados, cuando el uso de los datos sea esencial para un proyecto de investigación o documento científico.

Sin embargo, la autoridad federal puede restringir o denegar el uso de esta información, conforme a la Sección 13 de la norma, cuando considere que existen razones que amenacen el bienestar del país o de sus estados federales (*Federal Archives Act*, 2019).

De igual manera, la Sección 29 faculta al Servicio Federal de Inteligencia a transmitir datos personales de inteligencia estratégica extranjera a autoridades públicas nacionales como la Oficina Federal para la Protección de la Constitución, las autoridades constitucionales de protección de los *Länder* y el Servicio de Contrainteligencia Militar, ante la existencia de indicios para el enjuiciamiento de delitos, amenazas contra el orden democrático o para detectar temprano el peligro de atentados contra la infraestructura crítica, la integridad de las personas, los bienes públicos de la Federación o de los territorios regionales (BNDG, 2021).

Una situación similar se presenta en Colombia, donde el artículo 33 de la Ley 1.621 prolonga la reserva de datos sensibles de inteligencia por un máximo de treinta años, contabilizados desde de la recolección de la información. Este plazo es extensible por hasta quince años adicionales, cuando el Presidente de la República considere que su divulgación constituye una amenaza grave interna o externa contra la seguridad o la defensa nacional.

No obstante, antes de culminar el tiempo de reserva, el Primer Mandatario también puede autorizar, cuando lo estime conveniente, el levantamiento del secreto y la desclasificación total o parcial de la información, siempre que esta liberación contribuya al interés general y no entrañe una amenaza contra la vigencia del régimen democrático, la seguridad o la defensa nacional (Ley 1.621, 2013).

En el paradigma español, por su parte, las materias clasificadas pueden ser secretas o reservadas, conforme al nivel de protección requerido, según el artículo tercero de la Ley Nro. 9, sobre Secretos Oficiales.

De forma similar, el artículo tercero del Decreto 242, por el que se desarrollan las disposiciones de la Ley Nro. 9, menciona el calificativo de “secreto” para las materias vinculadas a datos que requieran del más alto nivel de protección, y cuya revelación no autorizada pueda causar perjuicios a la seguridad estatal; y el de “reservado”, para asuntos, actos, documentos y objetos cuyo conocimiento pudiese lesionar los intereses fundamentales del país.

Junto a lo anterior, el texto legal prescribe la necesidad de que las autoridades señalen el plazo de duración de esta calidad, así como la posibilidad de que sea suprimida o rebajada (Decreto 242, 1969).

Con todo, esta clasificación no rige para el caso del Senado y el Congreso de los Diputados, que siempre pueden acceder a la información que soliciten, en sesiones secretas, de acuerdo al artículo diez de la norma (Ley Nro. 9, sobre Secretos Oficiales, 1968).

En cuanto al modelo estadounidense, la Sección 3.001 de la *Intelligence Reform Act*, de 2004, incluye la nomenclatura "archivo de investigación en curso" (*current investigation file*), al aludir a informaciones o indagatorias vigentes durante (*Intelligence Reform and Terrorism Prevention Act*, 2004):

- Un lapso de cinco años, desde la fecha en que fue entregada una autorización de secreto/seguridad de alta importancia.
- Un período de diez años, desde el momento en que se declaró una autorización de seguridad.
- Un tiempo de quince años, a partir de la fecha en que se decretó una autorización de confidencialidad.

Asimismo, el Jefe de Estado tiene la facultad de elegir una repartición ejecutiva para (*Intelligence Reform and Terrorism Reform and Terrorism Prevention Act*, 2004):

- Dirigir revisiones diarias a las investigaciones que involucran secretos de inteligencia vinculados a programas de alta sensibilidad.
- Desarrollar e implementar políticas y procedimientos uniformes, para asegurar la eficacia de los procesos de liberación de reserva y definición de acceso a programas de alto impacto, incluyendo requisitos para la desclasificación de datos financieros.
- Asegurar el reconocimiento recíproco de acceso a información clasificada entre las distintas agencias de inteligencia del país, ejerciendo como última autoridad para dirimir disputas sobre acceso a datos reservados.

En tanto, la *President Executive Order No. 13.526*, de 29 de diciembre de 2009, fija un mecanismo uniforme de clasificación, salvaguarda y desclasificación de informes de seguridad nacional, considerando datos vinculados a la defensa frente al terrorismo transnacional.

A su vez, la Sección 1.2 de la norma diferencia entre tres niveles de clasificación de datos de inteligencia, a saber (*The President Executive Order No. 13526*, 2009):

- "*Top Secret*", para datos secretos y confidenciales, todos de carácter reservado, cuya revelación podría afectar de forma excepcionalmente grave a la seguridad nacional del país, tales como planes militares, programas nucleares, sistemas de armas, métodos de inteligencia, actividades de política exterior, desarrollos científico-tecnológicos y vulnerabilidades en infraestructura.
- "Secreto", aplicable a datos cuya divulgación no autorizada podría producir un grave daño a la seguridad nacional.
- "Confidencial", para la información cuyo conocimiento público pudiera causar cierto daño a la seguridad nacional.

El tiempo por el cual se prolongue la confidencialidad de ciertos datos, es atribución del Presidente y Vicepresidente de la República, además de los titulares de las agencias de inteligencia, conforme a la Sección 1.3 de la norma.

Cuando no sea posible definir la fecha exacta para desclasificar una información, este acto se producirá, por defecto, diez años después de la sanción del secreto, salvo que la propia autoridad decida extenderlo por 25 años e incluso más tiempo, previa recatalogación de los datos (*The President Executive Order No. 13526*, 2009).

Los líderes de las agencias de inteligencia también poseen la potestad para liberar del proceso de desclasificación a todos los datos específicos que se vinculen con la identidad de fuentes confidenciales o con nexos con servicios foráneos; la información vinculada al desarrollo de armas de destrucción masiva; la información perjudicial para los sistemas criptológicos del país; y la información relativa a planes militares, actividades diplomáticas o sistemas de infraestructura crítica (*The President Executive Order No. 13526*, 2009).

Por último, la Sección 3.7 alude al *National Declassification Center*, entidad establecida para coordinar los procesos de desclasificación informativa, así como para facilitar medidas que aseguren la calidad e implementen normas estandarizadas (*The President Executive Order No. 13.526*, 2009).

En el caso finlandés, la Sección 6 de la *Act on the Processing of Personal Data in Criminal Matters and in Connection with Maintaining National Security*, sostiene que la información personal debe ser analizada de manera adecuada a los propósitos del procesamiento y que toda información innecesaria puede ser borrada.

Asimismo, afirma que la necesidad de almacenar datos personales es revisada al menos cada cinco años, a menos que se disponga algo diferente por ley (*Act on the Processing of Personal Data in Criminal Matters and in Connection with Maintaining National Security*, 2023: 6).

La gran innovación en este país es la figura del *Ombudsman* de Protección de Datos, que de acuerdo a la Sección 21 de la norma, es una figura consultiva en torno al procesamiento de información, conforme a un análisis de impacto y de riesgos inherentes a las nuevas tecnologías, mecanismos y procedimientos sobre la información.

En tanto, según la Sección 24 de la *Act on the Openness of Government Activities*, son secretos oficiales los documentos relacionados con inteligencia militar, operaciones armadas e instalaciones de la defensa (*Act on the Openness of Government Activities*, 2015: 13-14).

En esta línea, la Sección 31 prescribe un lapso de 25 años para preservar el secreto de documentos oficiales, tiempo que aumenta a cincuenta años tras la muerte de la persona involucrada, al tratarse de información secreta sobre la vida privada. De no poderse determinar la fecha del deceso del individuo, el secreto se extiende por hasta cien años.

Israel proporciona otro modelo en la cautela de información sensible. Al respecto, el artículo 11 de la *General Security Service Law*, de 2002, establece que el acceso a bases de datos oficiales debe estar autorizado por cada jefe de servicio, con un detalle de la información requerida y sin exceder los seis meses (*General Security Service Law*, 2002).

4. Formación de agentes

Argentina cuenta con una Escuela Nacional de Inteligencia, concebida como “el instituto superior de formación, capacitación y perfeccionamiento, destinado a los integrantes del Sistema de Inteligencia Nacional” (Escuela Nacional de Inteligencia, 2023).

Sus planes de estudio deben ser visados por el Ministerio de Educación, a fin de contar con un control externo a la formación de los agentes de inteligencia.

Este centro de estudios opera en conjunto con la Secretaría de Planificación de Inteligencia Nacional, de la Agencia Federal de Inteligencia, principal órgano sectorial. Su currículum considera un curso básico de ingreso, de aprobación obligatoria, así como materias especializadas en inteligencia, seguridad, historia nacional y latinoamericana, derechos humanos, y género.

En Costa Rica igualmente existe un proceso formativo en torno a la inteligencia. Así, el artículo 13 del Reglamento de Organización y Funcionamiento, de la Dirección de Inteligencia y Seguridad Nacional, dispone que el personal de este servicio tenga que acreditar cursos impartidos por la misma Dirección de Inteligencia y Seguridad Nacional, así como por entes afines, como la Escuela Nacional de Policía.

De igual modo, tiene que participar en los programas de capacitación y entrenamiento nacionales o internacionales, afines a su especialidad (Reglamento de Organización y Funcionamiento, de la Dirección de Inteligencia y Seguridad Nacional, 2005).

Respecto a España, el *LISA Institute* imparte una serie de programas avanzados en materia de inteligencia, destacando el Máster de Analista de Inteligencia, junto a los cursos de Técnicas y Herramientas Avanzadas e

Ciberinvestigación, Analista Estratégico en Instalaciones Industriales, Prospectiva y Análisis Estratégico, Ciberinteligencia, y *Hacking* Ético (*LISA Institute*, 2023).

Por último, los soldados del *A'Man* israelí son entrenados en la Unidad de Inteligencia Militar y Ciberinstrucción, considerada la más grande de su tipo en el Medio Oriente, que adiestra a los uniformados y agentes en lenguaje y cultura de países enemigos, fundamentalismo islámico y otros cursos avanzados (*Israel Intelligence Agencies*, 2023).

5. Niveles de descentralización

Si el análisis busca determinar la distribución geográfica de los sistemas de inteligencia en cada país, existe al menos un par de casos en los que aparecen algunos indicios al respecto.

Es así como en Costa Rica, el artículo 11 del Reglamento de Organización y Funcionamiento, de la Dirección de Inteligencia y Seguridad Nacional, divide sus dependencias en (Reglamento de Organización y Funcionamiento, de la Dirección de Inteligencia y Seguridad Nacional, 2005):

- Oficinas centrales, que albergan la Dirección General, Subdirección General, Área de Recursos Materiales y Presupuesto, Área de Recursos Humanos y Capacitación, y grupos operacionales.
- Oficinas auxiliares, que pueden ser permanentes o transitorias, en cualquier lugar del país, conforme a las necesidades del servicio.

Por último, mientras en EE.UU., la Sección 119B de la *National Security Act* faculta al Director de Inteligencia Nacional a establecer uno o más centros de inteligencia nacional en el territorio norteamericano, considerando temáticas regionales (*National Security Act*, 1947); en Finlandia el antes mencionado SUPO cuenta con ocho departamentos regionales, que operan fuera del Área Metropolitana de Helsinki, desplegándose en locaciones como Joensuu, Kuopio, Lappeenranta, Oulu, Rovaniemi, Tampere, Turku y Vaasa, en un trabajo mancomunado con otras autoridades públicas, la policía y encargados fronterizos (SUPO, 2023b).

6. Mecanismos de control

Varios de los países analizados cuentan con fórmulas para supervigilar la función de inteligencia.

En el caso de Colombia, el artículo 18 de la Ley 1.621 determina que los inspectores policiales o militares que efectúen labores de inteligencia y contrainteligencia, tienen que rendir un informe anual reservado ante el Ministro de Defensa, con copia a la Comisión Legal de Seguimiento a las Actividades de Inteligencia y Contrainteligencia. El objetivo de este control es verificar la implementación de los principios, límites y fines enunciados en la ley, así como la armonización entre la norma vigente, la doctrina y métodos de inteligencia.

El control político también incluye la figura de la Comisión Legal de Seguimiento a las Actividades de Inteligencia y Contrainteligencia, que según el artículo siguiente del texto legal, se encarga de comprobar la eficiencia en la utilización de fondos públicos y de salvaguardar las garantías constitucionales (Ley 1.621, 2013).

El modelo español, por su parte, establece que el Centro Nacional de Inteligencia debe informar al Congreso de los Diputados, en sesiones secretas, acerca de las materias propias de su funcionamiento, así como del uso de créditos dirigido a gastos reservados, según lo mandata el artículo 11.1 de la Ley Nro. 11, reguladora del Centro Nacional de Inteligencia.

Siguiendo esta misma lógica, la Comisión del Congreso de los Diputados puede conocer los objetivos anuales de inteligencia y el informe anual elaborado por el Director del Centro Nacional de Inteligencia, junto con acceder a

otras materias clasificadas, a excepción de las vinculadas con las fuentes y medios del Centro Nacional de Inteligencia y de las que provengan de servicios extranjeros u organizaciones internacionales (Ley Nro. 11, Reguladora del Centro Nacional de Inteligencia, 2002).

La Sección 102A de la *National Security Act*, en tanto, puntualiza que el Director de Inteligencia Nacional de EE.UU. debe entregar un reporte semianual de las actividades del servicio al Presidente del Congreso, mientras la Sección 114 del mismo texto le obliga a preparar un Informe Anual al Congreso, referido al uso de agentes encubiertos en el último período fiscal (*National Security Act*, 1947).

En Finlandia, en tanto, el *Ombudsman* de Inteligencia es el órgano autónomo e independiente que supervisa la legalidad de las actividades de inteligencia civil y militar, mientras la Comisión de Supervigilancia de Inteligencia es responsable de fiscalizar las actividades del rubro (*The Intelligence Ombudsman*, 2023).

El líder del Servicio de Seguridad de Israel, a su vez, tiene que emitir al Primer Ministro, al Fiscal General del país y a la Comisión de Asuntos del Servicio, de la *Knesset* (Parlamento israelí), un documento trimestral sobre los permisos concedidos y sobre el modo de utilizar la información sensible, todo ello según el artículo 11 de la *General Security Service Law* (*General Security Service Law*, 2002).

De igual forma, el artículo 13 le indica al Primer Ministro el nombramiento de un Controlador del Servicio, encargado de conducir una auditoría interna de las acciones emprendidas por el sector.

Respecto a Polonia, las actividades del Jefe de la Agencia de Seguridad Interior y del Jefe de la Agencia de Inteligencia Extranjera, están sometidas al control de la Cámara de los Diputados (Ley sobre la Agencia de Seguridad Interior y la Agencia de Inteligencia Extranjera, 2002).

En el Reino Unido, el artículo 2 de la *Justice and Security Act*, de 2013, dispone que la Comisión de Inteligencia y Seguridad del Parlamento pueda examinar o supervisar el gasto, gestión y operación del Servicio Secreto de Inteligencia. Este órgano debe emitir un reporte anual al Primer Ministro y al Parlamento, para rendir cuenta de sus funciones, pudiendo excluir cualquier materia que considere perjudicial para las funciones afines al servicio (artículo 4).

Finalmente, otro actor con responsabilidad de rendición de cuentas es el Secretario de Estado, quien, conforme al artículo 12 de la misma norma, debe preparar un informe anual sobre sus actuaciones, junto con nombrar a un "Revisor" que emprenda un examen quinquenal de las actividades del servicio, poniéndolo en conocimiento del propio Secretario de Estado y del Parlamento, si bien el primero puede excluir del conocimiento de este último, aquellas materias que considere dañinas contra los intereses de seguridad nacional (*Justice and Security Act*, 2013).

Referencias

Act on the Openness of Government Activities. (2015). Disponible en: https://www.finlex.fi/en/laki/kaannokset/1999/en19990621_20150907.pdf.

Act on the Processing of Personal Data in Criminal Matters and in Connection with Maintaining National Security. (2023). Disponible en: https://www.finlex.fi/fi/laki/kaannokset/2018/en20181054.pdf.

Arrêté Portant Organisation de la Direction Générale de la Sécurité Extérieure. (2015, marzo 10). Disponible en: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000030375775.

BNDG. (2021, julio 5). Disponible en: https://www.gesetze-im-internet.de/bndg/BJNR029790990.html.

Decreto 242, por el que se desarrollan las disposiciones de la Ley Nro. 9, sobre Secretos Oficiales. (1969, febrero 20). Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-1969-263.

Escuela Nacional de Inteligencia. (2023, mayo 25). Disponible en: https://www.argentina.gob.ar/inteligencia/eni.

Federal Archives Act. (2019, mayo 8). Disponible en: https://www.bundesarchiv.de/EN/Navigation/Meta/About-us/Legal-Bases/Federal-Archives-Act/federal-archives-act.html.

Federal Data Protection Act. (2021, junio 23). Disponible en: https://www.gesetze-im-internet.de/englisch_bdsg/englisch_bdsg.html.

General Security Service Law. (2002). Disponible en: https://www.jewishvirtuallibrary.org/jsource/Politics/GeneralSecurityServicesLaw.pdf.

IFG. (2020, junio 19). Disponible en: https://www.gesetze-im-internet.de/ifg/BJNR272200005.html.

Intelligence Reform and Terrorism Prevention Act. (2004). Disponible en: https://www.govinfo.gov/content/pkg/PLAW-108publ458/html/PLAW-108publ458.htm.

Intelligence Services Act. (1994). Disponible en: https://www.legislation.gov.uk/ukpga/1994/13/contents.

Israel Intelligence Agencies. (2023, mayo 25). Disponible en: https://www.jewishvirtuallibrary.org/israel-intelligence-agencies.

Justice and Security Act. (2013). Disponible en: https://www.legislation.gov.uk/ukpga/2013/18/part/1/crossheading/oversight-by-the-intelligence-and-security-committee-of-parliament.

Ley Nro. 9, sobre Secretos Oficiales. (1968, abril 5). Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-1968-444.

Ley *Nro.* 11, Reguladora del Centro Nacional de Inteligencia. (2002, mayo 6). Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2002-8628.

Ley Nro. 19, de Transparencia, Acceso a la Información Pública y Buen Gobierno. (2013, diciembre 9). Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2013-12887.

Ley sobre la Agencia de Seguridad Interior y la Agencia de Inteligencia Extranjera. (2002, mayo 24). Disponible en: https://www.ilo.org/dyn/natlex/docs/ELECTRONIC/99891/119498/F1157569895/POL99891%20Pol.pdf.

Ley 1.621. (2013, abril 17). Disponible en: https://www.suin-juriscol.gov.co/viewDocument.asp?id=1685400.

LISA Institute. (2023, mayo 25). Cursos y Másteres en Seguridad, Análisis, Inteligencia, Ciberseguridad y DD.HH. Disponible en: https://www.lisainstitute.com/collections/cursos/inteligencia.

National Security Act. (1947). Disponible en: https://www.dni.gov/index.php/ic-legal-reference-book/national-security-act-of-1947.

Reglamento de Organización y Funcionamiento, de la Dirección de Inteligencia y Seguridad Nacional. (2005, julio 27). Disponible en: https://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=55219&nValor3=60492&strTipM=TC.

SUPO. (2023, mayo 25). *The mission of SUPO is to safeguard national security*. Disponible en: https://supo.fi/en/mission.

SUPO. (2023, mayo 25). *The organisation of SUPO*. Disponible en: https://supo.fi/en/organisation1.

The Intelligence Ombudsman. (2023, mayo 25). Disponible en: https://tiedusteluvalvonta.fi/en/oversight-of-intelligence.

The Israeli Security Agency (ISA)/Shin Bet/Shabak. (2023, mayo 25). Disponible en: https://www.jewishvirtuallibrary.org/the-israeli-security-agency-isa-shin-bet-shabak.

The President Executive Order No. 13526. (2009, diciembre 29). Disponible en: https://www.archives.gov/isoo/policy-documents/cnsi-eo.html.