colección de estudios internacionales

número 14, año 2013/14

bilduma nazioarteko ikasketen

collection of international studies

DIEGO NAVARRO BONILLA

Espionaje, seguridad nacional y relaciones internacionales

ceinik

Colección de Estudios Internacionales

Edita:
Cátedra de Estudios Internacionales / Nazioarteko Ikasketen Katedra

Dirección
Cátedra de Estudios Internacionales / Nazioarteko Ikasketen Katedra
Universidad del País Vasco / Euskal Herriko Unibertsitatea
Edificio Biblioteca, 6.ª Planta,
Apdo. 1397. 48080. Bilbao, Bizkaia

Teléfono: 0034 946015278
E-mail: ceinik@ehu.es
Web: www.ehu.es/ceinik

COLECCIÓN DE
ESTUDIOS INTERNACIONALES

DIEGO NAVARRO BONILLA

Espionaje, seguridad nacional y relaciones internacionales

ISSN: 2253-7953
ISBN: 978-84-9082-093-3

Depósito legal/Lege gordailua: BI-517-07

ÍNDICE

DIEGO NAVARRO BONILLA

Espionaje, seguridad nacional y relaciones internacionales

1. Introducción

El lapso de tiempo que va desde octubre de 2013 hasta mayo de 2014 ha visto incrementar la tensión en la relación entre Estados, como consecuencia de una masiva y sistemática filtración de información clasificada que marca un punto de inflexión en las relaciones internacionales. Nunca antes la acción de un *whistleblower* como Edward Snowden había llegado a socavar de manera tan profunda los principios y fundamentos que habían definido el contexto de interacción entre países, tanto aliados como manifiestamente adversarios. Frente a otras filtraciones contemporáneas, especialmente las orquestadas por Julian Assange y el movimiento Anonymous, este caso ha marcado una notable diferencia. Se suma así a las revelaciones de otros informantes públicos como Thomas Andrews Drake (2010, NSA), Shamai K. Leibowitz (2010, FBI), Stephen Jin-Woo Kim (2010, State Department), Chelsea Manning, (2013, US Army) y John Kiriakou (2012, CIA). Así fue cómo un exanalista de 29 años, consultor tecnológico de la empresa Booz Allen Hamilton subcontratada por la CIA y la NSA como administrador de sistemas, decidió convertirse en un *whistleblower*. Sorpresivamente, en junio de 2013 hizo públicos, a través de los periódicos *The Guardian* y *The Washington Post*, documentos clasificados como alto secreto sobre varios programas de la NSA, incluyendo los programas de vigilancia masiva PRISM y XKeyscore. Sorpresa, indignación, catástrofe, apoteosis, búsqueda, revuelo

internacional, llamadas a consultas, teléfonos pinchados, vigilancia masiva de todos contra todos…

La estela dejada por este ejemplo de *whistleblower* (fenómeno contemporáneo relativamente frecuente en Estados Unidos) se presta a numerosas reflexiones que van desde la ética de la inteligencia a la dicotomía entre seguridad y libertad de información, de la filosofía de la información a la transparencia, de las relaciones entre Estados a los mecanismos de control y reforzamiento de los sistemas democráticos. Fue así como quedó planteado el drama: para unos, Snowden era el nuevo villano, traidor y felón que divulgaba secretos que afectaban directamente a la seguridad nacional. Para otra inmensa mayoría, sin embargo, Snowden era un héroe: alguien que arriesga no sólo su posición cómoda sino su propia vida para denunciar actuaciones difícilmente aceptables de un sistema de vigilancia, almacenamiento e interceptación de información nunca visto en la historia. Por tanto, el dilema ley frente a ética estaba servido. Amy Davidson escribió en *The New Yorker* que Snowden era la razón por la que en Estados Unidos había existido una discusión sobre la privacidad y los límites de la vigilancia doméstica. Por su parte, Daniel Ellsberg, el informante de los Papeles secretos del Pentágono de 1971, declaró en una entrevista con la CNN que pensaba que Snowden había procurado un servicio "incalculable" a su país y que sus filtraciones podrían servir para que Estados Unidos no se convirtiera en un Estado de vigilancia. Añadió que Snowden había actuado con el mismo tipo de coraje y patriotismo que un soldado en combate.

En todo caso, el descubrimiento de las continuas operaciones de espionaje masivo, global y en muchos casos indiscriminado, sin diferencias en el objeto de atención de esas operaciones (ciudadanos, dirigentes políticos, organizaciones de todo tipo, etc.), llevadas a cabo por agencias de inteligencia de Estados Unidos solas o en connivencia con otras, ha tensionado notable-

mente el equilibrio de las relaciones internacionales. Es más, según algunos autores, todo ello está definiendo la época post 11-S caracterizada por una preeminencia letal de la búsqueda, obtención y acumulación de información por cualquier método, tratando de dar respuesta a lo que denominamos la "ilusión de la omnisciencia planetaria". De ahí que, automáticamente, la acción de los organismos de inteligencia haya vuelto a ser puesta en entredicho y en el centro de la polémica. La insólita comparecencia de los directores del MI6, MI5 y GCHQ ante el Comité de Inteligencia del Parlamento de Reino Unido o las explicaciones ofrecidas por el propio general Félix Sanz Roldán, Secretario de Estado Director del CNI español, en noviembre de 2013 ante la Comisión de Secretos Oficiales, han sido lo suficientemente reveladoras de la gravedad de los hechos. La alarma social generada como consecuencia de las informaciones destapadas por Snowden obligó a llevar a cabo estas comparecencias con el fin de aclarar y garantizar el sometimiento de la actuación de estos servicios de inteligencia a sus respectivos ordenamientos jurídicos. La insistencia en que en ningún caso estos servicios realizaron espionaje sobre sus propios ciudadanos fue el principal argumento expuesto.

¿Qué medios y qué controles podrían articularse entonces para sujetar esta vigilancia masiva? Las medidas conducentes a reforzar el régimen de garantías incluyen controles económicos (comisiones de gastos reservados), políticos (comisiones de secretos oficiales o, como ha indicado un parlamentario español no sin ironía, "de silencios oficiales") o judiciales previos (autorización de un magistrado para intervenir comunicaciones o permitir la entrada en domicilio). A este respecto, autores como José Manuel Ugarte han dedicado numerosas reflexiones al verdadero alcance de los controles existentes para supeditar a un sistema democrático robusto y maduro la actividad de inteligencia y neutralizar las extralimitaciones detectadas[1]. Junto a

1 José Manuel Ugarte**,** *El control público de la actividad de inteligencia en América Latina*, Buenos Aires, CICCUS, 2012.

estos controles, existe también una dimensión deontológica que afecta a los profesionales que forman parte de un organismo de inteligencia que también será objeto de atención en estas páginas[2].

2. Multidimensionalidad del espionaje

En gran medida, todo lo relacionado con el espionaje, ha vuelto recientemente a subrayar la tensión existente entre polos de interés y el equilibrio entre derechos. Se trataría de armonizar la relación que se produce entre poder ejecutivo, seguridad nacional y secreto, garantizando un uso adecuado y responsable de la inmensa capacidad de obtención, procesamiento y explotación de información por parte del Estado para alcanzar los objetivos de protección, seguridad y defensa de los intereses nacionales. De ahí que la dicotomía clásica entre secreto y transparencia alcance de nuevo toda su intensidad. Es lo que plantea Rahul Sagar en su último libro[3]. Los abusos producidos se han conocido no porque el poder judicial haya detectado vulneraciones del ordenamiento jurídico en materia de inteligencia, sino como consecuencia de una masiva filtración de información clasificada destapada por un funcionario procedente en origen de una agencia de inteligencia de Estados Unidos. Sin embargo, el espionaje sigue siendo un asunto caracterizado por dos premisas: por una parte, su naturaleza atemporal y, por otra, la multiplicidad de perspectivas desde las que poder abarcar su comprensión contemporánea.

El espionaje constituye una actividad que hunde sus raíces en la más temprana antigüedad[4]. Como señalase González Alcantud, "el espionaje ha

2 Diego Navarro Bonilla, "Information Management professionals working for intelligence organizations: ethics and deontology implications", *Security and Human Rights*, Vol. 24, n.º 3-4, 2013, pp. 264–279.
3 Rahul SAGAR, *Secrets and Leaks: The Dilemma of State Secrecy*, Princeton, Princeton University Press, 2013.
4 Diego Navarro Bonilla, *Espías: tres mil años de información y secreto*, Madrid, Plaza y Valdés, 2009.

sido y es una modalidad en la formulación del secreto en las sociedades organizadas"[5]. Y es precisamente la tensión dialéctica entre secreto y transparencia el fundamento de las regulaciones jurídicas que tratan de armonizar los derechos que protegen la información por un lado y el derecho de acceso a la información pública por los ciudadanos en sistemas democráticos, por otro. Recientes leyes como la española 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno (BOE 10 de diciembre de 2013) constituyen muestras de esa búsqueda del equilibrio.

Tradicionalmente, se ha considerado el siglo XIX como un momento clave en la atención prestada al espionaje como materia de regulación y reflexión jurídica. Es precisamente en ese siglo cuando se escribe un capítulo esencial en la historia del espionaje y de los organismos de inteligencia con la irrupción masiva de la telegrafía y la telefonía propiciando por fin la comunicación a distancia en tiempo real. Las características, modalidades y, sobre todo, consecuencias legales, internacionales e incluso doctrinales hallarían respuestas específicas en una incipiente jurisprudencia y también en obras cada vez más especializadas. Al amparo casi siempre de las lecciones aprendidas tras los conflictos militares o las crisis diplomáticas, se fue configurando un corpus internacional cada vez más intenso. Tempranas tesis doctorales como las de Colonieu[6] (1888) se convertirían en relevantes puntos de inflexión en el tratamiento de lo que desde el siglo XVI quedó englobado bajo la denominación de las "inteligencias secretas". Durante los siglos modernos, las innumerables menciones al espionaje, a la acción de los espías, al secreto y a la razón de Estado se verificaron en múltiples obras, tratados, manuales y compendios en los que es posible hoy rastrear la acción, las características, las repercusiones y la reflexión en torno al espionaje en

5 José Antonio González Alcantud, "El enigma del secreto: espionaje político", *Historia, Antropología y Fuentes Orales*, Vol. 2, n.º 34, 2005, pp. 5-28.
6 Victor Colonieu, *L'espionage au point de vue du droit international & du droit penal français*, Paris, A. Rousseau, 1888.

la Europa Moderna. La dirección de la guerra al amparo de la Revolución Militar moderna reservó no pocas reflexiones al espionaje en campaña en múltiples tratados de *re militari* por toda Europa. A su vez, la teoría política del Estado y las corrientes de pensamiento político reservaban importantes consideraciones al espionaje como acción de Estado y a los espías como "ministros del secreto". Paralelamente, un tercer ámbito de indudable importancia para comprender el alcance de la acción de los espías bajo sus más diversas modalidades procedía de la formación del perfecto embajador, considerado durante siglos como *spia onorata*. Los tratados y manuales de diplomacia moderna reflejaban la consideración compartida que se daba al embajador como muñidor de redes, misiones y acciones de penetración en el secreto del adversario, rival o enemigo para alcanzar el inmutable fundamento del espionaje: descubrimiento de las capacidades (medios y recursos) y, sobre todo, designios (es decir, intenciones y voluntad de ejecutar acciones) de quienes podían conceptuarse como enemigos, adversarios, rivales o, también, aliados[7].

Pero penetrar en todas sus dimensiones es tarea que requiere un enfoque integral e integrador. Bien desde una óptica tecnológica, documental, ética, histórica, técnica, doctrinal o incluso cultural, la ruptura del secreto o la penetración en ámbitos de producción de información reservados o sensibles es una realidad tan antigua como el mundo. La vigencia de los asuntos de inteligencia en general y, muy especialmente, de las operaciones de espionaje y contraespionaje en el mundo contemporáneo no ha hecho más que crecer y ganar en complejidades y ramificaciones que huyen claramente de los viejos paradigmas o planteamientos restrictivos de amigo vs. enemigo o de secreto vs. abierto. Aunque esta publicación aludirá a esas perspectivas,

7 Diego Navarro Bonilla, "'Secret Intelligences' in European Military, Political and Diplomatic Theory: An Essential Factor in the Defense of the Modern State (Sixteenth and Seventeenth Centuries)", *Intelligence and National Security*, Vol. 27, n.º 1, 2012, pp. 283-301.

no puede perderse de vista el principal objetivo, centrado en las repercusiones que el espionaje ha tenido y, especialmente, va a tener en el conjunto de relaciones entre Estados.

El estudio del espionaje y sus formulaciones requiere la comprensión de una actividad cuyos fundamentos permanecen estables en el tiempo aunque sus objetivos, métodos y, sobre todo, tecnologías disponibles sí hayan experimentado notables avances de un siglo a otro. Las aplicaciones de la "Espionage Act" de 1917, revela la convivencia entre el llamado "espionaje tradicional" y otras formas de acceso, obtención y revelación de secretos que no responden a este modelo de "espionaje para una potencia extranjera". Por otra parte, el espionaje afecta a dos vectores de fuerza: activo (espionaje) y pasivo (contraespionaje). Los Estados desarrollan operaciones de espionaje para penetrar en el secreto, pero, a su vez, lo contemplan como amenaza global cuando son otros Estados quienes tratan de socavar intereses propios. Sin embargo, frente a amenazas globales compartidas que requieren respuestas de coordinación y esfuerzo conjunto, en el espionaje se concitan intereses muy diversos y no es factible aplicar los mismos principios que ante otras amenazas comúnmente compartidas y presentes en las agendas internacionales de seguridad colectiva. Al mismo tiempo, es necesario determinar quién realiza operaciones de espionaje y quién es espiado, con qué objetivos, métodos, recursos y contexto. Agencias de inteligencia, empresas, particulares, aliados, ciudadanos, competidores, enemigos, rivales, etc., configuran el espectro de agentes tanto activos como pasivos. Las respuestas y las contramedidas para neutralizar su alcance serán llevadas a cabo en virtud de quién, contra quién, cómo y para socavar qué interés nacional se practique.

En este intento por definir las múltiples dimensiones del espionaje, conviene recordar que es reconocido globalmente como una tipología de

amenaza agresiva cuya incidencia y repercusiones en muchos ámbitos de la seguridad y la defensa de los intereses nacionales ha motivado su inclusión en libros blancos y estrategias de seguridad nacional mundiales. La persistencia de sus características fundamentales y nucleares a lo largo de los siglos corre paralela (y eso la convierte en altamente resistente) a la adaptación ágil y efectiva de la tecnología disponible para obtener datos e información sensible en ámbitos muy dispares. Es preciso asimismo identificar las principales áreas en las que las actividades de espionaje alcanzan su grado más alto de amenaza para la seguridad y la defensa de los intereses nacionales. La evolución de la amenaza y sus posibles tendencias determinarán asimismo las posibles respuestas de contingencia y anticipación. Por ello, se debería valorar tanto cuantitativa como cualitativamente el grado de amenaza atendiendo no sólo al espionaje exterior sino interior, así como la repercusión de los abusos en materia de información conocidos recientemente como consecuencia de la acción de los *whistleblowers*[8]. Todo ello no ha hecho sino profundizar en un debate de largo recorrido como es el que concita la dimensión ética y la actividad de inteligencia[9].

No obstante, la actualidad de la agenda de seguridad internacional varía continuamente el foco de atención mediático y si durante esos meses de 2013-2014 el interés por los asuntos de espionaje venían marcados por el binomio Snowden-NSA, en agosto de 2014 se vuelve sobre una realidad que está cambiando profunda, rápida y sorprendentemente el mapa internacional en Oriente Medio. La amenaza del Estado Islámico es de tal calibre y de tal repercusión (en gran medida por su extraordinario aparato de propaganda en la red) que el territorio iraquí está asistiendo a la rápida formación de una coalición liderada por Estados Unidos con países de la zona, incluyendo Irán

8 Edward Spence, "Government Secrecy, the Ethics of Wikileaks and the Fifth Estate", *International Review of Information Ethics*, Vol. 17, July 2012, pp. 38-44.
9 Jan Goldman, *Ethics of Spying: A Reader for the Intelligence Professional,* Vol. 2, Lanham/Toronto/Plymouth, Scarecrow Press, 2012.

y Siria, impensable apenas seis meses atrás. La unión de viejos enemigos frente a un enemigo transfronterizo común como los radicales islamistas admite muchas lecturas pero se subrayan para este caso dos: la consolidación de una respuesta internacional ante un ejemplo máximo de combate asimétrico que ya está sobre la mesa de la OTAN (cumbre de Gales, 4 sept. 2014) y el primordial papel que el espionaje, la infiltración y la contribución de la inteligencia van a tener una vez más, habida cuenta de que la presencia de tropas sobre el terreno sigue siendo una decisión tan controvertida como siempre. Por tanto, de nuevo, afrontar el espionaje y los "intelligence matters" requiere muchas perspectivas y enfoques: clásicos y atemporales en su fundamento último, modernos y mediáticos como corresponde a nuestro mundo global.

3. Espionaje e inteligencia

Con frecuencia se identifica el espionaje con la inteligencia. Sin embargo, ambos términos no son estrictamente sinónimos ya que el segundo engloba al primero. Los servicios de inteligencia generan un conocimiento especializado que es el resultado de un proceso sistemático y normalizado como consecuencia de la transformación de informaciones obtenidas por medios y recursos muy dispares, con métodos también muy diferentes, tanto de carácter abierto como secreto. Con independencia de que la inteligencia se estudie como proceso o como organización, su principal misión se orienta a minimizar los riesgos derivados de las amenazas y a potenciar las fortalezas para convertirlas en oportunidades. En toda época, pero especialmente en la actualidad, la definición de un buen sistema de inteligencia es una capacidad inestimable para afrontar satisfactoriamente el múltiple espectro de amenazas a la seguridad: desde la soberanía de la nación y su integridad jurídica y territorial hasta la defensa de los intereses comerciales, industriales y económicos mediante un sistema de inteligencia competitiva y económica.

En última instancia, invertir en inteligencia para garantizar los objetivos de una agenda de seguridad y defensa resulta rentable y ningún otro medio tiene la enorme capacidad anticipatoria, preventiva y prospectiva.

En todo caso, no se puede entender la actividad de inteligencia sin su reverso ineludible: la contrainteligencia. Penetrar en el secreto del adversario obliga a desplegar las capacidades para impedir que el adversario haga lo mismo con los secretos propios: incremento de la producción armamentística, situación de las bases militares, firmas de convenios económicos y acuerdos políticos, desarrollos tecnológicos y científicos punteros, etc., figuran entre los numerosos objetivos que deben ser protegidos de las acciones de un servicio extranjero. Inteligencia activa, y contrainteligencia defensiva, son por tanto, dimensiones de una misma realidad. Como se señaló en el *Glosario de Inteligencia*, "la función de contrainteligencia se dirige a la paralización y neutralización de todas aquellas actividades desplegadas por un servicio extranjero en suelo propio o contra intereses propios. Vigilar, controlar, alertar de las acciones ofensivas o latentes de organismos extranjeros se encomienda a divisiones especiales de contrainteligencia que, por su trascendencia y sensibilidad, ocupan una parte fundamental de la misión de los servicios de inteligencia"[10].

No puede olvidarse que el espionaje es esencialmente un medio de obtención: uno de los medios más antiguos y en muchas ocasiones decisivos de penetrar en el secreto y lograr la captación de información, no abierta o disponible sin autorización expresa. Lo hemos definido recientemente como:

> Toda acción perpetrada conscientemente para penetrar en un espacio informacional protegido o descuidado a fin de conseguir un incremento de conocimiento por medios encubiertos, insospechados o desconocidos por su

10 Miguel Ángel Esteban Navarro (Coord.), *Glosario de Inteligencia*, Madrid, Ministerio de Defensa, 2007.

legítimo productor o propietario. El espionaje busca de manera prioritaria la obtención de información no pública, protegida bajo diferentes niveles de clasificación y de accesibilidad muy limitada cuyo contenido es sensible y de alto valor para el conocimiento de capacidades e intenciones de un adversario, rival, enemigo o incluso aliado. El acceso no permitido y robo de esta información pone en riesgo al propietario de la misma generándole una vulnerabilidad en materia de seguridad nacional, en sus principios de bienestar social o en su posición competitiva en el marco de las relaciones internacionales"[11].

Los múltiples diccionarios, glosarios, enciclopedias, etc., definen el espionaje en torno a una serie de atributos y particularidades[12]. Con independencia de que el agente de espionaje sea un individuo o una organización pública o privada dedicada a las más variadas actividades, los daños que puede provocarles lo sitúan entre las acciones intrusivas de mayor espectro y nivel de agresividad. El espionaje afecta poderosamente a la seguridad nacional y a sus intereses políticos, comerciales, económicos y de infraestructura vital. El espionaje queda definido por la finalidad, aplicación práctica y uso que de lo obtenido se haga para sustentar fines muy dispares. No sólo es, por tanto, una actividad ilícita en sí misma, sino profundamente peligrosa en virtud de la finalidad para la que se emplee la información obtenida.

En la definición de espionaje es preciso determinar el conjunto de intereses, los objetos de atención (si son datos aislados o información agregada y valorada), los medios, recursos, técnicas y procedimientos, así como

11 Diego Navarro Bonilla, "Espionaje", en Luis de la Corte y José María Blanco (Eds.), *Amenazas a la seguridad nacional*, 2014 (en prensa).

12 Ver por ejemplo: K. Lee Lerner, y Brenda Wilmoth Lerner, *Encylopedia of Espionage, Intelligence and Security,* Detroit, Thomson Gale, 3 Vols., 2004; Miguel Ángel Esteban Navarro (Coord.), *Glosario de Inteligencia*, Madrid, Ministerio de Defensa, 2007; Jan Goldman, *Words of Intelligence: intelligence Professional´s Lexicon for Domestic and Foreign Threats*, Lanham, Toronto, Plymouth: Scarecrow Press, 2011; DIS (Dipartimento delle Informazioni per la Sicurezza, Presidenza del Consiglio dei Ministri, Italia), *Il linguaggio degli organismo informativi: glossario intelligence*, Roma, De Luca, 2012.

la responsabilidad tanto directa como indirecta en la comisión de operaciones de espionaje, bien sean tradicionales o de corte cibernético. Frente a los objetivos de otro tipo de amenazas a la seguridad nacional, el espionaje se desarrolla en situaciones informacionales presididas por unos niveles que oscilan entre el secreto y la discreción.

Es un error frecuente considerar a todo miembro de un servicio, con independencia de su perfil profesional, competencias, funciones, habilidades, puesto de trabajo y capacidades, como un espía. A su vez, todos los espías que trabajan estable o eventualmente para un servicio definen su nivel de pertenencia a ese servicio en virtud de su compromiso contractual, su dependencia laboral, su estatuto especial (como en el caso español)[13] o su grado de implicación y motivación para desarrollar esa actividad. El secreto queda entonces como componente intrínseco del espionaje, como actividad y atributo del espía como sujeto ejecutor de la función (que no la responsabilidad última) del espionaje. No hay que olvidar que el espía ejerce su actividad, bajo cualquiera de las modalidades clásicas (doble, obligado, libre, volante) y de sus motivaciones (económica, patriótica, aventurera, chantaje…) generalmente dirigido, contratado o supervisado por un organismo de inteligencia del Estado, aunque no de manera exclusiva[14].

De hecho, es preciso determinar el ejecutor de la acción de espionaje: el individuo o conjunto de individuos que en tiempo de guerra o de paz, siguiendo instrucciones de un servicio de inteligencia o no, obtiene una información de manera encubierta y sin autorización. Por ello, no se comprende

13 Xavier Boltaina, "El personal del Centro Nacional de Inteligencia: su vínculo jurídico como 'empleado público' y la afectación de sus derechos y deberes", *Inteligencia y Seguridad: Revista de Análisis y Prospectiva,* n.º 11, 2012, pp. 183-212.

14 Terence J. Thompson, "Toward an updated understanding of espionage motivation", *International Journal of Intelligence and Counter Intelligence*, Vol. 27, n.º 1, 2014, pp. 58-72.

la acción del espía sin la organización para la que trabaja, el organismo que le brinda apoyo logístico, le marca los objetivos o, llegado el caso, le paga por sus servicios, no siempre con una contraprestación económica.

En todo caso, con independencia de que la tecnología disponible en la actualidad consiga resultados espectaculares en las operaciones de obtención y volcado masivo de grandes volúmenes de información, el fundamento del espionaje se basa en dos principios inmutables: conocer las capacidades y las intenciones del objetivo espiado. Los principales bloques temáticos hacia los que se orienta toda acción de espionaje son de tres tipos:

1. Información secreta militar (orden de batalla de un ejército extranjero, tecnología de defensa, información sobre armamento, renovación y actualización de capacidades, etc.

2. Información secreta industrial para alcanzar ventaja competitiva frente a rivales económicos (planes estratégicos, proyectos de innovación de productos y servicios, invenciones y modelos en áreas sensibles, etc.).

3. Información secreta de naturaleza política (decisiones de gobierno, planes estratégicos, negociaciones internas y exteriores, desarrollo económico, acuerdos internacionales sectoriales, etc.).

4. Metadatos: Ilusiones omniscientes y espionaje masivo internacional

El deseo de un gobierno por desarrollar dispositivos capaces de suministrarle toda la información que de manera inadvertida fuera captada, es ciertamente una aspiración atemporal y una suerte de "ilusión por la omnis-

ciencia". Tal vez el estudio de las campanas fónicas secretas diseñadas por el jesuita Athanasius Kircher (ca.1603-1680) en su obra *Phonurgia Nova* publicada en 1673[15] sean un temprano y clarísimo ejemplo para comprender los medios de los que un gobernante puede servirse para escuchar todas las conversaciones que se produjeran en las calles, plazas y hasta pasillos de cortes y despachos de secretarios y príncipes extranjeros. Cuanta más información y cuantos más secretos quedasen penetrados y descubiertos de manera indiscriminada y masiva, más absolutos serían los atributos de su poder[16].

Lejos quedan sin duda estos diseños y prototipos de los dispositivos de espionaje masivo de nuestros días. Sin embargo, preludiaban la carrera tecnológica de las potencias modernas y contemporáneas por dotarse de sistemas y mecanismos de control de comunicaciones, de programas de pretendidas aspiraciones planetarias, completas, integrales y masivas. Algo que ha sido una constante desde el 11-S especialmente. Los títulos y objetivos de programas auspiciados por agencias como DARPA (*Defense Advanced Research Projects Agency*) y DISA (*Defense Information Systems Agency*) así lo muestran: *Information Awareness Office, Information Processing Technology; Information Exploitation Office,* etc. Por su parte, empresas filiales de agencias como la CIA hacían del desarrollo de una nueva generación de herramientas tecnológicas, aplicadas a la seguridad nacional su principal objetivo, como en el caso de In-Q-Tel. Entre las principales áreas de investigación apoyadas se situaron los programas de control de las comunicaciones electrónicas, el vaciado y control de millones de datos a partir de la minería de datos o la traducción automática, la biovigilancia o la aplicación de las herramientas de procesamiento automático del lenguaje natural.

15 Athanasii Kircher, *Phonurgia nova, sive, Conjugium mechanico-physicum artis & natvrae paranympha phonosophia concinnatum: quâ vniversa sonorvm natvra, proprietas, vires, effectuúmq[ue] prodigiosorum causa…* , Campidonae, Rudolphum Dreherr, 1673.

16 Marc Andrejevic, *Infoglut: How Too Much Information Is Changing the Way We Think and Know*, Abingdon, Taylor and Francis, 2013.

Durante el verano de 2013, la expresión "Big data", de hondas e inquietantes resonancias orwellianas se ha instalado en los medios de comunicación como el nuevo término de moda. Actualmente, no hay día que no aparezcan varios titulares en los medios de comunicación sobre este asunto. Incluso el impacto del "Big Data" como objeto de atención científica ha llegado a las salas de exposiciones. El vanguardista CCCB inauguró en mayo de 2014 una muy lograda muestra sobre las dimensiones del Big Data y las repercusiones del llamado "nuevo oro negro": los datos. Las monografías especializadas, comenzando por las traducciones a numerosas lenguas del libro de Mayer-Schönberger y Cukier[17], tratan de acercar al público general esta realidad que se sitúa en el centro de la actividad y la controversia en torno a las prácticas desarrolladas por los servicios de inteligencia en la actualidad. Si estos autores han denominado a la práctica del big data como de revolución, convendría entonces situar también esta revolución en el conjunto de innovaciones y cambios de paradigma que en materia de inteligencia ha venido sustentando desde hace veinte años la denominada "Revolución en los asuntos de inteligencia" que Deborah Barger ya describiera en un trabajo pionero[18].

Para cumplir con los objetivos que les marcan las Directivas Nacionales, los servicios de inteligencia deben afrontar hoy en día dos grandes retos dentro de la fase de obtención de información en bruto: la sobreabundancia de información en unos casos y el difícil procesamiento y conversión de toda esa masa informacional en verdadero y efectivo conocimiento aplicado para la acción, es decir, para la decisión. Por ello, se llevan a cabo medidas como la especialización de los órganos de obtención, la formación permanente de expertos, la adquisición de medios tecnológicos de obtención, procesamien-

17 Viktor Mayer-Schönberger y Kenneth Cukier, *Big Data: la revolución de los datos masivos*, Madrid, Turner, 2013.
18 Deborah Barger, *Toward a Revolution in Intelligence Affairs*, Santa Mónica, Rand Corporation, 2005. Ver también: William Lahneman, *Keeping U.S Intelligence Effective: The Need for a Revolution in Intelligence Affairs,* Maryland, Scarecrow, 2011.

to e integración de grandes volúmenes de datos, el uso compartido de datos entre diversos órganos de un servicio y la colaboración entre diversas agencias de inteligencia dentro de un Estado o de una alianza.

Sin embargo, en el debate sobre el espionaje contemporáneo, ha penetrado con fuerza la realidad de un término que se vincula con la teoría de la información y la documentación: los metadatos. Se dice que son millones de datos que refieren o relacionan con otros datos (metadatos), pero no son el contenido real. Dentro de la profesión biblioteconómica, este término acuñado por Jack Myers en los 60 se viene usando desde hace décadas. El metadato es entendido como aquella información mínima necesaria para identificar un recurso de información. El dato por sí solo no ofrece una unidad de comprensión completa, pero la unión de muchos metadatos nos ofrece información suficiente para perfilar y comprender una entidad de información superior. Así, ejemplos de metadatos son desde direcciones IP o DNS, encabezamiento de mensajes de correo electrónico, descripción de los archivos accesibles vía FTP hasta los términos extraídos por los motores de indización/búsqueda, fechas y autoría del documento, código y programación empleados, etc.

La Sociedad Española de Documentación e Información Científica los ha definido de manera muy clara: "metadato es toda aquella información descriptiva sobre el contexto, calidad, condición o características de un recurso, dato u objeto que tiene la finalidad de facilitar su recuperación, autentificación, evaluación, preservación y/o interoperabilidad"[19]. Por su parte, la Sociedad Americana de Archiveros entiende que:

> Metadata is frequently used to locate or manage information resources by abstracting or classifying those resources or by capturing information not

19 Sociedad Española de Documentación e Información Científica. http://www.sedic.es/autoformacion/metadatos/tema1.htm.

> inherent in the resource. Typically metadata is organized into distinct categories and relies on conventions to establish the values for each category. For example, administrative metadata may include the date and source of acquisition, disposal date, and disposal method. Descriptive metadata may include information about the content and form of the materials. Preservation metadata may record activities to protect or extend the life of the resource, such as reformatting. Structural metadata may indicate the interrelationships between discrete information resources, such as page numbers[20].

Este es el contexto general en el que se ha desarrollado la macro atención mediática sobre el papel y la responsabilidad que cabe atribuir a la NSA primero y a numerosos servicios de inteligencia después en el desarrollo de programas de obtención masiva de datos. Sin embargo, conviene profundizar en las implicaciones éticas que tienen el trabajo que realizan los trabajadores que prestan sus servicios no sólo en agencias de inteligencia gubernamentales sino también en unidades de inteligencia competitiva y de negocios o en empresas subcontratadas por estos servicios y agencias. Un colectivo de especial interés lo componen aquellos profesionales de la información y la documentación, formados en facultades de información y documentación y en departamentos de Biblioteconomía y Ciencias de la Documentación. A ellos, expertos en el manejo de recursos de información abierta (OSINF: *Open Source Information*), la expresión "metadata management" no les es desconocida en absoluto. Estándares como EAD (*Encoded Archival Description*), EAC (*Encoded Archival Context*), MARC (*Machine Readable Cataloging*), etc., son de uso cotidiano. Por ello, aunque tradicionalmente el impulso al desarrollo de formatos de metadatos ha procedido de la técnica multimedia y de la web semántica, la aplicación de la gestión de metadatos a organismos de inteligencia, seguridad y defensa se alza como un campo enormemente sugerente. En suma, por sus manos pueden acabar

20 Society of American Archivists, *A Glossary of Archival and Records Terminology* http://www2.archivists.org/glossary/terms/m/metadata.

pasando millones de datos de la más diversa procedencia situándose a las puertas del *data mining*.

En un reciente artículo, en el que se analizan las tendencias y principales retos a los que se enfrentan los profesionales de la información y la documentación actualmente, su autor, Arno Reuser, concluye: "Look for opportunities to assert the value of information professionals and the intelligence community"[21]. Como profesor de Información y Documentación y Gestión de documentos y fuentes abiertas suscribo este mismo llamamiento ya que desde una perspectiva profesional y competencial, es necesario plantear las interrelaciones entre estos dos ámbitos tan ligados: gestión y explotación de información y servicios de inteligencia. Es algo que ya habíamos puesto de manifiesto, en parecidos términos, en un artículo hace algunos años[22]. Sin embargo, en todos estos años apenas habíamos prestado atención a un asunto que se daba por asumido e integrado: el código deontológico de los profesionales de la información y la documentación. Los recientes acontecimientos vinculados a Snowden como paradigma del *whistleblower*, muestran la ingenuidad de aquella asunción y obligan a plantear con rotundidad la exigencia ética de los profesionales que manejan información, gestionan documentos y producen conocimiento y que, surgidos de nuestras aulas, pueden llegar a desempeñar puestos y responsabilidades de alto nivel en servicios u organismos vinculados a la comunidad de inteligencia nacional[23].

Este llamado "Information Landscape" es importante pero queda un tanto desdibujado si falla lo más fundamental: la confianza de la ciudadanía en sus instituciones (teóricamente en un sistema democrático), que velan por

21 Arno Reuser, "Trends in the Current Information Landscape and Their Significance for Researchers", *Online Searcher*, Jab./Feb. 2013, pp. 51-55.
22 Miguel Ángel Esteban Navarro y Diego Navarro Bonilla, "Gestión del conocimiento y servicios de inteligencia: la dimensión estratégica de la información*", El Profesional de la Información*, Vol. 12, n.º 4, 2004, pp. 269-281.
23 Diego Navarro Bonilla, "Information Management professionals… ", op. cit.

su seguridad y defensa, pero que se deslizan sospechosamente por una intrusión en la esfera privada de los datos, de los grandes datos. Se habla mucho de la ética en inteligencia y hay notables esfuerzos para tratar de armonizar lo que otros autores consideran un oxímoron[24]. Trabajos como los que desarrolla la *International Intelligence Ethics Association* o Jan Goldman al frente del *International Journal of Intelligence Ethics* proporcionan un marco de trabajo académico imprescindible sobre la dimensión ética del trabajo de inteligencia. No obstante, en el conjunto de comentarios, reflexiones y noticias recientemente aparecidas no se ha visto muy mencionada durante el escándalo Snowden, al menos no en España.

5. La pesca de arrastre: la falsa percepción de los metadatos y el "espionaje ciego"

La inteligencia generada a partir de fuentes abiertas de información (OSINT: *Open Sources Intelligence*) sufrirá la próxima gran transformación en este campo: su completa automatización. La máquina recupera la información requerida en virtud de los parámetros de búsqueda, ecuaciones definidas, aplicación de controles de términos a buscar, perfiles de usuarios según necesidades y requerimientos. En suma, ejerciendo la difusión selectiva de información que antaño elaboraban de manera muy pormenorizada los documentalistas. La obtención masiva de datos en tiempo real, en todas partes del mundo y de millones de individuos a la vez, por fuerza deviene en un sistema que, como poco, plantea problemas de eficiencia y eficacia: se busca todos los datos de todos porque no hay capacidad para discriminar y refinar a priori. Una cosa es que los grandes sistemas y capacidades tecnológicas permitan esa interceptación masiva de datos. Claro que es posible y se

24 Allison Shelton, "Framing the Oxymoron: A New Paradigm for Intelligence Ethics", *Intelligence and National Security*, Vol. 26, n.º 1, 2011, pp. 23-45.

hace. La cuestión trascendental no es ésa sino responder con seguridad a esta pregunta: ¿todos esos datos son pertinentes para la seguridad y la defensa? Si no es así, ¿qué se hace con los datos que deben ser desechados y eliminados por afectar a la intimidad de las personas? ¿Quién valora los "metadatos" no interesantes para un servicio de inteligencia? ¿Interesa todo? Estamos hablando por tanto de una suerte de sistemas de obtención de información ciegos, maximalistas, por cantidad y no por calidad.

Esa captura masiva de datos (*Data massive Gathering*) se asemeja a una pesca de arrastre en la que todo cae bajo las redes. Se obtienen datos pero sin capacidad de discriminación, valoración o preanálisis: cuando todo son datos, nada es inteligencia. El espionaje, como ha señalado recientemente el novelista Ian McEwan se convierte en algo mecánico y ciego. De pronto, "los servicios de inteligencia espían, sin preguntarse por qué ni para qué, así que no es extraño lo que ha ocurrido, pero sí fascinante"[25].

Entonces, ¿quién, cómo, de qué forma y en qué plazo se desechan y se tiene constancia de que se hace, los millones de datos que no interesan para los fines propios de identificación de amenazas, de confirmación de riesgos directamente vinculados a la seguridad nacional? Es ahí, de nuevo, donde el profesional de la información y la documentación deberá aplicar sus conocimientos y capacidades en el complicado, sistemático y muy técnico "refinado arte de la destrucción" de documentación, una vez aplicados protocolos de identificación, selección y valoración sometidos al escrutinio de grupos de trabajo muy competentes de juristas, archiveros y responsables de seguridad interna[26]. Por todo ello, las competencias en materia de identificación, selección y destrucción de datos y documentos perfectamente controlados por comisiones calificadoras de documentos adquiere un nuevo

25 Ver: *El Mundo*, 30 de octubre de 2013, p. 47.
26 Luis Hernández Olivera (Ed.), *El refinado arte de la destrucción: la selección de documentos*, Salamanca, Acal, 2003.

realce y perspectiva al amparo no sólo del *Records Management* sino de la protección de datos de carácter personal. La aplicación del código deontológico del profesional de archivos dentro de un organismo de inteligencia debería tener entonces un papel determinante para aplicar los principios, criterios y normas estrictas de aprovechamiento de los datos única y exclusivamente relevantes para una investigación en seguridad y defensa. El resto de datos, en caso de que se hayan obtenido, deben ser rápida y completamente eliminados, no almacenados "por si acaso" o acumulados en grandes repositorios de los que nadie acaba acordándose y con un destino incierto.

La recuperación discriminada, ponderada y bien refinada de datos se alza entonces no sólo como una obligación ética y legal de ajuste al derecho de protección de la información personal, sino también un indicador de calidad que redunda en la eficiencia y la eficacia de los resultados: no todos los datos valen para hacer inteligencia. Sin olvidar las implicaciones económicas que tiene la masificación de datos: ¿para qué gastar grandes cantidades de dinero público en sistemas automáticos que recuperan todo de todos? ¿Es eso eficiencia en el control de gastos con fines de inteligencia? Por ello, existen ya numerosas aproximaciones a los controles de calidad tanto en las fases de obtención y aprovechamiento de recursos de información abierta con fines de inteligencia procedentes de la disciplina Information/Intelligence Audit[27], así como enfoques orientados a validar la calidad del producto final de inteligencia[28]. Sin embargo, en las fases de obtención de información en bruto con la que generar nuevo conocimiento, esa automatización masiva y sin criterio puede devenir en un verdadero caos organizativo de grandes proporciones que amenaza con convertirse en otro gran error histórico como cuando la apuesta por la tecnología (SIGINT: *Signal Intelligence*) en detri-

27 Susan Henczel, *The Information Audit: a practical guide*, Munich, Saur, 2001; Andréa Vasconcelos Carvalho, *Auditoría de Inteligencia*, Gijón (Spain), Trea, 2012.
28 Giliam De Valk, *Dutch Intelligence: Towards a Qualitative Framework for Analysis,* Eleven International Publishing, The Hague, 2005.

mento de HUMINT (*Human Intelligence*) marcó una grave deriva de los servicios de inteligencia una vez que cayó el muro de Berlín y se proclamó el fin del enfrentamiento con los enemigos tradicionales o simétricos.

Buscar la respuesta en el universo de los metadatos y apostar por una automatización masiva de los procesos de obtención (*gathering*) y recuperación (*retrieval*) de información nos sitúa a las puertas de la dicotomía big data vs. big narrative en la que ha profundizado Evgeny Morozov. Se ha abierto ya una profunda división entre el conjunto de datos aislados que se alzan como indicios de correlación futura de posibles hechos frente a la tradicional necesidad de comprensión en profundidad y no sólo de manera automática del contexto y las causas variadas que explican el porqué de esos datos. De repente, otra de las inquietantes consecuencias de los documentos destapados por el caso Snowden y publicados por *The Guardian* es comprobar el mayor interés sobre la prevención y la inducción a partir de datos y no sobre la comprensión, el contexto, la explicación o las circunstancias en las que se generan esos datos. Al Big Data no le interesa comprender, sólo determinar cuándo se va a producir el hecho a partir de la interrelación y la correlación de piezas de información, de datos: de metadatos. Morozov, citando a Marc Andrejevic lo ha expresado meridianamente: "El coste en la adopción del Big Data por los servicios de inteligencia (y por casi todos los demás sectores públicos y privados) es la devaluación de la comprensión individual, encarnada por nuestra reticencia a investigar las causas de las acciones y saltar directamente a sus consecuencias. Pero, sostiene Andrejevic, mientras Google puede permitirse ser ignorante, las instituciones públicas no"[29].

Realmente éste es uno de los temas de debate de altura más relevante y actual más profundo en materia de inteligencia. Cuando tanto se está

29 Evgeny Morozov, "The challenge of managing great databanks", *El País*, 24 de junio de 2013, http://elpais.com/elpais/2013/06/24/opinion/1372068111_079679.html.

hablando de los metadatos interceptados por la inteligencia de señales al amparo del caso Snowden, autores como Morozov han destapado lo que algunos autores estiman como el gran y verdadero reto: big data vs. big narrative. ¿Qué papel van a jugar entonces los analistas de inteligencia frente a una mayor preeminencia del metadato, de la acumulación, de la conexión que establezca principios de vínculo entre hechos pero nunca accediendo a la comprensión del contexto de esos datos? La correlación y la inducción entre grandes volúmenes de datos está siendo la base no de la producción de conocimiento, sino de la acción inmediata. Los datos para actuar, no para comprender. Sin embargo, las decisiones deben estar basadas en conocimiento contrastado y no sólo en datos que generan indicios. ¿Para qué analizar, para qué comprender las causas últimas de los hechos si la automatización completa de la información, si la recuperación de datos nos ofrece ilusoriamente la base para actuar? Lo que se plantea es una gran brecha: del dato a la acción, sin pasar por el análisis, sin atender a su comprensión profunda.

Por todo ello, no se puede olvidar el enorme impacto que los metadatos tienen en la protección de los derechos fundamentales: "The risk of automatic processing of personal data has been already warned by the Council of Europe"[30]. La vicepresidenta de la Comisión Europea y responsable de Justicia, Viviane Reding, ha manifestado rotundamente la posición: "los datos personales de los europeos son un derecho fundamental no negociable". La Eurocámara ha aprobado la propuesta que regula claramente que cualquier cesión de datos de carácter personal de un ciudadano europeo a terceros requiere taxativamente una autorización previa del organismo regulador nacional de la protección de datos y un aviso al interesado[31]. Esto va

30 Recommendation CM/Rec(2012)3 of the Committee of Ministers to member states on the protection of human rights with regard to search engines; Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling (23 November 2010).

31 Gloria González Fuster, "Security and the future of personal data protection in the European Union", *Security and Human Rights*, Vol.23, n.º 4, pp. 33-342.

claramente dirigido a las empresas que cooperan con los servicios de inteligencia y vuelve a alertar sobre los peligros de la imparable privatización de la inteligencia. Pero eso sería otro tema.

6. Espionaje como amenaza a la seguridad

De forma global y unánime, el espionaje es conceptuado como amenaza a la seguridad nacional. Las principales estrategias nacionales de seguridad, los libros blancos de la defensa y cuantos documentos estratégicos identifican el listado de riesgos, peligros y amenazas se hacen eco de su incidencia. Por ejemplo, la Estrategia de Seguridad Nacional Española de 2013 incluye al espionaje entre las siguientes amenazas: conflictos armados, terrorismo, ciberamenazas, crimen organizado, inestabilidad económica y financiera, vulnerabilidad energética, proliferación de armas de destrucción masiva, flujos migratorios irregulares, emergencias y catástrofes, vulnerabilidad del espacio marítimo, vulnerabilidad de las infraestructuras críticas y servicios esenciales.

La principal incidencia del espionaje (especialmente el económico) se sitúa en la pérdida de conocimiento estratégico, competitividad y capacidad de desarrollo y avances como consecuencia del robo de conocimiento. En muchos libros blancos de la defensa y estrategias nacionales, el espionaje comparte espacio con otras amenazas de largo recorrido y otras que son la expresión de las adaptaciones a las demandas securitarias que impone la globalización. No obstante, a diferencia de lo que otras amenazas como el terrorismo de naturaleza islamista o la proliferación de armas químicas, nucleares o radiactivas, el espionaje no favorece las mismas políticas de coordinación y cooperación frente a un enemigo común y compartido. Los Estados han espiado, espían y espiarán: a posibles adversarios, aliados, rivales

o enemigos. Determinar quién lleva a cabo acciones de espionaje (agencias de inteligencia, empresas, particulares), a quién (aliados, ciudadanos, competidores, enemigos o rivales), cómo (medios tradicionales, de alta tecnología, combinados) y con qué intenciones, fines y propósitos son preguntas que determinan el tipo de respuesta a articular. Paralelamente, el reverso inevitable de la acción de los medios de espionaje es el contraespionaje. Neutralizar estas acciones de espionaje contrarias a los intereses nacionales, con independencia de que sean perpetradas por aliados, rivales o enemigos conduce a las funciones de contrainteligencia que todo organismo o agencia de inteligencia tiene entre sus mandatos. Es esta dialéctica espionaje/contraespionaje, inteligencia/contrainteligencia la que determina la propia historia de la información secreta[32]. Dentro de la Estrategia de Seguridad Nacional Española, los objetivos de la contrainteligencia como respuesta genérica al espionaje se cifran en: "Adoptar medidas en la defensa de los intereses estratégicos, políticos y económicos de España, para prevenir, detectar y neutralizar las agresiones encubiertas procedentes de otros Estados, de sus servicios de inteligencia y de grupos o personas, que estén dirigidas a la obtención ilegal de información". En todo caso, parece oportuno indicar una serie de recomendaciones generales para poner en práctica entre las que figura una concienciación mayor sobre los daños que provoca el descuido en la protección de información sensible, así como un reforzamiento de las competencias, habilidades y formación en materia de contrainteligencia, especialmente humana.

Sin embargo, hasta las revelaciones destapadas por Snowden, pensar en espionaje como amenaza a los intereses nacionales era hacerlo en un único sentido: el de un enemigo que trata de penetrar en secretos e información protegida. Lo habitual era, por tanto, concebir el espionaje bajo un parámetro de amenaza exterior, siempre desde fuera, que daña algún aspecto de la

32 Diego Navarro Bonilla, *Espías: tres mil años de información… , op. cit.*

seguridad nacional. El extraordinario material informativo descubierto pone de manifiesto que el espionaje se lleva en múltiples niveles y hacia todas las direcciones, encaminándose hacia una peligrosa deriva integral: interesa conocer todo, de todos: ciudadanos propios, enemigos externos, rivales económicos, adversarios políticos, amigos o no.

6.1. Espionaje económico

La gran facilidad de acceso y opciones de captación de datos de manera puntual o masiva que brinda la informática es una de las características que estrategias de seguridad, libros blancos y cualquier panorama internacional de riesgos y amenazas a la seguridad incluyen a la hora de definir el espionaje. No obstante, sería erróneo pensar que todo el espionaje se realiza hoy en día mediante técnicas informáticas o con recursos ultramodernos. Ello implicaría despreciar las experiencias milenarias que el espionaje y el contraespionaje tradicional han generado. Los métodos clásicos de penetración en las redes de comunicación, transmisión de datos y acumulación de información reservada siguen vigentes: "El espionaje de última generación lo es en tanto en cuanto los medios de interceptación y acceso a información protegida, lo son también de última generación. Pero cualquier organismo de inteligencia sabe por experiencia que los fundamentos, principios, bases y características definitorias del espionaje mantienen su vigencia desde hace siglos"[33].

El robo de secretos industriales para conseguir una ventaja competitiva es una realidad anclada en la propia Historia desde la más temprana Antigüedad[34]. Como consecuencia de las crisis energéticas y económicas globales, el espionaje económico e industrial ha alcanzado un protagonismo determinante entre el conjunto de variadas y particulares acciones de los espías

33 Diego Navarro Bonilla, "Espionaje", en Luis de la Corte… , *op. cit.*
34 Eduardo Juárez, *Venecia y el secreto del vidrio: Cuatrocientos años de monopolio*, Madrid, Catarata, 2013.

y ladrones de secretos de aplicación económica. Acuerdos comerciales, protección económica y aumento de los ingresos en las arcas públicas han sido siempre materias complementarias a la seguridad y la defensa de los intereses de un Estado. La dimensión económica de la información sensible contribuye a extender la protección del secreto. En muchas ocasiones, detrás de la organización de una campaña militar y antes de proclamar el estado de guerra con una potencia rival, se encontraba la necesidad histórica de proteger las rutas comerciales, los espacios ricos en materias primas y recursos energéticos y fortalecer los intercambios económicos entre aliados o rivales, garantizar la explotación de productos o defender los mercados abiertos con compradores y proveedores. En la actualidad, bajo la denominación de espionaje económico se esconde un conjunto dispar de actuaciones que han motivado numerosas intervenciones y dedicado ímprobos esfuerzos a su prevención como línea prioritaria recogida en las estrategias nacionales de seguridad.

Dos son las actividades fundamentales a la hora de contextualizar el robo de secretos bajo la denominación de espionaje económico. Por una parte la inteligencia económica y por otra, la inteligencia competitiva. Ninguna de las dos son un delito, pero el espionaje industrial sí lo es. Todos los países desarrollados llevan a cabo políticas de inteligencia económica, mientras su tejido empresarial se dota de las capacidades más eficaces para que cada empresa alcance ventajas continuas de la transformación estratégica de información en conocimiento para la acción y la decisión empresarial. Incluso asociaciones como *Strategic and Competitive Intelligence Professionals* promueven la formación de profesionales y su integración en estructuras tanto económicas como académicas. Mejorar la posición en un sector de negocio y hacerlo por encima de los resultados de los posibles o reales competidores es el fundamento de la inteligencia competitiva. Por ello, conviene diferenciar claramente los fundamentos y características de los tres términos para delimitar su incidencia en el conjunto de relaciones

internacionales entre potencias que se sirven de entramados empresariales para realizar múltiples intentos de penetración en el secreto del rival o adversario, incluyendo las acciones de influencia mediante lobbys o grupos de presión. Los objetivos de la inteligencia competitiva son: "planificar y adoptar medidas para mantener la competitividad de la empresa y afrontar con mayores garantías los rápidos y continuos cambios a los que se ve sometida toda organización"[35]. Para ello, la información política, social, económica, cultural, legal y tecnológica constituye un sistema que influye decisivamente sobre la empresa, sus decisiones, su contexto y su devenir. La identificación de indicadores y señales de cambio en ese entorno son determinantes para garantizar esa posición competitiva.

Por su parte, la inteligencia económica privilegia la acción de los Estados. Son ellos, a través de las oficinas económicas presidenciales o a través de las direcciones de inteligencia económica de sus propias agencias de inteligencia las que monitorizan la obtención y procesamiento de información financiera, económica y empresarial del Estado y del exterior con el propósito no sólo de salvaguardar los intereses nacionales, tanto en el interior como en el exterior, sino, sobre todo, incrementar esos niveles económicos en el contexto internacional. Naturalmente, son muchas las acciones y medidas emprendidas para alcanzar estos objetivos. De hecho, "la sensibilización de las empresas nacionales sobre la necesidad de adoptar medidas preventivas contra el espionaje económico, la realización de análisis macroeconómicos de los Estados en los que se pretende invertir o hay inversiones de empresas del país, la protección interna y la promoción y protección externa en el mercado de la industria nacional, el control del tráfico de material de defensa o de doble uso civil y militar y la creación de una cultura de la inteligencia económica", figuran entre las más habituales[36].

35 Miguel Ángel Esteban Navarro (Coord.), *Glosario de Inteligencia*, *op. cit.*

36 *Ibídem*.

6.2. Ciberespionaje

Según el informe elaborado por el *Center for Strategic and International Studies* (CSIS) en 2013 titulado *The Economic Impact of Cybercrime and Cyberespionage*, las pérdidas económicas por actividades de ciberdelincuencia y ciberespionaje suponen entre el 0,5 y el 2% del PIB de una nación. Actualmente, más de 30 países han definido ya o están a punto de consensuar sus propias estrategias de ciberseguridad, ciberguerra y ciberdefensa[37]. Sin embargo, bajo esta denominación genérica, se engloban múltiples amenazas concretas, de alcance, definición e incidencia específicas: desde la suplantación de identidad hasta la denegación de accesos o el robo de secretos. Todo ello, además, en continua evolución con escenarios como los identificados por el proyecto 2020 del *European Cybercrime Center* de Europol (EC3) en 2012, donde se subraya las graves repercusiones a corto plazo de la intrusión monetaria, manipulación de redes de información, destrucción de datos, evasión y movimientos fiscales ilegales, falsificación de moneda e identidades, etc.

Para entender el alcance de muchas de las operaciones de espionaje lanzadas semanalmente por unidades especializadas de las principales potencias, es preciso señalar las características del moderno campo de batalla: el ciberespacio. El espionaje digital o ciberespionaje es un tipo de ataque que aprovecha las vulnerabilidades de las redes de información y comunicación socavando los niveles de confidencialidad de la información secreta. Sistemas, repositorios de información sensible o de interés nacional, redes de comunicación, son los medios habituales para penetrar mediante formas muy desarrolladas de software malicioso en sus muy diversas modalidades: desde los gusanos hasta los troyanos. La incidencia del ciberespionaje ha

37 UNIDIR, *The Cyber Index: International Security Trends and Realities*, New York/Geneva, UN, 2013. http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf.

motivado respuestas muy concretas y de hondo calado en el conjunto de acciones emprendidas para garantizar la seguridad en esta frontera. En España, la creación del Mando Conjunto de Ciberdefensa, con el que las Fuerzas Armadas se protegerán frente a ciberataques y contribuirán a la ciberseguridad es una de ellas y coherente con la propia Estrategia de Seguridad Nacional y la Estrategia de Ciberseguridad Nacional, ambas de 2013. En ella, se especifica que el espionaje es uno de los Riesgos y Amenazas a la Ciberseguridad Nacional y entre las misiones más directamente encaminadas a afrontar el riesgo del ciberespionaje se encuentran: "Garantizar la disponibilidad, integridad y confidencialidad de la información, así como la integridad y disponibilidad de las redes y sistemas que la manejan y tenga encomendados". Por otra parte, es necesario destacar la dimensión internacional de la cooperación en materia de ciberseguridad cuando se afirma que uno de los objetivos de esta estrategia española es "contribuir a la mejora de la ciberseguridad en el ámbito internacional". Para ello, se adoptará una serie de medidas tales como la promoción, apoyo y desarrollo **"**de una política de ciberseguridad coordinada en la Unión Europea y en las organizaciones internacionales de Seguridad y Defensa en las que participa España, y se colaborará en la capacitación de Estados que lo necesiten, mediante la política de cooperación al desarrollo, ayudándoles a implantar una cultura de la ciberseguridad. Se fomentará la cooperación en el marco de la UE y con organizaciones internacionales y regionales como, la Agencia Europea de Defensa (EDA), la Agencia Europea de Seguridad de las Redes y de la Información (ENISA), el Centro Europeo de Ciberdelincuencia, adscrito a Europol, la Organización de Naciones Unidas (ONU), la Organización para la Seguridad y la Cooperación en Europa (OSCE), la Organización del Tratado del Atlántico Norte (OTAN) y la Organización para la Cooperación y Desarrollo Económico (OCDE), entre otras"[38].

38 Presidencia del Gobierno de España, "Estrategia de Ciberseguridad Nacional", Madrid, Gobierno de España, 2013.

7. Espionaje y relaciones internacionales

"Espiar a los amigos es totalmente inaceptable", señaló recientemente la canciller Ángela Merkel. Al mismo tiempo, la Comisión Nacional de la Informática y de las Libertades (CNIL) de Francia afirma, igualmente, que las prácticas de la DGSE no están fundadas legalmente. El espionaje entre países aliados no figura oficialmente entre las amenazas oficiales que afrontan los miembros de la Unión Europea o los aliados de la OTAN. La Estrategia de Seguridad Europea de 2003 incluye las necesarias menciones al terrorismo, la proliferación de armas de destrucción masiva, los conflictos regionales, la descomposición del Estado, o la delincuencia organizada. Todas ellas hacen suponer siempre que las amenazas consolidadas provienen de fuera, pero nunca de un país miembro hacia otro.

Mientras tanto, los millones de metadatos procedentes de la acción de dispositivos de escucha masiva se almacenan preventivamente hasta componer grandes repositorios de información. Durante los años 2013 y 2014, los escándalos por espionaje han marcado la actualidad mediática global. Si en un primer momento las relevaciones de Assange habían abierto una puerta a la sospecha sobre el alcance de los programas planetarios de interceptación de comunicaciones, el testimonio demoledor de Edward Snowden ha confirmado todos los extremos posibles. El mundo se ha visto inmerso en una dinámica de espionaje y penetración del secreto como nunca antes. Los asuntos de inteligencia ya no son únicamente dirigidos hacia la seguridad y la defensa nacional frente a las amenazas compartidas sino hacia lo que otros Estados, incluidos los aliados o amigos, realizan continuamente para incrementar sus conocimientos sobre lo que los demás hacen o pueden llegar a hacer.

En el transcurso de estos meses las tensiones entre países socios y teóricamente aliados se han disparado en 2013 con motivo del descubrimien-

to de los programas de interceptación masiva de comunicaciones, acceso a grandes volúmenes de datos de naturaleza personal (comunicaciones telefónicas y de mensajería electrónica volcados de manera sistemática, masiva y continuada en el tiempo gracias a programas de colaboración entre agencias y aplicación de sistemas como PRISM), económica y financiera que ha provocado un profundo replanteamiento no sólo de las relaciones internacionales de confianza entabladas entre países teóricamente socios, aliados y amigos a través de las acciones de sus servicios de inteligencia. La gran repercusión de todo ello hay que buscarla también en el profundo grado de desconfianza que ha provocado en una ciudadanía que ha conocido todas estas prácticas. De repente, ha tenido acceso a un caudal de informaciones clasificadas de tal alcance y magnitud que ha desvelado prácticas, resultados y acciones difícilmente comprensibles en materia de defensa de los derechos y libertades fundamentales.

A raíz del caso Snowden, las relaciones internacionales se han visto seriamente dañadas. Tal vez el caso más extremo haya sido el de Alemania donde la fiscalía por voz de Harald Range anunciaba en mayo de 2014 que investigará el alcance de lo que la inteligencia estadounidense ha realizado para penetrar en redes y sistemas del gobierno alemán, incluyendo los móviles de la canciller Merkel. Sin embargo, la interceptación de comunicaciones de ciudadanos alemanes no va a ser por ahora objeto de investigación a ese mismo nivel. Sin embargo, el carácter pragmático de las relaciones existentes entre Alemania y Estados Unidos ha recomendado no profundizar demasiado en todo ello con objeto de no dañar estas relaciones privilegiadas. La protesta, por tanto, continúa al más alto nivel pero cuidando mucho las formas y los niveles de respuesta.

Mientras, las reacciones europeas no se hicieron esperar y oscilaban desde la indignación al más alto nivel de Alemania hasta la sordina puesta

al asunto por muchos socios europeos que prefieren dejar que el problema pase. La revista alemana *Der Spiegel* examinó los actos de Snowden en un artículo titulado "Die Neuen Weltverbesserer", que se traduce por "Los nuevos mejoradores del mundo". La opinión pública norteamericana está polarizada y hasta un 65% de los jóvenes estadounidenses consideran a Snowden más un informante que un traidor, como consecuencia de su comprensión de la letal importancia de Internet y los peligros derivados de un uso masivo de los datos obtenidos por el Gobierno. En todo caso, voces tan relevantes como la del periodista Glenn Greenwald, quien publicó los documentos sobre el espionaje planetario llevado a cabo por la Agencia de Seguridad Nacional filtrados por Snowden resumió la trascendencia del debate global sobre lo ocurrido:

> "Por primera vez, hay un debate público mundial sobre el valor de la privacidad y la intimidad en Internet. Además, algunos países están poniendo en marcha reformas para limitar la vigilancia de los ciudadanos y para evitar que EE UU domine la Red. Hay empresas de telecomunicaciones norteamericanas que tienen mucho miedo de los efectos del espionaje en sus propias instalaciones, porque la gente no va a querer utilizar ni Facebook ni Google ni nada si piensa que los datos se pueden captar. El cambio más importante de todos es que la gente se ha dado cuenta de hasta qué punto se ha puesto en peligro su intimidad y su privacidad y ahora muchas personas están empezando a usar sistemas de encriptación para proteger sus comunicaciones y evitar así que los vigilen"[39].

¿Cómo afecta la actividad de inteligencia a las relaciones entre Estados? ¿Se prioriza la geopolítica a ultranza? ¿Cómo colabora un servicio de inteligencia con sus socios o servicios de países teóricamente aliados? Es ya un lugar común afirmar que, en asuntos de inteligencia, no hay amigos

39 Patricia Blanco, "Las nuevas limitaciones de EE.UU. a la NSA son simbólicas", *El País*, 29 mayo de 2014.

ni enemigos, sólo intereses parciales, mutuamente compartidos, revisables periódicamente y sometidos a una serie de reglas no escritas que rigen la particular interrelación entre organismos de inteligencia. Una de ellas es la mutua confianza que permite asentar la solidez de las colaboraciones a niveles estratégicos y, más concretamente, operativos conjuntos. Ni siquiera en tiempo de guerra, cuando las relaciones diplomáticas y los canales de comunicación entre Estados se han roto, dejan de existir canales alternativos de comunicación, generalmente conducidos por alguno de los servicios que componen la comunidad de inteligencia de esos países beligerantes. El problema de todo el asunto Snowden no es, como podríamos pensar, que unos Estados espíen, capten información, pinchen teléfonos o desarrollen operaciones encubiertas y acciones de influencia que bordean la legalidad para alcanzar posiciones competitivas en mesas de negociación. El problema tiene mayor carga de cinismo y realpolitik. De hecho, las reacciones de los Estados al saberse espiados por países teóricamente aliados han dejado muchas veces al desnudo el profundo sentido del problema: la vulneración de la discreción como uno de los principios sacrosantos. Que los Estados se espiaban entre sí, no admitía duda e incluso podía mantenerse bajo parámetros razonables de contención. Con lo que no se contaba era con que se destapase de manera tan global y masiva. La trascendencia de lo ocurrido ha obligado a cambiar agendas, proporcionar ruedas de prensa, dar explicaciones a una ciudadanía atónita ante lo que constituye un todos contra todos en materia de acceso a la información y a la penetración en los secretos: sean industriales, diplomáticos, políticos, militares o simplemente de alcoba.

Sin embargo, la tensión entre Estados como consecuencia de operaciones de espionaje también se produce bajo formas más tradicionales y continuadas de rivalidad en el tiempo. En este caso, con independencia de los documentos filtrados por Snowden, uno de los casos recientes más flagrantes de deterioro de relaciones internacionales ha vuelto a ponerse de

manifiesto tras la escalada en la tensión entre Estados Unidos y China a propósito del espionaje industrial. En mayo de 2014 Estados Unidos acusó por primera vez y de manera formal a China de llevar a cabo operaciones de espionaje económico. Acto seguido, Pekín exigió la retirada inmediata de la denuncia, llamó a consultas al embajador estadounidense y, como corolario, advirtió del más que evidente deterioro de relaciones entre ambas potencias. El caso se destapó cuando cinco militares pertenecientes a la potente unidad 61398 del Ejército de Liberación Popular chino, (Wang Dong, Sun Kailiang, Wen Xinyu, Huang Zhenyu y Gu Chunhui) fueron acusados de espionaje y de haberse infiltrado en las redes de información y comunicación de varias empresas y sindicatos estadounidenses para, a partir de ahí, comenzar a extraer informaciones confidenciales. No era la primera vez que miembros de esta unidad de ciberespionaje ocupaban las portadas internacionales: en febrero de 2013 se destapó el caso de la empresa de seguridad Mandiant, en la que presuntamente se habrían infiltrado. La relación de la fiscalía general de Estados Unidos sorprendió por la contudencia: "Esta Administración no tolerará las acciones de ningún país que ilegalmente intente sabotear a compañías americanas y socavar la integridad de la competición justa en el funcionamiento del libre mercado". Las reacciones chinas se concretaron inmediatamente: en primer lugar Pekín anunció la retirada del grupo de trabajo bilateral sobre ciberseguridad, mientras acusaba a Estados Unidos de propiciar sistemáticas actividades de escucha y vigilancia planetaria.

La *Commission on the Theft of American Intellectual Property* en su informe de 2013 había señalado con detalle el tipo y la cantidad de pérdidas económicas que Estados Unidos sufrió como consecuencia de la vulneración de la propiedad intelectual sobre avances científicos de doble uso, civil y militar. Además, recomendó la reforma de la *Economic Espionage Act* (EEA) de 1996, una de las herramientas con las que cuenta el gobierno federal de Estados Unidos para proteger el secreto económico y la innovación.

8. Respuestas y reformas: de la ética a los controles

Paralelamente al caso Snowden se conocen detalles de probable vulneración de códigos éticos y deontológicos por parte de otros profesionales siempre en aras de la seguridad nacional. Así, el informe de título tan directo y clarificador como *Ethics abandoned: Medical Professionalism and Detainee Abuse in the War on Terror (Institute on Medicine as a Profession/Open Society Foundation)*[40] denuncia la práctica de médicos y psicólogos que, trabajando para el Pentágono y la CIA, contribuyeron de manera evidente a la preparación y desarrollo de interrogatorios, torturas y tratos denigrantes de sospechosos terroristas. Se ha pedido al Comité de Inteligencia del Senado que investigue la veracidad y alcance de las conclusiones de este estudio.

Problemas morales en torno a la acción de los espías no se tratan aquí con el detalle deseado. Tampoco se abordan con intensidad las siempre fundamentales cuestiones relativas al llamado *oxímoron* por excelencia: la dialéctica inteligencia/ética, ya que no parece oportuno ni conduciría probablemente a ninguna conclusión sostenible reflexionar sobre la opinión de Montesquieu cuando señaló que "el espionaje será, puede ser, tolerable si es ejercido por personas honestas"[41].

No obstante, es preciso señalar que la dimensión deontológica del desempeño de sus actividades relativas al manejo de información, a la obtención de grandes volúmenes de datos y a su transformación en fuentes de conocimiento debe ser abordada con muchas más garantías y respeto. Es

40 Institute on Medicine as a Profession/Open Society Foundation (A task force report), *Ethics abandoned: Medical Professionalism and Detainee Abuse in the War on Terror*, November 2013. www.imapny.org/File%20Library/Documents/IMAP-EthicsTextFinal2.pdf.

41 Allison Shelton, "Framing the Oxymoron: A New Paradigm for Intelligence Ethics", *Intelligence and National Security*, Vol. 26, n.º 1, 2011, pp. 23-45.

preciso actuar simultáneamente en el terreno no sólo de los controles (políticos y judiciales) de la actividad de inteligencia para robustecer el sistema de garantías y derechos fundamentales. También es imprescindible el reforzamiento ético y deontológico de los profesionales de la información y documentación que pueden acabar trabajando en los servicios de inteligencia o en empresas y organismos colaboradoras de éstos, desde las mismas aulas de nuestras facultades. Robustecer la dimensión ética de la "Information Management" también es "cultura de inteligencia" y otorga como beneficio el refuerzo democrático de unos servicios de inteligencia que actúan bajo un marco legal más o menos garantista. Como se ha visto reiteradamente, la intrusión en la privacidad es una de las lacras más inaceptables que las sociedades sufren en aras a la seguridad nacional.

En todo caso, las acciones conducentes a la mejora y reforzamiento de los controles democráticos de la actividad de inteligencia siguen ocupando un lugar preeminente a la hora de diseñar ajustes y sometimientos legales. José Manuel Ugarte ha señalado que podrían articularse mejoras en los marcos normativos existentes[42]. Por ejemplo, creando nuevos controles al ejecutivo, incluyendo la figura de un inspector específico de la actividad de inteligencia, como en el caso canadiense. Para desarrollar un verdadero control de la actividad de inteligencia se debe contar con una voluntad política fuerte y también con medios materiales, es decir, que el órgano de control disponga de amplias facultades y que su actuación quede amparada por un amplio consenso social sobre el interés de la actividad de inteligencia, pero también de su sometimiento estricto a la ley. En América del Sur se perciben avances sustanciales bajo el modelo de leyes secretas que se van transformando en leyes públicas que propician estructuras de inteligencia sometidas a un ordenamiento jurídico transparente. Aún así, resulta imprescindible una segunda generación de reformas incluyendo órganos de control

42 José Manuel Ugarte, *op. cit.*

con suficientes facultades, pleno acceso a materias clasificadas, comisiones de control (económico, político, judicial previo), etc. Todo ello redundaría en una cultura del control orientada también hacia la eficiencia y la eficacia de los resultados finales de inteligencia.

9. Conclusiones

1. Que los poderes públicos han desarrollado y seguirán desarrollando operaciones de interceptación de comunicaciones es evidente y no hace falta remontarse a las campanas fónicas de Kircher. La cuestión a dilucidar es qué frenos legales dentro del régimen de garantías y protección de derechos fundamentales efectivos por un lado y éticos/deontológicos por otro se aplican como contrapeso de actuaciones masivas, indiscriminadas y totalmente fuera de control con respecto a millones de datos. La creciente e imparable automatización y los inevitables riesgos que va a conllevar la gestión y manejo de datos que afectan a la esfera personal e íntima del individuo obliga a subrayar el compromiso ético y deontológico de los servidores públicos en materia de inteligencia.

2. Los Estados seguirán colaborando, cooperando y realizando operaciones de espionaje y de interceptación de comunicaciones a todos, en todo lugar y cuanto más mejor. Si no se hace es porque no se dispone de la tecnología apropiada. Ser tecnológicamente dependiente tiene consecuencias negativas: un país que no dispone de las capacidades técnicas para desarrollar programas de obtención masiva, no podrá alcanzar ventajas estratégicas y además se sitúa en desigualdad. El asunto no es determinar si se espía, la cuestión es si se puede hacer con la tecnología disponible por un país. Las relaciones internacionales tras el caso Snowden, salvo casos puntuales de mayor incidencia de las protestas formales como Alemania o Brasil, seguirán desarrollándose bajo los mismos parámetros de geopolítica y geoestrategia práctica.

3. Todo lo anterior conduce hacia la siguiente aseveración: cuando se quiere controlar todo, espiar todo de todos, el sistema se colapsa. Obtener información es relativamente sencillo. Procesarla, analizar y convertir todo eso en conocimiento útil y preciso es lo que cuesta. El espionaje masivo proporciona una falsa ilusión de omnisciencia: pero vivir entre datos no nos convierte en más inteligentes.

4. En el contexto que contrapone la información al conocimiento, una nueva dicotomía ha aparecido: la de los riesgos del *big data* frente a la comprensión y al análisis (*big narrative*). Hace una década que se viene manejando una frase como un mantra: el reto es el análisis, no la obtención. El objetivo no es el análisis, sino la predicción: del *big data* al *big foreknowledge*. El destino es la prospectiva o los estudios de futuro. Si el objetivo era controlar, ahora es predecir conductas o acciones a corto/medio/largo plazo. Y ahí los datos son, como tantas veces se ha repetido, el nuevo oro.

5. Se habla mucho de análisis de inteligencia, de aplicación de técnicas avanzadas de comprensión de una realidad para articular una acción, una respuesta específica. Pero en muchas ocasiones, la inmediatez de los datos es lo que cuenta. No tanto el análisis de las causas ni los condicionantes del contexto en que se producen los hechos. Probabilidad y correlación entre datos parece ser el nuevo paradigma. Queda un limitado por no decir un escaso margen para capacidades como la intuición y, especialmente, la explicación analítica de los hechos en su contexto, circunstancias y comprensión integral.

6. La fase de obtención adquiere una extraordinaria importancia por su capacidad de suministro de datos en bruto y por las implicaciones éticas, legales y sociales que tiene la masiva captura de datos y metadatos sin discriminación. Los niveles de automatización en tareas de "gathering and information retrieval", van a ser tan masivos y alejados de la intervención humana que la

expresión "obtención ciega de información" acabará por priorizar la cantidad ingente de datos frente a la calidad del refinado y el preanálisis, provocando el consiguiente retardo en el sistema y la acumulación en el *storage* de aún más volúmenes de información en bruto que se harán totalmente inoperantes.

7. Todo lo que está abierto en Internet no significa que pueda ser ética y moralmente reaprovechado por terceros en grandes volúmenes de información. Las implicaciones éticas de la información abierta no han sido suficientemente analizadas y estudiadas.

8. Snowden ha marcado un punto de inflexión. No ha sido el único, porque ha habido un número importante de casos de filtraciones durante todo el siglo XX. Lo que lo hace sobresaliente es la magnitud. Querer espiar a todos todo el tiempo y en todo lugar sólo muestra una realidad bastante desilusionante: la incapacidad por discriminar lo que realmente importa. Cuando todo es espionaje, nada es inteligencia.

BIBLIOGRAFÍA

ANDREJEVIC, Marc, *Infoglut: How Too Much Information Is Changing the Way We Think and Know*, Abingdon, Taylor and Francis, 2013.

BARGER, Deborah, *Toward a Revolution in Intelligence Affairs*, Santa Mónica, Rand Corporation, 2005.

BENNY, Daniel J., *Industrial Espionage: Developing a Counterespionage Program,* Boca Ratón, CRC Press, 2013.

BLANCO, Patricia "Las nuevas limitaciones de EE. UU. a la NSA son simbólicas", *El País*, 29 mayo, 2014. http://internacional.elpais.com/internacional/2014/05/29/actualidad/1401384031_263771.html.

BOLTAINA, Xavier, "El personal del Centro Nacional de Inteligencia: su vínculo jurídico como «empleado público» y la afectación de sus derechos y deberes", *Inteligencia y Seguridad: Revista de Análisis y Prospectiva,* Vol. 11, 2012, pp. 183-212.

CARVALHO, Andréa Vasconcelos, *Auditoría de Inteligencia*, Gijón (Spain), Trea, 2012.

COLONIEU, Victor, *L'espionage au point de vue du droit international & du droit penal français*, Paris, A. Rousseau, 1888.

CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES, *The Economic Impact of Cybercrime and Cyberespionage*, Washington, CSIS, 2013. http://www.mcafee.com/sg/resources/reports/rp-economic-impact-cybercrime.pdf.

DIS (Dipartimento delle Informazioni per la Sicurezza, Presidenza del Consiglio dei Ministri, Italia), *Il linguaggio degli organismo informativi: glossario intelligence*. Roma, De Luca, 2012.

ENISA, *Threat Landscape 2013 Overview of current and emerging cyber-threats*, 2013, http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape-2013-overview-of-current-and-emerging-cyber-threats.

ESTEBAN NAVARRO, Miguel Ángel y Diego NAVARRO BONILLA, "Gestión del conocimiento y servicios de inteligencia: la dimensión estratégica de la *información", El Profesional de la Información*, Vol. 12, n.º 4, 2004, pp. 269-281.

ESTEBAN NAVARRO, Miguel Ángel (Coord.), *Glosario de Inteligencia*, Madrid, Ministerio de Defensa, 2007.

ESTEBAN NAVARRO, Miguel Ángel y Andrea CARVALHO, "La privatización de la inteligencia", en José Luis GONZÁLEZ CUSSAC (Ed.), *Inteligencia*. Valencia, Tirant lo Blanch, 2012, pp. 198-215.

GILL, Peter, *Policing Politics: Security Intelligence and the Liberal Democratic State,* Frank Cass, London, 1994.

GOLDMAN, Jan, *Words of Intelligence: intelligence Professional´s Lexicon for Domestic and Foreign Threats*, Scarecrow Press, 2011.

GOLDMAN, Jan, *Ethics of Spying: A Reader for the Intelligence Professional,* Vol. 2, Lanham/Toronto/Plymouth, Scarecrow Press, 2012.

GONZÁLEZ ALCANTUD, José Antonio, "El enigma del secreto: espionaje político", *Historia, Antropología y Fuentes Orales*, Vol. 2, n.º 34, 2005, pp. 5-28.

GONZÁLEZ FUSTER, Gloria, "Security and the future of personal data protection in the European Union", *Security and Human Rights*, Vol. 23, n.º 4, 2013, pp. 33-342.

GUEHENNO, Jean Marie, *Livre blanc défense et sécurité nationale*, Paris, La Documentation Française, 2013. http://www.gouvernement.fr/sites/default/files/fichiers_joints/livre-blanc-sur-la-defense-et-la-securite-nationale_2013.pdf.

HENCZEL, Susan, *The Information Audit: a practical guide*, Munich, Saur, 2001.

HERNÁNDEZ OLIVERA, Luis (Ed.), *El refinado arte de la destrucción: la selección de documentos*, Salamanca, Acal, 2003.

H. M. GOVERNMENT, *A Strong Britain in an Age of Uncertainty: The National Security Strategy*, 2010. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf.

INSTITUTE ON MEDICINE AS A PROFESSION/OPEN SOCIETY FOUNDATION (A task force report), *Ethics abandoned: Medical Professionalism and Detainee Abuse in the War on Terror,* November 2013. www.imapny.org/File%20Library/Documents/IMAP-EthicsTextFinal2.pdf.

JOYANES, Luis (Coord.), *Ciberseguridad, retos y amenazas a la seguridad nacional en el ciberespacio*, Madrid, Instituto Español de Estudios Estratégicos, Cuadernos de Estrategia 149, 2011.

JUÁREZ, Eduardo, *Venecia y el secreto del vidrio: Cuatrocientos años de monopolio*, Madrid, Catarata, 2013.

LAHNEMAN, William, *Keeping U.S Intelligence Effective: The Need for a Revolution in Intelligence Affairs,* Maryland, Scarecrow. 2011.

LERNER, K. Lee y Brenda Wilmoth LERNER, *Encylopedia of Espionage, Intelligence and Security,* Detroit, Thomson Gale, 3 Vols., 2004.

MAYER-SCHÖNBERGER Viktor y Kenneth CUKIER, *Big Data: la revolución de los datos masivo*, Madrid, Turner, 2013.

MOROZOV, Evgeny, "El reto de manejar grandes bancos de datos", *El País*, 24 de junio, 2013. http://elpais.com/elpais/2013/06/24/opinion/1372068111_079679.html.

NAVARRO BONILLA, Diego, *Espías: tres mil años de información y secreto*, Madrid, Plaza y Valdés, 2009.

NAVARRO BONILLA, Diego, "Secret Intelligences' in European Military, Political and Diplomatic Theory: An Essential Factor in the Defense of the Modern State (Sixteenth and Seventeenth Centuries)", *Intelligence and National Security*, Vol. 27, n.º 1, 2012, pp. 283-301.

NAVARRO BONILLA, Diego, "Information Management professionals working for intelligence organizations: ethics and deontology implications", *Security and Human Rights*, Vol. 24, n.º 3-4, 2013, pp. 264-279.

NAVARRO BONILLA, Diego, "Espionaje", en Luis DE LA CORTE y José María BLANCO (Eds.), *Amenazas a la seguridad nacional*, 2014 (en prensa).

OFICINA NACIONAL DE SEGURIDAD, *Los tratados internacionales sobre protección de la información clasificada*, Madrid, Ministerio de Defensa, 2009.

OLIER, Eduardo (Coord.), *La inteligencia económica en un mundo globalizado*, Madrid, Instituto Español de Estudios Estratégicos, Cuadernos de Estrategia 162, 2013.

PRESIDENCIA DEL GOBIERNO DE ESPAÑA, "Estrategia de Ciberseguridad Nacional", Madrid, Gobierno de España, 2013.

REUSER, Arno, "Trends in the Current Information Landscape and Their Significance for Researchers", *Online Searcher*, Jan./Feb. 2013, pp. 51-55.

SAGAR, Rahul. *Secrets and Leaks: The Dilemma of State Secrecy*, Princeton, Princeton University Press, 2013

SHELTON, Allison, "Framing the Oxymoron: A New Paradigm for Intelligence Ethics", *Intelligence and National Security*, Vol. 26, n.º 1, 2011, pp. 23-45.

SPENCE, Edward, "Government Secrecy, the Ethics of Wikileaks and the Fifth Estate", *International Review of Information Ethics*, Vol. 17, July, 2012, pp. 38-44.

THOMPSON, Terence J., "Toward an updated understanding of espionage motivation", *International Journal of Intelligence and CounterIntelligence*, Vol. 27, n.º 1, 2014, pp. 58-72.

UGARTE**,** José Manuel, *El control público de la actividad de inteligencia en América Latina*, Buenos Aires, CICCUS, 2012.

UNIDIR, *The Cyber Index: International Security Trends and Realities*, New York/ Geneva, UN, 2013. http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf.

VALK, Giliam De, *Dutch Intelligence: Towards a Qualitative Framework for Analysis,* Eleven International Publishing, The Hague, 2005.

WEGENER, Henning, "Los riesgos económicos de la ciberguerra", en Eduardo Olier (Coord.), *La inteligencia económica en un mundo globalizado*, Madrid, Instituto Español de Estudios Estratégicos, Cuadernos de Estrategia 162, 2013, pp. 177-221.

COLECCIÓN DE ESTUDIOS INTERNACIONALES

OTROS NÚMEROS DE LA COLECCIÓN

n.º 1, 2006 Fulvio Attiná

La doctrina preventiva: ¿Una innovación en el sistema político mundial? La reacción europea

n.º 2, 2007 Michael Keating

European Integration and the nationalities question

n.º 3, 2008 Daniel Innerarity

Un mundo desincronizado

n.º 4, 2008 Gonzalo Molina Igartua

Políticas e iniciativas para una energía inteligente en la Unión Europea

n.º 5, 2009 Carlos Taibo

Decrecimiento, crisis, capitalismo

COLECCIÓN DE ESTUDIOS INTERNACIONALES

OTROS NÚMEROS DE LA COLECCIÓN

n.º 6, 2009 Susanne Gratius

Reflexiones sobre izquierda y populismo en América Latina

n.º 7, 2010 Vicente Garrido

La no proliferación y el desarme en perspectiva histórica

n.º 8, 2010 Manuel de la Cámara

Rusia en el orden internacional

n.º 9, 2011 José Abu-Tarbush

Cambio político en el mundo árabe

n.º 10, 2011 Juan José Ibarretxe

The Basque Case: A comprehensive model for sustainable human development

COLECCIÓN DE ESTUDIOS INTERNACIONALES

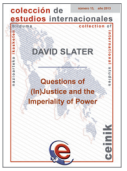
OTROS NÚMEROS DE LA COLECCIÓN

n.º 11, 2012 Javier Bilbao

Crisis económica y gobernanza en la UE: balance crítico y estrategias de salida

n.º 12, 2012 Dario Battistella

The Post-Cold War Order as a One-Dimensional World



n.º 13, 2013 David Slater

Questions of (In)Justice and the Imperiality of Power

COLECCIÓN DE
ESTUDIOS INTERNACIONALES

"Cuando todo es espionaje, nada es inteligencia". En este trabajo se aborda el espionaje en el contexto de las relaciones internacionales desde una perspectiva amplia. Es su objetivo tratar de comprender las múltiples dimensiones de las acciones llevadas a cabo por estados para penetrar en la información secreta de adversarios, rivales e incluso aliados. La controversia mundial motivada por las revelaciones de Assange primero y Snowden a lo largo de 2013 ha vuelto a poner sobre la mesa de la reflexión múltiples retos de la acción de los servicios de inteligencia. El reforzamiento de sus controles democráticos ocupa un lugar preeminente a la hora de diseñar ajustes y sometimientos legales sin olvidar la dimensión deontológica que afecta a los profesionales que forman parte de un organismo de inteligencia. Las agendas de seguridad y defensa internacional han tenido que ser revisadas como consecuencia de una dinámica de obtención masiva de datos con graves consecuencias en la tradicional dialéctica "seguridad vs. transparencia".

Diego Navarro Bonilla es Doctor en Documentación y profesor titular de Archivística en la Universidad Carlos III de Madrid. Fue fundador y director del Instituto "Juan Velázquez de Velasco de investigación en inteligencia para la seguridad y la defensa". Así mismo, ejerció como director del Máster en Analista de Inteligencia y de la revista Inteligencia y Seguridad: Revista de análisis y prospectiva. Recibió el Premio Nacional de Defensa (2003) y es autor de numerosos artículos y libros sobre espionaje y los servicios de inteligencia.

Universidad del País Vasco Euskal Herriko Unibertsitatea
Nazioarteko Ikasketen Katedra
Cátedra de Estudios Internacionales
BFA DFB
Bizkaiko Foru Aldundia
Diputación Foral de Bizkaia