Análisis GESI, 9/2015

Acerca del "secreto" en Inteligencia

Ernesto Vicente Iglesias

4 de abril de 2015

Lo primero que me viene a la mente cuando pienso en lo que conocemos como secretos de Estado, es que tienen que contener lo más parecido a la verdad, cuando se trata de temas políticos, estratégicos y de seguridad. Que son informaciones alejadas de las versiones oficiales y cercanas a los hechos concretos.

Cuando escuchamos una noticia en la radio y después la contrastamos con un periódico, tenemos la sensación de que sabemos lo que ha ocurrido. Pero no es exactamente así. A todos nos ha pasado que cuando vivimos una situación en primera persona, no se corresponde totalmente con lo que después se publica. La inteligencia que manejan los gobiernos, es el análisis que más se parece a la verdad de los acontecimientos. Que los secretos contengan esa gran parte de verdad, les da relevancia y los hacen apasionantes.

Lo que me ha motivado a escribir este trabajo es reflexionar sobre todo esto. Sobre el por qué es importante, que determinadas verdades constituyan auténticos secretos, de los que se protegen y no se cuentan. Reflexionar sobre por qué es importante que se violenten, durante unas horas, derechos de ciudadanos concretos para que la verdad de los hechos, nos acerque a una sociedad un poco más segura cada día.

Como ocurre con tantas palabras, el origen de la palabra secreto la encontramos en el latín. Secreto procede de la palabra *secretus* que viene del verbo secernere**,** que significa poner aparte, aislar. Según la RAE, secreto significa cosa que cuidadosamente se tiene reservada y oculta. No en vano, los nombres de algunos puestos profesionales, tienen que ver con los secretos que tienen que guardar. A los actuales ministros, antiguamente los llamaban secretarios. Y no por casualidad seguimos utilizando palabras o conjuntos de ellas como secretaria de dirección, secretario general o en los centros docentes, secretaría. Seguimos utilizando fórmulas como secreto profesional, que está incluso aceptado jurídicamente, secreto de confesión y como no **secretos de Estado**. Esta herencia nos recuerda, que en determinados puestos o niveles, las personas tienen que ser de confianza y discretas. Del mismo modo que en los lugares en los cuales se guarda información sensible, deben ser especialmente protegidos.

Tanto las actividades de los servicios de inteligencia como los resultados obtenidos de dichas acciones, tienen que permanecer en secreto. Esto es debido

a que las operaciones tienen que ser clandestinas y a que los resultados obtenidos durante el ciclo de la inteligencia tienen que ser solamente conocidos por personas muy concretas. No pueden ser públicas las actividades de inteligencia, porque nadie debe saber qué datos busca el Estado. Y no pueden ser públicas sus conclusiones de la inteligencia, porque nadie debe saber con qué información adicional cuenta el Estado. Cuando de lo que se trata es de la seguridad con mayúsculas, tan contraproducente es que se revele cuales son los datos o la información que está buscando un Estado, como los métodos que utiliza.

Cuando se conoce qué es lo que queremos saber o cómo hacemos para obtener información, el contrario descubre qué es lo que nos interesa y qué tiene que hacer para protegerse. Del mismo modo siguiendo en ésta línea, si se descubre cuál es la información que manejan los servicios de inteligencia de un estado es más fácil competir con él, ya sea pacíficamente o de manera violenta. Por eso entre otras cosas, los Estados tienen que tener secretos. Para que los contrarios solo vean las cartas que están sobre la mesa y desconozcan la mano de cartas que no les enseñamos. Si mostráramos todas nuestras cartas en un juego en el que el otro no lo hace, jugamos con desventaja y tenemos más posibilidades de perder la partida.

Todos los secretos no son iguales. La información que manejan los servicios de inteligencia tiene diferentes **grados de confidencialidad**. Que esto sea así, permite restringir el acceso a dicha información por quién no tiene que acceder a ella. La difusión de la información es más amplia cuando es menos relevante y viceversa. De todas maneras hay que tener en cuenta que actualmente para elaborar inteligencia se utilizan muchas fuentes abiertas. La variedad y la complejidad de los temas a estudiar en un mundo globalizado, así como la cantidad de información disponible hacen necesario una gran tarea de criba de datos de todo tipo. Otra cosa es la escasa difusión que se le dé al resultado de las tareas de inteligencia.

El problema surge, cuando en las actuales democracias liberales en pleno siglo XXI, con todo lo que eso conlleva, tenemos que conciliar libertad y seguridad. La sociedad que somos hoy, se ha construido en parte, sobre estas dos premisas. Mas es cierto que solemos sacrificar el derecho a la libertad, en pro del derecho que tenemos a la seguridad. Esto dicho de una manera grandilocuente. Realmente lo que sacrificamos son algunas libertades concretas en un momento determinado, por un bien mayor que es la integridad física de los ciudadanos. En ocasiones también se restringen libertades concretas, en pro de los derechos y libertades de otros ciudadanos, como el derecho a la propiedad privada o a la libertad de expresión. Pero el caso es que esto en Europa no está tan aceptado como en otras sociedades. Que se restrinjan algunas libertades en favor de la seguridad personal o colectiva, en ocasiones se vincula a otros intereses. El principal argumento que se esgrime para justificar que el Estado regule o restrinja temporalmente ciertas libertades, como el derecho a la intimidad o el derecho de manifestación, es que sin seguridad no hay libertad, ni se pueden ejercer derechos. Si en una sociedad no prevalece la seguridad, no es una

sociedad plenamente libre y en una sociedad insegura, los derechos ciudadanos serán más difíciles de practicar. Pero llegados a este punto y partiendo de que queremos una sociedad segura y de que estamos dispuestos a ceder un poquito de libertad ¿es indispensable que el Estado tenga secretos?

La respuesta como se empezaba a vislumbrar al principio de la introducción es que sí. Es un sí pragmático. Sobrevenido al comprobar que organizaciones y Estados, ocultan información y tratan de conseguir la información ajena, siguiendo sus intereses. Nos encontramos con varios problemas cuando nos planteamos todo esto, desde un punto de vista democrático, que aspira a la menor arbitrariedad posible y a que el Estado de derecho sea el que regule la vida civil y pública. El primero es **ético** ¿es ético por ejemplo, que una democracia espié a sus ciudadanos o a ciudadanos extranjeros y tenga secretos de Estado? El segundo seria **legal**. Como sabemos el secreto en ocasiones se hace necesario pero ¿cómo hacemos para que las actividades de los servicios secretos sean legales? Otro problema a añadir, es la **corrupción** o la arbitrariedad ¿cómo nos aseguramos de que el Estado no utilice la inteligencia y sus herramientas de espionaje, contra los ciudadanos que no suponen una amenaza? ¿O cómo podemos tener la certeza, de que sólo se pretende la seguridad del Estado y no otra cosa?

Los últimos, son problemas de inspección que ya cuentan con una solución, otra cosa sería su dimensión ética. Pero no está de más una revisión serena y crítica, de los mecanismos de fiscalización y control para que todo evolucione a la par que lo hace la tecnología y la sociedad. También deben variar si cambian nuestras necesidades de seguridad (no es lo mismo estar en guerra, que estar en un periodo de paz por ejemplo) porque los Estados tienen enemigos dentro y fuera de sus fronteras, propios y extraños, organizaciones no gubernamentales y estatales. Todos tienen secretos y buscan los nuestros y ninguno de los anteriores respeta las leyes ni sigue criterios deontológicos para sus fines.

Cuando los secretos dejan de serlo ¿Cómo se llegó a las revelaciones de WikiLeaks y Snowden?

WikiLeaks

El nombre de WikiLeaks surge de la unión de dos conceptos, **"Wiki"** que es el nombre que se le da en Internet, a la posibilidad de que sean también los usuarios de una página web, los que editar los contenidos de la misma y no sólo lo haga el administrador web. El segundo seria **"Leaks"** que significa, fuga, goteo, filtración y que hace referencia a las fugas de información sensible que se busca publicar en la red global. El nombre de WikiLeaks por tanto, persigue que se identifique la página, con un lugar en la red en el cual los internautas pueden colgar información que han sustraído de alguna organización que la pretendía ocultar.

Según sus **creadores**, WikiLeaks es «Un servicio público internacional cuya misión es permitir a periodistas e informantes poner a disposición del público

materiales que han sido censurados». No es menos cierto, que por otra parte, también es una página web que publica material confidencial sin plantearse las consecuencias de sus actos y sin demasiadas reflexiones deontológicas. Se financian gracias a donaciones privadas que reciben en cuentas de bancos europeos. No es descartable que tengan otras fuentes de ingresos. Y se dedican principalmente a publicar filtraciones de índole militar, política, religiosa y social.

En principio lo hacen preservando el anonimato de sus fuentes, aunque no siempre lo pueden asegurar, a pesar de sus medidas de seguridad. WikiLeaks es una organización internacional, creada entre otros, por el australiano **Julian Assange**. Es un activista a favor de la transparencia de datos y de la información casi total. Busca que los gobiernos y las organizaciones no tengan secretos para con la ciudadanía. En el desempeño de sus actividades, ha querido salir personalmente en los medios de comunicación de masas, como estrategia de una protección particular frente a las posibles y esperadas represalias, de cualquier Estado u organización de la que estuviera aireando trapos sucios.

Actualmente se encuentra refugiado en la embajada ecuatoriana de Londres. En principio, el propósito de esta organización es dar a conocer, esos datos, informes y material audiovisual que las dictaduras, credos, empresas privadas y también las democracias liberales, no quieren que vean la luz. Los temas que se tratan son dispares, pero tienen en común la confidencialidad y su posible relevancia mundial: la muerte de José Couso, los vuelos de la CIA, Guantánamo etc. Pero las revelaciones que han tenido más eco han sido las actividades de Estados Unidos en política exterior y sobre todo las operaciones militares en Afganistán e Iraq. Las noticias sobre posibles excesos por parte de los occidentales en estos dos conflictos, a menudo tienen un gran interés para la opinión pública mundial, que las vive y juzga con parámetros diferentes a si proceden de una dictadura u organización violenta.

El caballo de Troya de WikiLeaks dentro del ejército estadounidense, fue **el soldado Manning**. Presentado como un analista de inteligencia que resultó ser un joven soldado raso sin gran formación, ha sido condenado por grabar material confidencial y filtrarlo a los que luego lo divulgaron en la red. El soldado Manning filtró a WikiLeaks 470.000 registros de las guerras de Irak y Afganistán, 250.000 cables del Departamento de Estado y otros documentos clasificados, lo que ha supuesto un importantísimo revés para la diplomacia estadounidense, dando lugar a un debate internacional sobre el papel de Estados Unidos en el mundo y en concreto sobre su lucha contra el terrorismo islámico. Entre sus revelaciones más comprometidas, estuvieron los 90.000 folios sobre la guerra de Afganistán, que evidenciaron la inexactitud la administración Obama sobre el verdadero número de civiles muertos en el conflicto apuntando además a los vínculos entre los Servicios Secretos de Pakistán y la insurgencia talibán.

Debido a su conversación con un supuesto hacker amigo suyo, Manning no consiguió eludir la justicia norteamericana. Uno de los supuestos puntos fuertes de WikiLeaks, el anonimato en las filtraciones, se puso en tela de juicio. No se consigue siempre proteger a los**" Whistleblowers"** a los que tiran de la manta, a los filtradores. Hasta se podría entender que este tipo de iniciativas son **"honeypots"** indirectos. Es decir, que lo que a priori es una página que funciona como una herramienta para los filtradores, puede haberse ideado como un instrumento de control, de organizaciones que tienen la necesidad de tener constancia de quien filtra y que está revelando. Además otra utilidad de este tipo de páginas web es que pueden ser utilizadas por grupos que buscan influir en la opinión pública en favor de sus intereses. Un **lobby** por ejemplo, puede filtrar datos que perjudiquen a la competencia. O un país puede filtrar datos falsos sobre su potencial militar para confundir a un contrario etc. Después de las enormes publicaciones que ha llevado a cabo, no hay motivos para pensar que WikiLeaks es una trampa para deslealtades, pero no se puede descartar la existencia de "honeypots" ideados por Estados o empresas punteras que quieran estar al cabo de la calle de quién y qué están colocándolos en una situación de vulnerabilidad.

Aunque sea difícil de comprobar el cómo afectaron las revelaciones a la seguridad de Estados Unidos, cuál fue el resultado real, de las filtraciones efectuadas por el soldado Manning. Para muchas voces autorizadas, afectó tanto a la calidad de la seguridad estadounidense, como al número de bajas en zona de operaciones.

La NSA y Snowden

El problema de no tener inteligencia sobre el contrario, que información tiene, que puede pensar o que puede llegar a hacer, es precisamente ese, que no sabes lo que va a hacer el otro. Cuando pensamos en el contrario como un adversario político en el seno de una democracia liberal, el problema no es grave. En principio, las disputas se resuelven dentro de las reglas del juego dentro la legalidad vigente. En ocasiones la teoría no se ajusta a la realidad, pero en el interior de los Estados se presupone el juego limpio. No ocurre así, en el plano más conflictivo de las relaciones internacionales, pues las tensiones no se resuelven en buena lid. A nivel internacional, el secreto de las actividades clandestinas del Estado, así como sus resultados, revisten más importancia. Ya que cuando somos conscientes de que el adversario no se va a tener a reglas jurídicas o morales, hay que actuar responsablemente y conseguir información de forma discreta y mantenerla en secreto. Sobre todo cuando está en juego la seguridad física de los ciudadanos.

Todas las potencias, independientemente de su tradición democrática, desde el Reino Unido a China, explotan al máximo sus capacidades técnicas para obtener información de sus análogos. Hay una máxima no escrita, que reza que **cuando tecnológicamente, algo es posible de hacer, es muy posible que alguna potencia lo esté llevando a cabo**. Todos los países que tienen la

capacidad técnica y un especial interés en su política exterior graban más comunicaciones electrónicas de las que luego son capaces de analizar.

Los Estados Unidos no tienen una, sino varias agencias que se dedican a labores de información e inteligencia. El FBI se dedica a asuntos internos, la CIA es la que tiene competencias en el extranjero y la NSA vigila las comunicaciones de todos a nivel mundial. Esto es así por varias razones. Los Estados Unidos tienen diferentes enemigos, intereses de todo tipo a nivel mundial y tras el inicio de la Segunda Guerra Mundial una gran incertidumbre sobre lo que puede llegar a ocurrir. El punto de inflexión fue **Pearl Harbor**. Los norteamericanos sabían que los japoneses iban a atacar, pero no sabían dónde ni cuándo. Al ser plenamente conscientes, de cómo habían finalizado ellos con la Segunda Guerra Mundial y de que no eran los únicos que poseían material atómico, la incertidumbre sobre la magnitud de lo que podía llegar a ocurrir, si no se tenía información fiable pasó a un primer plano. Durante la conocida como Guerra Fría, una de las prioridades de los estadounidenses era tener la mejor inteligencia posible para que no se produjese un **Pearl Harbor nuclear**. Un ataque nuclear, inesperado o no, si bien es una cosa poco probable, no deja de ser algo posible, sobre todo antes de 1989 y la caída del muro de Berlín.

Tras la segunda guerra mundial, los Estados Unidos, siguieron dando forma a una serie de organizaciones que se dedicaban a capturar y descifrar las comunicaciones. En 1951 dentro de este contexto de posguerra nació la **NSA**. Los recursos eran limitados si los comparamos con los actuales, pero hay que tener en cuenta que a falta de otros peligros, la NSA dirigía su labor a controlar las comunicaciones entre Estados y estos no emitían tantos mensajes o llamadas como el grueso de la población mundial emite actualmente.

Desde finales de la década de 1970, la NSA colabora estrechamente con su agencia homóloga británica el **GCHQ**, Cuartel General de Comunicaciones Globales (Global Communications Headquarters). El ambiente era propicio, debido a la buena conexión existente entre el Presidente Ronald Reagan y la Primera Ministra Margaret Thatcher. Amén de la consolidación de la revolución de la información. Washington y Londres comenzaron a poner en común sus recursos tecnológicos, infraestructuras de escucha, medios de procesamiento y productos de inteligencia. La colaboración entre los dos países continúa a fecha de hoy y llegan a tener acceso al noventa por ciento de las telecomunicaciones mundiales. Se concluye, que los Estados Unidos y el Reino Uindo en estas lides, tienen entre ellos un mayor grado de confianza y colaboración, que con sus principales socios del club anglosajón de **inteligencia de los cinco ojos**, compuesto por: Australia, Canadá, Nueva Zelanda, Reino Unido y Estados Unidos.

El miedo a un ataque nuclear fue a menos, según fue destensándose la guerra fría. Con la caída del muro y la desaparición de la URRSS, parecía que se entraba en una etapa en la que no se tenía por qué temer un gran ataque a una base militar occidental y mucho menos un ataque en suelo norteamericano. Los atentados del 11 de septiembre de 2001 desmontaron la creencia de que la

inteligencia tenía que despreocuparse de grandes ataques inesperados. Más bien al contrario, se confirmó durante la década de los noventa, tanto por parte de las democracias occidentales como por parte de sus aliados, que habían cambiado al enemigo soviético, que respondía a un perfil militar clásico, por una red de organizaciones terroristas que tenían la capacidad de matar a cientos, o a miles de civiles, en ataques sorpresivos dentro de nuestras fronteras.

Siguiendo esta argumentación, tras los atentados de Nueva York, Madrid y Londres al principio del siglo XXI, quedó patente que el principal peligro ya era otro y que no se podía prescindir de la inteligencia para combatirlo más bien al contrario. Los servicios de inteligencia de Estados Unidos fallaron, de igual forma que lo hicieron otros a la hora de advertir los atentados. La amenaza era real y de posibilidades destructivas de gran magnitud, en un mundo y un contexto social muy diferente al de antes de la llegada de internet. En este ambiente de justificada preocupación, la CIA admitió que uno de los problemas que tenía para combatir a **Al Qaeda**, era que no tenía fuentes humanas en el entorno la organización. La CIA no tenía fuentes humanas y además era muy difícil obtenerlas, pues Al Qaeda contaba con unos lazos familiares en su estructura que lo dificultaban. Además a un grupo de ocho personas metidas en una cueva, no se le puede detectar como si fueran una división acorazada soviética, mediante fotografías aéreas. Las fotos de los satélites que localizan una batería de misiles no pueden controlar los cibercafés. Así que la NSA y su control de las comunicaciones, su inteligencia de señales basada en quien contacta con quién y qué le dice, pasó a ser muy relevante.

La NSA conjuntamente con las **empresas de telecomunicaciones privadas** de su entorno, fueron las encargadas de realizar el seguimiento de las comunicaciones de los yihadistas y otros. La finalidad era detener un nuevo ataque por parte de los islamistas radicales, interviniendo sus comunicaciones ya fueran por internet o telefónicas. Para abortar un nuevo Pearl Harbor, con sus elementos de sorpresa y magnitud, la misión era leer los planes y las ordenes de los terroristas. Uno de los problemas a los que se enfrentaba la NSA, era que tenía que espiar a ciudadanos de todo pelaje, europeos y estadounidenses incluidos, ya que algunos terroristas entraban dentro de la categoría de ciudadanos de pleno derecho. Los delincuentes en general y los terroristas en particular, son muy conscientes de las ventajas de residir en occidente, tanto a la hora de que no se espíe su intimidad sin límite, como a la hora de ser juzgados.

En 2002 el Presidente Bush, tras los ataques terroristas del 11 de Septiembre de 2001, autorizó a la NSA a que pudiera realizar escuchas sin tener que esperar a que lo autorizara un juez. Autorizó a la NSA a monitorizar, almacenar y analizar sin orden judicial previa, las llamadas telefónicas y los correos electrónicos de todos aquellos ciudadanos, estadounidenses o no, que pudieran tener alguna relación con la organización terrorista Al-Qaeda. Al no existir control judicial alguno, se permitía una arbitrariedad en el día a día, que solamente podía ser controlada por el propio personal de la NSA. Sus trabajadores no tenían que

cumplir la **Foreign Intelligence Surveillance Act (FISA)**, la cual prohíbe expresamente, espiar a ciudadanos estadounidenses dentro del país.

Aquí es donde entra en juego **Edward Snowden**, el conocido acusado de espionaje por parte de los Estados Unidos. Snowden fue acusado en junio de 2013 de tres delitos: robo de bienes del Estado, revelación de información concerniente a la defensa nacional y filtración de comunicaciones relativas a la inteligencia. Edward Snowden es un joven técnico informático que trabajó para la CIA, para la Agencia de Seguridad Nacional y para otras empresas que ofrecían sus servicios a la NSA. A deferencia de Assange al que le movían criterios económicos en sus revelaciones, a Snowden parece que le motivaron criterios morales. Siguiendo su versión, su determinación en la denuncia de ilegalidades, le llevó a filtrar información confidencial a periodistas de los diarios The Guardian y The Washington Post (periodistas como Glenn Greenwald, que suele publicar en The Guardian, la documentalista Laura Poitras, que publica en la revista alemana Der Spiegel y Barton Gellman que lo hace en The Washington Post) El primero reveló que Verizon, una empresa de telecomunicaciones, proporcionaba información al estado norteamericano sobre llamadas telefónicas de todo tipo. The Washington Post publicó que la NSA, mediante un programa informático denominado **PRISM** y la colaboración de empresas del sector de internet, tenía acceso a multitud de datos personales de ciudadanos estadounidenses. Se referían a información contenida en las redes sociales y en los buscadores web. Se reveló como la NSA y el FBI obtenían datos directamente de los servidores de Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube y Apple. Cuando se trataba de ciudadanos estadunidenses, la NSA pedía a Google por ejemplo que le pasara los datos. Mientras que si era en el extranjero los cogían directamente.

La prensa explicó a la opinión pública mundial, en qué consistió la **Patriot Act** y como eludir la FISA resultó ser una barra libre. Como el acceso a estas grandes cantidades de datos, se llevó a cabo en base a una orden judicial secreta, mediante la cual la NSA tenía acceso a registros telefónicos y en internet a millones de datos de usuarios. La Casa Blanca por su parte, defendió la necesidad de registrar las llamadas telefónicas de los ciudadanos para combatir al terrorismo. El problema, como se explicaba anteriormente, es que algunos sospechosos de ser o de colaborar con terroristas, son ciudadanos norteamericanos o de países aliados.

Tras el escándalo del caso Snowden, el actual presidente **Obama**, puso límites a los procesos de obtención de información de los servicios de inteligencia. Pero no puede recortar mucho las capacidades de recolección de datos, pues aproximadamente el 80% de la inteligencia que emplea la administración estadounidense para apoyar sus decisiones políticas proviene del ciberespacio. Se persigue por lo tanto, hacer compatibles los derechos civiles y la privacidad de los ciudadanos estadounidenses y algunos del resto del mundo, sin que cesen las actividades de la NSA. Que estas reformas, no supongan un menoscabo de las capacidades SIGINT del sistema de inteligencia de los Estados Unidos. Para Obama, los Estados Unidos no pueden dejar de utilizar sus

capacidades cibernéticas, así que en ningún caso, se está planteando el interrumpir sus actividades de inteligencia electrónica.

Hoy sabemos que se ha dado una **triple colaboración** entre las agencias de seguridad estadounidenses, las universidades y las empresas. Se ha primado y subvencionado, la investigación y el desarrollo de todo lo que contribuyera a una inteligencia competitiva que favoreciera la seguridad. Tras el 11 de septiembre, no se ha escatimado ni en medios ni en opciones. Se almacenaron y cribaron datos procedentes del ciberespacio y de las líneas telefónicas, también se suprimió el control judicial previo, incluso hay autores que apuntan a que Estados Unidos, puede haber creado y sus compañías haber distribuido, softwares incluso hardwares pensando en la futura obtención de información de ciudadanos, empresas, Estados u otras organizaciones.

Actualmente ¿Qué ha supuesto que se publique tanta información comprometida?

Las organizaciones públicas y privadas, deben reducir la fuga de información a su mínima expresión. Pero la filtración de información, es un fenómeno que va a seguir existiendo, de hecho ha existido siempre. Snowden no es el primer trabajador que se huye con documentación sensible o bien la filtra. En España como sabemos, los llamados **papeles del CESID** ocuparon muchos titulares de prensa. Un antecedente de las filtraciones actuales, se dio por ejemplo, cuando The New York Times publicó en 1971 los conocidos como **papeles del Pentágono**. Se publicaron una serie de documentos de índole política y militar, clasificados como alto secreto. Versaban sobre el papel de la administración norteamericana desde 1945 a 1967 en Vietnam. Aquella situación dejó al desnudo a Washington, frente al grueso de la opinión pública de un modo parecido, a como WikiLeaks y el caso Snowden dejan en evidencia actualmente a Washington.

Crytome y otras páginas de denuncia en internet son anteriores a WikiLeaks. Incluso puede que el monopolio mediático de WikiLeaks desfavorezca a otras páginas que estén filtrando información de una manera más profesional y responsable. Actualmente la creación de Julian Assange, es un referente entre las páginas que revelan información sensible. Pero sus fundadores no han sido pioneros en el género de la filtración, ya publicaban información confidencial la Federation of American Scientist, Project Censored, Global Research o Cryptome la más conocida. No han sido precursores en generar repercusión con lo filtrado, más bien lo han sido en el volumen y en las cualidades de los datos han filtrado, como cuando revelaron los mensajes tras los atentados del 11S. En total fueron colgados en la red 500.000 mensajes recibidos en la sede del Pentágono el día de los atentados, la mayoría emitidos por el FBI y la policía de Nueva York.

La publicación del **video "colateral murder"** fue para la web de develamientos el salto definitivo a la fama. En él se ve a un helicóptero de combate estadounidense disparando sobre un grupo de personas que pudieran

ser civiles. El video es un ejemplo de lo intentaba explicar anteriormente. Se han filtrado datos que generan mucha alarma social y que pueden influir en la opinión pública en general. Pero el ciudadano medio no es ajeno a la crueldad de los conflictos y a que los Estados compiten entre ellos. La revelación de información clasificada o la constatación del incumplimiento de las leyes internacionales, generan opiniones contrarias e incluso mártires contra occidente, por lo tanto es un problema. Pero tampoco están proporcionándoles a los gobiernos o a los ciudadanos de formación media, unos datos o una realidad que desconocen por completo. Por supuesto en algunos casos, este tipo de materiales pueden ser pruebas en un juicio que encause crímenes de guerra o situaciones similares. Pero lo realmente relevante de la filtración de metadatos, es cómo afecta al gran público a nivel mundial. Pues deslegitima a los gobiernos democráticos ante propios y extraños. Crea oposición política interior, da escusas y alas a las organizaciones terroristas, amén de que los Estados contrarios lo utilizaran en sus argumentaciones.

Edward Snowden es conocido por el gran público por haber puesto en evidencia a la administración de Obama. La importancia del caso Snowden es también, la repercusión que ha tenido todo lo que ha revelado de la NSA en los medios de comunicación de masas. Como apuntaba anteriormente, hay muchos ciudadanos formados y conscientes, de que las relaciones entre Estados son cuanto menos competitivas. Por supuesto a ciertos niveles, se sabía se toleraba y se aprovechaba. Pero otra cosa distinta es que se tenga que admitir que se ha estado escuchando los teléfonos de las presidentes de Alemania y Brasil.

A pesar de que se han producido filtraciones masivas, los resultados de las mismas no han sido muy grandes. WikiLeaks concretamente ha conseguido dos cosas, reputación en internet frente a sus competidores y llegar al gran público. A esos millones de ciudadanos que normalmente no se interesan por estos asuntos y que no están tan al cabo de la calle de lo que acontece en internet, algo muy difícil pues la red que está llena de competidores. Pero estas revelaciones no han modificado las realidades de Irak o Afganistán, no han ido más allá del escándalo. Es más incluso ha podido beneficiar en parte a la administración Obama al minimizar el impacto de las fuerzas mercenarias estadounidense.

También insinúan el apoyo de Irán a la insurgencias contrarias. Por otro lado tenemos las informaciones de Snowden. Con ellas sí que se ha conseguido una restructuración de las formas de la NSA y la palabra del Presidente diciendo que si ha ocurrido tal o cual cosa no volverá a ocurrir. Pero más allá del escándalo que supone que se esté espiando a todo el mundo sin distinción y que se publiquen los cables diplomáticos con los informes que remitían las embajadas, las consecuencias no han sido de la misma magnitud que la cantidad de lo filtrado. Digamos que aunque el grueso de la población se indigne, tampoco Edward Snowden estaba descubriendo el Mediterráneo. El resto de los gobiernos del globo, son conscientes de en qué punto se encuentra la tecnología actualmente y de que Estados Unidos controla la telefonía e internet. Y algunos, o bien estaban haciendo algo parecido o bien estaban colaborando. Si bien es cierto que organizaciones terroristas, insurgencias y gobiernos rivales de

occidente, hoy cuentan con una nutrida y variada información. Que en el caso de las organizaciones más pequeñas es poco probable que tuvieran.

Actualmente las tecnologías de la información son un arma de doble filo. Por un lado los Estados pueden controlar tanto a los delincuentes, como a los Estados rivales. Pueden utilizar determinadas herramientas en favor del espionaje industrial o para otras actividades que favorezcan sus intereses nacionales. Pero es un arma de doble filo porque los ciudadanos, ya sean leales o de dudosa lealtad a las instituciones y a la ley, utilizan los avances tecnológicos para sus fines personales. Por un lado es posible detener a ciudadanos españoles que deciden ir a combatir a Siria gracias a la monitorización de las comunicaciones y por otro lado, estas personas se radicalizan y van a la guerra entre otras cosas, gracias a los avances en las comunicaciones.

Marco legal en España ¿Qué leyes debe de cumplir un servicio de inteligencia perteneciente a un Estado de derecho? ¿A qué mecanismos de control debe de someterse?

El fenómeno de los secretos oficiales es universal. Los distintos ordenamientos jurídicos no difieren mucho entre sí, cuando comparamos los que regulan las democracias liberales. Varía el diferente grado de control que tienen los poderes legislativo y judicial, sobre las actividades que se llevan a cabo en nombre del ejecutivo, en los servicios de inteligencia. El caso español no es una excepción. Los legisladores también optaron por dos vías de control. De un lado el **control judicial previo** de sus actividades, que es una herramienta que obliga a motivarlas y limitarlas en el tiempo. La otra vía es el control parlamentario. Una **comisión** de diputados fiscaliza los gastos reservados y es conocedora de la **Directiva de Inteligencia**, así como de materias clasificadas.

Cuando hablamos de información clasificada y reservada se suelen dar dos situaciones complejas de compaginar con el Estado de derecho. La primera es cuando se puede acceder a información clasificada por parte de un parlamento que quiere controlar a un gobierno. La segunda seria cuando un juez o un tribunal pueden tener en su mano información reservada que considera relevante para juzgar un delito.

Un ejemplo famoso fue el de las **cintas del presidente Nixon**. Se acabó ordenando al presidente de los Estados Unidos que entregara a un Juez Federal unas cintas que estaban en su poder. A pesar de las diferencias entre el derecho anglosajón y el nuestro que deriva del romano, en este caso el espíritu de la legislación es el mismo. Lo que permitió que la Corte optara por que Nixon le diera las cintas al juez, fue que no constaba que la información solicitada perjudicara a la seguridad y la defensa nacional. Este caso es un ejemplo de cómo el poder judicial veló no solo por el derecho de los ciudadanos a obtener información de la administración, sino que también se veló por que tiene el Estado a no revelar información que atente contra la seguridad nacional.

La Constitución vigente, protege el derecho de los ciudadanos a ser emisores de información, a la libertad de expresión y a recibir información del Estado. Cuando se reflexiona acerca de lo que supone el secreto, entre el Estado y la ciudadanía, hablamos de los límites en la **información pasiva**, el derecho a recibir información por parte de la administración. No estaría en cuestión la **información activa**, que es la entendemos por libertad de expresión. Sí que está en cuestión, hasta qué punto es el ciudadano el que puede tener secretos de cara al Estado. Hay dos artículos constitucionales que limitan el ejercicio del derecho a la información. El art. 20.4 que explica que hay límites en el derecho a la información: honor, intimidad, imagen etc. Y el art. 105.b que explica que la ley regulará como los ciudadanos podrán acceder a los registros administrativos salvo en los casos que afecte a la seguridad y defensa del Estado, la averiguación de delitos y la intimidad de las personas.

Viene a dar continuidad a la **Ley de Secretos Oficiales** de 1968, modificada por la Ley de 1978, garantizando que en determinadas situaciones el Estado puede negarse a suministrar información tanto al ciudadano como a los poderes públicos. La contraposición entre los secretos oficiales y el derecho público a la información, se da en todas las democracias como advertíamos anteriormente. Por ejemplo en la década de los sesenta el caso Der Spiegel o el caso Chandler Vs. Director of Public Prosecutios, en Alemania y el Reino Unido respectivamente, que fueron antecesores del norteamericano caso Watergate y los Papeles McNamara.

No es baladí el discriminar que información, en caso de ser difundida, sería un peligro para la seguridad y la defensa de España y por lo tanto tiene que ser clasificada. Decidir que materias son susceptibles de ser clasificadas es una decisión que se lleva a cabo mediante un **acto formal**, por parte del Consejo de Ministros o la Junta de Jefes del Estado Mayor del Ejército, según las competencias de cada cual. Obviamente la decisión de clasificar una información no puede ser un acto arbitrario. Tienen que sumarse dos elementos un formal y otro material. El formal consiste en que la información sea potencialmente lesiva para la seguridad y la defensa del Estado. Mientras que por otra parte el elemento material consiste en que tiene que haber una motivación expresa. Tiene que existir un acto formal en el que se explique por qué existe una vulnerabilidad y se va a clasificar una información. Los conocidos como fondos reservados son un ejemplo de información clasificada.

Lo que se oculta a los ojos del gran público, los secretos oficiales, se pueden clasificar en dos categorías, **materias clasificas y materias reservadas**. Esto depende del grado de protección que se requiera. Una información secreta es susceptible de ser materia clasificada cuando pudiera dar lugar a riesgos o perjuicios a la seguridad del Estado o pudiera comprometer los intereses fundamentales de la Nación en lo referente a la defensa nacional, la paz exterior o el orden constitucional. Por otro lado, una información secreta será catalogada como materia reservada cuando a pesar de no responder a los requisitos anteriores, por su menor importancia, se crea que potencialmente puede tener la misma lesividad que si fuera material clasificado.

Las dos categorías están restringidas en cuanto a su conocimiento y divulgación. Así que el acceso materias clasificadas tiene que ser una concesión del Consejo de Ministros o de la Junta de Jefes del Estado Mayor. Esto no significa que estos dos órganos tengan patente de corso y que existan espacios de impunidad por parte del poder público. Hay cauces legales para que los jueces por ejemplo, puedan desarrollar su labor. Nada impide a un juez que se dirija al Consejo de Ministros por medio de una exposición razonada, para solicitar la desclasificación de un informe que le sirva en un proceso. Esto no significa, que pueda imponer sin más a un ministro que se le entreguen unos papeles. El gobierno puede negarse a entregarlos. Aunque esto pueda parecer un exceso, hay que tener en cuenta que puede haber motivos para ello y que el gobierno responde ante la justicia por sus actos y también ante el parlamento que ejerce el control político. La figura del Defensor del Pueblo, también entraría en ese tira y afloja como el que pueden llegar a tener un juez y el Consejo de Ministros, en lo que respecta a las materias clasificadas.

La Junta de Jefes del Estado Mayor no puede negarse a entregar este tipo de documentación al Defensor del Pueblo. Si lo puede hacer por el contrario el Consejo de Ministros. Si esto ocurre puede ponerlo en conocimiento de la comisión mixta del Congreso, entrando como en el caso anterior en el control parlamentario del gobierno ejecutivo. El control político, solamente tiene sentido hacérselo al gobierno no a la Junta como es lógico. Nuestro sistema normativo admite la existencia de actos políticos por parte del Gobierno, en principio inmunes al control jurisdiccional de la legalidad en temas de material clasificado. Un tribunal, no puede juzgar a los ministros por no compartir información clasificada o por los motivos políticos que les han llevado a clasificarla. Son las Cortes Generales las que controlan la acción del Gobierno como recoge la Constitución en su art. 66.2 La legalidad vigente también señala que tanto el Congreso de los Diputados como el Senado, tendrán acceso siempre a cuanta información reclamen, en la forma que se determine en los reglamentos, que normalmente es en sesiones secretas.

Sólo el Congreso tiene regulado un procedimiento específico de acceso a asuntos que hayan obtenido la calificación de clasificado y de reservado. Existen dos formas, **el procedimiento ordinario y el procedimiento excepcional**. En primero de los dos supuestos, se formará un grupo compuesto por el Presidente de la Cámara y por un representante de cada uno de los Grupos Parlamentarios, sin contar el grupo mixto, elegidos por tres quintos del Parlamento. Esta es la razón por la que se intenta que las diferentes marcas que batasuna ha tenido en las cortes no tengan grupo parlamentario. El procedimiento excepcional es más sencillo. Cuando la materia no es clasificada sino reservada, el gobierno facilita la información a los portavoces de cada grupo parlamentario o a los representantes de estos en una comisión al uso, sin necesidad de desarrollar, en los términos anteriores, una comisión especial para materia clasificada.

En resumen, que cuando existe un conflicto entre el poder judicial y el ejecutivo en torno a la desclasificación de secretos de Estado (materia clasificada) se

entiende que el si el gobierno resuelve que no desclasifica una información ejerce la potestad de la dirección política que el art. 97 de la Constitución atribuye al gobierno de la nación, sin que ello implique que el ejecutivo esté exento de control judicial y mucho menos político. Si bien es cierto que se han dado y pueden darse caso en los que un delito se quede sin resolver debido a esta interpretación que de la ley hacen los tribunales, amén de que todos los ciudadanos tenemos derecho a tutela judicial efectiva que puede no garantizarse del todo en estos casos. Pero la seguridad del Estado es un valor constitucionalmente protegido y no siempre se puede ceder ante las investigaciones judiciales. Además hay que tener en cuenta que la Ley de Secretos Oficiales trata de preservar al Estado y por extensión al conjunto de la ciudadanía. En ningún caso debe servir para proteger a las autoridades o funcionarios que personalmente puedan resultar relacionados con una causa penal.

En el futuro ¿Cómo se puede evitar la fuga masiva de información sensible? ¿Es posible?

Siguiendo la información que han publicado los medios de comunicación y las opiniones de autoridades en la materia, es posible hacerse una idea más o menos, de qué fue lo que ocurrió para que se filtraran tal magnitud de datos. Aun así, es difícil saber fehaciente que sucedió realmente. ¿Snowden tuvo o tiene alguna relación con los rusos, Manning era plenamente consciente de lo que hacía, Assange sólo busca notoriedad y dinero? Pero hay una cosa que está clara. En un momento dado dos ciudadanos norteamericanos Manning y Snowden, tomaron la decisión de filtrar información. El primero un soldado raso desplegado en zona de operaciones y el segundo un técnico que trabajaba para agencias de seguridad. Pero los dos con amplio acceso a bases de datos. Como este tipo de decisiones no se pueden controlar, porque al fin y al cabo, son decisiones que las toma el individuo y dependen nada más que de él, lo único que se puede hacer es prevenirlas.

Al menos en el caso del soldado Bradley Manning, parece que falló la selección de personal a la hora de ponerlo en un puesto con acceso a tanta información. Todo lo que ha publicado la prensa sobre él, puede ser una estrategia de la defensa. No obstante los responsables de la selección del personal destinado a manejar tantos datos sensibles, debe tener muy en cuenta como los candidatos son capaces de **gestionar sus emociones**, además del perfil psicológico o/y el técnico. La prensa describe al soldado como una persona despierta e inteligente pero inestable emocionalmente y con una infancia difícil. Tampoco resulta razonable que a un joven soldado de 23 años con la escasa formación y bagaje que da tan corta edad, se le coloque en un puesto que exige un alto grado de discreción. Si a esto añadimos que ha iniciado un cambio de género sexual, que aunque pueda ser una estrategia tras su condena, no apunta desde luego a que haya tenido una juventud fácil.

Si a Julian Assange le motivó la promoción profesional y económica, a Manning puede que le moviera un afán de notoriedad. Quién sabe si a Snowden no le

acabó moviendo su frustración profesional, más que su una fuerte creencia en los valores que tenían que regir su trabajo. La prensa igual que a Manning, describe a Snowden como un mal estudiante, pero que en cambio tenía una gran capacidad para la programación informática. No llegó a graduarse en el instituto y tampoco pudo entrar en las fuerzas de operaciones especiales porque se partió las dos piernas en el intento. Si bien es cierto que acabó trabajando para la NSA y la CIA. Que un joven de 29 años que es técnico en seguridad, con un buen pasar, que se gana bien la vida, acabe filtrando a la prensa tal cantidad de secretos, no puede ser simplemente porque sus actos no concuerdan con su escala de valores. Independientemente del perfil psicológico de los dos filtradores, que obviamente pasaron las pruebas pertinentes, tuvieron que verse resueltos a hacer lo que hicieron por motivaciones emocionales más allá de lo racional.

Sea como fuere e independientemente de qué fue lo que les motivó a dar el paso, la solución es blindarse en medida de lo posible. El proceso norteamericano por el cual tanto la **universidad,** como sobre todo las **empresas privadas** están adquiriendo un papel importantísimo, no ya en la colaboración, sino en posibilitar la inteligencia de señales, sitúa a los Estados Unidos en una situación de vulnerabilidad. Al final son muchas empresas privadas las que almacenan datos, las que tienen capacidad de monitorización y las que pueden tener desde videos, a correos o información de todo tipo. La comunidad de inteligencia es grande y tiene mucho personal. Y no todos son funcionarios muy institucionalizados y controlados como podemos imaginarnos desde un punto de vista europeo. Si el resultado de la colaboración privada en la inteligencia y de la ampliación de personal conlleva que más trabajadores tengan acceso un volumen cada vez mayor de información, las posibilidades de revelaciones crecen exponencialmente. Los datos numéricos relativos a cuanta gente tiene acceso a qué, dentro de las agencias norteamericanas de seguridad son contradictorios.

Además es inevitable que en pro de la seguridad converjan lo público y lo privado. Pero el resultado no puede pasar porque personal joven, que quizás no está emocionalmente todo lo estable que debiera, que puede que no haya recibido una formación específica sobre seguridad en organizaciones sensibles, tenga acceso a las mismas bases de datos que un Secretario de Estado. Edward Snowden por ejemplo, contaba en el desempeño de sus funciones, con sus claves propias y las claves de sus compañeros, pues se las facilitaban para que pudiera trabajar en distintos ordenadores, en los que se dedicó a copiar más información de la que pudo obviamente leer. Estuvo empleado en empresa privada de inteligencia Booz Allen Hamilton. Aunque es una empresa hermana de la Agencia Nacional de Seguridad y el trasvase de personal es habitual, no ha resultado una práctica inocua. En los Estados Unidos, el área de los contratistas, asume alrededor del 70 por ciento de los 52.000 millones de dólares del presupuesto nacional destinados a los servicios secretos. Manning pasaba una parte de la jornada directamente compilando datos en discos sin que nadie lo advirtiera.

La convergencia público privada es positiva e inevitable, es una necesidad por ejemplo la incorporación de la empresa privada al mundo de la inteligencia, sobre todo en la recolección de datos y en otros campos como la encriptación etc. Es ya un hecho y una útil herramienta, porque los avances tecnológicos van muy deprisa y la esfera pública por su idiosincrasia, no puede desenvolverse tan rápido. Mas esta situación pasa por que se aumente más el control sobre la información y el personal que la maneja.

Si las medidas de protección pueden fallar en el proceso de ampliación de personal, también hay un gran riesgo de fuga, duramente los procesos de reducción de personal en las organizaciones. De la misma manera cuando se renueva el material hay que ser especialmente diligente. La NASA en una ocasión estuvo a punto de vender unos ordenadores ya utilizados que no habían pasado por un proceso óptimo de formateado. La venta de material o la destrucción de material si no se hace adecuadamente, puede ser igual de peligrosa que la pérdida, la venta o el robo de documentos o datos en cualquier formato.

La gestión de la información reservada debe evolucionar a la par que lo hace la tecnología y la sociedad. Las empresas privadas, que colaboren o vayan a colaborar en el futuro próximo con los servicios de inteligencia de su país, sobre todo en países con poca tradición de colaboración, tienen que tener esto más en cuenta que las propias agencias de seguridad que obviamente trabajan discretamente a diario. En el mundo privado en general, esto de la seguridad en la información, se sigue asociando a los entornos militares constituyendo un hándicap para muchas entidades, en especial para la que por su labor, pudieran colaborar discretamente con el Estado. Un problema añadido, es que ya cuenten en su empresa con grandes volúmenes de datos que no hayan sido categorizados, según su nivel de reserva adecuada.

Como se ha ido desarrollando a lo largo de todo el trabajo, es importante un estricto control sobre determinados trabajadores para conocer su grado de confianza. **La fuerza de la cadena es igual a la de su eslabón más débil**. Pensando en el personal, es muy pertinente organizar actividades de formación y de concienciación de todos los usuarios y destinatarios de información sensible. Hay que evitar escenarios habituales de fuga de información. Para empezar no puede ser que todos los usuarios de un sistema de información, tengan la misma posibilidad de acceso sobre los mismos datos. Si el analista Manning podía hacer copias de los datos que se compartían en la red **SIPRNET**, como se apuntaba anteriormente, como si fuera el Secretario de Estado de Defensa de los Estados Unidos, algo no funcionaba adecuadamente. Aunque en ocasiones pueda resultar complicado o poco práctico, no es de recibo que no se tengan en cuenta los roles y las responsabilidades diferentes de cada trabajador a la hora de entrar en archivos de información reservada o clasificada.

Además de los lápices USB y de los discos, hay muchas maneras sencillas de sustraer información de una organización que no cuente con un plan de

seguridad competente. Desde llevarse el portátil para trabajar en casa, hasta mandar correos electrónicos en el mismo puesto de trabajo. Todas las oficinas de empresas susceptibles de colaborar con el CNI por ejemplo, no son un bunker completamente hermético. Un trabajador puede colgar información en una **nube** de internet. Puede sacar papeles, mediante un sistema de mensajería física, de una compañía de correos privada y externa a su organización. Puede guardar datos en su móvil o hacerle fotos a un monitor de ordenador. Incluso se puede llegar a copiar datos manualmente en un papel o a retenerlos en la memoria. Para que perdamos el control sobre la información relevante, no hace falta siempre que el trabajador utilice métodos complicados, basta con no tener un buen plan de seguridad que proteja lo que queremos que siga siendo secreto.

Existen soluciones basadas en técnicas criptográficas, que permiten el cifrado de la información cuando no se accede a ellas de una manera franca. O para transportarlas por la calle en un USB. Existen tecnologías orientadas a la protección de aquella información que precisa abandonar las dependencias de la organización. Ya sea con correos electrónicos, documentos ofimáticos, son las conocidas como soluciones **EDRM**. Posibilitan controlar quién accede al documento, a qué partes del mismo y definir las acciones que le están permitidas: copiar, pegar, editar imprimir, enviar etc. También se puede controlar cuando se puede acceder a la información, monitorizar las acciones que se realicen sobre el documento en tiempo real, bloquear el acceso a la información en cualquier momento. Son asimismo muy útiles las conocidas **marcas de agua**, que permiten identificar a los usuarios que le han ido dando forma al documento y también a los que han originado el mismo. Otra capacidad complementaria a **EDRM** sería la tecnología **DLP**. Está orientada a la monitorización de fugas. Permite el control de las salidas no deseadas de información en los medios y canales de comunicación controlados por la organización, tanto si la información está en uso, está en movimiento o se encuentra depositada en una base de datos.

Además y esto es muy interesante, el sistema puede clasificar los datos o la información como sensible, en base a diversos atributos relativos al emisor de la misma, al contenedor de destino, a los horarios, palabras clave, expresiones regulares o **marcas de agua**. Una tecnología específica de seguridad para ser utilizada en las bases de datos, es la que se conoce como soluciones **DAM.** Nos permite vigilar la actividad que se está realizando en diferentes servidores de bases de datos, pero trabajando independientemente del sistema general que gestiona todos los servidores de las bases de datos. Un programa que sirve para espiar sin ser vistos, que se está haciendo en las bases de datos, en tiempo real, de forma permanente y que alerta sobre comportamientos extraños o malintencionados. Esto se consigue también con las técnicas **FD,** utilizadas por bancos, compañías de seguros y operadores de telecomunicaciones. Son técnicas estadísticas que se apoyan en la minería de datos, que ayudan a detectar el fraude. Permiten detectar patrones habituales de comportamiento y descubrir transacciones fraudulentas que se apartan de dichos patrones. Lo importante de todas estas tecnologías y técnicas, además de que se utilicen es que se haga correctamente, que se desarrolle un adecuado **plan de implementación**.

Conclusiones

Hace mucho que internet ha dejado de ser el futuro para ser el presente. Pero eso no significa que tengamos que dejar de reflexionar sobre qué supone que nos relacionemos en una red mundial. Ha cambiado la forma de compartir información y la de guardar los secretos. Colgamos en la red tanto una foto vacacional, como el número para acceder a nuestras cuentas bancarias. Internet no es solo una mera herramienta de búsqueda de datos. Es un lugar de encuentro donde compartir e intercambiar información personal, profesional y socio cultural. Hay tanta comunicación y tanta información compartida en la red, que un solo Estado no puede por sí solo velar por su seguridad. Es vital que los Estados y las empresas privadas colaboren entre sí. Además es trascendental que sean conscientes de que hay que proteger la información, porque si no el resultado es que se publique **"lo secreto"** a nivel global.

El ciudadano en tanto que individuo virtual, se ha convertido en una fuente muy atractiva para la inteligencia, por los datos que aporta y por la información que genera. El rastro que dejamos con las nuevas tecnologías, es una mina de oro para los investigadores y analistas de todo tipo: páginas visitadas, comentarios escritos, fotos, videos, contactos, aplicaciones, horarios, situación GPS, conferencias vía Skype, claves, movimientos bancarios etc. Ningún gobierno sensato, que busque la seguridad de su gente puede renunciar a todo esto. Si esto ocurre a un nivel individual, las empresas y las administraciones públicas, forman un volumen de información mayor y más sensible. No podemos caer en la transparencia total, como pretenden los activistas Assange y Snowden, entre otros. No es de recibo que la información crítica de las administraciones públicas o las organizaciones privadas no tenga que estar protegida y deje de ser secreta. No se puede pretender una transparencia total y absoluta. Como tampoco se pueden violentar arbitrariamente, los derechos y las libertades de los ciudadanos. Que tiene derecho al honor, a la intimidad y a tener comunicaciones privadas de todo tipo.

El caso WikiLeaks y las revelaciones de Snowden sobre la NSA, no constituyen un punto y aparte en la labor de los servicios de inteligencia. Las agencias van a seguir trabajando como hasta ahora. En concreto, la administración de Obama y las que le sucedan, podrán regular mejor o peor las actividades de la NSA, pero no pueden prescindir de la inteligencia de señales tal y como está planteada. Si no se construyen agencias de seguridad formadas por varios países, al estilo de lo que hacen los estadounidenses y los británicos, no es posible que las democracias liberales dejen de relacionarse entre ellas con operaciones clandestinas y material clasificado. Un Estado que no tenga secretos no puede garantizar la seguridad, otra cosa es que se desclasifiquen documentos con el paso del tiempo. No es necesario un nuevo marco relacional entre los ciudadanos y sus servicios de inteligencia, que reequilibre los ámbitos de libertad y seguridad. Lo que es necesario es que se cumpla la ley y se controle jurídica y políticamente la labor de los servicios de inteligencia.

Ernesto Vicente Iglesias es politólogo y Máster en Estudios Estratégicos y Seguridad Internacional por la Universidad de Granada.