ieee.es
Instituto Español de Estudios Estratégicos

Documento
Opinión

30/2013 22 marzo de 2013

*Luis de Salvador Carrasco**

MEDIDAS DE CONTROL Y SEGURIDAD DE LOS CIUDADANOS: SUS RIESGOS

Visitar la WEB Recibir BOLETÍN ELECTRÓNICO

MEDIDAS DE CONTROL Y SEGURIDAD DE LOS CIUDADANOS: SUS RIESGOS

Resumen:

El acceso por parte de autoridades de terceros países a los datos PNR o SWIFT es una medida necesaria para implementar la coordinación en la lucha contra la delincuencia internacional y el terrorismo. Esta colaboración tiene varios puntos de conflicto: por un lado la posible vulneración de derechos civiles y, por otro, la posible utilización de esa información para labores de inteligencia más allá de la policial. Los casos anteriormente señalados han tenido impacto mediático desde la perspectiva de la violación de libertades, pero se olvida el segundo aspecto. En relación a este tema, se pone de manifiesto que existen otras fuentes de información sobre actividades de los ciudadanos, no sólo enmarcadas en intercambios entre gobiernos, sino fuentes más o menos abiertas que están en manos de particulares y administraciones públicas, y que se encuentran accesibles online a terceros.

Abstract:

The access from third countries authorities to PNR and SWIFT records is a measure needed to implement the law enforcement against international crime and terrorism. This collaboration has several troubles: the chance to violate civil rights, and on the other hand, the chance to process such data in intelligence activities beyond law enforcement. The above mentioned cases had an impact in the media from the point of view of violation of civil rights, but the second view was subdued. Concerning this topic, it is important to take into account that there are other sources of data about citizens, not only with regard to data communication between states, but other sources managed by private and public institutions, that are more or less open to third parties.

Palabras clave: PNR, SWIFT, SIS, Europol, fuentes abiertas .

Keywords: PNR, SWIFT, SIS, Europol, Open Sources

INTRODUCCIÓN

La lucha contra el terrorismo y la delincuencia internacional supone la recogida de datos de personas, como no puede ser de otra manera, y el intercambio de información entre los organismos de seguridad de distintas naciones. Esta forma de actuación es básica, fundamental y necesaria para contrarrestar unas amenazas que tienen una naturaleza cada vez más global y que no conocen fronteras.

La recopilación, filtrado y análisis masivo de información sobre ciudadanos posee un efecto acumulativo. Es evidente que ésta tiene en un impacto en el recorte de las libertades del individuo, independientemente de que se estime que cada medida de control pueda ser eficaz y considerarse una violación "necesaria" y "proporcional" de los derechos que nuestra sociedad considera fundamentales.

La Estrategia Española de Seguridad (EES) establece que una de las medidas que ha mejorado de forma notable la lucha antiterrorista ha sido la disponibilidad inmediata de información e inteligencia. Por lo tanto, dentro de sus líneas estratégicas de acción está la de mejorar dichos sistemas de información, en particular mejorando la coordinación entre organismos nacionales e internacionales, tanto a través de las comunicaciones con servicios policiales como de inteligencia de otros países.

Ahora bien, cabría preguntarse hasta qué punto la colaboración en materia de seguridad se convierte en sí misma en una vulnerabilidad, al permitir que terceros realicen labores de inteligencia sobre los datos cedidos con un propósito definido, desviando su finalidad. Este aspecto ha saltado a la luz en relación a la comunicación de datos de pasajeros en vuelos a Estados Unidos, o el acceso a los movimientos de capitales por parte de las autoridades del mismo país.

La EES es consciente de la amenaza del espionaje "por parte de Estados, grupos o personas, con la finalidad de lograr información para obtener ventajas políticas o económicas", destacando que "de particular importancia es también el espionaje económico". La EES señala que esta actividad "se ha adaptado al nuevo escenario de seguridad, aprovechando las posibilidades que ofrecen las nuevas tecnologías de la información y comunicación", y que es necesario "hacer frente a las actividades de servicios de inteligencia extranjeros".

En este aspecto, las intromisiones en y a través del ciberespacio para obtener información se han señalado como la principal amenaza de filtrado de información a terceros indeseados. Pero no es necesario recurrir a violaciones de los sistemas de información para acceder a los datos buscados. En algunos casos, esa información es directamente accesible por los gobiernos de otros países cuando acuerdos, o situaciones de hecho, permiten el acceso a

bases de datos. En otros casos, el acceso a dichas bases de datos por parte de otros gobiernos, o terceros de otra naturaleza, es fácilmente accesible de manera gratuita o previo pago.

En la búsqueda de una cooperación más efectiva y para facilitar trámites a ciudadanos e instituciones, las administraciones públicas y las entidades privadas han automatizado sus ficheros proporcionando acceso a los mismos a través de Internet. La consulta a través de la red supone un cambio cualitativo muy importante, ya que permite un acceso mucho más ágil y rápido a un volumen masivo de datos y sin necesidad de mantener una infraestructura de contactos o de personal de enlace. Ahora esa infraestructura es virtual y permite acceder a información sobre los empleados públicos y las operaciones del Estado, a datos sobre los ciudadanos a través del acceso a registros públicos, a información sobre movimientos de capitales o de viajeros y reservas. Cada uno de estos registros ofrece una visión parcial de parte de la sociedad, pero solapando unos con otros se puede crear una imagen bastante completa de la misma.

DATOS DE PASAJEROS Y RESERVAS

En relación a la comunicación de información sobre viajeros de vuelos comerciales, recientemente saltó a la luz la comunicación que se realiza a las autoridades estadounidenses de datos de pasajeros de vuelos que, sin destino a Norteamérica, sí sobrevuelan su espacio aéreo, lo que se materializaba en la posibilidad de vetar el embarque de algunos de ellos. Esto ha puesto de nuevo en actualidad el acceso por parte de terceros países a información sobre movimiento de personas.

Existen acuerdos para proporcionar datos API, es decir, información anticipada del pasajero que va a embarcar en una aerolínea, a las autoridades aduaneras del país de destino de un vuelo internacional. Esta información no se remite en todos los casos, sino sólo cuando el país al que se viaja ha puesto en marcha dicho requerimiento para las compañías aéreas, como por ejemplo el Reino Unido. Esto permite a dichas autoridades conocer nuestra llegada antes de aparecer en el control de inmigración, en algunos casos hasta 72 horas antes del vuelo. Por lo tanto, los datos API no entran en el mismo caso que se describía en el párrafo anterior, en el que se procesaban por las autoridades norteamericanas datos de pasajeros cuyo destino no era Estados Unidos.

En ambos casos, el objetivo de esa información enviada en el marco del programa Secure Flight , es alimentar el ATS , el sistema de selección automática del DHS (el equivalente a un Ministerio del Interior) que, por cada persona que cruza las fronteras de Estados Unidos, examina los datos recopilados de la misma para clasificar esa persona en un grupo de

interés, por ejemplo, como terrorista. La flexibilidad de tales sistemas es muy grande y sus posibilidades de uso mayores. En particular cuando tienen acceso a las registros PNR o Passenger Name Record.

Los registros PNR no equivalen a los datos API. PNR es el nombre genérico que se da a las fichas de pasajeros que generan las aerolíneas y agencias de viajes en sus sistemas de reservas con el propósito de gestión comercial de sus servicios. En él se archiva toda la información relativa al itinerario de un viaje específico, incluyendo datos sobre los pasajeros como tipo de comida, necesidad de silla de ruedas, medio de pago (que en caso de ser por tarjeta estaría incluido su número), datos del pasaporte, si son menores, etc. El análisis del conjunto de PNR de un viajero proporciona información sobre su conducta, su perfil, su religión, los cambios reflejados en sus preferencias y las coincidencias en asiento o vuelos con otros pasajeros.

La globalización de los sistemas de reservas ha dejado cuatro empresas principales en el sector: AMADEUS, Sabre, Galileo y Worldspan. AMADEUS es el sistema más extendido en Europa y se utiliza tanto para gestionar reservas de vuelos, como estancias en hoteles, entradas de teatro, etc. El grupo empresarial se distribuye entre varios países, estando la empresa cabecera en España, y la gestión de las bases de datos en Alemania.

En dichos sistemas, los datos de los perfiles de clientes se archivan sin límite de tiempo. Es el usuario del sistema que ha creado el perfil, p.ej. la agencia de viajes, el único que puede desactivarlo o cancelarlo. Cuando se desactiva, el sistema lo guarda durante 30 días en los que el usuario puede reactivarlo de nuevo, pero si pasados estos 30 días no se ha reactivado, el sistema procede a su eliminación definitiva. A nivel general, cada aerolínea puede acceder a los datos que la agencia de viajes ha incluido en el fichero PNR, siempre y cuando esté implicada en la información contenida en el PNR (al formar parte del itinerario) y para la gestión del servicio, como es el caso de necesitar generar los datos API.

Los accesos que realizan las autoridades aduaneras se pueden realizar, técnicamente, en modo PULL o en modo PUSH. Este último consiste en que las aerolíneas fijan una serie de parámetros (por ejemplo, vuelos con un determinado destino) y el sistema remite automáticamente a la autoridad de dicho destino los PNRs que cumplen las condiciones seleccionadas. Por el contrario, el modo PULL consiste en la habilitación de un acceso libre a los PNR por parte de las autoridades aduaneras de terceros países como si se tratara de la aerolínea misma, sin restricción a que, por ejemplo, el PNR accedido sea el correspondiente a un vuelo con destino a dicho país.

El sistema PUSH está actualmente activo para las autoridades canadienses, inglesas, australianas y norteamericanas bajo determinados acuerdos suscritos con la Unión Europea .

El sistema PULL, que permitía un acceso mucho más amplio, ha estado habilitado para las autoridades estadounidenses, australianas y neozelandesas en los últimos años. Como se ha señalado anteriormente, este sistema permitía acceder a los datos de viajeros sin restricciones, tanto con destino a sus respectivos países como a cualquier otro, e incluso a los registros de vuelos domésticos intra-europeos. Esta situación se produjo ante la presión que el gobierno estadounidense ejerció sobre las aerolíneas directamente , rompía el plano de igualdad con la Unión Europea, ya que permitía realizar un análisis de la información de viajeros mucho más allá de la prevención del terrorismo, y saltó a la luz ante la presión de las autoridades de Estonia cuando advirtieron que se había producido el acceso a datos de algunos personajes destacados de la misma nacionalidad.

INFORMACIÓN FINANCIERA

The Society for Worldwide Interbank Financial Telecommunication (SWIFT) es una compañía privada con sede en Bélgica que proporciona una red a las instituciones financieras de todo el mundo para enviar y recibir información sobre las transacciones económicas en un entorno seguro estandarizado y confiable. Entre otras cosas, define los códigos de identificación bancaria conocidos como códigos SWIFT. SWIFT no facilita la transferencia de fondos, sino que envía las órdenes de pago que deben ser resueltas por las instituciones financieras. Sus servicios se utilizan en, aproximadamente, el 80% de las transacciones internacionales, y dos tercios del volumen total de dichas transacciones se originan en países europeos. Los mensajes se procesan y almacenan en Bélgica, e incluyen información sobre origen y destino de la transacción, cantidades, nombres, direcciones y los valores utilizados en la misma. El almacenamiento no es permanente, sino durante 124 días.

El acceso a dichos datos es muy interesante para determinar el funcionamiento de redes de financiación ilegales, ya que permite construir un árbol de relaciones entre personas (físicas y jurídicas) que realicen transferencias internacionales. Para tener acceso a dichos datos se estableció el acuerdo TFTP (Programa de Seguimiento de la Financiación del Terrorismo), que es un acuerdo bilateral entre la UE y los EE.UU. que permite que los datos de mensajería financiera almacenados por SWIFT sean accedidos por el Departamento del Tesoro de EE.UU. bajo petición a los Estados. La ejecución del acuerdo está actualmente bajo el control de Europol, que tiene el rol de organismo verificador de la aplicación del acuerdo desde el punto de vista operativo. En particular, controla si las solicitudes de las autoridades de Estados Unidos para obtener datos de mensajería financiera cumplen con ciertos requisitos concretos.

Dicho acuerdo corrige una situación de desequilibrio que se originó cuando los servidores de respaldo de SWIFT estaban localizados en U.S.A. y, por lo tanto, bajo las competencias de la

PATRIOT Act, lo que permitía un acceso sin restricciones por parte de las autoridades estadounidenses, y sin control por parte de las autoridades europeas. Esta era una situación muy similar al caso PNR surgida, en este caso, ante las modificaciones del marco normativo que despojaron de protección a un fichero, en vez de la implementación de un sistema de acceso. De ello se desprende la importancia que tiene el estudio de las medidas legislativas de otros países, tanto en vigor como las propuestas, para tomar medidas preventivas antes de que una situación como la señalada vuelva a producirse.

Pero no sólo los datos alojados en los sistemas de SWIFT han sido accedidos o son accesibles. Todas las instituciones financieras norteamericanas han de permitir el acceso a sus registros bajo amenaza de que el Departamento del Tesoro congele sus activos. Por otro lado, y fuera del ámbito de las transacciones internacionales, los datos SWIFT no son los únicos ficheros con datos financieros accesibles por terceros. Hay otros datos accesibles, pero con información de naturaleza completamente distinta, como son los ficheros de solvencia, que contienen información del estado financiero de las personas incluidas en ellos. Existen ficheros negativos, gestionados por entidades privadas (ASNEF-EQUIFAX, EXPERIAN, CCI, etc.) o pública como es el caso de CIRBE. Los ficheros positivos, como PERSUS, contienen a aquellos ciudadanos que voluntariamente se suscriben, con el objeto de evitar el uso fraudulento de sus datos personales por terceros en perjuicio de su identidad, solvencia y patrimonio económico, para lo que se proporcionan datos como DNI, teléfono, cuentas corrientes, etc. El acceso a éstos se encuentra regulado, ya que está limitado a entidades crediticias, financieras, de tarjetas de crédito, etc., con intereses en los datos almacenados y, técnicamente, están protegidos por una serie de medidas de seguridad. La realidad es que dichos ficheros están amenazados por accesos a través de terceros, indebidos, abusos, filtraciones y fallos de seguridad, que dejan expuesta la información almacenada en ellos.

En relación a la información patrimonial, existen entidades que proporcionan una amplia variedad de datos sobre personas jurídicas (e indirectamente físicas como autónomos, administradores y otros) para estimar su solvencia, y que permiten la consulta a través de Internet mediante el procedimiento de suscripción. Frente a una mayoría de empresas que cumplen con la legislación, han aparecido algunos casos de mercado negro de datos para la evaluación de la solvencia y localización de personas físicas. Éstas también operan con mecanismos de suscripción y ofrecen la fusión de datos de diversas fuentes, como son censos electorales de distintos años, padrones municipales, repertorio de abonados a los servicios telefónicos, recopilación sistemática de datos de particulares en boletines oficiales, etc. Esto permite seguir los cambios de domicilios y otra información de contacto a lo largo del tiempo, buscar coincidencias con otras personas y establecer relaciones entre ellas.

INTERCAMBIO DE INFORMACIÓN PARA LA SEGURIDAD

El intercambio de información de carácter puramente policial es realmente la herramienta más interesante para hacer efectiva la coordinación de la lucha contra las distintas formas de delincuencia internacional. También es uno de los aspectos que más alarma social puede suscitar, a pesar de que realmente son los más protegidos, tanto técnica como jurídicamente, y donde más restrictivo es el flujo de información. Ese intercambio tradicionalmente se realiza de forma puntual en las redes de contacto establecidas en el marco de Interpol, Europol y foros específicos.

El Programa de La Haya, que se adoptó en el Consejo de Europa en 2004, recogía las prioridades de la Unión destinadas a reforzar el Espacio de Libertad, Seguridad y Justicia. Una de sus conclusiones para mejorar la cooperación en la lucha contra el terrorismo y el crimen organizado fue poner en marcha el llamado "Principio de Disponibilidad", que supone facilitar la cooperación entre las autoridades policiales y judiciales de los Estados miembros de la UE, permitiendo que la información sea intercambiable con el menor esfuerzo posible, lo que implica una mayor facilidad de acceso a bases de datos nacionales.

Ya se encontraba disponible una infraestructura tecnológica para acceso online a información compartida entre distintas autoridades europeas, como es el caso del Sistema de Información de Schengen o SIS. El propósito de este sistema es tener un volcado común y un mecanismo de intercambio de información de las bases de datos de señalamientos de cada país en relación a las personas buscadas para su detención, extranjeros incluidos en la lista de no admisibles, desparecidos, testigos, personas y vehículos sometidos a vigilancia y objetos robados o documentos. El acceso y volcado de dicha información está estrictamente controlado según lo dispuesto en el desarrollo legislativo del Acuerdo de Schengen , la información disponible online es muy limitada , y no es accesible por países fuera del acuerdo, proporcionándose información complementaria a través de los puntos de contacto de las oficinas SIRENE.

A su vez, en el marco de Europol, se desarrollaron una serie de sistemas para el intercambio de información online. Por un lado, la Aplicación Segura de la red de Intercambio de Información SIENA que se utiliza para gestionar el intercambio de información operativa entre los Estados miembros Europol y terceros países con los que se tiene un acuerdo de cooperación, estos últimos mediante un acceso indirecto. Por otro lado, el Sistema de Información de Europol EIS, alojado en La Haya, es una base de datos con información sobre sospechosos y personas condenadas, vehículos, documentos de identidad, organizaciones y métodos criminales, para la lucha contra todas las formas graves de delincuencia internacional y el terrorismo. Esta base de datos es accesible por las unidades nacionales de Europol, funcionarios debidamente autorizados y en situaciones específicas, terceros que

pueden tener acceso indirecto a través de Europol. Futuras versiones del sistema incluirán información biométrica, tales como perfiles de ADN, huellas dactilares y fotografías. Finalmente, se han desarrollado los Ficheros de Análisis o AWF (Analytical Work Files), que son bases de datos sobre un determinado expediente delictivo, que contienen información de delincuentes, sospechosos, contactos, colaboradores, víctimas, testigos e informantes. Es alimentado y accedido por las distintas autoridades nacionales y los miembros de Europol.

El Principio de Disponibilidad se desarrolla más aún en la llamada "Decisión de Prüm" de 2008, sobre la profundización de la cooperación transfronteriza. Concretamente, pretende mejorar los intercambios de información entre las autoridades encargadas de prevenir e investigar los delitos haciendo disponible la información contenida en ficheros nacionales a las autoridades homólogas de los países signatarios, con restricción de su utilización a la finalidad que justificó la transmisión. La decisión establece disposiciones sobre el acceso a ficheros automatizados de análisis de ADN, y su creación si no existieran. Permitirá realizar búsquedas a través de los puntos de contacto nacionales mediante un sistema de coincidencia. De igual forma, se establecerán sistemas automatizados de identificación dactiloscópica, lo que será una evolución de EURODAC y acceso a datos de los registros de matriculación de vehículos nacionales por matrícula y número de bastidor.

Para los casos de celebración de grandes acontecimientos sociales, se prevé el intercambio de datos de personas que se consideren una amenaza para el orden público y la seguridad, o se crea que van a cometer un delito, y la mejora del intercambio de información relativa a personas dentro del marco de lucha contraterrorista.

La infraestructura tecnológica que se disponía hasta el momento no era suficiente para cumplir con los requisitos establecidos en la nueva decisión, por lo que el 1 de diciembre de 2012 se puso en marcha de forma efectiva la Agencia Europea de Sistemas TIC de Gran Escala, encargada de la gestión operativa de grandes sistemas de información en el ámbito de Interior con su sede en Tallinn, con centros de desarrollo y respaldo en Estrasburgo y St. Johann en Pongau (Austria). Cumple con las tareas de gestión operativa del Sistema de Información de Visados (VIS), EURODAC y, partir de la primavera de 2013, la segunda generación del Sistema de Información de Schengen o SIS II.

El VIS contiene información, incluyendo datos de identificación biométricos, sobre las solicitudes de visado presentadas por nacionales de terceros países que requieren visa para ingresar a la zona Schengen y, por lo tanto, ha de ser accesible en las sedes consulares o a quien tenga éstas subcontratado el servicio de visados. El SIS II proporcionará nuevas funcionalidades, incluyendo la adición de los datos de identificación biométrica como fotografías e impresiones dactilares, y nuevas categorías. Los siguientes pasos serán integrar el Programa de Viajeros Registrados y el Sistema de Entrada/Salida, que forman parte de la

estrategia Smart Borders. En el mismo marco, se está desarrollando un sistema común europeo de índice de ficheros policiales y la forma de aumentar la eficiencia en la búsqueda y el intercambio de registros policiales entre los Estados miembros.

En el ámbito judicial, diversos Estados miembros entre ellos España, ya intercambian información sobre antecedentes penales electrónicamente en el marco del proyecto piloto Red de Registros Judiciales. Este proyecto ha dado lugar al Sistema Europeo de Información de Antecedentes Penales (ECRIS) para el intercambio y actualización de antecedentes penales y así imposibilitar el eludir su pasado criminal desplazándose de un país a otro. En la práctica, ECRIS es un sistema distribuido de interconexión de las bases de datos de los registros de antecedentes penales de todos los Estados miembros. Cada país tiene la obligación de mantener disponible los registros de antecedentes, y en el caso de condenas a un no-nacional, remitir esta información a su país de origen. ECRIS contiene información relativa a ciudadanos de la UE, no de nacionales de terceros países, por lo que se plantea ampliarse con un índice europeo de nacionales extracomunitarios condenados.

INFORMACIÓN DISPONIBLE ON-LINE

Tanto los registros PNR como SWIFT son mantenidos por empresas privadas y están sujetos a regulaciones internacionales. Hay otros registros que son mantenidos por las administraciones públicas y que son accesibles por terceros a través de Internet de forma más o menos directa, en algunos casos debido al impulso de la Ley 11/2007 de acceso electrónico de los ciudadanos a los servicios públicos.

Los censos y los padrones, de los que se habló anteriormente, son registros cuyo acceso está limitado a los supuestos electorales a los partidos políticos, administraciones y a la prestación de servicios públicos. La realidad es que comportamientos ilícitos ponen esta información al alcance de terceros. De la misma forma, la recogida masiva de datos de particulares a través de búsquedas en boletines oficiales (nombres, direcciones, DNI's y otros de nombramientos, multas y otras notificaciones) se encuentra regulada y limitada por los parámetros de los servidores, lo que no impide su utilización irregular de forma práctica.

Los registros públicos no son una novedad y su existencia proporciona garantías jurídicas a la actividad económica. Sin embargo, la informatización de los mismos y, sobre todo, la posibilidad de acceso a través de Internet de forma más o menos anónima y masiva, supone un cambio cualitativo en la forma de proporcionar acceso a dicha información. Por supuesto, la aplicación de la ley 11/2007 agiliza los trámites a los ciudadanos y empresas gestoras pero, por otro lado, proporciona una ingente fuente de información para cualquiera y en cualquier parte del mundo.

No todos los registros públicos son de libre acceso a través de la red, algunos son de acceso restringido a la existencia de un interés legítimo y otros son accesibles sorteando las disposiciones legales o mediante la colaboración de terceros, como gestorías en Internet. Entre ellos están, por ejemplo, la Administración General del Estado, el Registro Mercantil, el Registro General de Protección de Datos, el Registro de Marcas, el Registro de Fundaciones, el Registro Oficial de Auditores de Cuentas, el Registro de Bienes y Derechos Patrimoniales de Altos Cargos, el Registro de la Propiedad, el Catastro Inmobiliario, el Registro Civil y el Registro de Vehículos de la DGT. Aunque la mayor parte de los citados ofrecen información sobre personas jurídicas, de forma lateral, ofrecen bastante información sobre actividades de personas físicas, sus vinculaciones con empresas o la titularidad de derechos.

En otros casos, los requisitos de acceso a los registros son más complejos, precisan de firma electrónica o no están accesibles directamente a través de Internet, como son, por ejemplo, el Registro de Voluntades Anticipadas, Registro General de actos de última voluntad, el Registro de Contratos de Seguros de Cobertura de Fallecimiento o el Registro de la Propiedad Intelectual.

Esta no ha sido una lista exhaustiva de todos los registros en manos de la administración o de particulares que tienen una difusión en abierto de forma más o menos restringida. Por ejemplo, en el campo del marketing se encuentra el Fichero Común de Exclusión de Tratamientos Publicitarios, una Lista Robinson, que contiene información sobre datos de contacto de ciudadanos, relacionando direcciones postales, de correo, teléfonos, etc. La participación en el mismo es voluntaria y es accedido por empresas acreditadas en el sector.

Muchos colegios profesionales muestran sus listados de colegiados de forma libre en Internet. En el campo de los suministros, está el fichero CUPS o Código Universal de Punto de Suministro, que contiene información de los suscriptores a servicios de energía, incluyendo direcciones o información para facturación. Sin entrar en el conjunto de datos que estarán disponibles una vez se ponga en efecto la Ley de Transparencia, ya se encuentran disponibles para acceso on-line el Fichero de Altos Cargos o históricos en los portales de las diversas cámaras nacionales y autonómicas. Tampoco se entrará a enumerar los relativos a los servicios de Internet, telecomunicaciones, redes sociales, servicios buscadores de personas, etc., que constituirían un capítulo aparte. Hay que tener en cuenta que se ha llegado a estimar que los datos de cada español están incluidos en unas 300 bases de datos distintas.

CONCLUSIONES

El intercambio de información entre las autoridades de distintos Estados, aquellas encargadas de la seguridad y lucha contra el crimen y el terrorismo, es de capital importancia en un mundo globalizado. Sin ella, no es posible ni prevenir amenazas ni perseguir de forma efectiva la delincuencia organizada.

Este intercambio de información ha de cumplir varios principios. El primero de reciprocidad en la calidad de la información intercambiada, el segundo de proporcionalidad en la cantidad y calidad de la información solicitada. Aunque estos principios se cumplan, en el intercambio de información con otros países hay que ponderar también dos circunstancias: en qué medida se afecta a los derechos de los ciudadanos y el hecho de que, una vez que la información ha salido de nuestro control, dichos Estados pueden realizar otras tareas de inteligencia más allá de las declaradas, o incluso remitirlos a terceros.

Si bien esta última circunstancia es posible que se produzca, y por tanto es necesario tenerla en cuenta a la hora de ejecutar acuerdos de intercambio de información, esto no puede hacer que se pierda la perspectiva de qué datos ya se están proporcionando de forma más o menos abierta y de dónde se encuentran los auténticas vulnerabilidades a través de las que se filtra información.

Los casos PNR o SWIFT han de servir como ejemplo de lo importante que han de ser las tareas de vigilancia constante sobre nuevos productos, servicios o iniciativas regulatorias en el mundo de las tecnologías de la información. También de la necesidad de medir el alcance de los intercambios que se están realizando, de realizar una revisión crítica de los datos que se ponen de forma directa o indirecta accesibles a terceros y de incorporar mecanismos técnicos para detectar consultas masivas y sistemáticas a las bases de datos que se pueden consultar en abierto. Todo ello teniendo en cuenta no sólo la perspectiva de los derechos de los ciudadanos, sino también de su impacto real en el incremento de la seguridad global y, en tercer lugar, de los intereses nacionales.

*Luis de Salvador Carrasco**[i]
Doctor en Informática

NOTA:** Las ideas contenidas en los ***Documentos de Opinión son de responsabilidad de sus autores, sin que reflejen, necesariamente, el pensamiento del IEEE o del Ministerio de Defensa.