ieee.es
Instituto Español de Estudios Estratégicos

Documento
Opinión

33/2019 23 de abril de 2019

*Fernando del Pozo**

La responsabilidad de compartir y la necesidad de saber

La responsabilidad de compartir y la necesidad de saber

Resumen

La Unión Europea está poniendo en servicio el *Common Information Sharing Environment* para intercambio de información entre las agencias con competencias en seguridad marítima de los países miembros. Uno de sus principios básicos es la «responsabilidad de compartir», que deja atrás el anticuado «necesidad de saber», más fácil de codificar e implantar, pero fuente de importantes riesgos. Otros ámbitos no marítimos de aplicación y defensa de la ley deberían seguir este ejemplo.

Palabras clave

Seguridad marítima, información, inteligencia, necesidad de saber, responsabilidad de compartir, agencias de la ley.

The responsibility to share and the need to know

Abstract

The European Union is in the process of commissioning the Common Information Sharing Environment to exchange information between Member States' agencies with competences in maritime security and safety. One of its fundamental principles is the 'responsibility to share', which leaves behind the antiquated 'need to know', much easier to codify and enforce, but a source of important risks. Other non-maritime law-enforcing environments should follow the example.

Keywords

Maritime security, information, intelligence, need to know, responsibility to share, law-enforcing agencies.

Introducción

Parece ya lejano el 11 de septiembre de 2001, sin embargo, mucho de lo que a la fuerza aprendimos entonces sigue vigente, tanto en un plano teórico —lo que una ideología de odio puede llegar a acometer con el terrorismo como arma, sobre todo si incluye agentes suicidas— como en el práctico, es decir qué medidas se pueden tomar, qué sacrificios hay que hacer incluso en nuestra vida diaria para precavernos de tan enorme riesgo. Y todas esas lecciones aprendidas son muy válidas si consideramos que los actores de entonces, sus odios y pulsiones, la posición en el orden mundial de sus patrocinadores, siguen básicamente vigentes.

Que se han extraído lecciones nos lo demuestran cada día los registros y detectores de metales en aeropuertos, estaciones y edificios oficiales, los bolardos en las calles, las puertas de seguridad en las cabinas de los aviones, y otras muchas medidas que en general hacen la vida del ciudadano más ardua. Y que esas lecciones y medidas surten efecto lo prueba la ausencia ya durante varios años de noticias de secuestros de aviones y explosiones en trenes (toquemos madera), aunque los ataques terroristas en las calles y en centros de oración o diversión con explosivos, armas y vehículos son todavía una realidad, sobre todo en las ciudades europeas, pero también en el resto del mundo. Felizmente, ataques de la aterradora entidad de los del 11 de septiembre de 2001 no han vuelto a ocurrir, pero sabemos que voluntad no falta, y que un descuido puede ser fatal. Y en todo caso los ataques de menor escala que aquel que han seguido ocurriendo —Madrid, París, Londres, Niza, Barcelona…— son lo suficientemente dolorosos como para que necesitemos continuamente replantearnos y mejorar las medidas que se toman.

Una de las conclusiones más notables del informe conjunto del Congreso y Senado de los EE. UU. sobre los ataques terroristas del 11 de septiembre de 2001 tiene eco hoy todavía, porque a pesar de su claridad muy pocas medidas se han tomado para paliar los riesgos que a ello condujeron. Se trata, según la comisión, de que «las agencias no compartían adecuadamente información antiterrorista relevante antes del 11 de septiembre. Este colapso de comunicaciones fue resultado de un número de factores, incluyendo diferencias en las misiones de las agencias, aspectos legales y culturales. La información fue insuficientemente compartida, no sólo entre diferentes agencias de la

comunidad de inteligencia, sino también dentro de las agencias individuales, y entre las agencias de inteligencia y las de la ley»[1].

En palabras más directas: la información era suficiente, pero no fue adecuadamente compartida, porque la difusión de información en y entre las agencias policiales y de inteligencia se regía por el principio conocido como «*need to know*» (necesidad de saber, NTK), que estipula que el poseedor de una información decide sobre su difusión solo a la vista de las credenciales del presunto destinatario, que se establecen con dos preguntas contestadas solo por dicho poseedor: ¿tiene o no el destinatario necesidad de saberlo? y, ¿tiene acreditado el nivel de acceso necesario?

El más dramático —pero no único— ejemplo concreto de ello hay que espigarlo en el largo informe (838 páginas):

- Al parecer, a la CIA y otras agencias de inteligencia norteamericanas habían llegado rumores insistentes y creíbles de que Al-Qaeda planeaba ataques en EE. UU. usando aviones comerciales como arma, aunque no especificaban la identidad de los terroristas, ni el preciso modo de uso de los aviones.
- El servicio de aduanas sabía que ciertos individuos saudíes habían entrado con visas dudosas, excediendo el tiempo permitido para las de turismo, negocios o estudios.
- Mientras tanto, el FBI se había enterado de que en una cierta escuela de pilotos los instructores habían notado con extrañeza que algunos alumnos árabes ponían mucho empeño en las clases de navegación y vuelo (*executing turns and approaches*), pero no tenían ningún interés en las de despegue y aterrizaje.

Es evidente que, de estos tres elementos de información, de haber podido ser considerados en conjunto, el analista más lerdo habría sacado las conclusiones correctas, lo que hubiera permitido abortar el ataque, pero nunca estuvieron en las mismas manos. ¿La razón? NTK.

Este caso fue perfectamente documentado y publicado en dicho informe, inicialmente clasificado de *top secret* y posteriormente totalmente desclasificado. Pero, según algunos medios fidedignos de difusión, hay vehementes sospechas de que la incapacidad de las fuerzas de la ley para prevenir recientes ataques terroristas en

[1] Report of the Joint Inquiry into the Terrorist Attacks of September 11, 2001 – By the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence. Finding 9, p. 77. (Traducción del autor).

Europa, al menos los de París en noviembre del 2015 y de Barcelona en agosto del 2017, tuvieron su origen en un «colapso de comunicaciones» similar al descrito en el informe del Congreso y Senado sobre el 11 de septiembre del 2001.

Y es que el sistema *need to know* (NTK), prevalente no solo en EE. UU., sino en las agencias policiales y de inteligencia de Europa, adolece de varios fallos, alguno garrafal. En primer lugar, convierte al que ha obtenido la información en «dueño» de ella, con capacidad omnímoda para decidir sobre su distribución, y esto independientemente de su jerarquía objetiva y, por lo tanto, de su visión del panorama general, dejando abandonado su verdadero papel, que es el de contribuir a la tarea colectiva de construir inteligencia a partir de varias informaciones independientes. En segundo lugar, y tal vez más grave, claramente identificado en el ejemplo del 11 de septiembre, el NTK impide eficazmente las peticiones de información, ya que el que la necesita (por ejemplo, para confirmar, desmentir o completar otra existente) a menudo no sabe que aquello que necesita existe. Y no es preciso decir que las preguntas genéricas y dirigidas a una colectividad (del tipo de ¿quién me podría completar este rompecabezas?) tienen muy escaso éxito. El resultado de todos estos problemas es que las agencias de la ley y de inteligencia se convierten en compartimentos estancos.

No se disputa aquí que la protección de la información clasificada, que es el objeto del NTK, es muy importante. Volviendo al muy real ejemplo anterior, es evidente que la difusión pública de cualquiera de aquellos elementos de información habría dado al traste con las pesquisas (aunque tal vez habría desbaratado en parte sus planes). Pero no es menos evidente que el NTK es una respuesta excesiva y contraproducente para el objetivo, sobre todo de prevención, de las fuerzas del orden.

Es menester, por tanto, reemplazar el NTK por otro paradigma que facilite el cotejar, contrastar, o completar las informaciones dudosas, tentativas o incompletas con otros elementos, tal vez en posesión de otra agencia o fuerza de la ley, sin poner en riesgo su confidencialidad. Que permita que la información fluya en beneficio de la seguridad, pero sin comprometer las identidades de los confidentes u otros factores que podrían poner en riesgo las posteriores operaciones de las agencias de la ley.

Este nuevo paradigma existe, y se llama «responsabilidad de compartir» (*responsibility to share,* RTS), y ha sido integrado como uno de los principios fundamentales en la nueva herramienta de seguridad marítima que la Unión Europea se ha dado a sí misma tras

varios años de trabajos y experimentos, el *Common Information Sharing Environment* (CISE), que está empezando a entrar en funcionamiento[2] en la mayor parte de las naciones marítimas de la UE. Su potencial uso, sin embargo, trasciende el ámbito marítimo y debería ser considerado para todo el ancho campo de la seguridad frente a acciones deliberadas del hombre.

RTS significa que la persona en posesión de una información está bajo obligación de distribuirla a cualquiera que pueda legítimamente usarla y, si algún daño se produce por no distribuirla, el que lo ha impedido será tenido por responsable. He aquí la principal diferencia con el NTK: bajo el RTS existe una responsabilidad por no haber compartido (obviamente, si se demuestra que ello ha producido daño), mientras que bajo el imperio del NTK nadie puede ser castigado por haber sido excesivamente posesivo de la información obtenida, sea cual sea el resultado, pero sí por haberla difundido.

Naturalmente, RTS no es una nueva regla inventada de la nada para los exclusivos fines del CISE, sino que está basada en normas internacionalmente aceptadas. Así, el principio de solidaridad del Tratado de Funcionamiento de la Unión Europea, artículo 222, dice que «la Unión y sus Estados miembros actuarán conjuntamente con espíritu de solidaridad si un Estado miembro es objeto de un ataque terrorista o víctima de una catástrofe natural o de origen humano». No es preciso añadir que el espíritu de solidaridad así invocado incluye no sólo la reacción, sino también la prevención, objeto fundamental del intercambio de información.

También el artículo 24-2 de la Convención de las Naciones Unidas para el Derecho del Mar (*United Nations Convention on the Law of the Sea,* UNCLOS) dice que «el Estado ribereño dará a conocer de manera apropiada todos los peligros que, según su conocimiento, amenacen a la navegación en su mar territorial». Y el artículo 200 de la misma Convención establece que «los Estados cooperarán, […] para […] fomentar el intercambio de la información y los datos obtenidos acerca de la contaminación del medio marino». Aunque estos artículos, consistentes con el objeto de la UNCLOS, están principalmente concebidos para la seguridad frente a accidentes y fenómenos de la naturaleza, su extrapolación a la seguridad frente a acciones deliberadas del hombre parece lógica.

[2] Terminados los trabajos de desarrollo, el 1 de abril de 2019 comienza un periodo de transición de dos años de duración hasta su plena implantación.

Por su parte, y más literalmente aplicable al asunto que nos ocupa, el Convenio para la Represión de Actos Ilícitos contra la Seguridad de la Navegación Marítima (*Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation o SUA Convention*) dice en su artículo 13: «Los Estados Partes cooperarán en la prevención de los delitos enunciados en el artículo 3, en particular: a) adoptando todas las medidas factibles a fin de impedir que se prepare en sus respectivos territorios la comisión de dichos delitos, tanto dentro como fuera de ellos; b) intercambiando información, de conformidad con su legislación interna, y coordinando medidas administrativas y de otra índole adoptadas, según proceda, para impedir que se cometan los delitos enunciados en el artículo 3»[3]. Obsérvese que aquí sí habla directamente de delitos, no meramente de accidentes.

Todo ello son obligaciones que tienen que ser respetadas de buena fe, pero que están sujetas a ciertas restricciones, tales como las impuestas por la seguridad nacional, soberanía o confidencialidad comercial. Esas restricciones se mencionan indirectamente en el Convenio SUA en su ya citado artículo 13 («de conformidad con su legislación interna»), y en la UNCLOS artículo 302 («nada de lo dispuesto en ella se interpretará en el sentido de exigir que un Estado Parte, en el cumplimiento de las obligaciones que le incumban en virtud de la Convención, proporcione información cuya revelación sea contraria a los intereses esenciales de su seguridad»).

Pero estas limitaciones están atemperadas en nuestro caso, en primer lugar, por el hecho de que los actores son agencias de la ley u otras agencias del gobierno, lo que asegura que no debe haber beneficio personal o de otro modo ilegal en el uso de la información; y en segundo, y en nuestro inmediato ámbito internacional, por la común pertenencia de los participantes a la Unión Europea, lo que garantiza una muy importante comunidad de intereses, objetivos y actitudes.

Hay otras posibles restricciones más concretas:

- el secreto judicial, que puede ser decretado por un juez sobre ciertas actuaciones concretas, evidentemente una restricción insuperable, pero infrecuente y limitada en amplitud;

[3] Básicamente, y resumiendo una detallada casuística, el artículo 3 de la SUA describe los delitos de piratería, terrorismo y otros actos violentos cometidos contra buques o personas a su bordo.

- la confidencialidad comercial, p.e., el legítimo deseo de los armadores, particularmente de buques dedicados al comercio «tramp», de que sus competidores no sepan sus movimientos, pero de nuevo, los actores en cuestiones de intercambio de información son agentes de la ley, por lo que en principio no se beneficiarían de este conocimiento;
- las obligaciones contractuales, como las que imponen compañías de satélites de no compartir con terceros la información satelital obtenida (y eliminar así potenciales clientes para la misma información, lo que ocurre incluso con diferentes clientes que pertenecen al mismo estado, o a los distintos organismos de la Unión Europea), pero esto se puede remediar enmendando los contratos, borrando la cláusula y tal vez compensándola con un incremento en el precio, que podría ser enjugado por aquellas terceras partes, potenciales clientes individuales.

Naturalmente, una cosa es concebir la idea y otra aplicarla. Y su aplicabilidad suscita muchas preguntas que se pueden resumir en una: ¿cómo se puede asegurar—careciendo de poderes coercitivos— la adhesión de todos los participantes en una particular red de información, en este caso el CISE, al principio RTS? El asunto es más peliagudo de lo que parece. En efecto, la aplicación de NTK está basada esencialmente en la prohibición: «no compartir a menos que…». En cambio, RTS se basa en el estímulo positivo: «compartir a menos que…». Pero sucede que las prohibiciones son más fáciles de codificar y hacer cumplir que las normas positivas, aunque solo sea porque las prohibiciones tienden a ser universales y permanentes, mientras que las normas positivas están usualmente condicionadas a ciertas circunstancias. Así, es fácil prohibir cruzar la calle con el semáforo en rojo bajo pena de multa, pero eso mismo no se puede expresar como la obligación de cruzar en verde, ni mucho menos penalizar su incumplimiento, porque otras circunstancias que deben ser concurrentes pueden no concurrir, como la necesidad o el simple deseo de una persona de cruzar en un momento determinado.

De manera similar, una regla según la cual una agencia tiene prohibido compartir información con otra es más simple de enunciar y hacer cumplir que otra norma que estipule que la información debe ser compartida, lo que debe acompañarse de ciertas condiciones, tales como nivel de protección, asunto, inmediatez, etc. Existen también factores culturales que suelen trabajar en dirección a la restricción. Las agencias policiales suelen resistirse a compartir información que podría comprometer sus fuentes

o el rastro probatorio, además de que tienden a mantener la integridad de la operación, sin compartirla con otra fuerza policial que pudiera competir con ellos en prestigio o en el presupuesto del año próximo. Tal es la resistencia que incluso la situación general, que a menudo podría ser duplicada con fuentes abiertas, es a menudo clasificada de confidencial.

Esta dificultad para imponer una norma positiva se manifiesta incluso cuando, excepcionalmente, resulta fácil de codificar. Dentro del ámbito marítimo que es el que aquí nos ocupa, existe una norma positiva, claro ejemplo de ejercer la responsabilidad de compartir que, sin embargo, es rutinariamente ignorada en la mayor parte de las marinas militares de nuestro entorno, ciertamente incluida la Armada. Recientemente, en el transcurso de un año y medio, han sucedido cuatro notorias colisiones en la mar en las que uno de los actores ha sido un barco de guerra: *USS Lake Champlain* (mayo 2017), *USS Fitzgerald* (junio 2017), *USS John S. McCain* (agosto 2017), y *KNM Helge Ingstad* (noviembre 2018), con el resultado total de 17 muertos y uno de los barcos hundidos (el *Helge Ingstad*). Las cuatro parecen haber tenido una característica en común: ninguno de los cuatro barcos tenía activado el *Automatic Identification System* (AIS), moderno sistema de seguridad obligatorio para todos los buques de más de 300 Tm, cuyo principal objeto es evitar las colisiones entre buques, y esa falta contribuyó a crear la situación que terminó en colisión[4]. Los buques de Estado, y entre ellos los de guerra, están exentos de la obligación de llevar el AIS activado, en la idea de que algunas de sus misiones pueden aconsejar que su presencia sea inadvertida. Pero exención de la obligación de llevarlo encendido no es lo mismo que obligación de llevarlo apagado, y es fácil comprender que llevarlo apagado hoy en día, cuando todo el tráfico lo lleva activado, crea una situación de peligro superior a la prevalente cuando nadie lo usaba porque no existía, no hace tanto tiempo. Se entiende la exención de obligatoriedad, pero ello debe reservarse para cuando es realmente necesario, por ejemplo, en tiempo de guerra o llevando a cabo una operación policial que requiere sigilo. Llevarlo apagado por rutina es una grave imprudencia como los accidentes mencionados atestiguan.

Creo que la inusual facilidad de codificar esta norma positiva que, sin perjudicar en circunstancias normales la persecución del delito, mejora la seguridad frente a

[4] Al menos uno de ellos (*KNM Helge Ingstad*) conectó el AIS inmediatamente después de la colisión, cuando ya no era necesario pues la identificación había sido «al tacto», una clara indicación de mala conciencia.

accidentes, pone muy bien de manifiesto las dificultades que presenta la implantación del RTS, que son aún mayores cuando la norma es más difícil codificación y que se resumen en una resistencia pasiva corporativamente extendida, enraizada en un sentimiento de privilegio al que es muy difícil renunciar.

En resumidas cuentas, todas las dificultades para la implantación de la norma RTS son objetivamente superables, pero dependen en gran medida no solo de una correcta articulación de los qué, cómo y para qué, sino sobre todo de la buena voluntad de los participantes. Este es el factor que puede convertirlo en un éxito o en un fracaso, sea en el ámbito marítimo donde ya está formalmente implantado, pero aún sin experiencia, como con más motivo en otro cualquiera donde habrá que empezar desde cero. Porque RTS no tiene un procedimiento coactivo para forzar a su cumplimiento, como sí lo tiene NTK, por las razones que se han explicado antes. Algunos lo han caracterizado como «obligación moral», o como «ley suave» (*soft law*), calificativos que no hacen nada por mejorar sus expectativas de adopción sincera por parte de las agencias de la ley.

Pero este es un aspecto que solo el tiempo y el esfuerzo lograrán resolver. Un ambiente de confianza mutua solo puede empezar a consolidarse cuando un participante, el primero, actúa con confianza en los demás. Para apuntalar el necesario «contagio» del virus de la confianza la única herramienta posible es exponer al escrutinio público el grado de devoción de cada participante, denunciando públicamente —dentro del ámbito de que se trata— a los que son solo o principalmente «consumidores» de información, pero no contribuyentes. Una eventual expulsión del sistema a los recalcitrantes –la única medida punitiva posible– podría ser considerada, pero las dificultades para su aplicación pueden ser importantes, pues en lo tocante a seguridad nadie debería ser excluido por desganada que sea su participación. Al menos, en el ámbito del CISE, se pretende publicar periódicamente estadísticas de la información compartida, o meramente aprovechada, por cada uno de los participantes, y llevar a cabo auditorías detalladas de cumplimiento.

Lo que en ningún caso se puede permitir es una repetición de esos «colapsos de comunicaciones» que permitieron los terribles atentados que han sacudido nuestras sociedades estos últimos años. Todas las dificultades, culturales, corporativas, legales o comerciales, deberán ser superadas si queremos perseguir eficazmente a los terroristas y otros criminales, o, más importante aún, adelantarnos a sus siniestros planes. Al igual

que el CISE ha incorporado el *responsibility to share* entre sus principios básicos, las organizaciones que trabajan en otros ámbitos no marítimos, en España y en el resto de Europa, deberían también adoptarlo. Incrementar la confianza mutua entre las agencias de la ley y de inteligencia, nacionales y europeas, debe ser un objetivo irrenunciable. El ámbito marítimo lo ha comenzado con el CISE, los demás deben seguir.

*Fernando del Pozo**
Almirante (Ret.)
Director de Wise Pens International Ld