Cuadernos de la Guardia Civil

Revista de Seguridad Pública

Núm. 57-2018

GOBIERNO DE ESPAÑA
MINISTERIO DEL INTERIOR
GUARDIA CIVIL
DIRECCIÓN GENERAL

CUADERNOS DE LA GUARDIA CIVIL

REVISTA DE SEGURIDAD PÚBLICA

3ª ÉPOCA

Centro de Análisis y Prospectiva de la Guardia Civil
Guzmán el Bueno, 110
28003 MADRID
Teléf. 91 514 29 56
E-mail: CAP-cuadernos@guardiacivil.org

AUTORA Y PROPIETARIA

Dirección General de la Guardia Civil
ISSN: 2341-3263
NIPO: 126-15-005-2

EDITA

Ministerio del Interior
Secretaría General Técnica
Dirección General de la Guardia Civil
Centro Universitario de la Guardia Civil

Página oficial de Cuadernos de la Guardia Civil
http://www.guardiacivil.es/es/institucional/Cuadernos_de_la_Guardia_Civil/index.html

Lista de los números en KOBLI
http://bibliotecasgc.bage.es/cgi-bin/koha/opac-shelves.pl?op=view&shelfnumber=59

Catálogo general de publicaciones oficiales
http://publicacionesoficiales.boe.es/

A lo largo de los años, la Guardia Civil ha venido haciendo una gran labor divulgativa con la publicación de la Revista de Estudios Históricos, lo que ha contribuido a la comprensión de su carácter, su tiempo, sus actividades y funciones.

Desde 1989 este esfuerzo en difusión de cultura de seguridad ha desembocado en la elaboración de los "Cuadernos de la Guardia Civil".

Se trata de una publicación académico profesional, de contenidos originales y periodicidad semestral, con contenidos relevantes sobre seguridad nacional, seguridad pública, técnica policial, riesgos y amenazas, en todas sus dimensiones (histórica, jurídica, estratégica, táctica, etc.). Los géneros documentales admitidos son los artículos de investigación, los artículos profesionales, y la reseña de libros. Los destinatarios son expertos en seguridad, académicos y profesionales, tanto del sector público y privado, estudiantes, así como cualquier ciudadano interesado en la materia.

Cuadernos de la Guardia Civil está abierta a cualquier autor, a cuyos efectos se establecen dos periodos para la recepción de artículos: el 1 de junio y el 1 de diciembre. El primer número de cada año se publica durante el mes de febrero, y el segundo durante el mes de octubre. Se pueden publicar adicionalmente números especiales o suplementos. Los artículos propuestos serán enviados respetando las normas de publicación que figuran al final del número. Las propuestas se pueden enviar en formato electrónico a: CAP-cuadernos@guardiacivil.org

La evaluación y selección de los artículos se realiza previa evaluación mediante un sistema por pares, en el que intervienen evaluadores externos a la editorial, y posterior aprobación por el Consejo Editorial. Los artículos pueden ser escritos en español, inglés o francés.

La Revista Cuadernos de la Guardia Civil se compromete a mantener altos estándares éticos, y especialmente el "Code of conduct and best practices guidelines for journal editors" del Committee on Publication Ethics (COPE).

Los contenidos de la Revista Cuadernos de la Guardia Civil se encuentran referenciados en los siguientes recursos de información: LATINDEX, DICE (Difusión y Calidad Editorial de las Revistas Españolas de Humanidades y Ciencias Sociales y Jurídicas) y DIALNET.

Especial referencia merece su inclusión en el sistema bibliotecario de la Administración General del Estado, a través de la Plataforma KOBLI:

http://bibliotecasgc.bage.es/cgi-bin/koha/opac-shelves.pl?op=view&shelfnumber=59

Este servicio permite consultar y realizar búsquedas por cualquier criterio bibliográfico (autor, tema, palabras clave…), generar listas. Permite la descarga en formatos PDF, Mobi y Epub. Adicionalmente es posible la suscripción a un sistema de alerta, cada vez que se publique un nuevo número, solicitándolo a la cuenta : CAP-cuadernos@guardiacivil.org.

ÍNDICE

ARTÍCULOS

RESEÑA DE LIBROS

CIBERINTELIGENCIA, LA VÍA PARA LA CIBERSEGURIDAD

JOSÉ MARÍA BLANCO NAVARRO

DIRECTOR DE CIBERINTELIGENCIA ESTRATÉGICA EN PROSEGUR CIBERSEGURIDAD

RESUMEN

Internet y las Tecnologías de la Información y las Comunicaciones han contribuido decisivamente al desarrollo de nuestras sociedades. Organizaciones, empresas y ciudadanos cuentan con nuevas vías, eficientes, para comunicarse, relacionarse y prestar servicios. Pero a su vez, las nuevas tecnologías son explotadas por delincuentes, terroristas y grupos de crimen organizado, siendo Internet el objetivo de sus actividades, el medio o un facilitador de las mismas. En este marco, las empresas se ven obligadas a adoptar medidas para proteger sus valores: personal, infraestructura, patrimonio, datos e información, procesos de negocio y reputación.

Internet y las TIC se han convertido en un medio para la delincuencia tradicional, a la vez que un habilitador para nuevas actividades criminales. Las tecnologías de la información y comunicación permiten a las organizaciones criminales financiarse, adoctrinar y reclutar, gestionar su logística, blanquear capitales, planear ataques, cometer nuevos y viejos delitos de forma anónima, actuando como emprendedores delictivos en el marco de un modelo de negocio que se ha denominado “crimen como servicio”, sin necesidad de una fuerte infraestructura.

La nueva Estrategia de Seguridad Nacional (ESN) de 2017 es sensible a esta situación. En el capítulo 4, **considera como amenaza la vulnerabilidad del ciberespacio.** Las amenazas en el espacio digital son transversales, sirviendo el ciberespacio como facilitador y potenciador de gran parte del resto de amenazas (terrorismo, conflictos, crimen organizado, espionaje, inestabilidad económica, etc.).

A través de la identificación de las principales tendencias, se mostrará cómo la ciberinteligencia se convierte en la vía hacia la ciberseguridad, detallando su conceptualización, que carece de consenso, su proceso, y sus elementos y metodologías.

Palabras clave: Ciberseguridad, ciberinteligencia, tendencias, ciberespacio, amenazas, riesgos

ABSTRACT

The Internet and Information and Communication Technologies have made a decisive contribution to the development of our societies. Organizations, companies and citizens have new efficient ways to communicate, interact and provide services. But in turn, new technologies are exploited by criminals, terrorists and organized crime groups, with the Internet being the target of their activities, the medium, or a facilitator of them. In this framework, companies are forced to adopt measures to protect their values: personnel, infrastructure, assets, data and information, business processes and reputation.

The Internet and ICT have become a means of traditional crime, as well as an enabler for new criminal activities. Information and communication technologies allow criminal organizations to finance, indoctrinate and recruit, manage their logistics, launder money, plan attacks, commit new and old crimes anonymously, acting as criminal entrepreneurs within the framework of a business model that has been called “crime as a service”, without the need for a strong infrastructure.

The new National Security Strategy (ESN) of 2017 is sensitive to this situation. In chapter 4, it considers the vulnerability of cyberspace as a threat. Threats in the digital space are transversal, serving cyberspace as a facilitator and enhancer of many of the other threats (terrorism, conflicts, organized crime, espionage, economic instability, etc.).

Through the identification of the main trends, it will be shown how cyber-intelligence becomes the path towards cybersecurity, detailing its conceptualization, which lacks consensus, its process, and its elements and methodologies.

Keywords: Cybersecurity, Cyber-intelligence, trends, Cyberspace, threats, risks

1. TENDENCIAS EN CIBERSEGURIDAD

1.1. CONCIENCIACIÓN

El año 2017 resultó positivo en materia de concienciación, con la inestimable ayuda, a este fin, de Wannacry (12 de mayo) y su elevado impacto mediático. Incluso la reacción de Telefónica supuso un importante punto de inflexión en el tratamiento de estos riesgos. No fue el único caso, dado que meses después NotPetya (27 de junio) ponía de nuevo el foco internacional en los ciberataques. A ello se unen brechas de seguridad como la de Equifax, los denominados “Paradise Papers”, los casos Uber, Verizon, y una larga serie de incidentes (Online Trust Alliance, 2018).

Los ataques ejecutados en 2017 han servido para extraer importantes lecciones, que precisan ser incorporadas al acervo de ciberseguridad como “lecciones aprendidas”. El caso Equifax, en el que se expusieron los datos financieros de 143 millones de estadounidenses, muestra cómo las empresas que no protejan a sus clientes se exponen a acciones legales, a sanciones de reguladores y a un elevado impacto reputacional. Una segunda lección, derivada de dicho caso, es la necesidad de reevaluar qué se considera información sensible a proteger.

Wannacry y NotPetya fueron una llamada de atención, con varias enseñanzas: la función de los proveedores, en este caso Microsoft, para mejorar la ciberseguridad (en marzo había publicado actualizaciones que solventaban la vulnerabilidad que posteriormente fue explotada); la responsabilidad compartida entre empresas de tecnología y toda la cadena del sistema, incluyendo a proveedores, resto de *stakeholders*, clientes; y la necesidad de emprender una nueva Convención Digital de Génova, llamada que hizo Microsoft en febrero de 2017 para analizar la situación actual (Microsoft, 2017).

También de interés, a la hora del necesario aprendizaje, tuvieron los ataques de denegación de servicio (DDoS) del 21 de octubre, que afectaron a Amazon, Twitter, Netflix y GitHub, a través de la utilización de una red de bots de internet de las cosas, Mirai (USENIX, 2017).

A pesar de todo ello, el nivel de alerta del usuario (*"user awareness"*) continúa siendo muy bajo, un claro facilitador de la perpetuación de este tipo de ataques, más cuando se estima que en el 95% de los mismos la clave radica en el factor humano.

En el futuro se espera la llegada de nuevos "ciber-huracanes", utilizando el término empleado en el "MMC Cyber Handbook 2018". Cualquier organización debe asumir que va a ser atacada, siendo la única duda en qué momento se producirá dicho ataque.

1.2. REGULACIÓN

Organismos internacionales y Estados comienzan a ser conscientes de los riesgos del ciberespacio. La nueva Estrategia de Seguridad Nacional dedica varias reflexiones acerca de las denominadas amenazas híbridas, aquellas que combinan diferentes formas de ataque, tradicionales y no tradicionales, como los ciberataques o la manipulación de la información. Recoge, de esta manera, uno de los mayores riesgos a los que se están enfrentando las democracias en todo el mundo, procesos de desestabilización promovidos desde el exterior, por actores tanto estatales como no estatales, y que tratan de polarizar y fragmentar nuestras sociedades. Ataques que suponen una amenaza, que pudiera ser de carácter existencial, y que exigen una rápida reacción.

Sobre este tipo de acciones ya existían advertencias, como las de John Arquilla y David Ronfeldt a finales del siglo pasado en *"Networks and Netwars"* (2001) *o en "The Advent of Netwar"* (1996*).* Pero lo que es más llamativo, también lo anunciaron los coroneles chinos Qiaio Liang y Wang Xiang Sui, en su "*Guerra sin límites"* (1999*),* libro dirigido a explicar a sus compañeros de armas las características de la *guerra* moderna. En esa obra detallaban toda una estrategia tendente a derrotar al enemigo sin derramar su sangre, a través del ataque económico o el uso de la información. El objetivo que manifiestan es *"la destrucción estructural del enemigo".* Cualquier cosa puede ser un arma y cualquier individuo un soldado.

Los frentes regulatorios se centran en el conocimiento y registro de los ataques, en la protección de los datos personales y en la generación de estándares. En las XI Jornadas del CCN-CERT (2017), que bajo el lema "Ciberamenazas, el reto de compartir", reunió a cerca de 2.000 profesionales de la ciberseguridad en diciembre de 2017, se hizo un claro diagnóstico de la situación, mostrando una decidida voluntad en afrontar la situación y en devolver al ciudadano parte del poder que el uso de sus datos está generando a organizaciones, delictivas o no. En 2018 está prevista la creación de un Centro de Operaciones de Seguridad de la Administración General del Estado, que permita ofrecer una respuesta "más eficaz" ante las ciberamenazas.

Entre las prioridades en materia de ciberseguridad proteger la privacidad, facilitar el derecho al olvido en la Red, garantizar el honor y la intimidad, así como la defensa de la propiedad intelectual y la detección y defensa ante la desinformación, propaganda y la manipulación informativa.

Aunque en el tema de desinformación algunos sectores señalan que se puede tratar de justificar por esa vía un control de la libertad de expresión y de información, es evidente que se trata de cuestiones diferentes. La diversidad informativa, la existencia de medios con orientación política, y por tanto con sesgos informativos, no es un fenómeno nuevo. Y además es un fenómeno necesario, un pilar básico en un sistema

democrático. Pero en este caso el foco se pone básicamente en ataques desde el exterior, con la clara intención de desestabilizar el sistema democrático.

A todo ello se ha unido el debate sobre el odio en internet y redes sociales, con propuestas regulatorias para identificar a los usuarios (identidad digital). Otra tendencia en materia regulatoria puede ser la adopción de reglas para prevenir el pago de *ransomware*.

La entrada en vigor, en mayo de 2018, de la normativa de la Unión Europea de protección de datos personales, es, posiblemente, la gran revolución en materia regulatoria del año, generando dudas sobre las capacidades para su cumplimiento, gestión y supervisión. Su entrada en vigor va a exigir a las empresas esfuerzos y costes adicionales, en mayor medida en cuanto exista voluntad para actuar correctamente, concienciados sobre la importancia de la protección de los datos y no únicamente como la necesidad de satisfacer un requisito legal más. Las empresas se moverán entre el temor y la desorientación.

Entre sus contenidos destaca:

- La obligación de informar de violaciones de seguridad de datos a las autoridades nacionales, e incluso a los individuos, cuando el daño sea elevado, en un plazo de 72 horas. Su incumplimiento puede suponer multas de un 4% de los ingresos de la compañía (lo que puede poner en riesgo incluso su supervivencia). Marsh & McLennan Companies estima que las multas en el primer año podrían alcanzar los cinco billones de libras. El alto importe de las multas pudiera llegar a incentivar ataques a bases de datos empresariales con finalidad extorsiva.
- Se refuerzan los derechos de los individuos, en el uso de sus datos. Ninguna empresa podrá obtener datos personales sin notificar previamente a los individuos como serán almacenados, protegidos y compartidos con terceras partes. Su consentimiento debe ser libre, específico, informado e indudable, y marcándolo de forma afirmativa. También incluye el derecho al olvido, pudiendo solicitar en cualquier momento que sus datos sean borrados y no utilizados, o incluso su portabilidad.
- La figura del delegado de protección de datos adquiere una enorme relevancia.
- Su impacto sale del ámbito de la propia UE, al intentar involucrar a cualquier organización que obtenga o utilice datos personales de individuos sujetos a la jurisdicción de la UE.
- Las organizaciones están obligadas a realizar evaluaciones de impacto de datos, de carácter previo. No existiendo una cultura empresarial, salvo en ámbitos determinados, de evaluación de riesgos, puede suponer un verdadero quebradero de cabeza, especialmente para PYMES, a pesar del desarrollo de aplicaciones de la AEPD para facilitar el cumplimiento de este requisito, como “Facilita RGPD”.

Por otro lado, la Directiva de Seguridad de redes de Información (NIS- Network Information Security, 2016), que debería tener efecto en 2018, impone obligaciones a los Estados y operadores de infraestructuras: disponer de una estrategia de ciberseguridad, una autoridad competente nacional, existencia de Equipos de Respuesta a Incidentes de Seguridad Informática (CSIRT), e identificación por los Estados de los

Operadores de Servicios Esenciales (OSE) y los Proveedores de Servicios Digitales (PSD) establecidos en su territorio para cada sector. España aún no ha aprobado la trasposición interna que la UE fijó con fecha 9 de mayo como límite, aunque ya dispone de un borrador de Anteproyecto de Ley sobre la Seguridad de las Redes y Sistemas de Información. El Anteproyecto ha sido ya informado por el Consejo Nacional de Ciberseguridad, ha incorporado aportaciones del proceso de consulta previa y prosiguió su tramitación mediante la apertura del período de audiencia pública que se extendió hasta el 8 de enero de 2018.

Como efecto de la señalada concienciación, la Unión Europea ha desarrollado una intensa labor en los últimos meses de 2017, con medidas de gran calado, proponiendo reforzar la resiliencia, la disuasión y la respuesta de la UE a los ciberataques mediante:

- Establecimiento de una Agencia de Ciberseguridad de la Unión Europea más sólida, basada en la Agencia para la Seguridad de las Redes y la Información (ENISA), para ayudar a los Estados miembro a abordar los ciberataques (Parlamento Europeo, 2018).
- Creación de un esquema de certificación de ciberseguridad en toda la UE, que aumente la ciberseguridad de los productos y servicios en el mundo digital. La Comisión propone la creación de un marco europeo de certificación de ciberseguridad que se espera que ofrezca numerosos sistemas europeos de certificación de ciberseguridad individual, es decir, descripciones claras de los requisitos de seguridad que deben cumplir los productos, sistemas o servicios. Cumplir los nuevos requisitos facilitaría a las empresas el comercio transfronterizo y que los compradores comprendan las características de seguridad de los productos o servicios. Los ciudadanos y los usuarios finales de los productos, los proveedores de productos y los gobiernos nacionales serán los beneficiados del marco de certificación. La certificación desempeña un papel fundamental para aumentar la confianza y la seguridad en los productos y servicios que son cruciales para el mercado único digital. Sin un marco común para los esquemas de certificados de ciberseguridad válidos en toda la UE, existe un riesgo creciente de fragmentación y barreras en el mercado único. ENISA implementará este proceso de certificación. El uso del marco de certificación no es obligatorio a menos que esté prescrito en la futura legislación de la UE, sin embargo, habrá un incentivo para certificar la calidad y seguridad. Existen algunos esquemas de certificación en la UE, tales como el Commercial Product Assurance (CPA), desarrollado en el Reino Unido, la Certificaction Sécuritaire de Premier Niveau (CSPN), en Francia, o el Dutch Baseline Security Product Assessment (BSPA), en los Países Bajos.
- Un plan detallado de cómo responder de manera rápida, operativa y al unísono cuando ocurre un ciberataque a gran escala.
- Una red de centros de competencia en los Estados miembro y un Centro Europeo de Investigación y Competencia en Ciberseguridad, que ayudará a desarrollar y desplegar las herramientas y la tecnología necesarias para mantenerse al día con una amenaza en constante cambio y garantizar que nuestra defensa sea lo más fuerte posible.
- Una nueva Directiva sobre la lucha contra el fraude y la falsificación de los medios de pago distintos del efectivo para proporcionar una respuesta más

eficaz del Derecho penal al delito cibernético. El fraude de pago no en efectivo puede tomar diferentes formas. Los delincuentes pueden desencadenar la ejecución de pagos utilizando la información del pagador obtenida a través de, por ejemplo, suplantación de identidad, robo u obtención de información en sitios web dedicados que venden credenciales de tarjetas de crédito robadas en la *Darknet*. Los pagos también pueden ejecutarse fraudulentamente mediante tarjetas falsificadas o robadas, utilizadas para pagar en tiendas o retirar efectivo en cajeros automáticos o mediante el pirateo de sistemas de información para procesar pagos, por ejemplo, alterando los puntos de venta para transacciones con tarjeta o aumentando ilegalmente los límites de la tarjeta de crédito que permita que los gastos excedentes no sean detectados. La normativa actual no refleja las realidades del momento y no será suficiente para abordar los nuevos desafíos y desarrollos tecnológicos tales como monedas virtuales y pagos a través del móvil.

- Un marco para una respuesta diplomática conjunta de la UE a actividades cibernéticas maliciosas y medidas para reforzar la cooperación internacional en ciberseguridad, incluida la profundización de la cooperación entre la UE y la OTAN.
- El objetivo de impulsar el desarrollo de habilidades de alto nivel para los profesionales civiles y militares a través de la provisión de soluciones para los esfuerzos nacionales y la creación de una plataforma educativa y de capacitación en defensa cibernética.

1.3. HIBRIDACIÓN ENTRE LO FÍSICO Y LO LÓGICO

Las amenazas en el espacio digital son transversales, el ciberespacio sirve de facilitador y potenciador de gran parte del resto de amenazas que se plantean en el campo físico, y su carácter es global. El ciberespacio es una dimensión desde la que se generan riesgos en cualquiera de los ámbitos que señala, por ejemplo, la Estrategia de Seguridad Nacional (2017): terrorismo, crimen organizado, estabilidad económica, espionaje, conflictos, etc.

En el ámbito empresarial, y especialmente en procesos de internacionalización, ha aumentado la concienciación sobre cómo el ciberespacio es un ámbito que genera riesgos a la seguridad física de infraestructuras, y del personal y directivos. Las empresas, en esos procesos de internacionalización, no pueden dejar de acudir a zonas de conflicto, pero de enorme interés empresarial. Pero esos procesos deben contar con unos requisitos básicos de seguridad, y un conocimiento sociocultural. Cualquier tipo de riesgo para los desplazados (atentado, agresión, secuestro, asaltos y robos, robo de datos) y para las propias empresas (por rechazo a la presencia de empresas internacionales, por las características del negocio y posible oposición de comunidades y minorías) cuenta en el ciberespacio con un riesgo adicional. En el caso de autoprotección de los trabajadores, la actividad en Internet y redes sociales exige una "higiene" básica.

El reciente caso del secuestro del experto en criptomonedas y alto cargo de la compañía de intercambio de criptomonedas EXMO, Pavel Lerner, es paradójico, tras ser liberado después de pagar un millón de dólares en bitcoins.

Durante muchos años el pensamiento colectivo ha venido separando los impactos de la acción en ciberespacio y en el espacio físico. Nunca ha sido así, pero cada vez lo será menos.

Por otra parte, a la hora de entender algunos ciberataques es preciso disponer de un fuerte bagaje en geopolítica, geoeconomía y geoestrategia. Conflictos, procesos electorales, inversiones internacionales, alianzas, licitaciones internacionales, son cuestiones que pueden ser coetáneas a determinados tipos de ataques.

1.4. TENDENCIAS EN EL SECTOR/MERCADO

En todos los ámbitos se señala que, como ha comenzado a suceder en 2017, la ciberseguridad preocupará más a la dirección de las empresas. Siendo cierto, los comentarios de muchos directores de seguridad indican que la situación actual aún está lejos de lo deseable, al continuar percibiendo la seguridad como un coste. Pero la seguridad, y la ciberseguridad, seguirán cotizando en Bolsa. Al igual que las empresas que no son responsables socialmente o se ven involucradas en casos de corrupción ven afectadas sus cuentas de forma drástica, lo mismo sucederá con las empresas que no se muestren seguras en la gestión de datos e información de sus clientes y proveedores.

Gartner predice que en 2018 se producirá un incremento del gasto en ciberseguridad de un 8%, alcanzando los 96 billones de dólares (eSP European Solution Providers, 2018). A este crecimiento contribuye el nuevo marco regulador, además de los impactos de los ataques conocidos en 2017. La predicción de esta empresa para 2020 apunta a un incremento de un 35%, con más del 60% de las empresas invirtiendo en herramientas para seguridad de los datos, prevención de fugas de información, encriptación y auditoría.

Continuará el proceso de outsourcing de tareas a proveedores MSSPS (Managed Security Service Provider) y SaaS (Software as a Service). Gartner estima un gasto de 18,5 billones en 2018 un 11% más que en 2017.

Otro sector afectado será el de los ciberseguros, actor clave en la gestión de las ciberamenazas.

También a nivel organizacional se endurecerá la guerra por el talento en ciberseguridad, ante la elevada demanda de profesionales y la necesidad de incorporar perfiles multidisciplinares. Según ISACA, en 2019 se precisarán dos millones de nuevos empleos en ciberseguridad.

2. CIBERAMENAZAS

Para afrontar este apartado es preciso realizar una clasificación de las mismas. La Estrategia Nacional de Ciberseguridad (2013), pendiente de próxima actualización, contenía una clasificación confusa, en la que mezclaba riesgos y actores. A efectos de este trabajo vamos a considerar la siguiente tipología: cyberwarfare (ámbito político/económico y espionaje), ciberdelincuencia y ciber crimen organizado, terrorismo, sabotajes y hacktivismo (y aunque no sea tratado en el presente artículo, aquellas situaciones no controlables de fallos de sistema y accidentes y catástrofes).

Todo ello sin perder de vista que las fuentes de amenaza serán los Estados, actores no estatales al servicio o no de Estados, grupos criminales, grupos terroristas, hackers, hacktivistas o los denominados *insiders*.

2.1. CYBERWARFARE

Existiendo multitud de definiciones optamos por la combinación del US Department of Defense y las enseñanzas de Sun Tzu, para considerar cyberwarfare "al arte y la ciencia de lucha sin luchar, de derrotar al enemigo sin derramar su sangre".

Desde el ciberespacio se desarrolla una clara guerra política y económica, siendo la tecnología parte de ese engranaje. Así lo entendió Francia, por ejemplo, cuando en el año 1997 decidió crear una Escuela de Guerra Económica. La denominada inteligencia económica es una cuestión de Estado, centrada en la defensa de los intereses estratégicos nacionales, y a desarrollar en continua relación de confianza con las empresas.

El concepto de posverdad, tan de moda, ha puesto en evidencia cómo el ciberespacio, apoyado en desarrollos tecnológicos, se utiliza al servicio de procesos de engaño, decepción o manipulación, invocando a las emociones por encima de los hechos con ánimo desestabilizador, con la intención de polarizar la sociedad, de favorecer posturas radicales o extremistas desde el exterior, e influir y afectar a los procesos electorales.

El hecho es que las denominadas "fake news" funcionan, básicamente debido al sesgo de confirmación. Los seres humanos hacen suyas inmediatamente piezas de información, aunque sea falsa, que reafirme sus creencias. Todo ello lleva a pensar en la continuidad y crecimiento de este tipo de desinformación, a pesar de toda una serie de acciones desencadenadas para su control (fact-checks, concienciamiento de medios de comunicación tradicionales, sistemas de evaluación de información, compromiso de operadores para su detección, utilización de algoritmos o iniciativas educativas).

En este ámbito político-económico podríamos incluir también el espionaje, una cuestión tradicional que, en el día a día, sigue mostrando elevada casuística.

2.2. CIBERDELINCUENCIA Y CIBER CRIMEN ORGANIZADO

En este apartado asumimos las consideraciones del jefe del Grupo de Delitos Telemáticos de la Guardia Civil, que habitualmente destaca la necesidad de diferenciar ciberdelincuencia de cibercrimen organizado. No le falta razón, puesto que en la seguridad tradicional siempre se ha tratado de diferenciar entre ambos ámbitos. Todo ello asumiendo que posiblemente la definición de Europol de crimen organizado no encaje perfectamente para definir este nuevo y adaptativo cibercrimen organizado.

A estos efectos, Cohen y Blanco (2016), diferenciaban cómo se configuraba el crimen organizado tradicionalmente y cómo está sucediendo en la actualidad, especialmente debido a la utilización de Internet y las TIC:

Figura 1. Configuración actual del crimen organizado. Blanco y Cohen, 2016

El año 2018 seguirá presentando malware (que actuará en función de criterios de oportunidad), casos de extorsiones digitales, robos de identidad, el denominado fraude al CEO (que según Trend Micro supone nueve billones al año), ransomware en versiones RaaS (ransomware as a service), troyanos financieros, phishing, smishing, etc.

El "Cybercrime as a Service", que adopta modelos de gestión empresarial, es actualmente uno de los mayores negocios del mundo, junto a los tráficos ilícitos (armas, drogas y personas). El modelo Crime as a Service, potenciará el recurso a sistemas de croudsourcing criminal. Un claro ejemplo está en los ataques bancarios para obtener credenciales de tarjetas bancarias, que posteriormente son impresas por organizaciones criminales en diferentes países, y a su vez vendidas a otros grupos que acuden a los cajeros para extraer fondos. O con otras formas de atacar cajeros automáticos, ofreciendo cibercriminales "malware-as-a-service" en foros de deepweb, con manuales, videos y aplicaciones para acceder a los mismos. Quien paga por ese servicio solo tiene que elegir un cajero y seguir las instrucciones. Este modelo de negocio hace accesible la introducción en el cibercrimen de individuos no profesionales en nuevas tecnologías.

Los troyanos financieros son una buena fuente de ingresos para los criminales. Una vez infectado el equipo, y a través de "keylogging", roban las contraseñas tecleadas para acceder a los servicios bancarios. Utilizan técnicas sofisticadas, como técnicas "Man-in-the-Browser" (MiB), como "web injections" o redirecciones para ocultar operaciones. La proliferación de la banca a través del móvil ha afectado a ese negocio ilegal, que buscará cómo llevar sus ataques a esas plataformas móviles.

El recurso de muchas organizaciones a aplicaciones "serverless" amplifica también la superficie de ataque. Una vulnerabilidad es el tránsito de datos a través de una red, además de los niveles de privilegios que se definan. Este tipo de aplicaciones precisan unos protocolos de seguridad específicos y asegurar que el tráfico esté protegido por VPNs o encriptación. Igualmente, hay una ausencia de cultura de seguridad en aplicaciones Cloud, con las necesarias y pendientes políticas, procesos y controles.

El robo de más de dos billones de registros personales en 2017 será un factor clave para su utilización a lo largo de 2018 con diferentes fines. Y el robo masivo de datos personales, siguiendo casos como el de Equifax o Uber seguirá siendo un objetivo. El hacking de datos sanitarios seguirá creciendo.

El fraude al CEO o "Business e-mail compromise" es otra de las grandes fuentes de ingresos criminales y la tendencia apunta a un crecimiento, quizás matizado por un mayor perfilamiento de los objetivos.

Una tendencia será la especialización, con objetivos más dirigidos, ataques más sofisticados y elección de objetivos de mayor valor. El ransomware evolucionará de la extorsión a individuos hacia el ciber sabotaje y la disrupción de organizaciones. Investigadores de McAfee consideran a WannaCry, NotPetya u ONI como pseudo-ransomware, porque, aunque tengan parte de las características de dicha tipología delictiva su verdadero objetivo no es obtener rescates, sino actuar como pantalla de humo para la disrupción de los negocios, la exfiltración de datos o el robo de credenciales. El ransomware ha crecido un 2.000% en los últimos dos años.

Otra tendencia será la proliferación de ataques a criptomonedas, tanto al sistema que las soporta, como a las transacciones, los monederos y las personas. Según el Departamento de Seguridad Interior de Estados Unidos, un tercio de los intercambios de Bitcoin fueron hackeados entre 2009 y 2015, mientras que ha aumentado el número de ataques a inversores individuales. Los hackers han atacado a los intercambios, monederos, ICOs, Organizaciones Autónomas Descentralizadas, compañías de minería, servidores VP y servicios hosting. A finales de año el ataque a la compañía de minería NiceHash causó pérdidas de 60 millones de dólares. Es uno más de múltiples casos como el de Bitfinex (hackeo de 120.000 bitcoins, valorados en ese momento en 75 millones de dólares) o el de Mt. Gox (robo de 800 millones de dólares en Bitcoin). La empresa Chainalysis estima en 225 millones de dólares los robos a inversores en criptomonedas en 2017.

Internet de las Cosas, con la ilimitada expansión de productos conectados a la red (wearables, televisiones, frigoríficos, dispositivos de salud, juguetes...) llevará a que se amplifiquen los ataques a través de su utilización, por ejemplo, para DDoS. Pero también, y teniendo en cuenta el elevado coste de algunos dispositivos IoT para su secuestro virtual y petición de rescate. Los dispositivos IoT pueden permitir un permanente acceso de los criminales a la red de la víctima, generando puertas traseras en el sistema.

Se ha mencionado anteriormente el caso Mirai, una botnet que escaneaba continuamente dispositivos IoT con "user names" y claves de fábrica por defecto. Por esta vía se lanzaron potentes ataques DDoS. Symantec ha analizado las importantes vulnerabilidades de muchos dispositivos IoT (que no usan SSL, que permiten accesos por puertas traseras o que no disponen de actualizaciones de firmware encriptadas).

Los investigadores de Fortinet predicen que los criminales sustituirán botnets con clusters inteligentes de dispositivos comprometidos (hivenets), para lograr vectores de ataques más efectivos. "Hivenets" con capacidad de autoaprendizaje.

Toda la cadena de suministro seguirá siendo comprometida: proveedores, contratistas, socios, VIPS e individuos clave por acceso a información o credenciales. Los

cibercriminales detectarán el eslabón más débil de la cadena para lanzar el ataque y comprometer a la cadena completa.

Radware, finalmente, predice ataques a APIs, a proxy CDN (ataques a contenido dinámico, ataques DDos SSL-based, ataques a servicios no CDN, ataques directos a IP, ataques a aplicaciones web). Igualmente advierte de la automatización de la ingeniería social, el conjunto de técnicas utilizadas para engañar a individuos a efectos de obtener información o acceso a sistemas.

2.3. TERRORISMO

En el marco de los conflictos híbridos actuales no cabe descartar un avance en la confluencia de terrorismo y ciberataques.

A la hora de tratar el ciberterrorismo tenemos que separar dos cuestiones. La primera, el uso de internet y tecnologías de la información y las comunicaciones para favorecer sus actividades. La segunda, la realización de ciberataques o atentados apoyados desde el ciberespacio.

Sin duda Internet ha resultado un gran facilitador para el terrorismo. Una potente vía de comunicación, de carácter viral, a bajo coste, que permite la ubicuidad, la acción desde cualquier lugar y en cualquier momento y que facilita la ocultación del origen.

Frente a otros fenómenos, como el crimen organizado, la visibilidad y presencia es una característica propia del terrorismo. Es un acto de comunicación. Sin ello se diluyen sus efectos. Los grupos terroristas utilizan las redes para informar, adoctrinar, difundir sus mensajes y "éxitos", reclamar la autoría de los atentados, propaganda, captar y reclutar, planificar objetivos y atentados, formar y publicar tutoriales, etc. Pero es en la radicalización donde encuentran sus mayores ventajas, evitando el contacto físico y favoreciendo procesos de radicalización asistida (puesto que Internet no deja de ser interacción) y, en casos muy particulares, de autorradicalización.

Esa actividad de comunicación de grupos yihadistas era absolutamente libre y abierta hace años. La presencia de fuerzas y cuerpos de seguridad en internet y redes, especialmente desde los atentados de 2015, ha desplazado su acción hacia otras vías de comunicación, como la Deep Web, IRC o aplicaciones de telefonía móvil (especialmente Telegram). Pero, debido a esa necesidad de comunicar, siguen recurriendo a redes, foros y blogs clásicos. Los mensajes en aplicaciones móviles no permiten distribuir grandes documentos o videos, y cualquier link que se quiera compartir precisa de una web para su alojamiento. En ocasiones Twitter o Facebook sirven para una primera aproximación a objetivos para reclutamiento, vínculo que posteriormente se profundiza a través de Telegram.

En cuanto al segundo aspecto, la posibilidad de ciberatentados, sigue considerándose un hecho de baja probabilidad, alto impacto, pero quizás acortándose los plazos para su producción. El nivel técnico del denominado cibercalifato es muy bajo. Hasta el momento no se ha producido un ciberatentado, aunque sí pequeñas acciones de bajo impacto (denegación de servicios y acciones de hacking de bajo nivel). No son buenos ni programando, ni en malware (repletos de *bugs)*, encriptación, ni en acciones de hacking. A pesar de ello, oficiales de inteligencia de Estados Unidos han advertido

sobre la posible maduración de un cibercalifato, situación que en los últimos meses parece más controlada tras la caída de los feudos de Mosul y Raqqa del Daesh.

Quizás las acciones más preocupantes han sido acciones de hacking en las que han expuesto identidad y datos de personal vinculado a aparatos de seguridad. En todo caso, el escenario en el ciberespacio no es alentador, dada la facilidad para recurrir a herramientas, con dichos fines, creadas por grupos de crimen organizado (lo que se denomina *Crime as a Service),* que son efectivas y no precisan un desarrollo técnico propio. Es cuestión de tiempo que o bien desarrollen sus capacidades o bien las adquieran en el propio ciberespacio.

2.4. SABOTAJES

Los posibles ataques a infraestructuras críticas no son una cuestión de ciencia ficción. Por aquí se pueden producir futuras sorpresas estratégicas. Lo que militares norteamericanos han denominado un “Cyber Pearl Harbour” es un escenario que se otea en el horizonte. Hackers tienen en sus objetivos centrales nucleares, plantas químicas, sistemas eléctricos, sistemas de transporte y aviación. La ausencia de reporte de incidentes, hasta el momento, hace difícil ser conscientes de una amenaza que ya se ha manifestado.

En julio de 2017 el español Rubén Santamarta descubrió un fallo en los sistemas de las centrales nucleares que permitiría a un atacante simular fugas radioactivas o evitar que se detectaran. Una investigación que expuso posteriormente en el Black Hat de dicho año.

2.5. HACKTIVISMO

El hacktivismo continuará siendo una forma de acción en 2018, con campañas contra el sistema o acciones de “justicia”. Frente al activismo, que en general es admitido en las sociedades democráticas como una vía de ejercicio de política desde fuera de la política, aunque en ocasiones algunas de sus acciones puedan estar al límite de la legalidad, en el hacktivismo se suele producir una actividad delictiva.

Al margen de los tradicionales ataques de denegación de servicio, en general de bajo impacto, el mayor riesgo se genera por el acceso a datos e información de las organizaciones y de sus miembros. El hacktivismo puede comprometer instalaciones físicas, seguridad personal de empleados, datos e informaciones sensibles y afectar a la marca.

En todo caso, la tendencia apunta a su mantenimiento, pero representando un nivel muy bajo de amenaza. Como ha señalado repetidamente el CCN-CERT, no existe una articulación de un tejido hacktivista operativo insurgente en España, ni siquiera alrededor del movimiento Anonymous.

2.6. GAME CHANGERS

Entendemos por *game changers* aquellas variables que, sabiendo de su elevado impacto, existen dudas sobre si este va a ser positivo o negativo. La tecnología, en

general, es considerada un gran *game changer*, puesto que genera nuevos riesgos, siendo a la vez la vía para poderlos enfrentar.

2.7. INTELIGENCIA ARTIFICIAL Y MACHINE LEARNING

Elon Musk, el gurú de Tesla, afirmó recientemente que deberíamos tener más preocupación por la Inteligencia Artificial (IA) que por Corea del Norte. Nick Bostrom, que dirige el Instituto para el Futuro de la Humanidad y el Centro de Investigación de Estrategia de Inteligencia Artificial de la Universidad de Oxford, es otro de los líderes de opinión académica que ha mostrado su preocupación por la IA. La mayoría de los análisis prospectivos sobre 2018 señalan que durante este año se podría incrementar el uso de la IA por parte de los cibercriminales, frente a una situación anterior en la que la IA era una posible herramienta para luchar contra el cibercrimen, para detectar anomalías y establecer patrones. Se produciría, en ese caso, y pendiente aún de poder demostrar fehacientemente, una guerra de IA contra IA, de máquinas contra máquinas. Actividades automatizadas, como mostró el Reaper botnet en 2017, para localizar vulnerabilidades en código fuente y búsqueda de nuevos conceptos zero-day.

Imaginemos un malware que analiza la forma en que nos comunicamos con diferentes contactos, y que fuera capaz de simular ese estilo para enviar mensajes personalizados a tus propios contactos. El propio Vladimir Putin ha llegado a señalar que quien consiga el liderazgo en IA gobernará el mundo. Una declaración abierta, de claro carácter estratégico, a la que todo analista debe atender.

McAffee, señalando la importancia de Machine Learning para procesar grandes cantidades de datos, que pueden ayudar a detectar y corregir vulnerabilidades, conductas sospechosas o ataques zero-day, insiste en la importancia del intelecto estratégico humano, señalando que el factor de éxito será la inteligencia humana amplificada por la tecnología. Una reflexión importante en un entorno de “solucionismo tecnológico”, usando la terminología de Eugeny Morozov, en el que a cada problema se le busca una solución tecnológica o incluso se crean problemas que no existen a tal fin.

2.8. BLOCKCHAIN

Una prometedora revolución tecnológica, aplicable en multitud de sectores, que elimina intermediarios y logra seguridad en el acceso y uso de la información, pero que aún está en un estado de infancia en el desarrollo de aplicaciones. Esa situación hace que ahora mismo no esté en el foco de los cibercriminales, que se seguirán centrando en todo el ecosistema de las criptomonedas (inversores, intercambios, monederos, instalación de aplicaciones ocultas para minar aprovechando la CPU de sus equipos y la energía eléctrica de internautas).

Blockchain tiene utilidad para seguridad de las TIC. El almacenamiento de datos de una forma descentralizada y distribuida puede prevenir su hackeo. Pero la implementación de sistemas financieros basados en blockchain puede producir errores o vulnerabilidades aprovechadas por atacantes. En los dos últimos años se han detectado errores de este tipo en los denominados smart contracts, basados en Blockchain.

3. CIBERINTELIGENCIA PARA LA CIBERSEGURIDAD

3.1. CONCEPTO

Sin existir un amplio debate sobre la cuestión, ni siquiera un volumen significativo de publicaciones, sí existe consenso en la dificultad para definir este término. Así se expresó, en repetidas ocasiones, en la I Jornada de Inteligencia y Seguridad organizada por la Fundación Borredá el 30 de noviembre de 2017. El propio Javier Candau, jefe de Ciberseguridad del Centro Criptológico Nacional, así lo indicaba en el número 79 de Red Seguridad (2017), destacando cómo es un concepto recurrente, que se vincula a la oferta de servicios en ciberseguridad, pero sobre el cual no existe consenso y se utiliza de forma ambigua.

La ausencia de un concepto de general o, al menos, amplia aceptación tiene importantes consecuencias: impide determinar los elementos configuradores de la posible disciplina, los contenidos de la función a desarrollar, y el diseño de planes de formación (conocimientos y habilidades), así como el desarrollo de carrera profesional.

Atendiendo a su origen etimológico estamos ante un término formado por dos palabras: *ciber* (que se refiere al ciberespacio) e *inteligencia*. Esta sencilla aproximación aporta claramente una pista a seguir, la ciberinteligencia como la confluencia de dos posibles disciplinas.

La RSA (2012) define ciberinteligencia como *"el conocimiento sobre los ciber-adversarios y sus métodos, además del conocimiento sobre la posición de seguridad de una organización sobre sus adversarios en el ciberespacio y sus métodos"*. En base a este conocimiento las organizaciones desarrollan inteligencia accionable. Otra definición habitual, pero excesivamente limitada es la siguiente: "*el análisis de las capacidades, intenciones y actividades de un adversario en el ciberespacio"*. INSA (2015) lo define, de forma más acertada y completa, como *"los productos y los procesos del ciclo de inteligencia para analizar las capacidades, intenciones y actividades –no solo técnicas- de los potenciales adversarios y competidores en el ciberespacio"*. INSA considera a la ciber contrainteligencia como una subdisciplina. En cualquier caso, estas aproximaciones basadas únicamente en adversarios parecen limitativas, obviando que la acción de los mismos se desarrolla en un entorno, un contexto político, social, económico, legal, tecnológico que conviene analizar. Incluso la propia naturaleza del ciberespacio, las tendencias detectadas, las nuevas amenazas y oportunidades, que surgen a cada instante, son un conocimiento vital a manejar.

Carnegie Mellon Software Engineering (2013) define ciberinteligencia como *"la adquisición y análisis de información para identificar, seguir y predecir ciber-capacidades, intenciones y actividades que ofrezcan líneas de acción para apoyar la toma de decisiones"*. Este concepto está mucho más próximo a la conceptualización clásica de inteligencia.

La *"U.S. National Intelligence Strategy 2014"* (Office of the National Director of Intelligence, 2014) identifica la ciberinteligencia como una de las cuatro misiones de la Comunidad de Inteligencia. El Department of Homeland Security (2012), en un informe de 2012, *"DHS Task Force of Cyber Skills",* se acerca también al contenido de la función de ciberinteligencia: *"conocimiento de la superficie de ataque, sus objetos de*

mayor valor y objetivos, y cómo sus vulnerabilidades pueden ser explotadas; mantener un situational awareness sobre actores maliciosos; desarrollar técnicas y aplicaciones para contrarrestar, identificar y vigilar; en su versión más avanzada entender las motivaciones de los atacantes, su lenguaje, organización, comportamiento individual y grupal, con objeto de perfilar grupos, actores y campañas".

Javier Candau (CCN-CERT, 2017) muestra su coincidencia con la definición de ciberinteligencia propuesta por el profesor Manuel Torres Soriano: *"actividad analítica cuyo propósito es proporcionar información relevante para apoyar la toma de decisiones en cuestiones relativas al ciberespacio".*

Consideramos que, a la hora de adoptar una definición que aúne el mayor grado de consenso, es preciso atender tanto a la raíz del concepto, con sus dos componentes "ciber" e "inteligencia", como a la doctrina de inteligencia que muestra claramente el CCN-CERT, proponiendo el siguiente concepto: *"proceso (y producto final) de la obtención y análisis de datos e información en/sobre el ciberespacio, realizado por especialistas y orientado a la toma de decisiones, en tiempo, lugar y forma".*

3.2. ELEMENTOS INVOLUCRADOS EN LA DEFINICIÓN:

- Es un proceso característico de inteligencia.
- Sobre una materia, que es el ciberespacio. El ciberespacio es el centro de dedicación de la ciberinteligencia, tomando al mismo tanto como un medio del que obtener y analizar datos e información, como una fuente de riesgos y amenazas, como señala la Estrategia de Seguridad Nacional.
- Una interpretación amplia del concepto de ciberinteligencia incorporaría la denominada Inteligencia de Fuentes Abiertas (OSINT), en la medida en que se centra en la información en el ciberespacio, aunque sea con otros objetivos adicionales a la ciberseguridad (protección de eventos, directivos, marca y reputación, etc.). Básicamente, lo que denominamos como "vigilancia digital" es OSINT.
- Consideramos que la ciberinteligencia no se ciñe a analizar las capacidades de los adversarios, sino también a analizar el entorno en el que dichos competidores toman decisiones estratégicas. El análisis del entorno configura la (in) seguridad, y la ciber (in)seguridad, y al menos debe ser tratado de entender en la dimensión estratégica de la ciberinteligencia.
- Es realizado por especialistas, tanto en ciberseguridad como en análisis de inteligencia.
- Exige unos requisitos formales para poder ser considerado como inteligencia, y siendo válido para un momento y lugar.
- Es finalista, su objetivo es la acción, el apoyo a la toma de decisiones:
    1. Identificando riesgos y amenazas.
    2. Analizando las variables involucradas y los actores intervinientes.
    3. Determinando oportunidades (quizás la orientación actual de nuestras sociedades está muy basada en riesgos). Esto no se incluye en las definiciones clásicas.

4. La inteligencia debe responder a las clásicas 5W+H (who, what, why, when, where, how). En el ciberespacio, con personal técnico adecuado, se puede responder a qué sucede, cómo, cuándo y dónde. Más complejo es poder responder a quién y por qué (o para qué). Por ejemplo, no fue difícil analizar qué estaba pasando con Wannacry o con NotPetya, ni cómo se producía y propagaba. Pero sí es complejo decidir quién está detrás, por qué y para qué.
5. Debe considerar implicaciones posteriores: ¿qué será lo próximo?, ¿qué hacemos ahora?
6. A diferencia de lo señalado en la definición de Torres Soriano, la toma de decisiones no se limita únicamente al ciberespacio, sino que también abarca el mundo físico. Todo lo que sucede en el ciberespacio puede tener impactos en el día a día de personas y organizaciones. La hibridación entre mundo físico y mundo ciber tiende a ser absoluta.

Al igual que sucede con la Inteligencia, es imposible su consideración como una ciencia e incluso como una disciplina, aunque sí tiene elementos que configuran una profesión y una especie de arte (una forma de hacer y actuar). Como un área emergente está pendiente de desarrollar lo que se conoce como "tradecraft": conjunto de conocimientos y habilidades adquiridas a través de la experiencia en un oficio. Los elementos, de manera más concreta, y siguiendo a INSA (2015), serían:

- Un cuerpo común de conocimiento.
- Un marco de competencias.
- Un modelo dual de desarrollo, entre aspectos técnicos y analíticos.
- Unos planes de formación y desarrollo.
- Una carrera profesional.

3.3. TIPOLOGÍA

Realizando un estudio bibliográfico, algunas de las aportaciones de mayor interés han sido las realizadas por la Intelligence and National Security Alliance (INSA).

Ciberinteligencia Estratégica (INSA, 2014a)

Tal y como señala INSA, es posible que la Ciberinteligencia Estratégica tenga matices en su conceptualización en diferentes organizaciones en base a su tamaño, objetivo o misión.

Para INSA depende de seis criterios:

- La naturaleza e identidad del cliente.
- Las decisiones que debe tomar el cliente.
- El marco temporal en el que actuará.
- El alcance de la obtención de información.
- El carácter de los potenciales adversarios.

- El nivel de aptitudes técnicas para la función.

Características de la ciberinteligencia estratégica:

- Amplia en la obtención.
- Más allá del sector.
- Mira a medio y largo plazo.
- Es amplia en la consideración de posibles adversarios.
- Desarrolla un análisis del entorno.
- Es esencialmente una tarea no técnica.
- Es clave en el análisis de riesgos: amenazas, vulnerabilidades, impactos, políticas.

Un proceso de ciberinteligencia estratégica considera:

- Qué información se precisa por el decisor (Information Requirement).
- Qué información se precisa sobre el entorno que configura el ámbito espacial y temporal en el que las organizaciones se desenvuelven (político, social, económico, tecnológico, legal…)
- Qué información se precisa sobre amenazas y riesgos para nuestra organización o nuestros clientes.
- Qué información se precisa sobre potenciales adversarios.
- Qué posición tiene la organización en seguridad:
    1. Objetivos a proteger.
    2. Vulnerabilidades.
    3. Nivel de riesgo: bajo, medio o alto riesgo ciber.
    4. Qué valor tiene la información de la organización.
    5. Qué valor tienen los aspectos digitales en sus procesos.
    6. Qué requisitos legales tiene la información.

Ciberinteligencia operacional (INSA, 2014b)

Características:

- Orientada a los managers de IT, CIO, CISO.
- Utilizable para adopción de decisiones sobre riesgos.
- El énfasis se pone en los procesos y operaciones de la organización, incluyendo proveedores, aliados y socios, competidores, clientes y otras relaciones.
- Analiza a los adversarios, con mayor grado técnico que en el nivel estratégico.
- Combina tareas técnicas y no técnicas, orientadas a aquellos vectores que suponen mayor riesgo para la continuidad del negocio.

Ciberinteligencia táctica (INSA, 2014c)

Características:

- Según INSA es el nivel en el cual las "batallas se planifican y ejecutan".
- Se produce específicamente para los equipos de respuesta a incidentes.
- Su objetivo es la resiliencia: restaurar las operaciones y recoger evidencias para el análisis forense.
- El análisis sobre el atacante centra parte de los esfuerzos: modus operandi, motivaciones, capacidades, etc.
- Su carácter es técnico.

3.4. EL "PARA QUÉ" Y EL "CÓMO" DE LA CIBERINTELIGENCIA

De una forma simplificada, las organizaciones deben proteger a las personas, las instalaciones, los procesos de negocio, los bienes y valores, los datos e información, y la marca y reputación. La ciberinteligencia se configura como la vía para el logro de dichos objetivos.

Figura 2. Ciclo de Ciberinteligencia del National Institute of Standards and Technology (NIST)

En base a la definición señalada en apartado anterior, y considerando el ciclo del NIST, sería posible construir un ciclo o proceso más cercano al del análisis de inteligencia clásico.

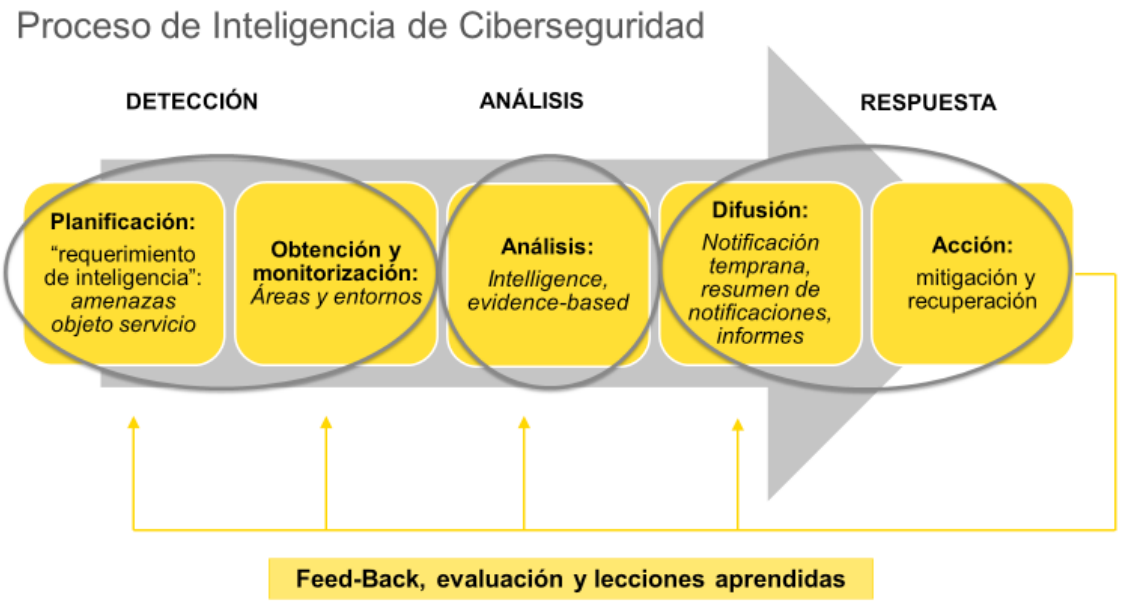

Figura 3. Proceso de Ciberinteligencia (Prosegur, 2017)

Las actividades del citado proceso son las siguientes:

1. **Definición, planificación y parametrización:** De acuerdo con el requerimiento de inteligencia (el "para qué" que genera la necesidad del análisis), se procede a determinar el alcance, plazos y recursos precisos. Posteriormente se lleva a cabo un plan para la parametrización de las fuentes y keywords sobre las herramientas de detección automatizada que se puedan utilizar, de manera que los sistemas queden preparados para la monitorización automática.

2. **Obtención y monitorización:** Una vez los sistemas de inteligencia han sido parametrizados y puestos en operación de acuerdo con la fase anterior, los mismos se encargarán de la recopilación automática de la información para la detección de potenciales eventos de ciberseguridad y su posterior análisis por parte de los operadores y analistas del servicio. En esta fase se realizan tareas como la propia obtención, filtrado, evaluación, clasificación e integración de la información.

3. **Análisis:** Estudio e interpretación de la información. A estos efectos se puede combinar el clásico método científico, con técnicas tanto cuantitativas como cualitativas, junto a las denominadas técnicas estructuradas de análisis de inteligencia, desarrolladas por los servicios de inteligencia. Estas aproximaciones, junto al análisis de riesgos, siguiendo la Norma ISO 31000, complementan marcos propios de la Ciberinteligencia, como el proceso NIST, The Kill Chain o el modelo de diamante. A ello se unen disciplinas que incrementan las capacidades del analista, ante las dificultades cuantitativas y cualitativas derivadas del elevado grado de infoxicación y de los crecientes procesos de manipulación, desinformación y engaño (posverdad): análisis semántico, Big Data, Machine Learning, algoritmos avanzados, ingeniería de sistemas de decisión, redes neuronales, etc.

4. **Acción. Resiliencia y respuesta:** Ante las posibles conclusiones y recomendaciones derivadas de las notificaciones e informes corresponderá al decisor la adopción de las medidas oportunas o necesarias.

5. **Retroalimentación y mejora continua:** Periódicamente se llevan a cabo ejercicios para compartir conocimientos, mejorar la calidad de los entregables, disminuir los tiempos de respuesta y abordar oportunidades de mejora. Igualmente abordan desviaciones y oportunidades de mejora en base a los resultados de los indicadores de medición de cada servicio, con el objetivo de mejorar de manera continuada y maximizar la eficiencia de las actividades, la calidad de los entregables y minimizar los tiempos de respuesta.

3.5. LA CIBERINTELIGENCIA COMO FACTOR DE COHESIÓN EN LA CIBERSEGURIDAD

La ciberinteligencia, adicionalmente, puede desempeñar un papel cohesionador de diferentes líneas de acción en ciberseguridad. Desde una visión estratégica, y sin ánimo de ser exhaustivo, algunas de las líneas de acción que pueden ser apoyadas por la ciberinteligencia serían:

Avanzar en concienciación.

Algunas recetas para mejorar la concienciación serían:

- El desarrollo de una labor didáctica. La complejidad del ciberespacio ha llevado a la utilización de un lenguaje muy técnico, difícil de seguir y entender. Por este motivo, hacia las empresas, es importante desarrollar una filosofía *"storytelling",* que traduzca el lenguaje técnico en implicaciones para las empresas, en posibles costes. A estos efectos la utilización de escenarios y simulaciones es un apoyo, posiblemente más eficaz que el recurso a la presentación de frías estadísticas.

- La utilización de casos de estudio y ejemplos para hacer comprender a las organizaciones cómo desde el ciberespacio se puede afectar a la seguridad de instalaciones e infraestructuras, la seguridad física de empleados y directivos, los procesos de negocio, los datos y la información, los valores y la marca y reputación.

Colaboración público-privada

Esta colaboración ya no es una opción, es la única vía. El fortalecimiento del marco normativo, por sí mismo, ya hará que exista un mayor grado de relación, aunque sea por vía de requerimiento de acciones de información y comunicación, o garantía de protección de datos.

Esta colaboración presenta multitud de vías para su desarrollo, como proyectos de investigación conjuntos, intercambios de información puntuales, coorganización de jornadas y talleres, grupos de expertos para debate, intercambio de buenas prácticas, etc.

Gobernanza en las organizaciones

Posiblemente el gran reto a abordar, donde es preciso desarrollar una verdadera cultura de ciberseguridad en las organizaciones. La ciberseguridad debe actuar de forma transversal y los responsables de estas áreas sentarse muy cerca del Consejo de Dirección.

Inteligencia en sentido amplio

La inteligencia, definida como el proceso de obtención y análisis de la información para apoyar la toma de decisiones, es una de las vías para poder gestionar los riesgos, atendiendo a diversos objetivos que se plantean en el campo de la ciberseguridad. Uno de ellos pudiera ser cómo reducir el periodo entre el que un sistema es comprometido y es detectada la intrusión. Según FireEye es de 469 días en Europa (siendo la media mundial de 146).

El análisis de lecciones aprendidas y el estudio de casos forman parte de las tareas a desarrollar desde la inteligencia. Procesos para los cuales existen metodologías que ayudan a enmarcar un proceso que no debe ser tan intuitivo, en caso de existir, como sucede en ocasiones.

La inteligencia también debe tener como misión su propio autodesarrollo a través del apoyo tecnológico preciso. La tecnología, por una parte, es fuente de amenazas, pero a su vez se configura como posible solución a muchos riesgos.

Por otra parte, como proceso de análisis, la inteligencia camina de la mano de la geopolítica, la geoeconomía o la geoestrategia. Un entendimiento del entorno, a través de la inteligencia estratégica, puede proveer del contexto necesario para entender algunos riesgos cibernéticos.

Finalmente, y de nuevo sin ánimo exhaustivo, la inteligencia es la base para desarrollar la necesaria *Cyber Awareness,* similar a lo que conocemos como consciencia situacional (*situational awareness),* el mantenimiento de un elevado nivel de alerta ante posibles señales débiles (eventos que pueden sugerir una tendencia o que, conectados con otros eventos, generen nuevos riesgos).

Análisis de riesgos

La base para gestionar cualquier tipo de riesgo es partir de un buen análisis y evaluación de riesgos. Una evaluación que debe ser continua. En 2017 Gartner proponía un modelo CARTA (Continuous Risk and Trust Assessment Approach, 2017), un proceso continuo de evaluación y reajuste. Pero no hace falta ser Gartner para llegar a esa conclusión. El análisis de riesgos se debe desarrollar en tiempo real. Las metodologías de análisis de riesgos deben evolucionar, para incorporar aproximaciones como el análisis de datos, las redes neuronales y otras técnicas de minería de datos, el juicio de los expertos, el análisis bayesiano, etc.

Gestión de crisis

Cualquier incidente ciber es capaz de producir una crisis. Las organizaciones deben prepararse para estas situaciones, específicamente a través de simulaciones. Que cuando el momento se produzca existan protocolos de acción y la comunicación a desarrollar. Mientras que las crisis pueden ser improvisadas, la gestión de crisis nunca debe improvisar.

Seguridad desde el diseño

Garantizar la seguridad desde el mismo momento en que se diseña un producto o servicio puede ser la mejor manera de prevenir.

Prospectiva

En entornos que denominamos VUCA (acrónimo de volatilidad, incertidumbre, complejidad y ambigüedad), la capacidad para interpretar qué está sucediendo es un valor para las organizaciones, que se debe complementar con las capacidades para identificar posibles escenarios futuros, con objeto de adoptar en el presente las decisiones estratégicas que eviten los más desfavorables y, si es posible, nos guíen a los más beneficiosos para nuestras organizaciones. La prospectiva no es una técnica de adivinación, sino que cuenta con técnicas específicas para su desarrollo.

Pensar en futuro es una obligación. Conocemos más cosas del futuro de las que solemos creer. Pensar en futuro induce elementos causales en su devenir.

Tradecraft, el oficio del analista de ciberinteligencia

Finalmente, y desde el punto de vista de la Ciberinteligencia, es preciso desarrollar lo que se conoce como *Tradecraft,* el oficio: qué conocimientos son precisos, qué aptitudes y qué actitudes, qué habilidades se exigen para poder entender las actuales ciberamenazas y poder luchar contra ellas. Todo ello a nivel estratégico, operativo y táctico. Implica adicionalmente el establecimiento de un plan de carrera, que considere la formación precisa y las condiciones para la promoción.

4. CONCLUSIONES

Frente a la falta de consenso sobre la definición y delimitación de la ciberinteligencia es posible apuntar que la misma puede contar con los mismos fundamentos que la doctrina de inteligencia clásica, nacida en el ámbito militar y de la seguridad física. Los elementos caracterizadores de la misma son coincidentes, una forma de pensar orientada a la acción, un proceso racional de obtención y análisis de información, una finalidad en el apoyo a la toma de decisiones, y unas características propias (tiempo, forma y lugar) que permiten diferenciar la inteligencia de la información o el conocimiento.

Los intereses a proteger de Estados, organizaciones o empresas coinciden en el ámbito físico y en el ciberespacio: las personas, las infraestructuras, la información y los datos, los procesos de negocio, los bienes y valores, y la marca y reputación. Los seis elementos pueden ser atacados tanto físicamente como a través del ciberespacio. Internet y las Tecnologías de la Información y las Comunicaciones son un facilitador o potenciador de lo que se denomina en la literatura anglosajona como *"cyber enabled crimes",* referido a aquellos delitos que pueden realizarse tanto con apoyo tecnológico como sin él.

La definición propuesta de ciberinteligencia como "*proceso (y producto final) de la obtención y análisis de datos e información en/sobre el ciberespacio, realizado por especialistas y orientado a la toma de decisiones, en tiempo, lugar y forma",* goza del contenido necesario para ser adoptado, tanto en el ámbito público como en el sector privado, facilitando la creación de un lenguaje común que, aún lejos de poder configurar una disciplina, ***sí defina a una actividad profesional.***

Al igual que la inteligencia ha contribuido clásicamente a la seguridad física, la ciberinteligencia lo hace hacia la ciberseguridad. La sociedad digital se enfrenta a retos hasta ahora desconocidos, riesgos probables de muy incierto impacto. Parte de los

planteamientos distópicos del futuro se centran bien en ciberataques, bien en formas híbridas o combinadas de acción. Los conflictos en el ciberespacio se acrecientan, sustituyendo viejas formas de enfrentamiento. Los ciberdelitos y, lo que es más serio, el cibercrimen organizado, disponen de los mejores recursos: tecnólogos, hackers, abogados, blanqueadores, expertos en sistema financiero. Incorporan a sus acciones desarrollos como la Inteligencia Artificial. Los terroristas, hasta el momento, han utilizado Internet en funciones de propaganda y comunicación, adoctrinamiento, captación y reclutamiento. Es decir, un uso de Internet y las TIC como medio, pero no como el fin de los ataques. Cuentan con la intención, y las capacidades para ello no son tan necesarias, en un modelo de negocio de "Crime as a Service". Las capacidades precisas pueden ser adquiridas o arrendadas a otros grupos criminales.

En este marco, la Ciberinteligencia se enfrenta a los siguientes retos:

- Su conceptualización, como base para la determinación del "oficio" de analista de ciberinteligencia.
- *Tradecraft* u oficio. Determinación de conocimientos y habilidades, junto al desarrollo de un plan de formación y una carrera profesional para los analistas de ciberinteligencia. El documento de ENISA (2015) es una de las propuestas más elaboradas en este sentido.
- El desarrollo de metodologías propias o adaptadas de otras disciplinas o profesiones.
- El apoyo de nuevas tecnologías, en ningún caso sustitutivas del ser humano.

BIBLIOGRAFÍA

Arquilla, J. y Ronfeldt D. (2001). Networks and Netwars. The Future of Terror, Crime, and Militancy. RAND Corporation. Extraído el 2 de julio de 2018 de: https://www.rand.org/pubs/monograph_reports/MR1382.html

Arquilla, J. y Ronfeldt D. (1996). The Advent Of Netwar 1996. RAND Corporation. Extraído el 2 de julio de 2018 de: https://www.rand.org/pubs/monograph_reports/MR789.html

Blanco, J. M. y Cohen, J. (2016). Macro-environmental factors driving organized crime. Using Open Data to Detect Organized Crime Threats. Springer.

Candau, J. (2017). Ciberinteligencia, complemento perfecto para la ciberseguridad. Red Seguridad 4º trimestre 2017. Extraído el 2 de julio de 2018 de: http://www.redseguridad.com/especialidades-tic/inteligencia/ciberinteligencia-complemento-perfecto-para-la-ciberseguridad

Carnegie Mellon University (2013). Cyber Intelligence Tradecraft Project: Summary of Key Findings. SEI Emerging Technology Center. Extraído el 2 de julio de 2018 de: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=40201

Centro Criptológico Nacional (2017). XI Jornadas CCN-CERT Ciberamenazas, el reto de compartir. Extraído el 2 de julio de 2018 de: https://www.ccn-cert.cni.es/xijornadas.html

Department of Homeland Security (2012). Cyber Skills Task Force Report. Washington, DC: Homeland Security Advisory Council.

Gartner (2017). CARTA (Continuous Risk and Trust Assessment Approach, 2017). Extraído el 2 de julio de 2018 de: https://www.gartner.com/smarterwithgartner/the-gartner-it-security-approach-for-the-digital-age/

Gobierno de España (2017). Estrategia de Seguridad Nacional. Extraído el 2 de julio de 2018 de: http://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/presidenciadelgobierno/Documents/2017-1824_Estrategia_de_Seguridad_Nacional_ESN_doble_pag.pdf

Gobierno de España (2013). Estrategia de Ciberseguridad Nacional (2013). Extraído el 2 de julio de 2018 de: https://www.ccn-cert.cni.es/publico/dmpublidocuments/EstrategiaNacionalCiberseguridad.pdf

Intelligence and National Security Alliance INSA (2013) Operational Levels of Cyber Intelligence. Extraído el 2 de julio de 2018 de: https://www.insaonline.org/operational-levels-of-cyber-intelligence/

Intelligence and National Security Alliance INSA (2014a) Strategic Cyber Intelligence. Extraído el 2 de julio de 2018 de: https://www.insaonline.org/strategic-cyber-intelligence/

Intelligence and National Security Alliance INSA (2014b) Operational Cyber Intelligence. Extraído el 2 de julio de 2018 de: https://www.insaonline.org/operational-cyber-intelligence/

Intelligence and National Security Alliance INSA (2014c). Tactical Cyber Intelligence. Extraído el 2 de julio de 2018 de: https://www.insaonline.org/tactical-cyber-intelligence/

Intelligence and National Security Alliance INSA (2015). Cyber Intelligence: Preparing Today's Talents for Tomorrow's Threats. Extraído el 2 de julio de 2018 de: https://www.insaonline.org/cyber-intelligence-preparing-todays-talents-for-tomorrows-threats/

eSP European Solution Providers (2018). 2018 Security Spending to Reach $96bn . Extraído el 2 de julio de 2018 de: http://www.it-sp.eu/index.php?option=com_content&view=article&id=3651:gartner-2018-security-spending-to-reach-96bn&catid=38:security&Itemid=74

Liang, Q. y Xiangsui, W. (1999). Unrestricted Warfare. Beijing: PLA Literature and Arts Publishing House.

Microsoft (2017). A Digital Geneva Convention to protect cyberspace. Extraído el 2 de julio de 2018 de: https://www.microsoft.com/en-us/cybersecurity/content-hub/a-digital-geneva-convention-to-protect-cyberspace

MMC Cyber Handbook 2018. Extraído el 2 de julio de 2018 de: https://www.mmc.com/content/dam/mmc-web/Global-Risk-Center/Files/mmc-cyber-handbook-2018.pdf

NIST (2018). Cybersecurity Framework. Extraído el 2 de julio de 2018 de: https://www.nist.gov/cyberframework

Office of the National Director of Intelligence (2014). The National Intelligence Strategy of the United States of America. Extraído el 2 de julio de 2018 de: https://www.dni.gov/files/documents/2014_NIS_Publication.pdf

Online Trust Alliance (2018). Cyber Incident & Breach Trends Report Review and analysis of 2017 cyber incidents, trends and key issues to address. Extraído el 2 de julio

de 2018 de: https://otalliance.org/system/files/files/initiative/documents/ota_cyber_incident_trends_report_jan2018.pdf

Parlamento Europeo (2016). Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión. Extraído el 2 de julio de 2018 de: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016L1148

Parlamento Europeo (2018). ENISA and a new cybersecurity act. Extraído el 2 de julio de 2018 de: http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI%282017%29614643

RSA (2012). Getting Ahead of Advanced Threats. The Security Division of EMC. Extraído el 2 de julio de 2018 de: https://www.rsashare.com/leadership/articles/getting-ahead-of-advanced-threats.htm

USENIX (2017). Understanding the Mirai Botnet. Vancouver, BC, Canada. Extraído el 2 de julio de 2018 de: https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-antonakakis.pdf

Fecha de recepción: 21/06/2018. Fecha de aceptación: 25/06/2018

CUESTIONES CONTROVERTIDAS EN EL EJERCICIO DE LA POTESTAD ADMINISTRATIVA SANCIONADORA

J. LEANDRO MARTÍNEZ-CARDÓS RUIZ

LETRADO MAYOR DEL CONSEJO DE ESTADO

RESUMEN

La potestad administrativa sancionadora está sujeta *mutatis mutandis* a los principios propios del derecho penal constitucionalmente instituidos. Cabe la inversión legal de la carga de la prueba en los procedimientos sancionadores. Los documentos públicos expedidos por funcionarios que tienen reconocida la condición de autoridad hacen prueba por sí solos, pero no los formalizados por quienes son simples agentes de la autoridad o por organismos privados de control autorizados. El incumplimiento de la obligación de identificar a un conductor por parte del titular del vehículo en la legislación de seguridad vial por parte de determinados familiares no es sancionable por aplicación de lo dispuesto en la Ley de Enjuiciamiento Criminal. Los procedimientos sancionadores instruidos contra quienes están ligados por contratos o concesiones demaniales no se rigen por las determinaciones reguladores de los procedimientos sancionadores, quedando la duda sobre si les resulta de aplicación el efecto previsto en el artículo 25.1.b) de la Ley 39/2015, de 1 de octubre.

Palabras clave: Procedimiento sancionador, carga de la prueba, autoridad pública, organismos de control autorizados, deber de identificar a los conductores de vehículos, procedimientos sancionadores en materia de contratación y dominio público.

ABSTRACT

The administrative sanctioning power is subject “mutatis mutandis” to the principles of criminal law constitutionally instituted. The legal reverval of the burden of proof in sanctioning procedures is feasible. Public documents issued by officials holders of the condition of authority are proof by themselves, but those formalized by simple agents of the authority or authorized private oversight agencies are not. The infridgement of the obligation to identify a driver of your own car by certain family members is not punishable by road safety legislation, in application of the provisions of the Spanish Ley de Enjuiciamiento Criminal. The sanctioning procedures against those bound by contracts or public concessions are not regulated by the sanctioning procedures. Doubt remains if the effects of article 25.1.b) of Law 39/2015, from October 1st, is applicable to them.

Keywords: Sanctioning procedure, burden of proof, public authority, authorized control bodies, duty to identify, automobile drivers, sanctioning procedures contracting and public domain.

1. ALGUNOS ASPECTOS DE LA REGULACIÓN DE LA POTESTAD SANCIONADORA EN LAS LEYES 39/2015 Y 40/2015, DE 1 DE OCTUBRE

1. La aprobación de las Leyes 39/2015 y 40/2015, ambas de 1 de octubre, del Procedimiento Administrativo Común y del Régimen Jurídico de las Administraciones Públicas, regulan la potestad y algunos aspectos del procedimiento sancionador. Poco innovadoras son sus previsiones, aunque sí es distorsionadora –y confusa- la técnica legislativa empleada a la hora de hacerlo. Dispersar las normas aplicables en la materia en ambas leyes, sin ningún criterio racional o lógico, dificulta su aplicación por el operador jurídico. Insertar las previsiones especiales aplicables al procedimiento sancionador a lo largo del texto de la primera de las disposiciones citadas, la Ley 39/2015, de 1 de octubre, constituye un claro ejemplo de mala técnica legislativa, que menoscaba la seguridad jurídica de los destinatarios de la norma. Y, finalmente, no solventar problemas apreciados durante los años de vigencia de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, denota la premura con que las leyes citadas se elaboraron y aprobaron. Procede examinar algunas de las cuestiones no resueltas por la nueva regulación.

2. La potestad sancionadora de la Administración está sujeta a los principios inspiradores del orden penal, según ha declarado reiteradamente el Tribunal Constitucional (desde las *Sentencias de 30 de enero y 8 de junio de 1981*). Ello comporta que le resultan de aplicación los principios de legalidad, tipicidad, culpabilidad y proporcionalidad y el derecho a la presunción de inocencia, según ha declarado reiteradamente el Tribunal Constitucional desde las ya lejanas sentencias de 10 de junio de 1981, 7 de abril de 1982 y 29 de enero de 1983.

   Así lo reconoce la Ley 40/2015, de 1 de octubre, de Régimen Jurídico de las Administraciones Públicas. Su artículo 25.1 previene que:

   "1. *La potestad sancionadora de las Administraciones Públicas se ejercerá cuando haya sido expresamente reconocida por una norma de rango de Ley, con aplicación del procedimiento previsto para su ejercicio y de acuerdo con lo establecido en esta Ley y en la Ley de Procedimiento Administrativo Común de las Administraciones Públicas..."*

   Los principios de irretroactividad, de tipicidad, de culpabilidad, de proporcionalidad y responsabilidad están igualmente acogidos en la misma norma legal (artículos 26 y ss.).

   La regulación legal consagra pues los principios de culpabilidad y personalidad, que rigen inexorablemente en nuestro derecho. En virtud del primero, en el ámbito sancionador, resulta inadmisible un régimen de responsabilidad objetiva o sin culpa (*Sentencia del Tribunal Constitucional 246/1991, de 19 de diciembre*). Y, en virtud del segundo, se "prohíbe expresamente el traslado de la responsabilidad personal a persona ajena al hecho infractor al modo de una exigencia de responsabilidad objetiva sin intermediación de dolo o culpa" (*Sentencia del Tribunal Constitucional 219/1998, de 22 de noviembre*).

   La imposición de sanciones exige a la Administración la prueba de los hechos imputados; prueba que no puede ser mera presunción, salvo que expresamente

así lo establezca la ley. En efecto, la presunción constitucional de inocencia, con rango de derecho fundamental, supone que solo sobre la base de pruebas cumplidas, cuya aportación es carga de quien acusa, esto es, de la Administración, podrá ser sancionado alguien. Toda sanción ha de apoyarse en una actividad probatoria de cargo o de demostración de la realidad de la infracción que se reprime, sin la cual la sanción misma no es posible (*Sentencias del Tribunal Supremo de 26 de diciembre de 1983, 20 de febrero y 11 de marzo de 1985, 11 de febrero de 1986, 21 de mayo de 1987, 4 de febrero de 1991*, *346/2006, de 11 de diciembre, 131/2003, de 30 de junio*, entre otras). En otros términos, "*la carga de la prueba corresponde a quien acusa, sin que nadie esté obligado a probar su propia inocencia*" (*Sentencia del Tribunal Constitucional de 26 de abril de 1990*). Por consiguiente, la presunción de inocencia origina que, en los procedimientos sancionadores, la carga de la prueba recaiga sobre la Administración. No es el imputado el que tiene que probar su inocencia. Si así fuere, habría de probar un hecho negativo (*probatio diabólica*): la inexistencia de conducta tipificada o de participación en los hechos. El Tribunal Constitucional –en la *sentencia 76/1990, de 26 de abril*- lo prohíbe expresamente por entrañar una inversión de la carga de la prueba y, con ello, un menoscabo de la presunción de inocencia.

La prohibición de la inversión de la carga de la prueba no es incompatible, sin embargo, con los efectos derivados de la presunción de legalidad de los actos administrativos sancionadores. Esta presunción de legalidad no es contraria a la de inocencia, pues solo comporta la carga de accionar o impugnar la sanción por el expedientado.

3. La presunción de inocencia impone a la Administración en el procedimiento sancionador la carga de probar los hechos y la participación del expedientado en su comisión, según ha declarado el Tribunal Constitucional –*Sentencias 169/2003, de 29 de septiembre y 131/2003, de 30 de junio*, entre otras-. Y al expedientado, por su parte, compete la prueba de las circunstancias excluyentes, atenuantes o extintivas de la responsabilidad. Esta última regla no comporta que la Administración esté exonerada de acreditar la culpabilidad del inculpado. La presunción de inocencia comporta también la obligación administrativa de probar la culpabilidad del expedientado.

   Salvo en los casos expresamente previstos, los hechos no pueden entenderse acreditados, ni exclusivamente de la presunción de verdad de las actas o denuncias de los agentes administrativos (*Sentencia del Tribunal Constitucional de 26 de abril de 1990*), ni de la simple manifestación de una de las partes, pues estas son simplemente un elemento más que ha de ser valorado en el conjunto de las actuaciones practicadas. Para que dichas actas o denuncias hagan prueba es preciso que se trate de "*documentos formalizados por los funcionarios a los que se reconoce la condición de autoridad pública y que observándose los requisitos legales correspondientes se recojan los hechos constatados por aquellos*", según previene el artículo 77.5 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. Conviene observar que la condición del funcionario debe ser la de "autoridad pública", no la de "agente de la autoridad".

   La cuestión no es baladí por cuanto el acta levantada por el funcionario que no es autoridad pública no hace prueba por sí, de ahí que la legislación especial

sea especialmente prolija en la atribución de dicha condición al personal inspector (e.g.: Ley 16/1987, de 30 de julio, de Ordenación de Transportes Terrestres, artículo 33). En este sentido no tiene el mismo tratamiento jurídico la denuncia formulada por un agente de la Guardia Civil en el ejercicio de funciones inspectoras en materia de transporte terrestre que la hecha en el ejercicio de funciones de tráfico o de caza. En el primer caso, hace prueba sin más aditamentos. En el segundo, ha de ir acompañada de otros elementos de ratificación.

4. La cuestión planteada adquiere perfiles singulares en los frecuentes casos en los que las inspecciones y comprobaciones de hechos que dan lugar a la incoación de procedimientos sancionadores no son llevadas a cabo por funcionarios sino por entidades privadas habilitadas para ello –organismos de control autorizados-.

   La mayor parte de las disposiciones sectoriales, las que la regulan –Ley de Industria, Ley 43/2002, de 20 de noviembre, de Sanidad Vegetal- previenen que las actas de inspección levantadas por el personal de estos organismos de control autorizados tienen valor probatorio, sin perjuicio de cualesquiera otros medios admitidos en derecho que pudieran emplearse. Ahora bien, debe observarse que la posición jurídica de dichos organismos de control autorizados, aunque revestidos de competencias para llevar a cabo las correspondientes inspecciones, no es equiparable sin más a la de los funcionarios públicos. Su personal ni es funcionario, ni tiene reconocida la condición de autoridad. Por este motivo, las leyes sectoriales no establecen que las actas levantadas por ellos hagan prueba en los términos previstos en el artículo 77.5 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. Su valor hay que ponderarlo en cada caso concreto y para hacerla, por lo general, exige que vayan acompañadas de otros elementos que confirmen su contenido. Además, frente a lo que puede suceder con los documentos a que se refiere el mencionado artículo 77.5 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común, el simple relato de hechos contenido en esas actas levantadas por los organismos de control autorizados no es de por sí acreditativo de la realidad y certeza de lo narrado. Por consiguiente, no cabe –sin perjuicio de la valoración que corresponda hacer en cada caso concreto-, imponer sanciones con base única y exclusivamente en las actas levantadas por dichos organismos cuando, bien de las propias circunstancias concurrentes, bien de otros elementos probatorios, no puede alcanzarse la certeza de la realidad de los hechos constitutivos de infracción y de la participación de los imputados.

5. Se observa por otra parte que, en ocasiones, la simple existencia de indicios determina la imposición de sanciones por parte de la Administración, sin dejar constancia en la resolución sancionadora, ni de los hechos que sirven de fundamento a dichos indicios, ni del razonamiento lógico seguido para concluir que se ha cometido la infracción. La jurisprudencia ha declarado que la prueba indiciaria puede constituir una prueba suficiente para destruir la presunción de inocencia y para justificar la imposición de una sanción (*Sentencia del Tribunal Constitucional 45/1997, de 11 de marzo*). Ahora bien, para que la prueba indiciaria prive de eficacia a la presunción de inocencia es preciso partir de unos hechos plenamente probados, deducir de manera palmaria de los citados

hechos la comisión de la infracción y ser posible el control riguroso de la deducción alcanzada conforme a criterios coherentes y lógicos (*Sentencias del Tribunal Constitucional 116/2007, de 21 de mayo; 45/1997, de 11 de marzo*, entre otras). La verificación de la concurrencia de estos tres requisitos obliga a la Administración a acreditar de forma patente los hechos que constituyen el indicio; en segundo lugar a dejar constancia del proceso mental racional seguido –esto es, conforme con las reglas del criterio humano- y, finalmente, la inclusión en la resolución sancionadora del razonamiento por el que se deduce la certeza del hecho presunto.

6. En la tramitación de los expedientes sancionadores han de observarse escrupulosamente las reglas establecidas para la práctica de las pruebas; en especial, las atinentes a las garantías formales necesarias. El derecho de defensa comprende no solo el de conocer qué se imputa al interesado -pues solo conociendo dichas imputaciones es posible articular de forma completa y cierta dicha defensa-, sino también el de poder oponer frente a ellos las oportunas excepciones y defensas y participar en la práctica de las pruebas que sirven de sustento a la decisión de la Administración.

   El derecho a la prueba exige que sean practicadas “sin desconocimientos y obstáculos” (*Sentencias del Tribunal Constitucional 104/2003, de 2 de junio; 128/2003, de 30 de junio; 157/2000, de 12 de junio,* etc.). No pueden serlo de cualquier manera. Han de llevarse a cabo asegurando al encartado, al momento de su práctica, ciertas garantías entre las que se cuenta, de un lado, la posibilidad de contradicción, lo que implica que esté presente y participe en su ejecución y, de otra parte, la inmediación del instructor, esto es, que sea este quien dirija su práctica.

   Por todo ello, ha de velarse por la estricta observancia de las reglas reguladoras de la práctica de la prueba y de su valoración en cada caso concreto, ponderando las específicas circunstancias concurrentes y orillando cualquier forma de aplicación mecánica de criterios valorativos. Y, aún con más rigor, en el caso de que dichas diligencias se basen en actuaciones desarrolladas por entidades privadas colaboradoras de la Administración como son los organismos de control autorizados.

7. Por otra parte, la Ley 40/2015, de 1 de octubre, de Régimen Jurídico de las Administraciones públicas, no regula el procedimiento administrativo sancionador sino que establece los principios que lo informan. Sigue la estela de la Ley 30/1992, de 26 de noviembre. La Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común, por su parte disciplina de manera dispersa algunos aspectos de dicho procedimiento. Esta falta de sistemática y de rigor en la labor legislativa, ha hecho que sean múltiples las disposiciones de rango legal y reglamentario que los disciplinen. Y ello tiene consecuencias desafortunadas por cuanto es difícil establecer criterios unitarios en la materia, apreciándose una dispersión en la interpretación y aplicación de las normas sancionadoras por parte de las Administraciones Públicas.

   Un examen –aún somero- de las normas y de los procedimientos sancionadores permite colegir que, en relación con determinados extremos, no existe unidad de

criterio a la hora de abordar unas mismas cuestiones. Así, en lo tocante a la suspensión del procedimiento administrativo sancionador en tanto existan en tramitación diligencias penales, las normas utilizan diferente terminología y criterios a la hora de dar preferencia al orden jurisdiccional penal. En ocasiones, establecen distintos momentos en los que la suspensión por razón de la tramitación de las diligencias termina: unas veces, la paralización cesa al dictarse sentencia; otras veces, cuando la sentencia penal es firme (caso de la Ley 21/2003, de 7 de julio, de Seguridad Aérea, Ley 38/2003, de 17 de noviembre, General de Subvenciones, etc.); no faltan los casos en los que se cita el archivo como hito en el que dicha suspensión se levanta (Ley 58/2003, de 17 de diciembre, General Tributaria). Y en fin, en otros casos, la paralización del procedimiento administrativo sancionador viene determinada por la iniciación de actuaciones judiciales o también por la incoación de actuaciones por parte del Ministerio Fiscal.

La falta de criterios uniformes constituye un baldón predicable de las mencionadas Leyes 39/2015 y 40/2015, de 1 de octubre. La cuestión debió ser resuelta en ellas. No se hizo por la premura y precipitación con que se elaboraron y por su falta de rigurosidad.

2. UN CASO SINGULAR: EL DEBER DEL TITULAR DEL VEHÍCULO DE CONOCER Y FACILITAR A LA ADMINISTRACIÓN LOS DATOS NECESARIOS PARA IDENTIFICAR AL CONDUCTOR

La Administración de tráfico ha venido promoviendo –y obteniendo- durante los últimos años la aprobación de una legislación especial reguladora de su actividad, siguiendo la estela de la Administración tributaria. Dicha legislación especial adquiere tintes de excepcionalidad en muchas ocasiones por cuanto se funda en principios diametralmente opuestos a los que informan la regulación general. Se trata de una legislación que carece de justificación, puesto que la seguridad vial no es más relevante que otra infinidad de materias sectoriales desenvueltas por la actividad administrativa y que se sujetan a las reglas generales de ordenación pública. Se trata además de una legislación especialmente lesiva para los derechos de los administrados, en la que poco importan sus garantías y en la que se las sacrifica sin rubor en aras de una eventual eficacia de las medidas encaminadas a evitar las víctimas de los accidentes de tráfico.

La pérdida de garantías alcanza umbrales especialmente relevantes en el ámbito del ejercicio de la potestad sancionadora por infracciones de la Ley de la Seguridad Vial, dándose casos verdaderamente anómalos.

Un caso singular –si no es anómalo- que se presenta con ocasión de los expedientes sancionadores de tráfico es aquel en que se requiere al titular de un vehículo a motor para que facilite a la Administración los datos necesarios para identificar al conductor.

En vía administrativa, el Consejo de Estado ha examinado la cuestión en varias ocasiones (*Dictámenes 1989/2009, de 18 de febrero de 2010 y 2337/2010//643/2010, de 21 de diciembre de 2010,* entre otros) ante la imposición mecánica de sanciones a los administrados por parte de la Administración en los casos de infracción del referido deber.

El artículo 93 del Real Decreto Legislativo 6/2015, de 30 de octubre, por el que se aprueba el texto articulado de la Ley sobre Tráfico, circulación de Vehículos a Motor

y Segundad Vial, dispone "*en el supuesto de que no se haya producido la detención del vehículo, el titular, el arrendatario a largo plazo o el conductor habitual, en su caso, dispondrán de un plazo de veinte días naturales para identificar al conductor responsable de la infracción".* Y caso de no hacerlo, se le puede imponer una sanción. Este precepto, trasunto del artículo 72 del anterior texto refundido de la misma Ley de 1990, tiene su origen en el antiguo artículo 278.1 del Código de la Circulación, que fue interpretado por el Tribunal Constitucional en la Sentencia 219/1998. El Alto Tribunal señaló que el artículo 278.1 del Código de la Circulación se basaba en el principio correcto de la responsabilidad personal por hechos propios (principio de la personalidad de la pena o sanción), al decir que "serán responsables de las infracciones (...) los conductores de vehículos (...) que las cometiesen". Señaló el Alto Tribunal que no se puede inferir de la notificación de la denuncia y de la advertencia de la posible exigencia de la multa al titular del vehículo, que dicha previsión resulte una legitimación a la Autoridad de Tráfico para imponerle directamente la sanción pecuniaria, ni por ello la exonera de proseguir las pertinentes diligencias de prueba para conseguir la identificación del conductor. La advertencia no puede convertirse -por la pasividad de la Administración- en una presunción *iuris et de iure* que no resulta, en los términos absolutos que entraña dicha presunción, del artículo 278 del Código de la Circulación.

El precepto vigente se configura legalmente como un deber de colaboración del titular de un vehículo con la Administración en la identificación del conductor supuestamente responsable. Deber que es inherente al hecho de ser titular o conductor habitual. Su incumplimiento constituye una infracción autónoma en materia de tráfico y circulación de vehículos, que obliga al titular del automóvil a *"conocer y facilitar"* los datos necesarios para proceder a esa identificación cuando sea requerido.

No obstante, en la Sentencia del Tribunal Constitucional 111/2004, dictada en un recurso de amparo interpuesto contra resolución que imponía una multa por no haber aportado datos suficientes para identificar al conductor de un vehículo que había cometido una infracción de tráfico -en este caso faltaba el número de DNI del conductor-, el Alto Tribunal señaló que la necesidad de motivación debe vincularse con el derecho a la legalidad sancionadora consagrado en el artículo 25.1 de la Constitución. Los aspectos esenciales de la interpretación de la norma tipificadora deben expresarse en la motivación de la resolución con el fin de permitir la comprobación de si la decisión sancionadora es fruto previsible de una razonable aplicación judicial o administrativa de lo dispuesto en la Ley. El Alto Tribunal añadió que no solo vulneran el principio de legalidad las resoluciones sancionadoras que se sustenten en una subsunción de los hechos ajena al significado posible de los términos de la norma aplicada sino que son también constitucionalmente rechazables aquellas aplicaciones que, por su soporte metodológico o axiológico, conduzcan a soluciones esencialmente opuestas a la orientación material de la norma y, por ello, imprevisibles para sus destinatarios. En resumen, el Tribunal Constitucional concluyó que el titular de un vehículo no puede ser sancionado por no haber facilitado, a los efectos de la identificación, el número de DNI del conductor si ya había notificado su nombre. Y este criterio debe ser tenido en cuenta por la Administración.

Se ha suscitado también la cuestión de la eventual existencia de una contradicción entre el deber del titular de conocer y facilitar los datos del conductor a la Administración instructora y la posible exención de ese deber de facilitar los datos (conocidos) en el caso de que el conductor resultara ser una de las personas a las que se refiere el artículo 261 de la Ley de Enjuiciamiento Criminal.

Como es sabido, este último precepto se expresa en estos términos: "Tampoco estarán obligados a denunciar: 1. El cónyuge del delincuente. 2. Los ascendientes y descendientes consanguíneos o afines del delincuente y sus colaterales consanguíneos o uterinos y afines hasta el segundo grado inclusive; 3. Los hijos naturales respecto de la madre en todo caso, y respecto del padre cuando estuvieren reconocidos, así como la madre y el padre en iguales casos".

Resulta especialmente significativo que una persona no pueda ser sancionada penalmente por no denunciar a su cónyuge, autora de un ilícito –v.gr. un asesinato- y sí lo pueda ser por no comunicar a la autoridad de tráfico que conducía su vehículo. Si el derecho es solo un instrumento formal de fuerza o violencia, la norma legal que ampara la situación es irreprochable. Pero si el derecho es algo más –aún orillando la idea de justicia, si es simplemente ordenación razonable, la regulación vigente carece de legitimidad.

En este último sentido, el Consejo de Estado ha considerado –desde el dictamen antes citado 2337/2010//643/2010, de 21 de diciembre de 2010- que la Ley de Enjuiciamiento Criminal ocupa una especial posición en el sistema sancionador, cuyos principios y criterios alcanzan no solo a los procedimientos penales sino también al ejercicio de las potestades sancionadoras por parte de la Administración pública. El *ius puniendi* estatal aparece, en nuestro sistema constitucional, compartido entre los órganos judiciales penales y la Administración (*Sentencia del Tribunal Constitucional 188/2005*) de modo que esos principios informadores no pueden diferir en uno y otro supuesto.

Así las cosas, la exclusión del deber de denunciar a determinadas personas resulta de aplicación también en el procedimiento sancionador administrativo de tráfico, sobre todo si se tiene en cuenta la relevancia de los bienes protegidos. Y es que, a la potestad sancionadora de la Administración, como se ha dicho, le son aplicables los principios sustantivos derivados del artículo 25.1 de la Constitución y las garantías procedimentales concedidas al ciudadano en el 24.2, como es doctrina constante del Tribunal Constitucional desde la Sentencia 18/1981.

3. UN CASO EXCLUIDO: PROCEDIMIENTOS SANCIONADORES DE PERSONAS VINCULADAS CON LA ADMINISTRACIÓN POR LA LEGISLACIÓN DE CONTRATOS DEL SECTOR PÚBLICO O POR LA LEGISLACIÓN PATRIMONIAL DE LAS ADMINISTRACIONES PÚBLICAS

El artículo 25.4 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico de las Administraciones Públicas establece que "las disposiciones de este capítulo no serán de aplicación al ejercicio por las Administraciones Públicas de la potestad sancionadora respecto de quienes estén vinculados a ellas por relaciones reguladas por la legislación de contratos del sector público o por la legislación patrimonial de las Administraciones Públicas".

En virtud de esta previsión, queda consolidado el criterio de que las penalidades impuestas al contratista o al concesionario de bienes de dominio público no tienen la condición de sanciones administrativas. Por consiguiente, no se sujetan a las prescripciones establecidas para los procedimientos sancionadores. Las penalidades y sanciones que las Administraciones públicas pueden imponer a los contratistas y concesionarios son instrumentos –convencionales y legales- de coerción propios, distintos de las sanciones en estricto sentido, que se insertan en las relaciones bilaterales.

Tienen una naturaleza peculiar. No derivan de las potestades administrativas generales sino de concretas relaciones convencionales o actos específicos de atribución –licencias o autorizaciones-. En eso se diferencian de las sanciones administrativas previstas en las normas sectoriales específicas, cuya regulación general procedimental se establece en las leyes 39/2015 y 40/2015, de 1 de octubre. El que deriven de relaciones convencionales o de actos concretos de atribución no implica, por otra parte, que tengan que estar previstas en el correspondiente pliego de condiciones o título habilitante. Las facultades coercitivas o sancionadoras de la Administración pueden nacer –y lo hacen- directamente de la Ley. Lo que se quiere decir es que las sanciones administrativas son punitivas, castigan conductas en tanto que las aplicables en el seno de las relaciones contractuales y dominicales son instrumentos resarcitorios o coercitivos, encaminados a que el contratista lleve a efecto el servicio contratado, aunque los términos del contrato ofrezcan dudas, porque de lo contrario se pueden seguir perjuicios irreparables para la causa pública. En otros términos, las sanciones aplicables en las relaciones contractuales y dominicales son primordialmente coercitivas, encaminadas a asegurar el cumplimiento de las prestaciones, aunque en ocasiones adquieran tinte punitivo.

La exclusión del ámbito de la regulación contenida en los artículos 25 y siguientes de la Ley 40/2015, de 1 de octubre, de este tipo de sanciones tiene consecuencias claras. No rigen los principios de culpabilidad y proporcionalidad. Se debilita el de tipicidad y resulta inaplicable la presunción de inocencia. Pero a lo que aboca la exclusión es a una duda: en concreto, a la pervivencia de la doctrina jurisprudencial de la caducidad de los procedimientos por aplicación del plazo máximo de tramitación cuando no se ha dictado resolución (Ley 39/2015, de 1 de octubre, artículo 25.1.b).

Sabido es que la Audiencia Nacional, primero, y el Tribunal Supremo, después, sentaron el criterio de que los procedimientos de resolución de contratos por causa imputable al contratista, los de declaración de caducidad de las concesiones por incumplimiento de los concesionarios y los de imposición de penalidades están sujetos a los plazos máximos de tramitación legal o reglamentariamente establecidos (hoy Ley 39/2015, artículo 25.1.b). Y que su superación, sin haberse dictado y notificado la correspondiente resolución al interesado, comporta automáticamente que quedan incursos en causa de caducidad, debiendo archivarse. Esta doctrina jurisprudencial no nació porque se considerara que las potestades ejercidas por la Administración fueran materialmente sancionadoras. Nació como fórmula de los órganos judiciales para quitarse de en medio, de la manera más expeditiva y directa, sin necesidad de entrar en el fondo de los asuntos, numerosos recursos contencioso-administrativos. No había construcción teórica alguna que la sustentara. Luego, la jurisprudencia ha tratado de vestir su actuación con dudosos criterios sustantivos. La cuestión que se plantea ahora es la relativa a si dicha doctrina puede pervivir tras la manifestación legal contenida en el artículo 25.4 de la Ley 40/2015, de 1 de octubre. Y parece que, a tenor de los artículos citados, la respuesta es negativa, por cuanto las sanciones impuestas en el ámbito de las relaciones contractuales y demaniales no participan de la naturaleza de las sanciones punitivas.

Fecha de recepción: 18/01/2018. Fecha de aceptación: 25/06/2018

LOS ORÍGENES HISTÓRICOS DE LA GUARDIA CIVIL COMO POLICÍA JUDICIAL EN LAS LEYES DE ENJUICIAMIENTO CRIMINAL DE 1872 Y 1882

JESÚS NARCISO NÚÑEZ CALVO

DOCTOR EN HISTORIA Y CORONEL DE LA GUARDIA CIVIL

RESUMEN

Tras la importante reforma del Código Penal en 1870 se aprobó la Ley provisional sobre organización del Poder Judicial. En una de sus disposiciones transitorias se dispuso la organización "de la policía prejudicial y judicial, para que en el futuro quedase suficientemente asegurada la protección de las personas, la seguridad de los bienes, la prevención de las causas criminales y el descubrimiento de la verdad en los sumarios." Dos años después, en 1872, se promulgó la Ley provisional de Enjuiciamiento Criminal donde se determinaba quienes debían auxiliar a los jueces y constituir la policía judicial. Una década más tarde, en 1882, entraba en vigor una nueva Ley de Enjuiciamiento Criminal que continúa hoy día. En ambas leyes solo se citaba expresamente una única institución de seguridad pública: la Guardia Civil, creada en 1844. Respecto al resto, se limitaban a realizar referencias genéricas. En el presente trabajo se analiza y explica la razón de ello. Ambas leyes constituyen una referencia historiográfica de primer nivel que contribuyen a acreditar, una vez más, que el Cuerpo de la Guardia Civil es la institución de seguridad pública y Policía Judicial más antigua que existe actualmente en España.

Palabras clave: Guardia Civil, policía judicial, seguridad pública, Ley de Enjuiciamiento Criminal.

ABSTRACT

After the important reform of the Criminal Code in 1870, the provisional Law for the organization of the Judicial Power was approved. In one of its transitory provisions, the organization of the pre-judicial and judicial police was established, so that in the future the protection of persons, the security of property, the prevention of criminal cases and the discovery of the truth in the summaries was guaranteed. Two years later, in 1872, the Provisional Criminal Prosecution Law was enacted, which determined who should assist the judges and establish the judicial police. A decade later, in 1882, a new Criminal Prosecution Law came into force, which, with its modifications, continues until today. In both laws, only one public security institution was specifically mentioned: the Civil Guard. Regarding the rest, they only made generic references. In this paper, the reason for this is analyzed and explained. Both laws constitute a first level historiographic reference that contributes to prove, once again, that the Civil Guard Corps is the oldest public security institution and judicial police that currently exists in Spain.

Keywords: Spanish Civil Guard, judicial police, public security, Law of Criminal Procedure.

1. INTRODUCCIÓN

La Ley de Enjuiciamiento Criminal es la que regula las actuaciones judiciales en materia Penal en España.

Como consecuencia de la aprobación de la Constitución de 1º de junio de 1869, elaborada tras el derrocamiento de Isabel II, fue necesario reformar el Código Penal que estaba en vigor desde su promulgación el 6 de junio de 1850.

Dicho texto estuvo vigente durante dos décadas hasta que el 18 de junio de 1870 fue aprobada su modificación. Transcurridos apenas tres meses, el 15 de septiembre, se aprobó la Ley Orgánica del Poder Judicial. Dicha norma dio lugar, dos años después, a la aprobación por Real Decreto de 22 de diciembre de 1872 de la Ley provisional de Enjuiciamiento Criminal.

Tras estar en vigor casi una década fue promulgada una nueva Ley por Real Decreto de 14 de septiembre de 1882. Publicada tres días después en la *Gaceta de Madrid*, antecedente histórico de nuestro actual Boletín Oficial del Estado, entró en vigor el 3 de enero de 1883.

Y desde entonces, a pesar de haber sido objeto de numerosas reformas, la más reciente data de 5 de octubre de 2015, sigue estando vigente.

Consideraciones jurídicas aparte hay que precisar que ambas leyes constituyen una muy interesante referencia historiográfica de primer nivel para acreditar al Cuerpo de la Guardia Civil como la institución de seguridad pública y de policía judicial más antigua que existe actualmente en España.

La actual redacción del artículo 283 de la Ley de Enjuiciamiento Criminal textualmente dice:

Constituirán la Policía judicial y serán auxiliares de los Jueces y Tribunales competentes en materia penal y del Ministerio fiscal, quedando obligados a seguir las instrucciones que de aquellas autoridades reciban a efectos de la investigación de los delitos y persecución de los delincuentes:

Primero. Las Autoridades administrativas encargadas de la seguridad pública y de la persecución de todos los delitos o de algunos especiales.

Segundo. Los empleados o subalternos de la policía de seguridad, cualquiera que sea su denominación.

Tercero. Los Alcaldes, Tenientes de Alcalde y Alcaldes de barrio.

Cuarto. Los Jefes, Oficiales e individuos de la Guardia Civil o de cualquier otra fuerza destinada a la persecución de malhechores.

Quinto. Los Serenos, Celadores y cualesquiera otros Agentes municipales de policía urbana o rural.

Sexto. Los Guardas de montes, campos y sembrados, jurados o confirmados por la Administración.

Séptimo. Los funcionarios del Cuerpo especial de Prisiones.

Octavo. Los Agentes judiciales y los subalternos de los Tribunales y Juzgados.

Noveno. El personal dependiente de la Jefatura Central de Tráfico, encargado de la investigación técnica de los accidentes.

Este trabajo se va a remontar hasta el origen del texto de dicho artículo y se van a esclarecer cuáles fueron las motivaciones del legislador, respecto a la Guardia Civil y las

demás instituciones de seguridad pública, que dieron lugar a su redacción e inclusión en una ley que medía milimétricamente cada una de las palabras que la componían.

2. LA EVOLUCIÓN DEL MODELO POLICIAL ESPAÑOL (1812-1872)

En primer lugar vamos a referenciar qué Cuerpos garantes de la seguridad pública y auxiliares de las autoridades judiciales existían cuando se elaboró y entró en vigor la mentada Ley provisional de Enjuiciamiento Criminal de 1872, así como cuales eran sus despliegues y atribuciones como policía judicial.

Pero previamente es necesario conocer, aunque sea someramente, los antecedentes inmediatos principales de dicha estructura de seguridad pública que, sin duda alguna, debieron contribuir a su redacción y aprobación en los términos que se hizo.

A veces se habla con ligereza o desconocimiento de todo ello, no exento en ocasiones de ciertos intereses corporativistas que desvirtúan una verdad y una realidad que antaño nunca fueron cuestionadas, intentando reescribirse en los últimos años una historia policial que nunca lo fue.

También es necesario precisar, aunque no es el objeto del presente trabajo, que abordar y exponer al lector la historia de las instituciones de seguridad pública del siglo XIX, y muy especialmente la de la primera mitad, es una tarea tremendamente complicada, incluso para los investigadores más capacitados y expertos en la materia.

De hecho, la consulta de sus obras así lo acredita, pues salvo la Guardia Civil, cuya historia está perfectamente clara desde el mismo momento de sus partidas de gestación y nacimiento en 1844 hasta la actualidad, ninguna otra institución de seguridad pública española puede afirmar y mucho menos acreditar lo mismo.

Es por ello que resulta interesante conocer brevemente, por orden cronológico, cual fue la evolución del modelo policial español desde nuestra primera Constitución, aprobada el 19 de marzo de 1812, hasta la entrada en vigor de la primera Ley de Enjuiciamiento Criminal seis décadas después.

Es decir, cómo se evolucionó desde un modelo policial basado prácticamente en instituciones de escasa capacidad y durabilidad, cuyo ámbito de actuación era local, aunque fueran proyectadas con ánimo de extenderse progresivamente por todo el territorio nacional. Y cómo se llegó a un modelo potente, robusto y eficaz liderado por lo que realmente fue y sigue siendo la primera policía del estado, tanto en antigüedad, como en número de efectivos y despliegue.

Si bien en la España de principios del siglo XIX existía la oportuna legislación que sancionaba a los malhechores que perpetraban delitos, se carecía de una institución de ámbito estatal, de carácter civil o militar que, debidamente organizada, instruida y dotada de los reglamentos y medios pertinentes, se encargara de velar por la seguridad pública.

Tal cometido se había venido encomendando tradicionalmente al Ejército, circunstancia que realmente no era ni del agrado de quienes lo mandaban ni de quienes lo integraban, pues sus competencias eran otras bien diferentes, no estando adiestrados para perseguir delincuentes. El problema de seguridad pública existente, que era muy grave, requería una solución policial en vez de una respuesta militar.

2.1. LA MILICIA NACIONAL

La Constitución de 1812, sin perjuicio del denominado "Ejército permanente," intentó implantar una solución definitiva para ello. Dispuso en su artículo 362 la creación en cada provincia de cuerpos de milicias nacionales, de ámbito local, compuestos por habitantes de cada una de ellas, en proporción a su población y circunstancias.

El 18 de abril de 1814, estando todavía Fernando VII, en "ausencia y cautividad," se aprobó por las Cortes su reglamento provisional, asignándosele entre sus funciones las de patrullas de seguridad pública y las de perseguir y aprehender en el pueblo y su término, a los desertores y malhechores[1].

Aquello no tuvo apenas recorrido y hubo que esperar al inicio del denominado "Trienio Liberal" para el establecimiento de la Milicia Nacional por Real Decreto de la Junta Provisional, de 25 de abril de 1820[2], y la consiguiente aprobación de su reglamento, que no modificó las funciones recogidas en el que se había redactado seis años antes[3].

La seguridad pública seguía siendo una prioridad para los gobiernos de la época, pero no fueron capaces de crear una institución armada, civil o militar, adecuada para ello y de ámbito estatal, lo cual quedó patente una vez más con la aprobación del Reglamento provisional de Policía, por Real Decreto de 6 de diciembre de 1822[4].

Tal y como exponía su artículo 1º, la seguridad de las personas y bienes, así como la conservación del orden público, estaba a cargo de los jefes políticos[5] en todos los pueblos de su provincia, los alcaldes en sus respectivos pueblos, "auxiliados en la forma que se deba por los demás individuos de ayuntamiento y de los ayudantes de barrio, donde deba haberlos".

Estos constituían realmente la única institución policial de seguridad pública de la época, si bien de ámbito local, teniendo obligación de prestarles debido auxilio en tales funciones el "Ejército permanente," la Milicia Nacional, "y aún los vecinos", conforme se establecía en el artículo 3º.

Realmente se trataba de una policía de ámbito local, sin cohesión ni cualificación ni medios para poder desempeñar su labor de forma eficaz y eficiente. Todavía quedaban dos décadas para que el Estado vertebrara bajo esos parámetros la seguridad pública española, con la creación y despliegue de la primera policía estatal: la Guardia Civil.

1 Gaceta de la Regencia de las Españas, núm. 68, 10/05/1814, pp. 498-505.
2 Gaceta de Madrid, núm. 71, 26/04/1820, p. 465.
3 Ibídem, pp. 465-469.
4 Ibídem, núm. 376, 26/12/1822, pp. 1.891-1.892.
5 Dicha figura, antecesora del gobernador civil, nació del artículo 324 de la Constitución de Cádiz, en el que se establecía que el gobierno político de las provincias residía en el jefe superior, nombrado por el Rey en cada una de ellas. Posteriormente la "Instrucción para el gobierno económico-político de las provincias," aprobada por Decreto de la Regencia de fecha 23/06/1813, dedicó su capítulo III a los jefes políticos, disponiendo en su artículo 1º que "reside en él la superior autoridad dentro de la provincia para cuidar de la tranquilidad pública, del buen orden, de la seguridad de las personas y bienes de sus habitantes, de la ejecución de las leyes y órdenes del Gobierno; y en general de todo lo que pertenece al orden público y prosperidad de la provincia." Gaceta de la Regencia de las Españas, núm. 94, 24/07/1813, p. 786.

Muy interesante a efectos de acreditar las carencias del modelo policial de 1822 y la necesidad de contar con apoyos externos, dada su propia incapacidad, es el Capítulo V del mentado reglamento, dedicado íntegramente a la seguridad de los caminos.

El artículo 35 fijaba que para perseguir a los malhechores y proporcionar la seguridad en los caminos se destinarían las tropas del ejército permanente que permitiesen las circunstancias, poniéndose de acuerdo para ello la autoridad militar del distrito o provincia correspondiente y el jefe superior político.

El artículo siguiente disponía que en ausencia de dichas tropas o cuando fuese necesario auxiliarlas lo haría la Milicia Nacional de cada localidad, por orden de sus alcaldes o jefe político de la provincia.

Finalmente el artículo 37 exponía que si por la frecuencia de robos no se estimasen suficientes dichas fuerzas, quedaban autorizados los jefes políticos, con el acuerdo de las diputaciones provinciales, a formar por un tiempo determinado partidas de escopeteros.

En 1823 se aprobó por las Cortes la Ley de 3 de febrero, la "Instrucción para el gobierno económico-político de las provincias", estableciéndose que competía a los alcaldes, bajo la inspección de los jefes políticos, la conservación de la tranquilidad y del orden público, y la seguridad y protección de las personas y bienes de los habitantes de sus respectivos distritos. Para ello, y conforme se disponía en el articulado de su Capítulo III, podían disponer de la "Milicia Nacional local", que estaba directamente a sus órdenes para esos menesteres, o requerir el auxilio del "Ejército permanente" o de la "Milicia Nacional activa" que se hallare en su pueblo. Y si no hubiera dichas fuerzas podían solicitarlas al jefe político de la provincia para que este a su vez lo peticionara al jefe militar correspondiente.[6]

Es decir, era un modelo policial insatisfactorio e ineficaz. Es por ello que sin perjuicio del desarrollo y evolución dispar que fue teniendo la Milicia Nacional, cuyos resultados también hay que decir que no fueron nada provechosos, se continuaron proyectando infructuosamente en paralelo nuevas instituciones policiales, de carácter militar o civil, para velar por el orden y la seguridad pública.

2.2. LA LEGIÓN DE SALVAGUARDIAS NACIONALES

Mención especial merece este proyecto que el teniente general Pedro Agustín Girón Las Casas, ministro de la Guerra y padre del futuro fundador de la Guardia Civil, nuestro II duque de Ahumada, presentó el 30 de julio de 1820 a las Cortes para su aprobación.

Se trataba, frente al resto de instituciones de seguridad pública de ámbito local o regional de la época, de un cuerpo de ámbito nacional y carácter militar destinado exclusivamente a lograr la paz y la seguridad interior del país.

Aunque se trataba de un proyecto que fue muy superado en todos los aspectos por el de la Guardia Civil, era realmente muy novedoso en cuanto a su concepción.

6 PARGA, J. (1836). Instrucción para el gobierno económico-político de las provincias. La Coruña: Imprenta de Iguereta.

Con él se pretendía "el exterminio de los malhechores y la seguridad en los caminos, objeto principal de su instituto, cuyas circunstancias no se han podido lograr jamás a pesar de las medidas del Gobierno y de los esfuerzos y sacrificios de los pueblos." Fue rechazado en la votación por considerarse "medida atentatoria a la libertad y desorganizadora de la Milicia Nacional"[7].

2.3. LOS CELADORES REALES

Fueron creados por la Junta provisional de Gobierno, al mismo tiempo que se producía la invasión francesa para restaurar el Absolutismo en España con Fernando VII a la cabeza. En cada provincia debía haber una compañía, siendo en Zaragoza la primera que se organizó el 4 de mayo de 1823.

Dos años después, por Real Decreto de 1º de septiembre, se dispuso la creación de un regimiento, pero su plantilla nunca llegó a completarse. Formó parte del Arma de Caballería del Ejército y dependía, a efectos de servicio, de la recién creada Superintendencia general de la Policía.

Casi dos años más tarde, tras informes negativos de esta, por Real Orden de 13 de mayo de 1827, volvió a ser reducido a una compañía, circunscribiéndose su ámbito de actuación a Madrid y alrededores. Terminó por desaparecer poco después[8]. A este respecto hay que decir que fue muy habitual en esa época que proyectos de creación de cuerpos de seguridad pública con ambición de despliegue nacional terminaran prácticamente limitados a la ciudad de Madrid, donde residía la Corte, y su zona próxima de influencia.

2.4. LA POLICÍA GENERAL DEL REINO

Fue creada por Real Decreto de 8 de enero de 1824[9]. Se trató de un ambicioso e interesante proyecto que, al igual que sucedió con otras instituciones de seguridad pública de la época, nació con vocación de permanencia y ámbito estatal, pero fracasó en el intento al no conseguir ni lo uno ni lo otro. Ni tuvo continuidad en el tiempo ni vertebró el Estado al no conseguir desarrollar apenas su despliegue territorial.

Precisamente sería la razón principal de su creación, la de policía política o secreta que predominaba sobre el resto de funciones, expresada veladamente por el propio rey Fernando VII al inicio de la exposición de motivos, lo que tres lustros después llevaría a su abolición en los términos más duros, como se verá más adelante, que nunca ha visto una resolución oficial:

Entre las atenciones que al verme restituido a la plenitud de los derechos legítimos de mi soberanía, reclaman con urgencia mi paternal solicitud, he considerado como una de las más importantes el arreglo de la Policía de mis Reinos, la cual debe hacerme conocer la opinión y las necesidades de mis pueblos, e indicarme los medios de reprimir el espíritu de sedición, de extirpar los elementos de discordia, y de desobstruir todos los manantiales de prosperidad.

7 AGUADO, F. (1983). Historia de la Guardia Civil. Madrid y Barcelona: Ediciones Históricas, Cupsa y Planeta, vol. I, pp. 163-166.

8 SIDRO, J. y QUEVEDO, A. (1858). La Guardia Civil. Historia de esta institución y de todas las que se han conocido en España con destino a la persecución de malhechores, desde los tiempos más remotos hasta nuestros días. Madrid: Autores, pp. 448-449.

9 Gaceta de Madrid, núm. 6, 13/01/1824, pp. 25-28.

Una de sus debilidades iniciales fue también no disponer de fuerza propia suficiente acorde con las numerosas competencias de diverso tipo asignadas, razón por la cual en su artículo XV se dispuso los apoyos necesarios.

Concretamente se estableció que cuando la Policía precisara para el desempeño de sus funciones, el auxilio o cooperación de fuerza armada, podría utilizar ("ínterin establezco un Cuerpo militar especialmente encargado de la seguridad de los pueblos y de los caminos") de sus alguaciles y dependientes; y en caso necesario invocar el auxilio de los comandantes militares, de los ayuntamientos, jueces y tribunales, de los jefes de la Real Hacienda, "y de cuantos tengan fuerza armada de que disponer."

Si bien es cierto que constituyó en su inicio un prometedor y significativo avance respecto al resto de instituciones de seguridad pública que hasta esa fecha se habían creado, le perjudicó letalmente su singular y excesiva implicación política con algunos de los gobiernos bajo los que sirvió.

Ello terminó provocando no solo que no terminara desarrollando su proyecto inicial, sino que fuera incluso objeto de durísimos reproches por los gobiernos que sucedieron a los que habían hecho un uso abusivo de sus capacidades, siendo condenada finalmente a su abolición definitiva.

Por Real Orden de 14 de agosto de 1827 se revisó y modificó su reglamento de 20 de febrero de 1824, procediéndose a una significativa reducción de personal y presupuestos, así como de atribuciones y competencias[10].

Si bien un Real Decreto del Ministerio de Fomento, de 25 de septiembre de 1833[11], publicado al día siguiente, víspera del fallecimiento de Fernando VII, volvió brevemente a fortalecerla parcialmente, ello apenas duró un mes.

Así, por Real Orden de 23 de octubre siguiente, tras comenzar exponiendo que la Policía General del Reino debía circunscribirse "en los límites de que nunca debió salir, que ejercitando su vigilancia sobre algunos no lo haga sino en el interés de la seguridad de todos; y que, en lugar de instrumento de vejaciones, sea un medio de gobierno, y por consiguiente un elemento de protección," se ordenó al superintendente general, "haga inmediatamente revisar y refundir en este sentido los reglamentos del ramo, suprimiendo en ellos toda precaución exorbitante, toda formalidad vejatoria, toda traba, en fin, que no sea absolutamente exigida por la necesidad de conservar el orden y de asegurar el reposo general"[12].

La situación se fue complicando cada vez más para dicha institución policial hasta que, tras la creación del Ministerio del Interior[13], por Real Decreto de 13 de mayo de 1834[14], se terminó dictando el Real Decreto de 4 de octubre de 1835[15], mediante el que quedó "suprimida la superintendencia general de policía, creada en virtud del Real Decreto de 8 de enero de 1824."

10 Ibídem, núm. 99, 18/08/1827, pp. 393-394.
11 Ibídem, núm. 117, 26/09/1833, p. 499.
12 Ibídem, núm. 131, 24/10/1833, p. 562.
13 ROJAS, J.; y DE ANDRÉS, R. (2015). Ministerio del Interior. Dos siglos de historia. Bilbao (Vizcaya): Ministerio del Interior, pp. 44-46.
14 Gaceta de Madrid, núm. 84, 15/05/1834, p. 385.
15 Ibídem, núm. 283, 05/10/1835, pp. 1.121-1.122.

Otro Real Decreto de fecha 25 del mismo mes suprimió la contaduría general de policía, incorporándola a la del "Ministerio de lo Interior"[16], que a su vez por Real Decreto de 4 de diciembre siguiente, pasó a denominarse "Ministerio de la Gobernación del Reino"[17].

El final definitivo de la Policía General del Reino vendría mes y medio después de serle conferida, por la Regente María Cristina de Borbón, la presidencia del Consejo de Ministros al capitán general Joaquín Baldomero Fernández-Espartero Álvarez de Toro[18]. Este, cuatro semanas después, se hizo cargo de la regencia al renunciar y exiliarse aquella[19].

Así, por Real Decreto de 2 de noviembre de 1840, tomando en consideración lo que con dicha fecha había expuesto el ministro de la Gobernación, Manuel Cortina Arenzana, a la Regencia provisional del Reino, se decretó que quedaba "abolida la policía secreta y prohibido hacer ningún gasto con tal objeto". Igualmente se dispuso que se propondría con urgencia la organización que debiera tener la "policía de protección y seguridad pública" ejercida por las autoridades que la ley reconoce[20].

Sin embargo, a pesar de instarse de forma expresa tal urgencia, su organización, como se verá más adelante, se demoraría aún más de tres años como consecuencia, entre otras causas, de las constantes crisis políticas y sucesivos cambios de gobierno que padeció la nación.

Finalmente, la puesta en marcha del nuevo proyecto terminó por motivar la creación de la primera institución de seguridad pública desplegada en todo el territorio nacional que con permanencia de futuro terminó por vertebrar el Estado: la Guardia Civil.

2.5. LOS SALVAGUARDIAS REALES

Fueron creados por Real Decreto de 25 de febrero de 1833. Se trataba de un Cuerpo integrado por 500 hombres, bajo la dirección y dependencia de la Superintendencia de Policía de Madrid.

Dicho Cuerpo estaba destinado a prestar su servicio en Madrid y en sus inmediaciones, así como a servir de base para constituir el de todo el Reino. El proyecto era alcanzar una plantilla de 10.075 hombres, de los cuales 2.016 serían de caballería, aspirando a poder desplegarse por todas las provincias. Sin apenas desarrollo ni éxito alguno fue disuelto en 1839[21].

2.6. EL RAMO DE PROTECCIÓN Y SEGURIDAD

A pesar de que en el mentado Real Decreto de 1840 sobre abolición de la Policía General del Reino se urgía la reorganización de la "policía de protección y seguridad pública", ello no se llevó a cabo con la inmediatez que la situación requería.

16 Ibídem, núm. 306, 28/10/1835, pp. 1.213-1.214.
17 Ibídem, núm. 347, 08/12/1835, p. 1.386.
18 Ibídem, núm. 2.159, 20/09/1840, p. 1.
19 Ibídem, núm. 2193, 20/10/1840, p. 1.
20 Ibídem, núm. 2.207, 03/11/1840, p. 2.
21 SIDRO, J. y QUEVEDO, A.; op. cit., p. 450.

Realmente la situación de la Seguridad Pública en España era deplorable. Y no solo en sus caminos, si bien era donde más se manifestaba al afectar directamente a la libertad de movimientos de personas y mercancías entre las poblaciones, siendo constantemente asaltadas y desvalijadas.

Dado que no había todavía en España una institución policial, de naturaleza civil o militar, que velara expresamente por la seguridad pública en todo el territorio nacional, era el Ejército quien tenía que asumir en poblaciones y caminos dichas funciones. Y la verdad que con poca fortuna y ninguna gloria.

El desolador escenario que se padecía quedó perfectamente reflejado en una carta que el ministro de la Guerra, mariscal de campo Manuel de Mazarredo Mazarredo, escribió el 31 de diciembre de 1843, al ministro de Gobernación, José Justiniani Ramírez de Arellano:

Siendo continua la diseminación en que se encuentra la mayor parte de las tropas de Infantería, Caballería y Milicias, a causa de la persecución de ladrones y malhechores de todas especies a que están constantemente destinadas en innumerables partidas y destacamentos, en términos de no poder atender como conviene al servicio de las guarniciones y demás que les son peculiares; y no pudiendo esto dejar de producir males inmensos, como V.E. conocerá, a la disciplina del Ejército …; se hace preciso tratar de remediarlo, lo cual pudiera hacerse por medio de una fuerza pública que bajo dependencia inmediata del Ministerio de la Gobernación del digno cargo de V.E. y con la denominación que fuese más adecuada, se organizase convenientemente, relevase a las tropas de aquel servicio y se encargase de él en todos los pueblos, caminos y demás puntos de la superficie de la península.[22]

No había transcurrido un mes de dicha carta cuando por Real Decreto de 26 de enero de 1844, bajo el gobierno de Luis González Bravo, se creó en el seno del Ministerio de Gobernación, el Ramo de Protección y Seguridad.

En el inicio de su exposición de motivos, si bien se reconocía que “por muy lamentables que sean algunos antecedentes que en España ofrece la organización del ramo de seguridad”, y que “la abolición completa de la policía trae su origen del año 1840”, era indispensable que el gobierno pudiera “velar eficazmente por las personas y los bienes de todos”[23].

Aunque se recogía expresamente que el reiterado Real Decreto de 2 de noviembre de dicho año había llegado a “suprimir del todo la institución, limitándose a la parte peligrosa y repugnante” –la policía secreta- fruto de la corrupción y la manipulación por intereses de los responsables políticos de algunos de los gobernantes de aquella época, bien era cierto que se “reconoció la necesidad imperiosa de organizar la policía”[24].

También se criticaba que dicha policía, apellidada de protección y seguridad pública, pudiera seguir estando exclusivamente en manos de las autoridades populares, “a quienes la instrucción de febrero de 1823 confiaba el desempeño de un servicio tan ajeno de la índole de su instituto, como incompatible con la mudanza periódica y frecuente de la autoridad municipal”.

Dicha norma se trataba de la ya mentada “Instrucción para el gobierno económico-político de las provincias”, que durante los años siguientes a su aprobación había

22 LÓPEZ, D. (2004). La Guardia Civil y los orígenes del Estado centralista. Madrid: Alianza Editorial, p. 92.

23 Gaceta de Madrid, núm. 3.422, 27/01/1844, p. 2.

24 Ibídem, núm. 2.207, 03/11/1840, p. 2.

sido objeto, como consecuencia de los vaivenes políticos, de diversas suspensiones y reposiciones[25], hasta que –y no sería la última vez- había sido otra vez derogada por Real Decreto de 30 de diciembre de 1843[26].

Hasta ese momento había sobrevivido, tras la abolición del modelo policial vigente en 1840, una estructura de seguridad pública muy frágil y débil, implantada solo en determinadas poblaciones del territorio nacional y subordinada prácticamente en su mayor parte a las autoridades locales.

En definitiva, el citado Real Decreto de 26 de enero de 1844 sentaba los cimientos para que la seguridad pública fuera exclusivamente de responsabilidad del gobierno de la nación, tanto en su dirección como en composición de personal y dotación de medios, alejándola de la dirección y responsabilidad municipal.

Es decir, se aspiraba verdaderamente a crear por fin, una policía de ámbito estatal y desplegada en todo el territorio nacional. Consecuente con ello, comenzaba su articulado disponiendo que el servicio de protección y seguridad pública estaría exclusivamente a cargo del Ministerio de Gobernación de la Península, y de sus respectivos agentes en las provincias. Y finalizaba disponiendo que el ministro debía proponer, "con la urgencia que el servicio público reclama, la organización de una fuerza especial destinada a proteger eficazmente las personas y las propiedades, cuyo amparo es el primer objeto del ramo de protección civil".

Y hasta tanto se creara dicha "fuerza especial", se dictó el 30 de enero una Circular del *Ministerio de la Gobernación de la Península* en que se contenían las reglas que habían de observarse para la rápida organización del Ramo de Protección y Seguridad Pública en las capitales de provincia, estableciendo tres categorías, así como la reducida plantilla que tenían que tener inicialmente[27].

2.7. EL CUERPO DE LA GUARDIA CIVIL

Casi dos meses después, el 28 de marzo, se dictó un real decreto que disponía la creación de esa "fuerza especial", que fue denominada "Cuerpo de Guardias Civiles," de carácter civil y dependiente del Ministerio de la Gobernación: "con el objeto de proveer al buen orden, a la seguridad pública, a la protección de las personas y de las propiedades, fuera y dentro de las poblaciones", si bien, en cuanto a la organización y disciplina, dependería de la jurisdicción militar[28].

Tal y como se seguía exponiendo, el Gobierno necesitaba de una fuerza disponible para proteger las personas y las propiedades, pues no existía entonces institución policial de ámbito estatal alguna, resultando "la Milicia o el Ejército inadecuados para llenar este objeto cumplidamente o sin perjuicios".

El resto de la historia fundacional es ya sobradamente conocida, por lo que solo se hace a continuación una breve referencia de lo más destacable. El proyecto inicial era

25 SOSA, F. y DE MIGUEL, P. (1987). Creación, Supresión y Alteración de Términos Municipales. Madrid: Instituto de Estudios de la Administración Local, pp. 20-24.
26 Gaceta de Madrid, núm. 3.395, 31/12/1843, pp. 1-3.
27 Ibídem, núm. 3.428, 02/02/1844, pp. 1-2.
28 Ibídem, núm. 3.486, 31/03/1844, pp. 1-2.

que esa nueva "fuerza especial" que se iba a crear fuera realmente la fuerza armada y uniformada que tendría el Ramo de Protección y Seguridad para poder cumplir sus cometidos, pero ahora bajo las órdenes directas de los jefes políticos de las provincias y no bajo las de los alcaldes.

Sin embargo, ese proyecto que hubiera terminado abocado al fracaso como había sucedido con los que le precedieron, ya que adolecía de importantes vulnerabilidades, cambió de rumbo al comisionarse por Real Orden de 15 de abril de 1844 al mariscal de campo y II duque de Ahumada, Francisco Javier Girón y Ezpeleta, como su director de organización[29].

En tan solo cinco días elaboró un detallado informe en el que expuso con claridad y contundencia sus enmiendas y reparos al contenido del Real Decreto de 28 de marzo. El hecho de que el teniente general Ramón María Narváez y Campos asumiera el 3 de mayo la presidencia del Consejo de Ministros y la cartera del Ministerio de la Guerra, favoreció la rápida aprobación de las modificaciones propuestas por el duque de Ahumada[30].

Diez días más tarde, el 13, se publicó un nuevo y definitivo real decreto recogiendo las modificaciones propuestas. El anterior quedó sin efecto, desechándose además la idea de que la Guardia Civil fuera una fuerza civil[31].

Conforme a la nueva y definitiva norma fundacional, la Guardia Civil tenía naturaleza militar y quedaba sujeta, según se disponía en su artículo 1º, al "Ministerio de la Guerra por lo concerniente a su organización, personal, disciplina, material y percibo de sus haberes, y del Ministerio de la Gobernación por lo relativo a su servicio peculiar y movimiento".

Al objeto de que el nuevo cuerpo policial desplegara por toda la geografía española y se convirtiera en la primera institución de seguridad pública del Estado que llegara a todos los ciudadanos, se dispuso la creación de 14 Tercios, uno por Distrito militar, integrados a su vez por 34 Compañías de Infantería y 9 Escuadrones de Caballería. Su primera plantilla se fijó en 14 jefes, 232 oficiales y 5.769 de clases e individuos de tropa.

Una cuestión muy importante a destacar es que el nuevo Cuerpo que acababa de crearse era para atender la seguridad pública, tanto en el interior de las poblaciones como en el exterior de las mismas. Este hecho tiene suma trascendencia ante la errónea creencia de algunos que consideran que la Guardia Civil nació solo para garantizar el orden y la ley en el ámbito rural. La Guardia Civil fue fundada para garantizarlos también en el interior de todas las poblaciones, comenzando por Madrid, capital del Reino.

Sin embargo, en el interior de algunas de las poblaciones más importantes había comenzado también a establecerse una estructura, muy reducida en número y despliegue, del nuevo Ramo de Protección y Seguridad. A esta se le confería la responsabilidad de la dirección en los servicios competentes del Ministerio de la Gobernación, conforme a las instrucciones concretas que se impartieran por los respectivos jefes políticos de cada provincia.

29 Ibídem, núm. 3.506, 20/04/1844, p. 1.

30 LOPEZ, M. (1995). La Guardia Civil. Nacimiento y Consolidación (1844-1874). Madrid: Editorial Actas, pp. 38-39.

31 Gaceta de Madrid, núm. 3.530, 14/05/1844, pp. 1-2.

No hay que olvidar que inicialmente la Guardia Civil fue gestada para constituir la potente y robusta fuerza armada uniformada del Ramo de Protección y Seguridad.

De hecho, el Reglamento para el Servicio de la Guardia Civil, aprobado por Real Orden del Ministerio de la Gobernación, de 9 de octubre de 1844[32], concretó las normas de relación y coordinación del servicio, en el ámbito de sus competencias, con los responsables locales del citado Ramo, encarnados por los comisarios de distrito y los celadores de barrio.

No obstante, a pesar de la claridad de su redacción y de algunas normas complementarias que posteriormente se dictaron, se produjeron algunos intentos de uso indebido de fuerzas del nuevo Cuerpo por parte de algunos representantes del citado Ramo. Estos erróneamente entendieron que se trataba de una subordinación absoluta, lo cual no era así, ni en la letra ni en el espíritu del Reglamento.

Dicha interpretación, interesada por parte de algunos, ocasionó inicialmente una serie de conflictos que las autoridades gubernativas responsables resolvieron prácticamente siempre a favor de la Guardia Civil.

Ello, junto a ciertas reorganizaciones sufridas en el seno del Ramo, amén que este no había llegado a alcanzar ni la entidad ni el despliegue previstos, terminó por provocar que en el nuevo Reglamento de Servicio para la Guardia Civil, aprobado por Real Orden de 2 de agosto de 1852, se omitiera ya toda relación expresa con aquel. Para el cumplimiento de las misiones competencia del Ministerio de la Gobernación, las relaciones con la Guardia Civil serían exclusivamente a través de su cadena de mando con el gobernador civil de la provincia[33].

Transcurridos 28 años desde su fundación, la Guardia Civil había desplegado en la mayor parte del territorio nacional y duplicado más del doble su plantilla. Todo lo contrario que había venido sucediendo con el resto de instituciones de seguridad pública precedentes que, creadas desde la Constitución de 1812, por una u otra razón, habían fracasado y desaparecido.

Al inicio de 1872, año de aprobación de la Ley provisional de Enjuiciamiento Criminal, el benemérito Cuerpo, que ya estaba plenamente consolidado y con más años de existencia ininterrumpida que cualquier otro de los que le precedieron. No solo seguía manteniendo la misma identidad corporativa fundacional de 1844 sino que además era la fuerza de seguridad pública más numerosa y con mayor despliegue territorial que nunca antes había existido en España.

El 1º de enero de 1872 tenía una plantilla de 86 jefes, 596 oficiales y 12.636 clases e individuos de tropa. Es decir, había pasado de los 6.015 de 1844 a los 13.318 efectivos de 1872. Estaba desplegado territorialmente en 50 Comandancias encuadradas en 14 Tercios e integradas a su vez por 112 Compañías y 352 Secciones de Infantería así como 14 Escuadrones y 77 Secciones de Caballería. A efectos de servicio toda esa Fuerza estaba distribuida en 394 Líneas y 1.586 Puestos[34].

32 Ibídem, núm. 3.679, 10/10/1844, pp. 1-2.
33 Ibídem, núm. 6.636, 23/08/1852, pp. 1-2.
34 Escalafón General de los jefes y oficiales de la Guardia Civil en 1º de enero de 1872. Madrid: Imprenta del Boletín Oficial de la Guardia Civil, 1872, pp. 5 y 6.

3. LA LEY PROVISIONAL DE ENJUICIAMIENTO CRIMINAL DE 1872

El 15 de septiembre de 1870, durante la Regencia del general Francisco Serrano Domínguez, que siguió al derrocamiento de Isabel II, tras el triunfo dos años antes de la Revolución denominada "La Gloriosa," se aprobó la Ley provisional sobre organización del Poder Judicial[35].

En su Disposición Transitoria 3ª se establecía que el Gobierno debía proceder a reformar los procedimientos criminales con sujeción a determinadas reglas, siendo una de ellas:

Organización de la policía prejudicial y judicial, de manera que quede para lo futuro suficientemente asegurada la protección de las personas, la seguridad de los bienes, la prevención de las causas criminales y el descubrimiento de la verdad en los sumarios.[36]

Apenas tres meses antes se había efectuado una importante reforma del Código Penal, al objeto de adaptarlo a las exigencias de la Constitución aprobada el 1º de junio de 1869, como consecuencia del cambio de Régimen propiciado por la mentada revolución liberal.

Transcurridos dos años, por Real Decreto de 22 de diciembre de 1872, siendo ya Amadeo I rey de España, se aprobó la Ley provisional de Enjuiciamiento Criminal, cuyo Título III trataba sobre las autoridades competentes para instruir sumario y de la policía judicial[37].

En su artículo 191 se establecía textualmente:

Serán auxiliares de los Jueces de instrucción, y de los municipales en su caso, y constituirán la policía judicial:

1. *Las Autoridades administrativas encargadas de la seguridad pública y de la persecución de todos los delitos o de algunos especiales.*
2. *Los agentes subordinados de las mismas para el objeto del párrafo anterior.*
3. *Los Alcaldes, Tenientes de Alcalde y Alcaldes de barrio.*
4. *Los Jefes, Oficiales e individuos de la Guardia Civil o de cualquier otra fuerza destinada a la persecución de malhechores.*
5. *Los Serenos, Celadores y cualesquiera otros agentes municipales de policía urbana o rural.*
6. *Los guardas particulares de montes, campos y sembrados, jurados o confirmados por la Administración.*
7. *7Los Jefes de establecimientos penales y los Alcaides de las cárceles.*
8. *Los Alguaciles y dependientes de los Tribunales y Juzgados.*[38]

¿Y cuáles eran las obligaciones de quienes constituían aquella policía judicial, que hoy día denominamos como *"genérica"* al objeto de diferenciarla de la actual "específica"?.

35 Ley Orgánica del Poder Judicial de 15 de septiembre de 1870 y Ley Adicional a la misma de 14 de octubre de 1882, ampliada con notas, referencias y disposiciones aclaratorias. Madrid: Imprenta E. de la Riva, 1882, 293 págs.

36 Gaceta de Madrid, núm. 263, 20/09/1870, p. 3.

37 Ibídem, núm. 359, 24/12/1872, pp. 949-952.

38 Ley Provisional de Enjuiciamiento Criminal. Madrid, Imprenta de la Biblioteca de Instrucción y Recreo, 1873, p. 50.

Pues esas obligaciones eran las detalladas en el artículo siguiente, el 192, de la mentada Ley provisional: la averiguación de los delitos públicos que se cometieran en su territorio o demarcación; practicar, según sus atribuciones, las diligencias necesarias para comprobarlos y descubrir a los delincuentes, recogiendo y poniendo a disposición de la autoridad judicial todos los efectos, instrumentos o pruebas del delito, de cuya desaparición hubiere peligro[39].

En el artículo 191 hay que destacar muy significativamente que la Guardia Civil era la única institución de seguridad pública que se citó e identificó expresamente por su denominación corporativa como constitutiva de la policía judicial: "los Jefes, Oficiales e individuos de la Guardia Civil".

En cambio, se emplearon fórmulas genéricas descriptivas para el resto: "los agentes subordinados de las mismas para el objeto del párrafo anterior", es decir, los que estaban bajo las órdenes de las autoridades políticas, gubernamentales o municipales, encargadas de la seguridad pública y "cualquier otra fuerza destinada a la persecución de malhechores".

Tal precisión no se debió ni al capricho ni a la dejadez del legislador sino que estuvo motivada por tres razones muy concretas y que le diferenciaban de las demás, a las que se refería de forma tan genérica. Evidentemente si en 1872 hubiera existido alguna otra institución de seguridad pública, similar a la Guardia Civil, bien seguro que hubiera sido también expresamente citada. La realidad es que no fue mencionada ninguna otra por la sencilla razón de que no había ninguna otra análoga.

¿Y por qué sí la Guardia Civil? ¿Por qué no quedó subsumida dentro de la referencia genérica como el resto? ¿Es que no existía realmente ninguna otra institución de seguridad pública en ese momento? ¿Y si existían, cuál era la verdadera razón para referirse a ellas de una forma tan genérica?

Pues en primer lugar, hay que destacar que las funciones de policía judicial descritas en el artículo 192 ya las venían ejerciendo en toda su plenitud todos los miembros de la Guardia Civil desde el primer momento de su andadura, siendo una característica que le diferenció de otras fuerzas de seguridad pública que le precedieron.

En concreto quedaba perfectamente recogida en el artículo 37 de su mentado Reglamento para el Servicio de 1844:

Todo Jefe (sic) de partida de Guardia civil se halla facultado para instruir la sumaria información de cualquier delito cometido a su vista, denunciado por los transeúntes u otras personas halladas fuera de población, y perpetrado próximamente a la denuncia, presentando la sumaria al Juez lo mas antes posible, sin que en ningún caso pueda exceder este plazo de cuatro días, contados desde aquel en que se verifique el suceso que motive la sumaria.[40]

De hecho, en el artículo 32 del Capítulo I de su *Cartilla*, aprobada por Real Orden del Ministerio de la Guerra, de 20 de diciembre de 1845, relativo a "Prevenciones generales para la obligación del Guardia Civil," se disponía que "para facilitar a los

39 Por Ley de 30/12/1878, se aprobó la publicación de una compilación general de las disposiciones vigentes desde 1855 sobre Enjuiciamiento Criminal con un total 1.026 artículos, reproduciéndose textualmente como artículo 433 el contenido íntegro del artículo 191 de la Ley provisional de 1872. RUIZ, H. (1880). Compilación general de las disposiciones vigentes sobre el enjuiciamiento criminal. Madrid, Imprenta de la Revista de Legislación, pp. 101 y 102.

40 Gaceta de Madrid, núm. 3.679, 10/10/1844, pp. 1-2.

individuos del Cuerpo, el modo de instruir los sumarios", autorizados por el artículo 37 citado, se adjuntaban los formularios correspondientes, "al tenor de los que deberán proceder según los casos que se les presenten"[41].

A este respecto hay que significar también que el artículo 3º del Capítulo I del citado Reglamento ya disponía que la Guardia Civil tenía por objeto, además de la conservación del orden público y la protección de las personas y las propiedades, fuera y dentro de las poblaciones, "el auxilio que reclame la ejecución de las leyes".

Consecuente con ello, el artículo 4º establecía que el Ministerio de Gracia y Justicia, así como las autoridades judiciales podían requerir la cooperación de la Guardia Civil por conducto de la autoridad civil y, caso de urgencia, aquellas podían entenderse directamente con sus jefes.

El articulado correspondiente, del 20 al 23, ambos inclusive, se desarrollaba en la Sección II de su Capítulo II que tenía como título indicativo "De las autoridades judiciales". En ellos se regulaba el conducto que debían seguir las diferentes autoridades judiciales para requerir el auxilio de la Guardia Civil, tanto en función de la urgencia como del tipo de servicio a prestar. Es decir, a través de los jefes políticos de cada provincia, del comisario del Ramo de Protección y Seguridad que había en cada partido judicial o directamente al mando más caracterizado de la Guardia Civil.

Más adelante, en el Capítulo III, el artículo 45 reiteraba la obligación que tenía la Guardia Civil de auxiliar a las autoridades judiciales "para asegurar la buena administración de la justicia." Y en el siguiente, se establecía la obligación de los miembros del Cuerpo de "dar a los Jueces de primera instancia de los partidos oportuna cuenta de todos los delitos que lleguen a su noticia, remitirles las sumarias que instruyan, y poner a su disposición los delincuentes".

La modificación del Reglamento para el Servicio de 1852 apenas supuso variación alguna respecto a su relación con las autoridades judiciales. Solo la supresión de cualquier referencia a la intermediación de la figura del comisario de distrito y la prohibición de emplear a la Guardia Civil en el servicio de custodiar los reos en capilla y escoltarlos hasta después de ser ejecutados, función reservada a las tropas del Ejército.

A toda esa poderosa razón, de venir ya ejerciendo todos sus componentes las referidas funciones, lo que de por sí le revestía por derecho propio del carácter de lo que la Ley provisional de 1872 denominaba policía judicial, había que añadir otra también muy importante.

La segunda razón es que la Guardia Civil era en 1872 la única institución de seguridad pública que contaba desde hacía casi tres décadas con un sólido despliegue territorial de ámbito nacional, circunstancia que no concurría en el resto, cuya presencia geográfica era muy limitada.

La mentada Ley provisional sobre organización del Poder Judicial de 1870, había distribuido la administración de la justicia por todo el territorio nacional no colonial, en distritos con su audiencia en cada uno de ellos, en partidos con sus correspondientes tribunales, en circunscripciones, con sus pertinentes jueces de instrucción, y en términos municipales con sus oportunos jueces municipales.

41 Cartilla del Guardia Civil. Madrid: Imprenta de D. Victoriano Hernando, 1846, 183 págs.

Es decir, existía un extenso despliegue territorial de juzgados de instrucción y municipales donde la única institución de seguridad pública que existía en la jurisdicción de todos ellos era la Guardia Civil, circunstancia que como ya se ha expuesto no concurría en el resto.

En cambio el Ramo de Protección y Seguridad, por razones principalmente de austeridad presupuestaria, no solo era objeto de sucesivas reorganizaciones sino que cada vez veía disminuir más su despliegue y entidad, como por ejemplo ocurrió por Real Decreto de 2 de diciembre de 1847, que suprimió todas las comisarías de partido, dejando solo las ubicadas en las capitales de provincia[42].

Realmente terminó durante un largo periodo de tiempo circunscribiéndose principalmente a Madrid y algunas otras ciudades importantes. El modelo policial proyectado a principios de 1844 sobre la base de un sólido Ramo de Protección y Seguridad, dependiente del Ministerio de Gobernación y que tuviera una robusta fuerza armada uniformada policial desplegada por todo el territorio nacional, no terminó de consolidarse.

La Guardia Civil fue fortaleciéndose y creciendo en número, despliegue y prestigio pero desde dicho Ministerio no se quiso terminar de renunciar a disponer sobre todo en Madrid, como capital del Estado, de una fuerza policial de carácter civil bajo su único y exclusivo mando. Ello dio lugar a un sin fin de resoluciones y reorganizaciones que realmente ni resultaron eficaces ni eficientes hasta que a principios del siglo XX se consolidó un modelo policial dual.

Sirva como ejemplo de ese dilatado periodo, previo a la entrada en vigor de la Ley provisional de Enjuiciamiento Criminal de 1872, una relación de disposiciones referidas a creación, cambios y reorganizaciones que se padecieron en ese endeble e inestable modelo policial urbano frente a la estabilidad y fortaleza que fue adquiriendo la Guardia Civil.

Por Real Orden de 1º de octubre de 1849 se redujo en Madrid la plantilla de los "Salvaguardias", denominación que había sido adoptada el año anterior para los agentes del Ramo de Seguridad y Protección [43]. Por Real Decreto de 25 de febrero de 1852 se reorganizó nueva y parcialmente el Servicio de Protección y Seguridad de Madrid y pasó a denominarse de Vigilancia[44]. Consecuente con lo anterior, por Real Orden de 9 de marzo de 1852 el Servicio de Protección y Seguridad pasó también a denominarse de Vigilancia, en todo el Reino, y los Salvaguardas pasaron igualmente a adoptar el nombre de Vigilantes[45]. Por Real Decreto de 4 de abril de 1854 se dio una nueva organización al "ramo de vigilancia pública y municipal de Madrid"[46], la cual quedó sin efecto por Real Decreto de 13 de septiembre siguiente[47]. Por Real Decreto de 5 de noviembre de 1856 volvió a organizarse la vigilancia pública y municipal de Madrid[48]. Por Decreto de 1º de junio de 1870 se reorganizó el Cuerpo de Orden Público de la provincia de Madrid[49], volviendo a

42 Gaceta de Madrid, núm. 4.828, 03/12/1847, p. 1.
43 Ibídem, núm. 5.499, 03/10/1849, p. 2
44 Ibídem, núm. 6.468, 08/03/1852, p. 1.
45 Ibídem, núm. 6.474, 14/03/1852, p. 1.
46 Ibídem, núm. 471, 16/04/1854, pp. 1-4.
47 Ibídem, núm. 621, 14/09/1854, p. 1.
48 Ibídem, núm. 1.403, 06/11/1856, p. 1.
49 Ibídem, núm. 154, 03/06/1870, p. 1.

reorganizarse por Decreto de 2 de julio siguiente, donde se determinó el personal de que se había de componer[50]. Por Decreto de 20 de febrero de 1871 se creó, con el nombre de Cuerpo de Orden Público, una fuerza destinada para la vigilancia de Madrid y sus afueras[51], la cual fue reorganizada por Real Decreto de 28 de junio del año siguiente[52].

4. LA LEY DE ENJUICIAMIENTO CRIMINAL DE 1882

En la década que estuvo en vigor la Ley provisional de Enjuiciamiento Criminal de 1872, el país sufrió diversos avatares políticos de gran trascendencia, que tuvieron su lógica repercusión en la redacción de la nueva legislación.

El 1º de enero de 1882 la Guardia Civil seguía siendo la institución de seguridad pública con mayor número de efectivos y despliegue territorial aún que una década antes. De hecho era la única que tenía ámbito estatal.

Tenía ya una plantilla de 100 jefes, 703 oficiales y 15.380 clases e individuos de tropa. Es decir, había pasado de los 6.015 de 1844 y de los 13.318 efectivos de 1872 a los 16.183 de 1882. Estaba desplegado territorialmente en 50 Comandancias encuadradas en 16 Tercios e integradas a su vez por 129 Compañías de Infantería, así como 15 Escuadrones y 78 Secciones de Caballería. A efectos de servicio toda esa Fuerza estaba distribuida en 440 Líneas frente a las 394 del año 1872 y en 2.041 Puestos frente a los 1.586 del año 1872[53].

Por Real Decreto de 14 de septiembre de 1882[54], siendo ya Alfonso XII rey de España, se aprobó la definitiva Ley de Enjuiciamiento Criminal, que hoy día sigue todavía en vigor si bien con algunas modificaciones y reformas[55].

La nueva norma introdujo numerosas novedades respecto a la anterior, pasando de 849 artículos que tenía la provisional de 1872, a un total de 998, fruto en su mayor parte de los cambios legislativos producidos durante la década que medió entre ambas.

Respecto al tema concreto de interés, significar que el artículo 191 de la Ley de 1872 pasó a ser el 283 de la de 1882, en cuyo Libro II, Título III, relativo a la Policía Judicial, se seguía reproduciendo textualmente su punto 4º sobre el carácter de policía judicial que tenían los jefes, oficiales e individuos de la Guardia Civil.

El resto del artículo se mantuvo igual salvo en dos aspectos. En la introducción se amplió para establecer que la policía judicial debía auxiliar también al Ministerio Fiscal. Y en el punto 2º se sustituyó “los agentes o subordinados de las mismas para el objeto del párrafo anterior” por la nueva redacción de “los empleados y subalternos de policía de seguridad, cualquiera que sea su denominación”[56].

50 Ibídem, núm. 188, 07/07/1870, pp. 2-3.
51 Ibídem, núm. 88, 29/03/1871, pp. 713-714.
52 Ibídem, núm. 181, 29/06/1872, p. 928.
53 Escalafón General de los Jefes y Oficiales de la Guardia Civil en 1º de enero de 1882. Madrid: Imprenta del Boletín Oficial de la Guardia Civil, 1882, pp. 11 y 12.
54 Ha de significarse que para ello se estuvo a lo dispuesto en la Ley sancionada en 11/02/1881 y promulgada en virtud del Real Decreto de 22/06/1882, tomando como base la Compilación general de 16/10/1879.
55 Gaceta de Madrid, núm. 260 a 283, de 17/09/1882 a 10/10/1882.
56 Ibídem, núm. 275, 30/09/1882, p. 920.

Esta última modificación se debió principalmente a que, durante esa década entre ambas leyes, se había creado y organizado por dos veces una nueva institución de seguridad pública: "la policía gubernativa y judicial".

Una fue durante el breve periodo de la Primera República. Se creó por Decreto del Ministerio de la Gobernación, de 22 de octubre de 1873[57], disponiéndose que su titular quedaba autorizado para organizarla en las provincias según lo creyere conveniente. Así fue solo en las de Madrid, Sevilla y Barcelona[58].

Apenas pudo desarrollarse siquiera en sus capitales ya que, cuando habían transcurrido un par de meses, el siguiente gobierno republicano derogó el decreto fundacional por otro de fecha 11 de enero de 1874, ya que "no puede satisfacer con la urgencia y perentoriedad que el caso exige las patrióticas manifestaciones de la opinión", restableciéndose provisionalmente el Decreto de 28 de Marzo de 1871[59].

La segunda vez fue poco más de un lustro después, ya restablecida la monarquía y siendo rey Alfonso XII. Se volvió a crear para Madrid, por Real Decreto del Ministerio de la Gobernación, de 6 de noviembre de 1877[60]. Su titular se convertía simultáneamente en jefe superior de la policía en dicha ciudad, residencia de la Corte.

Hay que destacar muy significativamente que en su exposición de motivos, tras recoger la necesidad de contar en Madrid, dadas sus singulares características, con una policía gubernativa específica, como fuerza pública urbana, se lamentaba el desastre legislativo que se llevaba padeciendo en ese aspecto desde 1844: "nada menos que doce o trece decretos orgánicos y reglamentos que se han sucedido con breve vida y con escaso provecho, haciendo de todo punto imposible con la insubsistencia de sistema y con la incesante variación de personas, la formación de un Cuerpo de funcionarios probos e idóneos".

El ejemplo a seguir y conseguir era, según el legislador, el del éxito y prestigio del benemérito Instituto de la Guardia Civil:

Formar un Cuerpo de funcionarios idóneos, con opción á premios, con sujeción a castigos, con seguridad en su carrera, que consigan por su buen proceder hacer simpático al pueblo su delicado servicio, como lo ha conseguido la Guardia civil, que es en rigor el Cuerpo de policía de los campos y de los caminos, y que ha logrado ser por todos estimada y bendecida, excepto por los delincuentes y por los que propenden a serlo. Y para todo ello es necesario que así como la misma Guardia civil ha llegado á ser independiente de la política, salvándose tan útil institución aun en medio de los trastornos de radicales revoluciones; así también la policía gubernativa obre dentro de su esfera con independencia absoluta de las opiniones políticas de los gobernantes y de las necesidades de otra especie de vigilancias que puedan tener los mismos, subsistiendo igual siempre y cumpliendo su deber eminentemente social, sin estar á todas horas expuesta á desaparecer o a desnaturalizarse a cualquiera de los cambios, que la alternada sucesión de los partidos en el poner, ocasiona necesariamente en las esferas gubernamentales.

Conforme se disponía su artículo 1º, la Policía Gubernativa y Judicial de Madrid pasaba a componerse de dos servicios: el de Vigilancia y el de Seguridad. En su artículo 5º se establecía que el primero sería prestado por "empleados" civiles, auxiliados por

57 Ibídem, núm. 296, 23/10/1873, pp. 195-196.

58 Fueron creadas sucesivamente por Órdenes del Ministerio de la Gobernación de 24/10/1873 en Madrid (Gaceta de Madrid, núm. 298, 25/10/1873, p. 216); de 23/12/1873 en Sevilla (Gaceta de Madrid, núm. 357, 23/12/1873, p. 772); y de 23/12/1873 en Barcelona (Gaceta de Madrid, núm. 357, 23/12/1873, pp. 772-773).

59 Ibídem, núm. 12, 12/01/1874, pp. 93-94.

60 Ibídem, núm. 316, 12/11/1877, pp. 457-458.

"subalternos." He ahí la razón de esa variación en la redacción del punto 2º del artículo 283 de la Ley de 1882.

Lo de "cualquiera que sea su denominación" era simplemente consecuencia de los diferentes nombres que se iba dando a las sucesivas instituciones policiales que intentaban implantarse a nivel nacional en las grandes ciudades y que hasta la Ley de 27 de febrero de 1908, reinando ya Alfonso XIII, no comenzó a ser verdaderamente una realidad a nivel nacional[61].

Regresando al mentado Real Decreto de 1877, significar que en el artículo 6º se determinaba que el servicio de "Seguridad" dentro de la Corte, es decir en el casco urbano, se prestaría por "un cuerpo organizado a imitación de los cuerpos militares",y por un Tercio de la Guardia Civil en las afueras de la población[62].

5. CONCLUSIONES

En definitiva, y al igual que había ocurrido en la Ley de 1872, el único Cuerpo citado como tal, con su propia denominación en la nueva Ley de 1882, como policía judicial, fue el de la Guardia Civil.

En cambio, ambas normas, dictadas por distintos gobiernos, se referían de forma genérica al resto de actores, tales como las autoridades administrativas encargadas de la seguridad pública y de la persecución de todos los delitos o de algunos especiales; los agentes o subordinados de las mismas (o empleados y subalternos de policía de seguridad, cualquiera que sea su denominación); los alcaldes, tenientes de alcalde y alcaldes de barrio; los serenos, celadores y cualesquiera otros agentes municipales de la policía urbana y rural; los guardas particulares de montes, campos y sembrados, jurados o confirmados por la Administración; los jefes de establecimientos penales y los alcaides de las cárceles; así como los alguaciles y dependientes de los tribunales y juzgados.

Todo ello no solo constituía un sólido testimonio más de la plena consolidación del benemérito Instituto como Cuerpo de Seguridad Pública sino también como Policía Judicial.

No hay que olvidar que a lo largo de todo ese periodo, desde su fundación en 1844 hasta 1882, tan convulso de la historia de España, se habían sucedido monarquías, regencias y hasta una república con diferentes gobiernos, amén de varios pronunciamientos militares y guerras civiles.

Igualmente hay que recordar que ese periodo de tiempo había sido testigo de creaciones, reorganizaciones, transformaciones y desapariciones de otras instituciones

61 Ibídem, núm. 60, 29/02/1908, pp. 873-875.

62 Se trataba del 14º Tercio de la Guardia Civil. Por Real Orden del Ministerio de la Guerra, de 06/04/1859, la Guardia Urbana de Madrid pasó a denominarse Guardia Civil Veterana, integrándose en el Cuerpo de la Guardia Civil (Gaceta de Madrid, núm. 97, 07/04/1859, p. 1). Por Decreto de 28/09/1862 se reorganizó, tomando el nombre de Tercio Veterano de la Guardia Civil y por Real Orden de 07/12/1864 se dispuso que su nueva denominación fuera la de Tercio de Madrid. Tras el triunfo de la Revolución de septiembre de 1868, conocida por "La Gloriosa", que supuso el destronamiento y exilio de Isabel II, se procedió por Decreto del Gobierno Provisional, de 20/10/1868, a su disolución (Gaceta de Madrid, núm. 296, 22/10/1868, p. 2), creándose seguidamente para la vigilancia de las afueras de la Corte un nuevo Tercio de la Guardia Civil que tomó el número 14º.

policiales, que por una u otra razón, de índole político, social o económico, no terminaban ni de asentarse ni de desarrollarse.

Lo cierto es que el prestigio de la Guardia Civil ante la Sociedad, su eficacia en el servicio contra toda clase de delincuencia, su carácter militar que cohesionaba y disciplinaba una fuerza policial robusta, y su amplio despliegue territorial por toda la geografía nacional fueron sin duda alguna sus mejores puestas en valor frente a la caótica situación institucional, política y social que padeció el país durante ese periodo.

A tenor de todo lo expuesto se puede concluir afirmando que "los jefes, oficiales e individuos de la Guardia Civil", siendo como pertenecían a la única institución de seguridad pública de ámbito estatal y que además era la más antigua que existía como tal durante los periodos de vigencia de las Leyes de Enjuiciamiento Criminal de 1872 y 1882, constituían y siguen constituyendo la policía judicial española también más antigua.

BIBLIOGRAFÍA

Cartilla del Guardia Civil. Madrid: Imprenta de D. Victoriano Hernando, 1846.

Escalafón General de los Jefes y Oficiales de la Guardia Civil en 1º de enero de 1872. Madrid: Imprenta del Boletín Oficial de la Guardia Civil, 1872.

Escalafón General de los Jefes y Oficiales de la Guardia Civil en 1º de enero de 1882. Madrid: Imprenta del Boletín Oficial de la Guardia Civil, 1882.

Gaceta de la Regencia de las Españas. Varios años.

Gaceta de Madrid. Varios años.

Ley Orgánica del Poder Judicial de 15 de septiembre de 1870 y Ley Adicional a la misma de 14 de octubre de 1882, ampliada con notas, referencias y disposiciones aclaratorias. Madrid: Imprenta E. de la Riva, 1882,

Ley Provisional de Enjuiciamiento Criminal. Madrid, Imprenta de la Biblioteca de Instrucción y Recreo, 1873.

AGUADO, F. (1983). Historia de la Guardia Civil. Madrid y Barcelona: Ediciones Históricas, Cupsa y Planeta.

LÓPEZ, D. (2004). La Guardia Civil y los orígenes del Estado centralista. Madrid: Alianza Editorial.

LOPEZ, M. (1995). La Guardia Civil. Nacimiento y Consolidación (1844-1874). Madrid: Editorial Actas,

PARGA, J. (1836). Instrucción para el gobierno económico-político de las provincias. La Coruña: Imprenta de Iguereta.

ROJAS, J.; y DE ANDRÉS, R. (2015). Ministerio del Interior. Dos siglos de historia. Bilbao (Vizcaya): Ministerio del Interior.

RUIZ, H. (1880). Compilación general de las disposiciones vigentes sobre el enjuiciamiento criminal. Madrid, Imprenta de la Revista de Legislación.

SIDRO, J. y QUEVEDO, A. (1858). La Guardia Civil. Historia de esta institución y de

todas las que se han conocido en España con destino a la persecución de malhechores, desde los tiempos más remotos hasta nuestros días. Madrid: Autores.

SOSA, F. y DE MIGUEL, P. (1987). Creación, Supresión y Alteración de Términos Municipales. Madrid: Instituto de Estudios de la Administración Local.

Fecha de recepción: 20/06/2018. Fecha de aceptación: 25/06/2018

REDES DE TRÁFICO DE MATERIAL NUCLEAR Y RADIOLÓGICO UNA POSIBILIDAD O UNA REALIDAD

JOAQUÍN MARIANO PELLICER BALSALOBRE

SERVICIO DE CRIMINALÍSTICA DE LA GUARDIA CIVIL

RESUMEN

Aunque el terrorismo nuclear y radiológico son amenazas reales y globales, la construcción de un dispositivo nuclear sofisticado por un grupo terrorista no es probable. No obstante, un dispositivo de dispersión radiológica (RDD) construido usando material nuclear o radiológico es un riesgo real. Esta hipótesis conduce a la pregunta sobre si existen redes de tráfico de material nuclear o radiológico relacionadas con organizaciones criminales. Desde 1995 la Base de Datos de Incidentes (ITDB) de la OIEA recopila y analiza los incidentes de tráfico ilícito confirmados por los estados. La ITDB incluye tanto los actos intencionados como no intencionados de "adquisición no autorizada (v.g. robo), ofrecimiento, posesión, uso, transferencia o eliminación de material nuclear o radiactivo, tanto si es intencionado como no intencionado, con o sin cruce de fronteras"[1]. Analizando los datos de la ITDB podría concluirse si la existencia de redes criminales de tráfico nuclear o radiológico es real o no.

Palabras clave: Incidentes, OIEA, redes criminales organizadas, terrorismo nuclear, tráfico nuclear.

ABSTRACT

Although nuclear and radiological terrorism are real and global threats, a sophisticated nuclear device constructed by terrorist group is not likely. However a radiological dispersal device (RDD) built by using nuclear or radiological material is a real risk. This hypothesis leads to the question if there are trafficking networks of nuclear or radiological material related with criminal organizations. Form 1995 the IAEA´s Incident and Trafficking Database (ITDB) collects and analyses state-confirmed illicit trafficking incidents. ITDB includes both intentional and unintentional acts of "unauthorized acquisition, (e.g. by theft), supply, possession, use, transfer, or disposal of nuclear and other radioactive materials, whether intentionally or unintentionally, with or without crossing international borders"[2]. By analyzing ITDB data it could be concluded whether the existence of criminal networks of nuclear or radiological trafficking is real or not.

Keywords: Incidents, IAEA, nuclear trafficking, nuclear terrorism nuclear organized criminal networks.

1 http://www-ns.iaea.org/security/itdb.asp
2 http://www-ns.iaea.org/security/itdb.asp

1. INTRODUCCIÓN

El tráfico ilícito de material nuclear y radiológico es una preocupación de los servicios de seguridad de los estados, organizaciones internacionales y organismos (nacionales e internacionales) responsables de la seguridad. La presente investigación se centrará en el análisis de cuatro tipos de incidentes con material nuclear y radiológico que pueda ser empleado con fines maliciosos, desde la forma más sofisticada e improbable de la construcción de un artefacto nuclear a la más sencilla y probable como la elaboración de un dispositivo de dispersión radiológica (RDD[3]) mediante la unión de material radiológico a un explosivo convencional o de elaboración casera.

El objetivo de este trabajo consiste en establecer si existe relación y, en su caso, de qué tipo entre determinados incidentes y el tráfico ilícito de material nuclear y radiológico por parte de posibles grupos de receptores o usuarios finales con finalidad maliciosa.

2. HIPÓTESIS

Se pretende responder a la pregunta de si existen redes de tráfico ilícito de material nuclear y radiológico que conformen un mercado negro estructurado desde los suministradores hasta los usuarios finales con fines maliciosos. La hipótesis inicial es que no existe un verdadero mercado negro estructurado de redes de tráfico de material nuclear y radiológico, debido a la difícil obtención y manejo de los mismos, alto control gubernamental e intergubernamental, así como bajo interés por parte de los grupos criminales organizados. Las redes criminales organizadas de tráfico ilícito de bienes no incluyen entre sus actividades principales el tráfico ilícito de material nuclear y radiológico, aunque ocasionalmente sí pueden participar si el beneficio económico es alto. Esta situación dificulta el acceso al material nuclear y radiológico por parte de grupos con fines maliciosos.

Para responder a la pregunta de investigación se estudiarán cuatro tipos de incidentes que aparecen en el informe del CSN, que pueden estar relacionados con el tráfico ilícito y se exponen a continuación:

- Violación normativa/posesión no autorizada.
- Pérdida.
- Robo/sustracción.
- Desconocido.

3. DEFINICIÓN DEL RIESGO

El tráfico ilícito de materiales NRBQ representa una amenaza para la paz y la seguridad internacionales tal y como recoge la resolución S/RES/1540 del Consejo de Seguridad de Naciones Unidas, que sumada a la amenaza terrorista incrementa el riesgo del empleo de este material en atentados por parte de grupos con intenciones maliciosas.

3 Radiological Dispersion Device.

La OTAN diferencia dos tipos de amenazas por parte de grupos terroristas y que se exponen a continuación:

- Nuclear: consistente en el empleo de armas nucleares. Las dificultades de su fabricación minimizan esta posibilidad para actores no estatales, quedando limitada su obtención a través de un tercer estado o bien en el mercado negro. Ambas posibilidades no están exentas de dificultad, la primera debido al riesgo que correría el estado suministrador de sufrir una represalia. En el caso de la adquisición en el mercado negro procedente del robo de arsenales se carece de los códigos necesarios para su detonación, que se encuentra bajo el control del poder político.
- Radiológica: consiste en el empleo de elementos, fuentes y mecanismos con componentes radiológicos, asociados a un artefacto explosivo improvisado (IED[4]). Se trata de material radiactivo no fisionable, aunque puede provocar contaminación, además de los efectos mecánicos y térmicos de la explosión. Este es el riesgo más probable, por su sencillez, de materialización de la amenaza de este fenómeno terrorista. La liberación de material radiológico se puede llevar a cabo mediante artefactos de dispersión radiológica, que puede usar explosivo (RDD) o no, y artefactos de exposición radiológica.

El fenómeno de terrorismo radiológico no implica exclusivamente el empleo de material nuclear o radiológico por parte de grupos terroristas. Hay que tener en cuenta la posibilidad de ataque a instalaciones nucleares[5] o a instalaciones radiactivas[6].

Aunque solo algunos estados son productores y exportadores de material nuclear y/o radiactivo, muchos mas son usuarios del mismo y la gran mayoría constituyen un medio de interconexión para el transporte y el comercio mundial de este tipo de materiales. Esta circunstancia incrementa a nivel mundial la posibilidad de ataques terroristas que involucren material o instalaciones.

El Convenio Internacional para la Represión de los Actos de Terrorismo Nuclear de 2005 (Convenio sobre el Terrorismo Nuclear) en su artículo 2 considera que comete delito quien:

1. Comete delito en el sentido del presente Convenio quien, ilícita e intencionalmente:

a) Posea material radiactivo o fabrique o posea un dispositivo:

i) Con el propósito de causar la muerte o lesiones corporales graves; o

ii) Con el propósito de causar daños considerables a los bienes o al medio ambiente;

b) Utilice en cualquier forma material radiactivo o un dispositivo, o utilice o dañe una instalación nuclear en forma tal que provoque la emisión o entrañe el riesgo de provocar la emisión de material radiactivo:

i) Con el propósito de causar la muerte o lesiones corporales graves; o

4 *Improvised Explosive Device*.

5 "…aquellas del ciclo nuclear, excepto las fábricas de producción de elementos combustibles de uranio natural o torio. Las fábricas de armamento nuclear, almacenes y bases de despliegue del mismo son también instalaciones nucleares, aunque en España no existe ninguna". Ortega García, J. (2013). Medidas de defensa en España frente al terrorismo nuclear, Documento Marco 5/2013, Instituto Español de Estudios Estratégicos.

6 "…las instalaciones radiactivas son las que tienen fuentes de radiaciones ionizantes a partir de unos determinados niveles de actividad". ". Ortega García, J. *Op cit.*

ii) Con el propósito de causar daños considerables a los bienes o al medio ambiente; o

iii) Con el propósito de obligar a una persona natural o jurídica, una organización internacional o un Estado a realizar o abstenerse de realizar algún acto.

2. También comete delito quien:

a) Amenace, en circunstancias que indiquen que la amenaza es verosímil, con cometer un delito en los términos definidos en el apartado b) del párrafo 1 del presente artículo; o

b) Exija ilícita e intencionalmente la entrega de material radiactivo, un dispositivo o una instalación nuclear mediante amenaza, en circunstancias que indiquen que la amenaza es verosímil, o mediante el uso de la fuerza.

3. También comete delito quien intente cometer cualesquiera de los actos enunciados en el párrafo 1 del presente artículo.

4. También comete delito quien:

a) Participe como cómplice en la comisión de cualesquiera de los actos enunciados en los párrafos 1, 2 ó 3 del presente artículo; o

b) Organice o instigue a otros a los efectos de la comisión de cualesquiera de los delitos enunciados en los párrafos 1, 2 ó 3 del presente artículo; o

c) Contribuya de otro modo a la comisión de uno o varios de los delitos enunciados en los párrafos 1, 2 ó 3 del presente artículo por un grupo de personas que actúe con un propósito común; la contribución deberá ser intencionada y hacerse con el propósito de fomentar los fines o la actividad delictiva general del grupo o con conocimiento de la intención del grupo de cometer el delito o los delitos de que se trate (Convenio sobre el terrorismo nuclear, 2005).

La Guía Técnica 30-2012 del Consejo de Seguridad Nuclear establece hasta cinco tipos de grupos de emergencia (I a V). En el grupo IV de emergencias incluye los actos terroristas o criminales en los que se utilice el material radiactivo cuyo riesgo asociado consiste en la posibilidad de sobreexposición y efectos deterministas. Incluye aquellas situaciones en las que pueda producirse un riesgo debido a prácticas o actividades no reguladas. Son tres los tipos de riesgo a los que pueden dar lugar:

- Exposición externa.
- Contaminación externa.
- Contaminación interna.

Además de los actos terroristas la aparición de fuentes radiactivas fuera del control regulador podría ser indicativo de alguna clase de actividad criminal o ilícita como:

- Pérdida, abandono, robo o uso no autorizado de fuentes de alta actividad o de fuentes huérfanas.
- Caída de satélites con fuentes radiactivas dentro del territorio nacional.
- Dispersión de materiales nucleares o radiactivos procedentes de actividades militares.

Una de las amenazas mayores sobre las instalaciones nucleares la constituye el sabotaje, definido por el Real Decreto 1308/2011[7] como “todo acto deliberado

7 Real Decreto 1836/1999, de 3 de diciembre, por el que se aprueba el Reglamento sobre instalaciones nucleares y radiactivas.

cometido en perjuicio de una instalación nuclear o de los materiales nucleares o fuentes radiactivas objeto de uso, almacenamiento o transporte, que pueda entrañar directa o indirectamente un peligro para la salud y la seguridad del personal, el público o el medio ambiente como consecuencia de la exposición a las radiaciones o de la emisión de sustancias radiactivas" (Real Decreto 1308/2011).

Especialmente susceptibles son las instalaciones de procesado de material metálico, de eliminación y tratamiento de residuos, centros de investigación y hospitalarios y aduanas.

3.1. SEGURIDAD EN LAS INSTALACIONES Y ALMACENAMIENTO

Las instalaciones nucleares y radiactivas necesitan de un régimen de protección física que las resguarde contra el robo, sustracción, hurto o cualquier otra apropiación ilícita de los materiales que allí se utilicen, almacenen o transporten. Los riesgos que pueden sufrir este tipo de instalaciones son el extravío o robo del material y el sabotaje. El Real Decreto 1308/2011 establece la "amenaza base de diseño" como forma de diseño y evaluación de los sistemas de protección física de fuentes, materiales e instalaciones frente a la actuación de *outsiders/insiders* para la retirada no autorizada de material. Las instalaciones que pueden verse amenazadas según la Guía Técnica 30-2012 del CSN son:

- Instalaciones de almacenamiento centralizado o definitivo de combustible irradiado fuera de los emplazamientos de las centrales nucleares.
- Reactores nucleares de potencia <100 MW empleados en buques de propulsión nuclear (en seco).
- Instalaciones de almacenamiento de combustible irradiado en lo que fueron emplazamientos en centrales nucleares (en húmedo).
- Instalaciones de gestión de residuos de media actividad.
- Instalaciones nucleares en desmantelamiento sin almacenamiento de combustible nuclear.
- Instalaciones de irradiación industrial.
- Instalaciones de radiografía industrial.
- Instalaciones de radioterapia.
- Instalaciones que utilicen aceleradores de partículas.
- Instalaciones de braquiterapia.
- Instalaciones de gestión de residuos de baja actividad. Instalaciones de irradiación industrial, equipos de control de procesos e instalaciones de radiografía industrial que utilizan fuentes de radiación con tasas de dosis sin blindaje inferior a 100 mGy/h a 1 metro.
- Instalaciones o lugares donde pueden aparecer fuentes radiactivas fuera de control.

Los riesgos principales a los que están expuestas las instalaciones pueden ser la posibilidad de sucesos catastróficos o actos malintencionados que puedan dar lugar a daños en blindajes y el robo o pérdida de fuentes (cuya probabilidad aumenta en el caso de tratarse de fuentes móviles).

El almacenamiento de material nuclear, radiactivo y radiológico es muy variable, este puede realizarse en armarios y cuartos seguros en laboratorios de investigación y diagnóstico, centros sanitarios, industrias, hasta instalaciones de servicios para una central nuclear. La violación de los controles de acceso, una arquitectura de seguridad ineficaz y deficiencias en el control de las cantidades del material almacenado puede dar lugar al extravío o sustracción del mismo y que pase inadvertida para los responsables.

3.2. TRANSPORTE Y CUSTODIA

Particularmente importante es el riesgo relacionado con el transporte de materiales nucleares que puedan dar lugar a sucesos contemplados en la escala de INES[8], de hecho se ha ampliado debido a la necesidad de comunicación de los sucesos relacionados con el transporte de materiales radiactivos y fuentes. Esto es debido a la globalización del transporte comercial, en especial del contenerizado, que supone el 80% del transporte mundial y vía al tráfico ilícito de cualquier tipo de material. No obstante existen sucesos que constituyen tráfico ilícito sin propósitos delictivos, consistentes en el desplazamiento ilegal con carácter involuntario. Los riesgos derivados del transporte se exponen a continuación:

- Dispersión del material radiactivo.
- Emisión de radiaciones.
- Daños derivados del calor emitido.
- Criticidad: posibilidad de una reacción en cadena durante el transporte de material fisionable.
- Sustracción o extravío del material transportado.

3.3. CLASIFICACIÓN DE LAS FUENTES RADIOACTIVAS SEGÚN LA NORMA RSG-19 DEL OIEA

Se trata de una clasificación de peligrosidad descendente. La exposición durante unos pocos minutos a una fuente de categoría 1 puede resultar fatal. Las fuentes de categoría 5 son las de menor peligro potencial, que pueden representar dosis excesivas si no se encuentran controladas de manera adecuada.

8 Escala Internacional de Sucesos Nucleares y Radiológicos, se emplea para comunicar al público de manera rápida y coherente la importancia desde el punto de vista de la seguridad de sucesos asociados a las fuentes de radiación.

Categoría	Fuente
1	Generadores termoeléctricos de radioisótopos (GTR) Irradiadores Fuentes de teleterapia fija de haces múltiples (cuchillo gamma)
2	Fuentes de radiografía gamma industrial Fuentes de braquiterapia de elevada/media tasa de dosis
3	Calibradores industriales fijos con fuentes de actividad altac Calibradores para diagrafía de pozos
4	Fuentes de braquiterapia de baja tasa de dosis (salvo placas oculares e implantes permanentes) Calibradores industriales sin fuentes de actividad alta Densitómetros de huesos Eliminadores de estática
5	Fuentes de braquiterapia de baja tasa de dosis, placas oculares e implantes permanentes Aparatos de análisis mediante fluorescencia por rayos X (FRX) Aparatos detectores por captura de electrones Fuentes de espectrometría Mössbauer Fuentes de examen mediante tomografía por emisión de positrones (TEP)

4. DEBILIDADES

El fenómeno de la globalización no solo ha provocado el incremento espectacular de los movimientos de mercancías, capitales y personas, sino que, asociado a la revolución de las tecnologías de la información y comunicaciones, la diseminación e intercambio de información ha crecido de manera exponencial. Lo que constituye un entorno muy favorable para el desarrollo de actividades relacionadas con el contrabando de cualquier tipo de bienes e intercambio de información sensible. Por lo que la violación de las medidas de control de los movimientos de materiales y bienes de equipo, así como la transferencia de intangibles tales como conocimiento y tecnología son los dos pilares sobre los que la Estrategia de Seguridad Nacional de 2017 hace hincapié en cuanto a las medidas de prevención y control de la proliferación.

La inestabilidad en determinados estados y regiones con instalaciones nucleares y radiológicas es una fuente constante de preocupación por diversos motivos:

- Riesgo de adquisición material y tecnología mediante el robo.
- Niveles de corrupción elevados que permiten sortear las medidas gubernamentales de control.
- Incapacidad para realizar un control efectivo de las exportaciones, localización e interceptación del tráfico ilegal.
- Medidas de seguridad insuficientes o inadecuadas que facilitan la pérdida o extravío de material, abandono, robo, uso y posesión no autorizada.

- Presencia de grupos terroristas con capacidad suficiente para realizar operaciones de obtención de material, en ocasiones con control de una parte del territorio.

La detección del tráfico ilícito tiene dificultades que residen en el ingente volumen de tráfico de mercancías, especialmente por vía marítima. El control de mercancías en el interior de contenedores en instalaciones portuarias implica el empleo de tecnología de detección radiológica que requiere de complejos y voluminosos equipos, así como de tiempo de escaneo que ralentiza el tráfico de mercancías con el coste asociado al tiempo. Hay que añadir que el empleo de blindajes que hacen opacos los materiales a los sistemas de detección supone un verdadero desafío tecnológico en cuanto a eficacia.

5. CRIMINALIDAD DEL TRÁFICO ILÍCITO DE MATERIAL NUCLEAR Y RADIOLÓGICO

Según la Oficina Internacional de la Policía Criminal (INTERPOL) existe la creencia errónea por parte de las redes de delincuencia organizada que el material NRBQ, en especial el nuclear y radiológico, es muy valioso. Esta creencia les lleva a los delincuentes a perpetrar robos, posesión ilegal o no autorizada, transferencia ilegal, etc., con la expectativa de obtener un alto beneficio de su venta en el mercado negro. Este fenómeno es bastante común en economías débiles y con nulo o escaso control regulatorio, está motivado por el valor de los residuos como chatarra de las fuentes radiactivas sin mayor interés en el radioisótopo. En países industrializados sí se puede dar tráfico ilegal de dispositivos de uso industrial que contienen una fuente con el objetivo de evitar los costes de adquisición legal de dichos dispositivos por parte usuarios finales privados.

El mayor riesgo reside en el robo de material radiactivo por parte de grupos con fines maliciosos o terroristas para ser empleado en la radiación intencional de personas o provocar contaminación, solicitud de un rescate mediante la extorsión o el chantaje, construcción de un RDD y, aunque menos probable por sus dificultades asociadas, la construcción de un arma nuclear táctica.

Según datos de la DSTO[9] (Zaitseva, 2010) se produjo una eclosión de casos a inicios de los años noventa relacionada con operaciones policiales y de inteligencia a raíz del incremento del riesgo de tráfico de este material como consecuencia del colapso del antiguo bloque soviético. De hecho la quinta parte de los casos de tráfico ilícito fueron impedidos entre 1991 y 2009 por este tipo de operaciones (Fig. 1), lo que ha ido reduciendo paulatinamente este tipo de tráfico ilícito. La mayoría de las operaciones contra el tráfico ilícito llevadas a cabo por fuerzas policiales han sido contra la transferencia de material con motivación económica.

9 Stanford Database on Nuclear Smuggling, Theft, and Orphan Radiation Source.

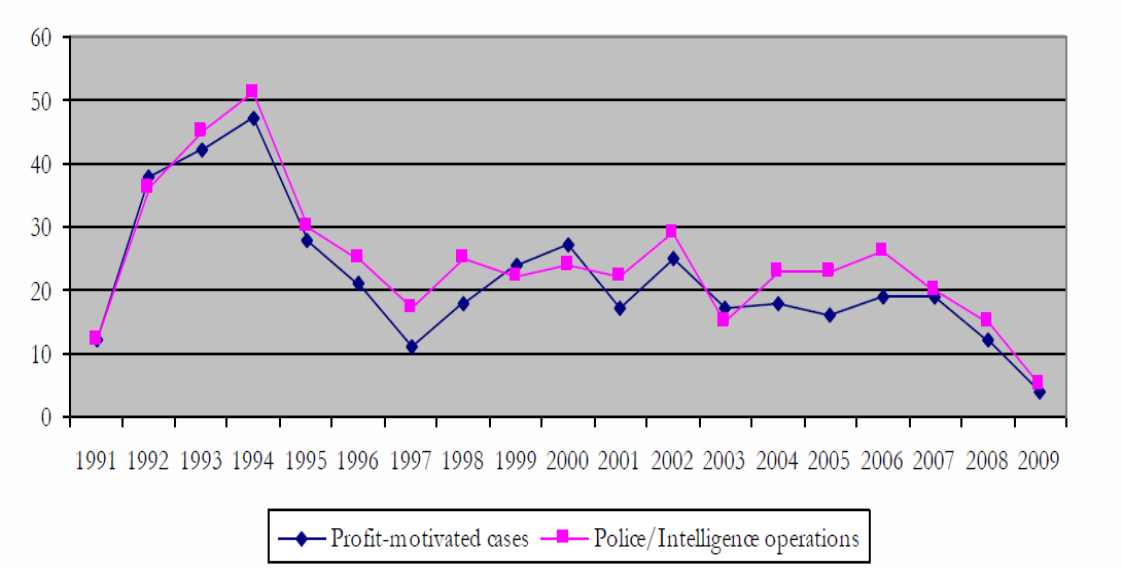

Fig. 1: Comparativa de casos con motivación económica e incidentes detectados por fuerzas policiales y de inteligencia entre 1991 y 2009 (fuente DSTO).

La paulatina reducción de este tráfico ilícito es consecuencia directa de la aplicación de medidas de control en los países vecinos de la ex-URSS. El incremento observado desde finales de la década de los noventa está relacionado con la instalación de sistemas de detección radiológica en otros países, lo que ha permitido que afloraran incidentes relacionados con el tráfico con motivación económica que antes no se detectaba.

Según la Organización Internacional de la Energía Atómica el 54% de los incidentes muestran evidencias de actividades criminales como el robo, contrabando, posesión o venta ilegal. Desde 1998, al igual que los datos de intervención policial de la DSTO, el número de incidentes ha ido en aumento. Analizando los datos de incidentes de tráfico ilícito que recoge la OIEA en su base de datos de incidentes y tráfico ilícito (ITDB[10]) se observa un incremento de material radiológico y contaminado (no nuclear) realmente llamativo, llama la atención el del material contaminado a la par que el radiológico. Aún siendo difícil determinar la motivación criminal, se puede establecer que es la expectativa de un alto valor de venta de las fuentes y dispositivos, así como de los contenedores de protección, el principal atractivo para los delincuentes, teniendo en cuenta que el 60% de los casos reportados en la ITDB no se ha recuperado el material robado.

No obstante se han registrado algunos casos de intento de adquisición de material nuclear y radiactivo con intenciones maliciosas. Igualmente se tiene constancia del intento de venta de uranio de bajo enriquecimiento (LEU[11], U-235 al 3-4%), usado como combustible nuclear, a dichos grupos como si se tratara de uranio enriquecido (HEU[12], U-235 al 90%).

10 *Incident and Trafficking Data Base.*
11 *Low Enrichment Uranium.*
12 *High Enrichment Uranium.*

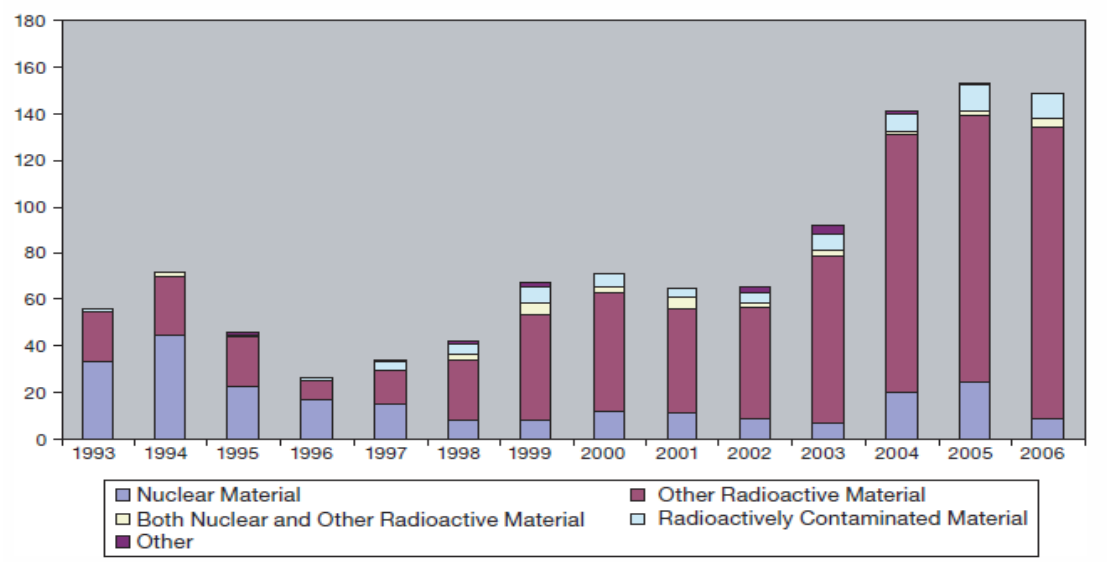

Fig. 2: Incidentes confirmados a la ITDB entre 1993 y 2006 (fuente OIEA).

La información sobre los incidentes basada en los datos del informe de la OIEA permite establecer algunas ideas sobre los patrones de criminalidad en el tráfico ilegal del material nuclear y radiológico:

- Se trata de actividades oportunistas de sustracción sin comprador predeterminado;
- Desconocimiento del valor real de la mercancía robada;
- Desconocimiento del funcionamiento de las redes de contrabando;
- Baja profesionalidad de los delincuentes;
- Intentos de estafa de compradores potenciales de escasa competencia técnica.

Según la ITDB en los incidentes con material nuclear o radiológico hay dos tipos de traficantes. El primer grupo compuesto por no profesionales, normalmente sin antecedentes, que se apoderan de manera ilícita del material motivados por la expectativa de obtener un beneficio de su venta. Normalmente se trata de personal que trabaja en las instalaciones, denominados *insiders*, o bien delincuentes comunes que irrumpen en las instalaciones con idéntica motivación. El segundo grupo está compuesto por traficantes mas o menos organizados que se dedican al contrabando de bienes como actividad lucrativa.

6. CONTRABANDO DE MATERIAL NUCLEAR Y RADIOLÓGICO

Un análisis del suministro y la demanda basado en 700 incidentes de tráfico ilícito recogidos por la DSTO (Zaitseva y Hand, 2003) entre 1991 y 2002, permite establecer las diferentes tipologías criminales a lo largo de la cadena de contrabando de material nuclear y radiológico. El análisis realiza una clasificación de las cadenas de contrabando en suministradores, intermediarios y usuarios finales.

6.1. SUMINISTRADORES

Las cadenas de suministro se inician con el personal que tiene acceso a las instalaciones por razones laborales, son los denominados insiders, suelen ser trabajadores de instalaciones civiles o militares. La distracción de material se dio con relativa frecuencia en Rusia tras la caída de la URSS, al relajarse los controles gubernamentales de seguridad debido al deterioro de las condiciones económicas (Zaitseva y Hand, 2003). Son los que incrementan el riesgo de robo debido a la capacidad que tienen para sortear las medidas de seguridad, así como evitar la detección del suceso hasta que el material se encuentra fuera del control de los legítimos responsables. Suelen actuar a iniciativa propia o por encargo y juegan un papel esencial en el acceso al material por parte de grupos terroristas.

- Personal empleado civil de instalaciones nucleares.
- Personal militar con acceso a equipamiento de nuclear de uso militar.
- Responsables de seguridad (civiles y militares).
- Outsiders, que procedían a la sustracción de material nuclear de antiguas instalaciones.

6.2. INTERMEDIARIOS

Grupos y organizaciones delictivas dedicados a la búsqueda de compradores potenciales, negociación y transferencia a usuarios finales (Zaitseva y Hand, 2003).

- Amateurs, generalmente desconocen la naturaleza del material que están manipulando o bien su conocimiento es muy escaso. Circunstancia que, asociada la escasa o nula precaución, provoca exposiciones peligrosas a radiación tanto a ellos como a los que les rodean.
- Comercializadores oportunistas y empresas, que abarcan desde los torpes y chapuceros hasta los de gran nivel de sofisticación en la constitución de redes de contrabando, en las que este material supone una actividad lucrativa adicional.
- Grupos criminales organizados. No existen datos que evidencien este extremo, se especula que sobre dos posibilidades. La primera que son capaces de evitar la detección de su actividad de contrabando. La segunda explicación, y mas plausible, es la ausencia de interés por el incierto y escaso beneficio potencial, así como el riesgo de comprometer el resto de actividades ilícitas que conforman su verdadero negocio.

6.3. USUARIOS FINALES

Constituye la mayor fuente de preocupación y es donde reside la verdadera amenaza del material de contrabando (Zaitseva y Hand, 2003).

- Estados que se encuentran en proceso de adquisición de tecnología nuclear y donde el riesgo de proliferación es alto.

- Estados fallidos o partes de un estado bajo el control de actores no estatales con infraestructuras capaces de la producción de RDD o incluso de armas nucleares tácticas.
- Organizaciones terroristas con capacidad suficiente como para producir y detonar un RDD o una bomba nuclear táctica. Algunas de ellas disponen de un know-how suficiente para su construcción, aunque la falta de infraestructura para su construcción y posterior detonación reduce significativamente la probabilidad del suceso.
- Otros grupos no estatales como sectas religiosas y movimientos separatistas que, si bien se podrían incluir dentro de las organizaciones terroristas, se trata de grupos de extensión difusa o indeterminada difícilmente identificables.
- Grupos de criminalidad organizada en cuyas actividades se emplea el chantaje, la extorsión o el asesinato, para lo que pueden valerse del empleo del material adquirido para la radiación intencionada.

7. MEDIDAS DE REDUCCIÓN DEL RIESGO

Los aspectos clave a tener en cuenta a la hora de reducir el riesgo engloban el control de las exportaciones y la gestión de la seguridad nuclear y radiológica. Igualmente necesario es el desarrollo legislativo nacional de las medidas propuestas por los convenios y demás instrumentos, así como el desarrollo de capacidades forenses nucleares dentro de los planes de respuesta nacionales al objeto de afrontar cualquier situación que comprometa la seguridad nuclear o radiológica.

7.1. CONTROL DE LAS EXPORTACIONES E IMPORTACIONES

La amenaza de uso de materiales nucleares y radiológicos después de los atentados del 11 de septiembre de 2001 llevó a la adopción de medidas e instrumentos para el control y prevención del contrabando de este tipo de material y tecnología. Como resultado de la irrupción de esta nueva amenaza se ha llevado a cabo un importante desarrollo del control radiológico en las fronteras. En el año 2004 la Agencia Estatal de Administración Tributaria (AEAT) y el Departamento de Energía de los Estados Unidos (DOE[13]) firmaron un MOU[14] con el objetivo de detectar e interceptar el tráfico ilícito de materiales nucleares y radiactivos. El objetivo es la disuasión, detección e intercepción del tráfico ilícito de este tipo de materiales en las redes de comercio internacional contenerizado a través de la iniciativa *Megaport*, mediante el empleo de dispositivos de detección (pórticos detectores, portales espectrométricos, equipos manuales, radiámetro y dosímetros de lectura directa, escáneres con detección gamma y neutrónica).

En el protocolo de actuación diseñado en caso de detección de movimiento inadvertido o tráfico ilícito de material radiactivo en puertos de interés general participan: Agencia Estatal de Administración Tributaria (AEAT), Secretaría de Estado

13 *Department of Energy.*

14 MOU, acrónimo de Memorandum of Understanding (en inglés). Se trata de un documento de acuerdo bilateral o multilateral en el que se expresa una convergencia de deseo entre las partes, indicando la intención de emprender una línea de acción común. No se trata de un compromiso legal que pueda ser defendido en instancias judiciales.

de Seguridad (Ministerio del Interior) Secretaría de Estado de Transportes (Ministerio de Fomento), Secretaría General de Energía (Ministerio de Industria), Consejo de Seguridad Nuclear (CSN), Empresa Nacional de Residuos Radiactivos (ENRESA).

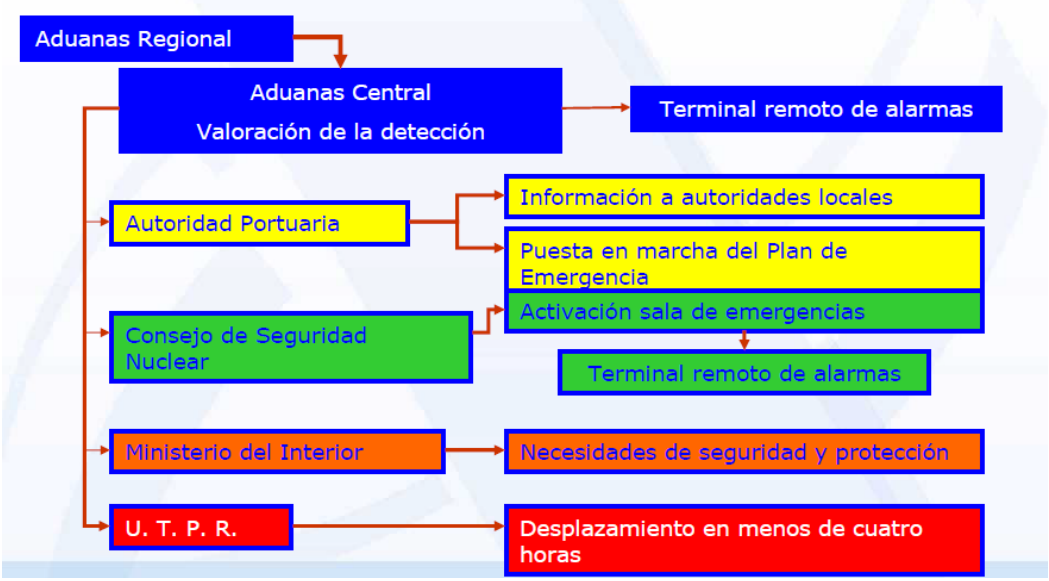

Fig. 3: Protocolo de actuación diseñado en caso de detección de movimiento inadvertido o tráfico ilícito (fuente AEAT).

7.2. GESTIÓN DE LA SEGURIDAD NUCLEAR Y RADIOLÓGICA EN ESPAÑA

El Real Decreto 1308/2011 establece una serie de medidas en las instalaciones nucleares haciendo del robo el riesgo prioritario y obligando a sus titulares a una serie de requisitos mínimos de protección física, registro documental de localización, uso, movimientos e inventario. El Real Decreto 1086/2015[15], que modifica el anterior reforzándolo, establece la creación de una "Unidad de Respuesta"[16] y una "respuesta de entidad adecuada"[17].

7.3. NORMAS BÁSICAS INTERNACIONALES

Existe un amplio abanico de normas internacionales contra la proliferación en general. Son de especial relevancia los instrumentos para hacer frente al terrorismo nuclear que recoge la Iniciativa Global Contra el Terrorismo Nuclear:

- Convenio para la Represión de Actos de Terrorismo Nuclear.

15 Real Decreto 1086/2015, de 4 de diciembre, por el que se modifica el Real Decreto 1308/2011, de 26 de septiembre, sobre protección física de las instalaciones y los materiales nucleares, y de las fuentes radiactivas.

16 "Constituida por una Unidad de la Guardia Civil ubicada permanentemente en el interior de las centrales nucleares y aquellas instalaciones nucleares que se determine por Ley conforme a la amenaza base de diseño, para proporcionar una respuesta de entidad adecuada en caso de materialización de las amenazas antisociales de origen humano que puedan determinar o elevar el riesgo de robo o sabotaje".

17 "Reacción de oposición a un ataque o intrusión, para neutralizarlo o contenerlo mitigando sus efectos. Para la hipótesis planteada en la amenaza base de diseño, su alcance dependerá, entre otros factores, del número y configuración de las zonas vitales a proteger, de las características físicas del emplazamiento y del diseño de la propia instalación".

- Convención sobre Protección Física de los Materiales Nucleares y su enmienda de 2005.
- Resoluciones 1373 y 1540 del Consejo de Seguridad de Naciones Unidas.
- Reglamento 450/2008 del Parlamento Europea y del Consejo, por el que se establece el código de control aduanero.

La normativa exhorta a los estados al establecimiento de sistemas que permitan contabilizar y controlar los materiales nucleares y radiactivos, así como las medidas necesarias de protección física y adaptación de la normativa legal interna. Igualmente establece la necesidad de dotarse de capacidades de detección de dichos materiales y dispositivos al objeto de prevenir su tráfico ilícito y poder realizar un control policial fronterizo eficaz.

7.4. NORMATIVA ESPAÑOLA Y MEDIDAS LEGALES

En la legislación española existe normativa encaminada al control aduanero comunitario y de fronteras al objeto de garantizar la seguridad y protección de la comunidad y el medio ambiente, así como medidas de vigilancia y control y procedimientos de actuación ante el hallazgo de fuentes huérfanas.

Respecto al control de fuentes como una de las medidas críticas para la prevención de actividades que pudieran estar relacionadas con el terrorismo nuclear, así como garantizar el control de las fuentes radiactivas, es destacable la siguiente normativa nacional:

- Real Decreto 783/2001, de 6 de julio, por el que se aprueba el Reglamento sobre Protección Sanitaria contra Radiaciones Ionizantes (Modificado por RD 1439/2010).
- Real Decreto 229/2006 de 24 de febrero, sobre el control de fuentes radiactivas encapsuladas de alta actividad y fuentes huérfanas.
- Real Decreto 1308/2011, de 26 de septiembre, sobre protección física de las instalaciones y los materiales nucleares, y de las fuentes radiactivas.
- Instrucción del CSN IS-18 de 2 de abril de 2008 sobre los criterios aplicados por el CSN para exigir a los titulares de las instalaciones radiactivas la notificación de sucesos e incidentes radiológicos.
- Catálogo nacional de instalaciones o actividades que puedan dar lugar a situaciones de emergencia por riesgo radiológico.

Para la persecución de los delitos relacionados con el tráfico ilícito de material nuclear y radiactivo, así como de actividades terroristas relacionadas se modificó el Código Penal en los capítulos I y V de los títulos XVII y XXII respectivamente:

Artículo 345:

"1. El que, contraviniendo las leyes u otras disposiciones de carácter general, adquiera, posea, trafique, facilite, trate, transforme, utilice, almacene, transporte o elimine materiales nucleares u otras sustancias radiactivas peligrosas[18]…, será castigado con la pena de prisión de uno a cinco años, multa de seis a dieciocho meses, e inhabilitación especial para profesión u oficio por tiempo de uno a tres años".

18 Que causen o puedan causar la muerte o lesiones graves a personas, o daños sustanciales a la calidad del aire, la calidad del suelo o la calidad de las aguas o a animales o plantas.

Artículo 566:

"1. Los que fabriquen, comercialicen o establezcan depósitos de armas o municiones no autorizados por las leyes o la autoridad competente".

Artículo 567:

"1. Se considera depósito de armas de guerra la fabricación, la comercialización o la tenencia de cualquiera de dichas armas, con independencia de su modelo o clase, aun cuando se hallen en piezas desmontadas[19].

2. Se consideran armas de guerra las determinadas como tales en las disposiciones reguladoras de la defensa nacional[20]".

7.5. ANÁLISIS FORENSE NUCLEAR

Las capacidades que proporciona el análisis forense nuclear pueden permitir el establecimiento de relaciones entre el material nuclear y radiológico y transporte, posesión y uso sin el control legítimo de los estados. Consiste en el análisis integral de cualquier muestra o evidencia de material contaminado dentro de cualquier contexto de violación de la legislación civil, penal o internacional. Mediante el análisis forense nuclear se pretende la identificación de los materiales, cómo, dónde y cuándo se han intentado usar. Las técnicas forenses junto con los datos de la base de datos ITDB de la OIEA pueden permitir establecer las relaciones entre el material y su posible intento de uso ilícito. De esta manera se puede determinar la existencia de relaciones entre personas, lugares, materiales y/o sucesos. Igualmente permite proporcionar información a las autoridades judiciales y policiales sobre:

- Identificación de materiales y legitimidad de su posesión.
- Conexión ilícita entre el material y los individuos.
- Determinación de la trazabilidad desde el punto de origen hasta el de incautación.
- Identificación de los materiales y si su posesión está fuera del control regulado.

El análisis forense nuclear es un componente crítico en materia de seguridad nuclear que permite realizar un control de la trazabilidad de un material nuclear desde el origen en un país, el tráfico ilícito a través de otro y su empleo con fines terroristas en un tercero. De esta manera se pueden identificar los materiales radiactivos por sus características únicas, intensificando la seguridad. Para llevar a cabo este proceso analítico es necesario disponer de dos tipos de capacidades:

- Capacidades esenciales consistentes en medidas gubernamentales para:
    1. Facilitar una respuesta rápida y apropiada de acuerdo con planes de respuesta nacionales.

19 Se considera depósito de armas químicas, biológicas, nucleares o radiológicas o de minas antipersonas o de municiones en racimo la fabricación, la comercialización o la tenencia de las mismas. El depósito de armas, en su vertiente de comercialización, comprende tanto la adquisición como la enajenación.

20 Se consideran armas químicas, biológicas, nucleares o radiológicas, minas antipersonas o municiones en racimo las determinadas como tales en los tratados o convenios internacionales en los que España sea parte. Se entiende por desarrollo de armas químicas, biológicas, nucleares o radiológicas, minas antipersonas o municiones en racimo cualquier actividad consistente en la investigación o estudio de carácter científico o técnico encaminada a la creación de una nueva arma química, biológica, nuclear o radiológica, o mina antipersona o munición en racimo o la modificación de una preexistente.

2. Determinar violaciones de la legislación nacional y facilitar el cumplimiento de la ley.
3. Evaluar las necesidades de aplicación de medidas avanzadas.
4. Fortalecimiento de los controles nacionales de materiales nucleares y radiactivos.
5. Facilitar la asistencia mutua entre estados.

- Capacidades avanzadas complejas que requieren de infraestructuras y personal especializado para la identificación del origen del material para mejorar la identificación en base a las características únicas del material. Proporcionan información crítica para determinar si la seguridad nuclear se ha visto comprometida. Permiten a las fuerzas del orden establecer relaciones en caso de incidentes separados:

  1. Espectrometría de masas, microscopía electrónica, simulación de producción de materiales.
  2. Monitoreo ambiental y caracterización de materiales.

8. ANÁLISIS DE LOS INCIDENTES DESDE ENERO DE 2013 A JULIO DE 2015

En este apartado se analiza la distribución de incidentes por cada una de las tipologías y las circunstancias asociadas para determinar su posible relación con el tráfico ilícito de material nuclear y radiológico.

8.1. Valoración general de cada tipología de incidente

De la totalidad de incidentes que han tenido lugar el 83% podría guardar *a priori* algún tipo de relación con fenómenos de tráfico ilícito de material nuclear o radiológico. El 17% restante se correspondería con la detección de material contaminado, eliminación incorrecta o fallos en las entregas o envíos.

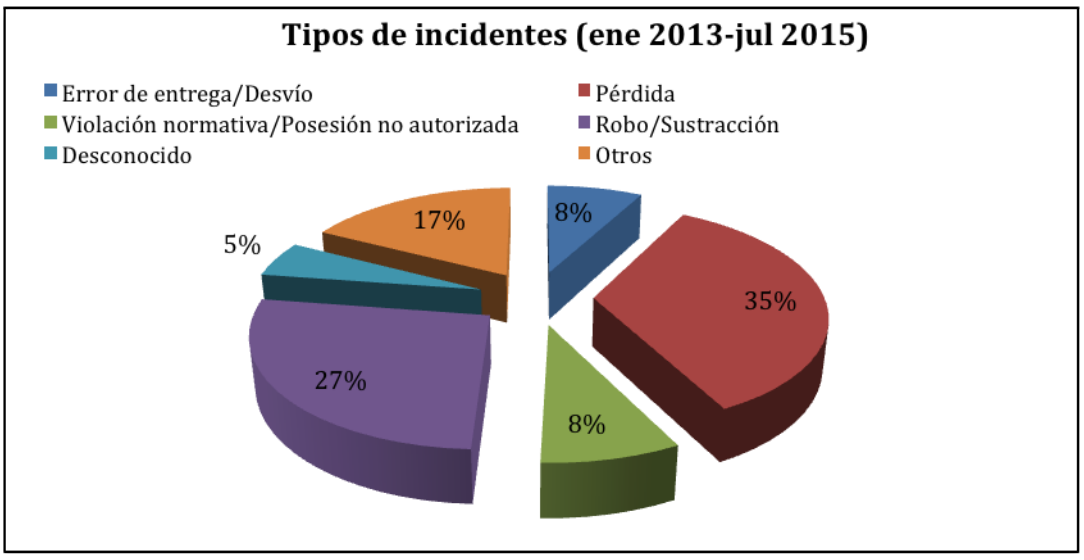

Fig. 4: Distribución de incidentes por tipo en el periodo de enero de 2013 a julio de 2014 (elaboración propia).

La evolución de la serie temporal de los incidentes susceptibles *a priori* de guardar relación con el tráfico ilícito se muestra en el siguiente gráfico:

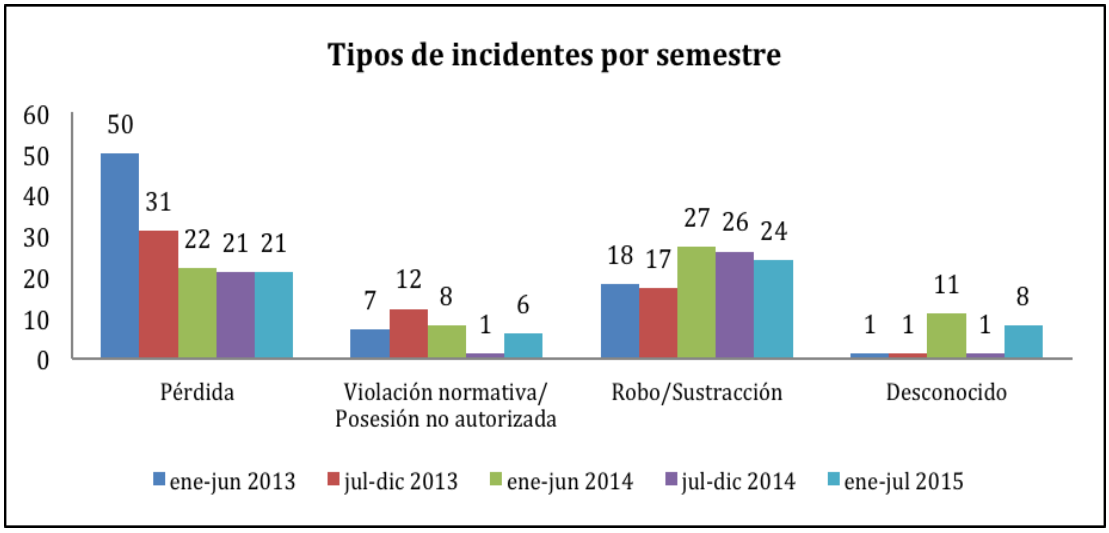

Fig. 5: Distribución del tipo de incidentes por semestre en el periodo de enero de 2013 a julio de 2014 (elaboración propia).

8.1.1. Pérdidas

Se observa un descenso de las pérdidas o extravíos de material al inicio de la serie temporal, manteniéndose constante a partir de 2014. La mayoría de las cuales implican fuentes de uso industrial o médico. Solamente existen datos de recuperación del 21% del material extraviado.

La mayor parte de los extravíos se deben a negligencias durante su uso industrial. Del material no recuperado solo un incidente involucraba material de categoría 1, se trataba de un cuchillo gamma de uso médico cuya pérdida fue notificada en Toronto (Canadá), el 10 de enero de 2014, y que se aún se está investigando.

Los de categoría 2 y 3 son incidentes relacionados con errores logísticos en el material o extravíos durante el transporte o como consecuencia de accidentes de tráfico.

Un incidente de pérdida que concluyó con la detención de cuatro personas ocurrió el 7 de mayo de 2014 en unas obras de construcción en Puliu (China). Tras advertir la pérdida de una fuente de Ir-192 por parte de la compañía Engineering Inspection Development Co Ltd. Y no fue comunicada su desaparición hasta dos días después. Dicha fuente fue hallada el 10 de mayo en Nanjing (Jiangsu, China), cuando uno de los trabajadores que lo había recogido del suelo se deshizo del pequeño dispositivo arrojándolo a la basura, al tener conocimiento de que la policía lo estaba buscando. Es un ejemplo de negligencia por parte de los responsables de la empresa y de trabajadores con escaso conocimiento y responsabilidad.

La no recuperación de dichas fuentes podría relacionarse con el intento de venta irregular por parte de personas que los encuentran y pretenden lucrarse con la venta de un material cuyo escaso valor desconocen o bien como chatarra, coincidiendo con los estudios de Zaitseva y Hand en 2003.

8.1.2. Violación normativa/Posesión no autorizada

Esta clasificación es bastante heterogénea, en el sentido que incluye material que viola la regulación obligatoria para su control o almacenamiento. La falta de control puede desembocar en posesión no autorizada. Se ha optado por incluirlas de manera conjunta porque, a partir del segundo semestre de 2014, se reportan únicamente posesiones no autorizadas. Debe tenerse en cuenta que el incumplimiento de cualquier normativa actualizada puede constituir una posesión no autorizada sobre cualquier material que previamente se poseía de forma legal.

El descenso observado a partir del segundo semestre se corresponde con el cambio de denominación del incidente reportado, por lo que solo se registran como posesión no autorizada los que ciertamente constituyen una tenencia o posesión sin autorización. De este tipo de incidentes siete destacan como posesión no autorizada, siendo recuperados por las autoridades en todos los casos. No obstante hay seis incidentes destacables.

El primero de ellos tuvo lugar el 15 de enero de 2015 en Arkansas (Estados Unidos), en las que el *Department of Health Radioactive Materials Program* informaba del hallazgo, en un domicilio particular, de sendos envases contiendo óxido de uranio (3% U-235) de uso nuclear.

El segundo incidente, que sí implicaría tráfico ilícito, tuvo lugar en Moldavia en el curso de una operación policial en el que dos individuos fueron arrestados, en un intento de venta de material de cuyas características y uso no se ha informado.

El tercer incidente constituye un tráfico ilícito transfronterizo en el que se detuvo a dos individuos que trataban de cruzar la frontera entre Austria y Eslovaquia con radionúclidos de uso médico y sin la documentación necesaria para el transporte de dicho material.

El cuarto se saldó con una persona detenida en Sao Paulo (Brasil) por posesión de 22 bidones conteniendo material médico radiactivo sin licencia en una compañía de transportes.

Un quinto incidente destacable es la detención de una azafata, el 23 de agosto de 2013, en el aeropuerto de Domodedovo (Moscú, Rusia), con una baraja de naipes que excedía varias veces los límites de radiación permitidos.

Por último en el aeropuerto de Simferpol (Ucrania), el 4 de julio de 2013, se detuvo a un ciudadano procedente de Sebastopol Crimea, portando un reloj de un avión MIG que emitía radiación gamma cien veces por encima del nivel normal y dijo haberlo adquirido como souvenir.

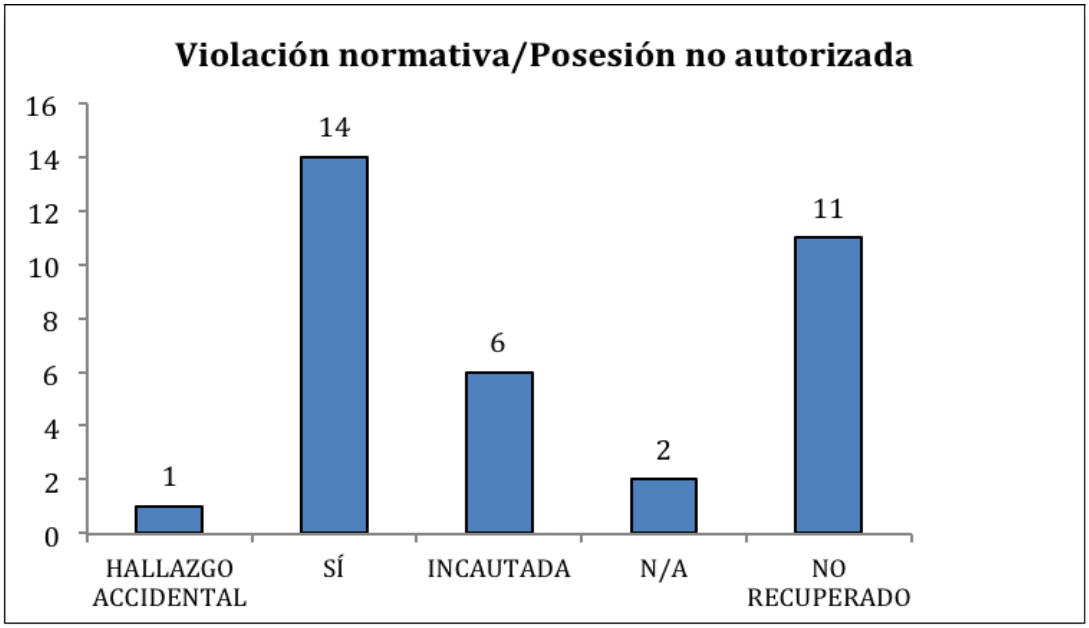

Fig. 7: Circunstancias de recuperación del material/mercancía (elaboración propia).

8.1.3. Robo/Sustracción

Los incidentes que constituyen robo o sustracción se mantienen constantes con una ligera tendencia al alza. El 80% de los robos implican algún tipo de dispositivo o aparato de uso industrial, especialmente empleados en la construcción o minería (principalmente contienen materiales como el Ir-192, Cs-137 y Am-241). Los robos se producen durante el transporte de los dispositivos o por violación de las medidas de seguridad en los lugares de operación. Es destacable que de los 14 robos o sustracciones informadas el 57% son comunicadas por Estados Unidos, seguidas de las seis de Francia, cuatro de México y tres de Ucrania.

Son de destacar los siguientes robos de material que escapan a la tipología referente a material de uso industrial y que, en principio, no parecen obedecer a intereses maliciosos. En España ha tenido lugar un solo incidente en todo este tiempo y se trató de un robo, en Almendralejo (Badajoz) en 2014, de un medidor de humedad y densidad de suelos en un vehículo aparcado, que contenía fuentes de Cs-137 y Am-241/Be.

Los siguientes incidentes resultan de interés por tratarse de sustracciones cuyos autores fueron arrestados y constituían tipos delictivos directamente relacionados en los que el material nuclear o radiológico no era una cuestión secundaria en la comisión de dicho delito y estaba directamente relacionado con los fines para los que se perpetraba.

- Ucrania. El 5 de abril de 2015 un hombre y una mujer intentaron remover 100kg de metal radiactivo de la zona de exclusión de la antigua central nuclear Chernobyl. Al parecer pretendían su venta como chatarra. El 6 de abril de 2015 dos hombres fueron arrestados en un intento similar de sustracción de unos 200 kg de chatarra de metal. La proximidad temporal y características de los sucesos de sustracción de metal contaminado de la antigua central de Chernobyl lleva a pensar que es una práctica habitual que no se reporta por dos posibles razones no excluyentes entre ellas. La primera porque no

se atrapa a los autores en el momento de la comisión del robo y la segunda porque no se puede tener un control inventario de la chatarra metálica en el interior de la zona de exclusión, por lo que no se advierten otros robos o pasan desapercibidos para las autoridades.

- Rusia. El 25 de marzo de 2015 se produjo la detención de un profesor universitario en Moscú, que poseía en su domicilio 14kg de sustancias radiactivas que se sospecha proceden de algún enterramiento. Se trataba de una posesión ilegal con la pretensión poco creíble de procurar proporcionar inmortalidad a un amigo mediante radiación. Aunque se trata de posesión ilegal se entiende sustracción de un emplazamiento previo como confesó el presunto autor.

- México. El 2 de diciembre de 2013 fue robado un camión que transportaba material de baja radiactividad que iba destinado al Instituto Nacional de Investigación Nuclear del Estado de México. Contenía 60 g de Co-60, un material radiactivo potencialmente fatal empleado en radioterapia. Hasta el 4 de diciembre de 2014 no fue recuperado el material cuando el camión fue hallado en Temascalapa. Todo el personal expuesto durante la apertura del camión fue sometido a controles de radiación y los autores detenidos.

- Estados Unidos. El 23 de agosto de 2013 el Departamento de Seguridad Interior (*Department of Homeland Security* –DHS-) detuvo a Patrick Campbell, natural de Sierra Leona, en el Aeropuerto Internacional JFK de Nueva York por contrabando de uranio. Se trataba de un intento de venta de polvo de uranio (*yellowcake*) mediante la respuesta a un anuncio colocado por el DHS, que se mostraba interesado en la compra de polvo de uranio para Irán. Campbell respondió al anuncio y se ofreció a vender 1,000 toneladas tras negociar vía Skype. Resultó detenido en el aeropuerto con una muestra de la sustancia oculta en la suela de sus zapatos. Se trata de un verdadero intento de tráfico a gran escala. Aún queda por determinar si tenía acceso a esa cantidad de polvo de uranio o simplemente trataba de estafar a potenciales compradores. Lo que sí confirma el hecho es la intencionalidad de venta ilícita de material, pero por parte de *freelance* que no forma parte de redes dedicadas al tráfico de dicho material de manera exclusiva. Posiblemente por la falta de un mercado negro lo suficientemente amplio como para que el negocio resulte bastante lucrativo.

- Kazajistán. En 2013 se produjo el arresto de un ingeniero y tres de sus cómplices por el intento de venta de manera ilícita de Cs-1735, sustraído hacía 22 años, antes de entregarlo a sus conocidos para su venta, esperando obtener un beneficio de un cuarto de millón de dólares. El descubrimiento se llevó a cabo mediante la introducción de un agente encubierto en la operación de intento de venta.

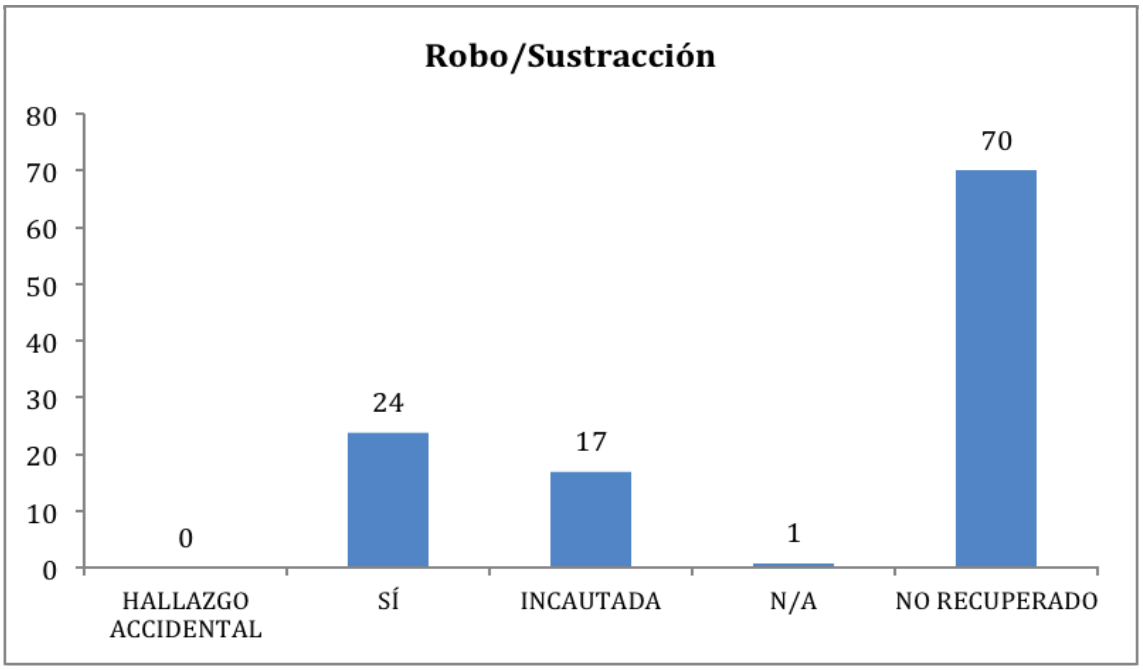

Fig. 8: Circunstancias de recuperación del material/mercancía ROBADO/SUSTRAÍDO (elaboración propia).

8.1.4. Incidentes de tipo desconocido

Se trata de incidentes que no reportan detalles suficientes para su clasificación o bien no se corresponden con otras categorías. De los 24 incidentes reportados, 8 de ellos podrían estar relacionados con actividades ilícitas o terrorismo, por lo que merecen ser destacados:

- Ucrania. El 30 de abril de 2014 el Servicio de Contrainteligencia de Ucrania (SBU) se incautó de una fuente ionizante de 1,5 kg, posiblemente de U235, en un vehículo en la región de Chernivtsi. Se trataba de un vehículo con matrícula de la región de Transnistria (Moldavia). La operación se saldó con nueve detenidos ucranianos y uno ruso. Se sospecha de las intenciones ilícitas para el empleo de dicho material, aunque no se trata de cantidad suficiente para la construcción de un DDR. Las características y circunstancias del suceso sí podrían apuntar a un fenómeno de tráfico ilícito transfronterizo en una red delincuencia organizada transnacional entre Moldavia, Ucrania y Rusia.

  El 18 de mayo de 2015 tuvo lugar el hallazgo de cinco contenedores por parte de un habitante de Odessa (Ucrania) en el interior de su apartamento. Los servicios de emergencia encontraron tres fuentes de radiación ionizante y dos lámparas radiactivas. Se supone la procedencia de una planta especial de radón.

- Rusia. El 19 de marzo de 2013, en el Aeropuerto Internacional de Domodedovo (Moscú), se detuvo a un individuo procedente de Yerevan (Armenia). El individuo portaba un bloque del motor de un helicóptero que había comprado en un viaje de negocios y pretendía introducirlo en el país a través de la puerta de acceso a viajeros sin bienes que declarar.

El 4 de abril de 2013 se detectó un paquete de 800 g en la oficina de correos de Orenburg (Rusia) con unos niveles de radiación diez veces superiores al nivel de radiación de fondo. Se trataba de un indicador de aeronave de un coleccionista que lo había vendido y lo remitía al cliente en Moscú. Aunque no se trate de una intención delictiva, sí existe un intercambio de material radiactivo a cambio de un beneficio económico, que desembocó en una investigación posterior.

- Kazajistán. El 2 de junio de 2015 inspectores de la estación de Tobol en Kostany (Kazajistán) detectaron niveles elevados de radiación en un vagón de carga. Tras la inspección se advirtió que dicho vagón llevaba docenas de toneladas de concentrado de zirconio de Kokshetau a Novorossiysk.

- Estados Unidos. El 6 de diciembre de 2013, tras una alarma de radiación en Modern Landfill en York (Pennsylvania), se descubrieron dos núcleos de un generador de Mo99. Dichos núcleos habían sido robados entre el 12 y 19 de noviembre en la concesión de farmacia nuclear del Cardinal Health.

  El 26 de abril de 2014 el concesionario de Can Metals Ltd. comunicó la sustracción de un dispositivo Thermo Niton propiedad de la empresa durante la realización de estudios de materiales en México rompiendo contacto con la empresa. Tras investigaciones se descubrió que dicho empleado había adquirido una casa en el Estado de Arizona. No encontrándose rastro alguno del dispositivo ni del empleado.

- Alemania. El 17 de abril de 2015 el nuevo propietario de una casa descubre la existencia de productos químicos y explosivos en el interior de la vivienda. Tras la inspección del servicio de bomberos encontraron varios objetos del tamaño de un pulgar con Ra-226. Al parecer habían sido abandonados por el anterior propietario, en cuyo nuevo domicilio se encontraron más productos químicos peligrosos y material explosivo.

- India. El 24/01/2013 el grupo rebelde indio UFLA, en el nordeste del estado de Assay fue sorprendido por una patrulla del ejército con un artefacto improvisado que contenía 1,5 kg uranio y material explosivo. Fuentes de la inteligencia india informaron de las intenciones de hacerlo detonar coincidiendo con la celebración del Día de la República. Aunque se desconoce su procedencia y tipología, parece ser que se trata de producto obtenido por sustracción de un emplazamiento minero.

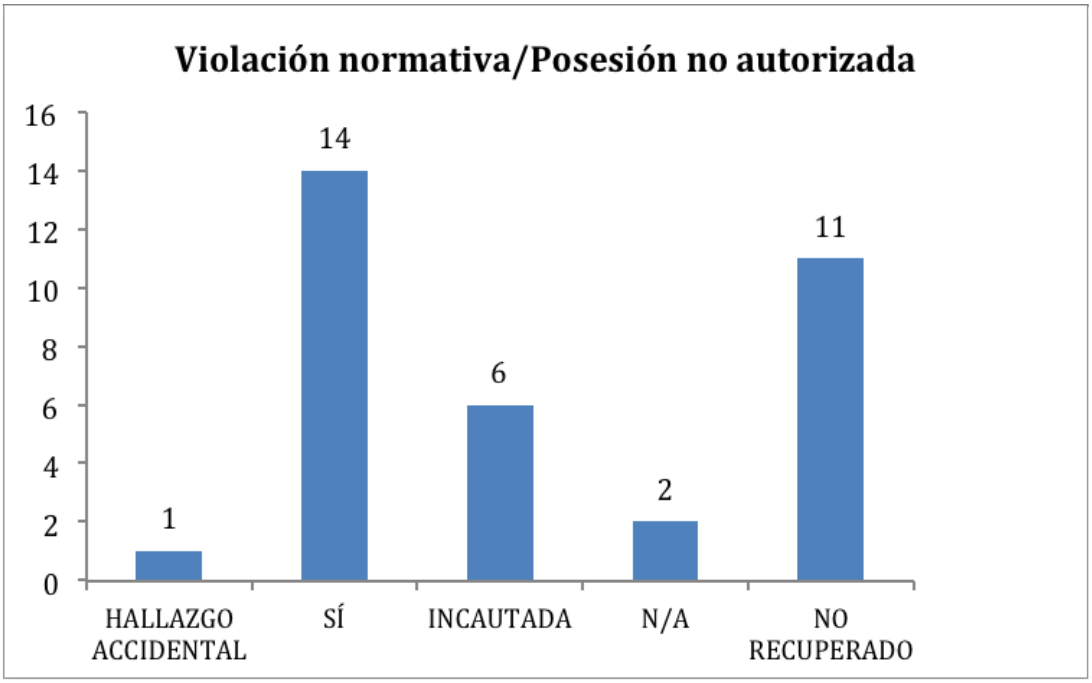

Fig. 9: Circunstancias de recuperación del material/mercancía que violaba la normativa o se poseía sin autorización (elaboración propia).

Examinando los robos durante el transporte se observa que la mayoría de estos se producen cuando el medio de transporte se encuentra estacionado. Un dato relevante es que solamente en 14 de los 62 robos el material es sustraído junto con el vehículo. Las razones por las que no se sustrae junto con el vehículo no se pueden establecer con precisión, pero lo que sí es evidente que en los 48 restantes el objetivo del robo era la mercancía transportada.

8.2. Sobre la intervención de las fuerzas de seguridad (militares y policiales) en el esclarecimiento de los incidentes

En la casuística objeto del presente estudio las fuerzas de seguridad han participado en 28 incidentes con buenos resultados en cuanto a la recuperación del material, incluso en el caso de robo en el que se consiguió recuperar el 83% del material. En ocho de los quince casos de recuperación se produjo alguna detención. De los otros tres en los que no se recuperó el material, en uno de ellos se produjo alguna detención (Sibusiso Solomon Mkhize y Sasa Esael Vulay[21]).

21 11/11/2013, robo de uranio enriquecido al 0.38% con U-238 y valorado en 80$ en Durban (Sudáfrica).

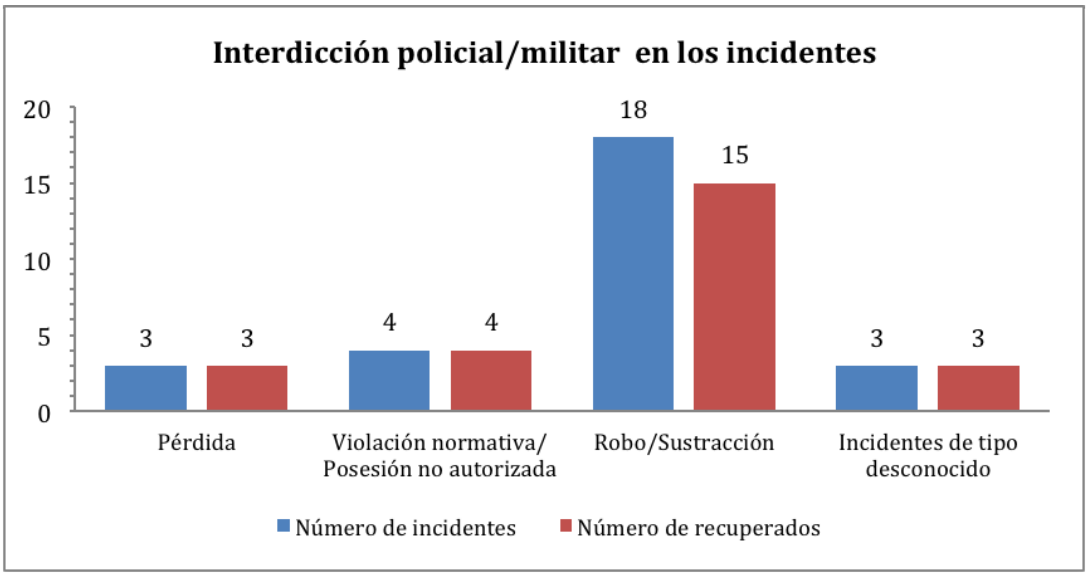

Fig. 12: Recuperación de material por parte de las fuerzas de seguridad (elaboración propia).

9. CONCLUSIONES

La mayor parte de los incidentes analizados se corresponde con pérdidas o robo/sustracción de material. Si bien se trata de materiales que no se emplean en la construcción de artefactos nucleares, si suponen un riesgo potencial, y muy alto en ocasiones, para la salud de las personas o de contaminación ambiental. Se trata de materiales de uso industrial o médico.

La mayor parte de las pérdidas son consecuencia de la negligencia en la custodia por parte de quienes operan con el mismo, sea en la logística o en el empleo de dispositivos de medición.

Los robos y sustracciones de material obedecen a varias tipologías según circunstancias. La principal vulnerabilidad reside en el transporte de material o de dispositivos. Por un lado se observa una sustracción del interior del vehículo, por lo que se puede concluir que la carga es el objetivo del robo. En otras ocasiones es una consecuencia del robo del vehículo, objetivo primario de quien lo lleva a cabo. En los robos en emplazamiento fijo encontramos la acción de insiders que asignan un valor excesivo a los materiales por las medidas de seguridad que los rodean, o bien por tratarse de dispositivos de medida de precisión que supuestamente pueden ser vendidos fuera de los circuitos autorizados eludiendo las tasas impuestas. El robo de material de emplazamientos donde ha habido instalaciones nucleares no parece habitual, pero algunos aspectos indican que podría ser mucho más frecuente que el observado. Las razones estriban en la proximidad en tiempo y lugar de los dos incidentes de sustracción de chatarra en Chernobyl en 2015, cuya interdicción parece casual. La ausencia de más incidentes puede achacarse a varias circunstancias: la primera de ellas debido a la situación en Ucrania desde 2014, que podría haber empeorado la vigilancia y control de la instalación; la segunda se debe a que no existe un inventario preciso del material confinado que se actualice y gestione como en una que estuviera operando con normalidad.

Muchos incidentes de tipo desconocido o de posesión ilícita están relacionados con el hallazgo de material de forma casual o la adquisición de piezas o dispositivos como

souvenirs procedentes del desguace de material militar y/o aeronáutico en Rusia y repúblicas ex-soviéticas.

Solo dos incidentes implican un intento de tráfico ilegal propiamente dicho, pero sin que exista una red criminal constituida. El intento de contrabando de polvo de uranio para su venta a Irán parece ser producto de un freelance que pretendía obtener beneficio de la venta de una gran cantidad, aprovechando la coyuntura del bloqueo del programa nuclear iraní. El segundo caso, que tiene lugar en Kazajistán es una clara actuación de insiders con conocimiento del material y el de su potencial valor de venta en el mercado negro.

El descenso de las pérdidas en la serie temporal puede correlacionarse con la introducción de medidas de buenas prácticas en la gestión logística de materiales y dispositivos.

La intervención de las autoridades policiales y militares en la resolución de los incidentes puede considerarse muy satisfactoria, incluso en los incidentes de robo en los que han intervenido con una recuperación del 83%. Aunque los otros incidentes en los que han intervenido son escasos, la recuperación del material ha sido total en todos ellos.

BIBLIOGRAFÍA

Consejo de Europa (2003). Directiva 2003/122/EURATOM DEL CONSEJO sobre el control de las fuentes radiactivas selladas de actividad elevada y de las fuentes huérfanas, Diario Oficial de la Unión Europea, 345, de 31 de diciembre de 2003, pp 97-105, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:346:0057:0064:ES:PDF

CSN (2012). Guía técnica del Consejo de Seguridad Nuclear para el desarrollo y la implantación de los criterios radiológicos de la Directriz Básica de Planificación de Protección Civil ante el Riesgo Radiológico, CSN, Colección Informes Técnicos 30-2012, https://www.csn.es/documents/10182/27786/INT-08-04%20Gu%C3%ADa%20t%C3%A9cnica%20del%20Consejo%20de%20Seguridad%20Nuclear%20para%20el%20desarrollo%20y%20la%20implantaci%C3%B3n%20de%20los%20criterios%20radiol%C3%B3gicos%20de%20la%20Directriz%20B%C3%A1sica%20de%20Planificaci%C3%B3n%20de%20Protecci%C3%B3n%20Civil%20ante%20el%20Riesgo%20Radiol%C3%B3gico

CSN (2014). CNS Global Incidents and Trafficking Database. 2013 Annual Report, James Martin Center for Nonproliferation Studies.

CSN (2015). CNS Global Incidents and Trafficking Database. 2014 Annual Report, James Martin Center for Nonproliferation Studies.

CSN (2015). CNS Global Incidents and Trafficking Database", James Martin Center for Nonproliferation Studies. , http://www.nti.org/analysis/reports/cns-global-incidents-and-trafficking-database/

CSN (2015). Guía de ayuda para la elaboración de las disposiciones a tomar en caso de emergencia aplicables al transporte de materiales radiactivos por carretera, Guía de Seguridad 6.3 (Rev. 1). Colección de Guías de Seguridad CSN, https://www.csn.es/documents/10182/896572/GS%2006-03%20Revisi%C3%B3n%201%20-%20Gu%C3%ADa%20de%20ayuda%20para%20la%20elaboraci%C3%B3n%20

de%20las%20disposiciones%20a%20tomar%20en%20caso%20de%20emergencia%20aplicables%20al%20transporte%20de%20materiales%20radiactivos%20por%20carretera

CSN (2015). Guía de ayuda para la aplicación de los requisitos reglamentarios sobre transporte de material radiactivo (Actualizada según el ADR de 2015), Guía de Seguridad 6.5. Colección de Guías de Seguridad CSN, https://www.csn.es/documents/10182/896572/GS%2006-05%20(Actualizaci%C3%B3n%20de%20Anexos%20ADR%202015)%20Gu%C3%ADa%20de%20ayuda%20para%20la%20aplicaci%C3%B3n%20de%20los%20requisitos%20reglamentarios%20sobre%20transporte%20de%20material%20radiactivo

Garrido Rebolledo, V. (2012). Terrorismo nuclear. ¿Nuevo desafío a la seguridad?, Política Exterior, nº 148, julio-agosto de 2012, pp. 82-92.

GICNT (2015). Exchanging nuclear forensics information. Benefits, Challenges & Resources, Global Initiative to Combat Nuclear Terrorism, Nuclear Forensic Working Group, junio de 2015.

GICNT (2015). CNS Global Incidents and Trafficking Database. Tracking publicly reported incidents involving nuclear and other radioactive materials. 2014 Annual report, Global Initiative to Combat Nuclear Terrorism, Nuclear Forensic Working Group, abril de 2015.

Gobierno De España (2017). Estrategia de Seguridad Nacional. Un proyecto compartido de todos y para todos, http://www.dsn.gob.es/sites/dsn/files/Estrategia_Seguriad_Nacional_2017.pdf

Gobierno de España (1999), “Real Decreto 1836/1999, de 3 de diciembre, por el que se aprueba el Reglamento sobre instalaciones nucleares y radiactivas”, https://www.boe.es/boe/dias/1999/12/31/pdfs/A46463-46482.pdf

Gobierno de España (2010). Real Decreto 1564/2010, de 19 de noviembre, por el que se aprueba la Directriz básica de planificación de protección civil ante el riesgo radiológico, https://www.boe.es/boe/dias/2010/11/20/pdfs/BOE-A-2010-17808.pdf

Gobierno de España R (2014). Real Decreto 1546/2004, de 25 de junio, por el que se aprueba el Plan Básico de Emergencia Nuclear, https://www.boe.es/boe/dias/2010/11/20/pdfs/BOE-A-2010-17808.pdf

Gobierno de España (2011). Real Decreto 1308/2011, de 26 de septiembre, sobre protección física de las instalaciones y los materiales nucleares, y de las fuentes radiactivas, http://www.boe.es/diario_boe/txt.php?id=BOE-A-2011-15723

Gobierno de España (2015). Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal”, Boletín Oficial del Estado núm. 77, de 31 de marzo de 2015, pp 27061-27176 https://www.boe.es/diario_boe/txt.php?id=BOE-A-2015-3439

Hidalgo García, M., Velarde Pinacho, G. y otros (2011). Proliferación de AMD y de tecnología avanzada, Cuadernos de Estrategia nº 153, Instituto Español de Estudios Estratégicos, septiembre 2011.

IAEA (1980). Convención sobre la protección física de los materiales nucleares, 1979 (Convención sobre materiales nucleares), https://www.iaea.org/sites/default/files/infcirc274r1_sp.pdf

IAEA (2007). Combating illicit trafficking in Nuclear and other Radioactive Material. IAEA nuclear security series no. 6 technical guidance, http://www-pub.iaea.org/MTCD/publications/PDF/pub1309_web.pdf

IAEA (2014). Incidents of nuclear and other radioactive material out of regulatory control 2014 Fact Sheet, https://www.iaea.org/sites/default/files/infcirc274r1_sp.pdf

INTERPOL (2014). La lucha contra el tráfico ilícito de bienes. Guía para responsables politicos, http://www.interpol.int/es/Criminalidad/Tr%C3%A1fico-de-productos-il%C3%ADcitos/Asistencia-jur%C3%ADdica/Publicaciones-jur%C3%ADdicas

Lothar, K. (2003). Anáilisis forense nuclear y tráfico ilícito, Boletín OIEA nº 45/1, https://www.iaea.org/sites/default/files/45102592123_es.pdf

ONU (2005), "Convenio internacional para la represión de los actos de terrorismo nuclear, 2005 (Convenio sobre el terrorismo nuclear), consultado el 2 de noviembre de 2015, https://treaties.un.org/doc/db/Terrorism/spanish-18-15.pdf

ONU (2004), "Resolución del Consejo de Seguridad S/RES/1540(2004)", 28 de abril de 2004, consultado el 2 de noviembre de 2015 http://www.un.org/es/comun/docs/?symbol=S/RES/1540%20(2004)

ONU (1968), "Tratado de no-proliferación de armas nucleares", consultado el 2 de noviembre de 2015, https://www.iaea.org/sites/default/files/10403500308_es.pdf

Ortega García, J. (2013). Medidas de defensa en España frente al terrorismo nuclear, Documento Marco 5/2013, Instituto Español de Estudios Estratégicos, http://www.ieee.es/documentos/areas-tematicas/retos-y-amenazas/2013/DIEEEM05-2013.html

Secretaría de Estado de Nergía (2015). Energía nuclear. Transporte", http://www.minetur.gob.es/energia/nuclear/Transportes/Paginas/transporte.aspx

Secretaría de Estado de Nergía (2015). Vigilancia Radiológica en el reciclado de materiales metálicos, http://www.minetur.gob.es/energia/nuclear/vigilancia/paginas/vigilancia.aspx

Soteras, F. y Pita R. (2009). Posibilidad real de materialización de la amenaza NRBQ por grupos terroristas en España", ARI 35/2009, Real Instituto Elcano, febrero 2009.

Zaitseva, L. y Hand, K (2003). Nuclear Smuggling Chains Suppliers, Intermediaries, and End-Users, American Behavioral Scientist, Vol. 46 No. 6, February 2003 pp. 822-844.

Zaitseva, L. (2010). Nuclear Trafficking: 20 Years in Review, American Behavioral Scientist, Contribution to WFS Meeting, Erice, August 2010.

Fecha de recepción: 07/06/2018. Fecha de aceptación: 25/06/2018

COMPETENCIA EN COMPORTAMIENTO NO VERBAL EN LA DETECCIÓN DE AMENAZAS

JOSÉ MANUEL PETISCO RODRÍGUEZ

CTE. JEFE DE ÁREA DOCENTE DE LA ESCUELA MILITAR DE CIENCIAS DE LA EDUCACIÓN (EMCE).LICENCIADO EN PSICOLOGÍA. ACADEMIA CENTRAL DE LA DEFENSA

RESUMEN

En las últimas décadas los gobiernos de muchos países, con el fin de proteger a sus ciudadanos, han invertido cantidades ingentes de dinero en tecnologías para la detección temprana de amenazas (sistemas de videovigilancia, sistemas de seguimiento satelital, sistemas E-Warning, etc.). Sin embargo, son pocos los que han puesto en marcha programas de entrenamiento para mejorar las habilidades del personal de primera línea para reconocer amenazas reales que atenten contra la seguridad. El reconocimiento de una potencial amenaza para un agente de las Fuerzas y Cuerpos de Seguridad, para un combatiente que vela por la seguridad de un destacamento en una misión internacional, o que lleva a cabo actividades de control de fronteras, o de vigilancia urbana, o para cualquier funcionario que desarrolla labores en aduanas y, en general, para cualquier funcionario encargado de hacer cumplir la ley puede ser vital para salvar su vida y las de los demás. En este artículo se analizan distintos motivos por los que mejorar las habilidades de dichos actores, en la lectura e interpretación del comportamiento no verbal, puede redundar en una seguridad personal y colectiva más eficaz.

Palabras clave: Detección de amenazas, comportamiento no verbal, seguridad, ceguera atencional, ceguera por cambio.

ABSTRACT

In recent decades, the governments of many countries have invested enormous amounts of money in technologies for early threat detection (video surveillance systems, satellite tracking systems, E-Warning systems, etc.) in order to protect their citizens. However, few have launched training programs to improve the skills of front-line personnel to recognize real threats put security at risk. Detection of a potential threat is crucial for an agent of the Security Forces and Bodies, for personnel responsible for security of military compounds in operations, border security, street patrol, customs control and for any law enforcement officials, as this could save their lives and the lives of others. This article analyzes different reasons why improving the skills of these actors in reading and interpreting nonverbal behavior can result in more effective personal and collective security

Keywords: Threat recognition, non-verbal behavior, security, attentional blindness, change blindness.

1. INTRODUCCIÓN

Tener formación en comportamiento no verbal cada día está siendo más valorado y demandado en ámbitos profesionales tan dispares como la educación, la política, la inteligencia, el protocolo, la investigación policial, los procesos de mediación o la negociación. Sin embargo, en el ámbito de la seguridad se sigue demandando invertir en tecnologías como escáneres, equipos de video-vigilancia, controladores de presencia y un largo etcétera. En los sectores de defensa y de seguridad (pública o privada), muchas de las soluciones propuestas e implementadas, también se han centrado en la tecnología, olvidando quizás que el mejor sistema de reconocimiento de patrones de conducta y detección de amenazas reside en el propio cerebro humano.

En el caso del Ministerio del Interior, en el año 2016 llevó a cabo una importante inversión para coordinar, desarrollar e implantar bases de datos, sistemas de información y sistemas de comunicaciones de utilización conjunta o compartida por las Fuerzas de Seguridad del Estado, creando el Centro Tecnológico de Seguridad (CETSE). O si nos centramos en las mejoras en equipación, recientemente la Guardia Civil ha incorporado más de 900 vehículos y más de 6.000 chalecos antibala de última generación[1].

En el caso de Defensa, el Área de Planificación de la Dirección General de Armamento y Material (DGAM) desempeña una importante labor en la planificación y desarrollo de las mejores tecnologías para dotar al soldado del futuro. Pero la Estrategia Española de Seguridad de 2011 ya consideró los ciberataques como una amenaza real y en crecimiento. Por ello, en 2013 se creó el Mando Conjunto de Ciberdefensa y desde entonces las inversiones en proyectos de nuevas tecnologías de Ciberdefensa han ido en aumento. En la actualidad el ciberespacio ha pasado a ser una parte fundamental para garantizar el bienestar de los ciudadanos y la Seguridad Nacional.

Toda inversión que redunde en la seguridad de los ciudadanos, o del profesional de seguridad[2], bienvenida sea; pero no deberíamos dejar de lado la formación y en ella incluir la capacitación, de quienes velan por la seguridad de los demás, para reconocer potenciales amenazas.

2. LAS TAREAS DE VIGILANCIA Y LA LIMITACIÓN DE NUESTROS RECURSOS ATENCIONALES

Todo personal que vaya a desempeñar tareas de vigilancia y seguridad debería establecer una línea base de la actividad normal de su entorno de actuación. Sería conveniente que observaran cómo actúan normalmente las personas que circundan esos lugares, cómo actúan cuando se acercan a ellos, cómo caminan, qué distancias mantienen, qué hacen con sus manos, si les miran o rehúyen la mirada, etc. Esta línea base resultará de suma utilidad a la hora de detectar posibles amenazas, ya que a partir de ella podrán determinar si hay algo agregado o eliminado; en definitiva, si hay alguna anomalía respecto de la “normalidad”.

1 Nota de prensa del Ministerio del Interior de fecha 23/02/2018. Disponible en http://www.interior.gob.es/prensa/noticias/-/asset_publisher/GHU8Ap6ztgsg/content/id/8407410

2 Entiéndase en sentido genérico y en adelante también aplicable a equipos de patrulla, combatientes que realizan tareas en checkpoints, soldados de combate, agentes de policía, guardia civil, etc.

Se debe observar el entorno buscando cualquier tipo de cambio y darle sentido en el contexto de la situación concreta. Pero ocurre que, aunque el ser humano tiene un campo de visión de 180 grados, solo un pequeño porcentaje de ese campo proporciona visión de alta calidad. Según cita Hallinan (2009), solo se obtiene visión de alta resolución en un ángulo de dos grados. Ello condiciona que perdamos los detalles que se producen fuera de dicha zona de visión, ya que la atención que se presta a un área de enfoque disminuye la capacidad de enfocar otra área (Chabris y Simons, 2010, págs. 37-38). Pero además, en una situación altamente estresante, cuando alguien se ve envuelto en una situación potencialmente letal, su visión puede verse afectada por algún tipo de distorsión visual.

En tareas de vigilancia de alto riesgo, donde peligra nuestra integridad física, cuando el corazón late desbocado, normalmente se pierde la visión periférica (aparece la visión de túnel), se ve afectada la profundidad de visión y se produce una pérdida de la visión de cerca (Grossman y Christensen, 2014, pág. 95). Todo ello se traduce en más problemas para detectar y reaccionar eficazmente ante la amenaza y que una amenaza real (como por ejemplo un hombre con un cuchillo) parezca estar más cerca de lo que está realmente.

Sin embargo, saber de la existencia de esta "visión de túnel", puede suponer una ventaja para un combatiente o un componente de las fuerzas de seguridad, ya que es probable que al adversario le esté ocurriendo lo mismo. En tales situaciones, moverse rápido a la izquierda o a la derecha, hará que el combatiente o agente desaparezca del campo de visión del adversario y que se vea obligado a perder un precioso tiempo para parpadear, echarse hacia atrás y volverle a buscar a través de su "tubo visual". Esa pequeña ventaja puede salvar su vida.

Pero además de los problemas de reducción del campo de visión, la búsqueda de cualquier tipo de cambio se puede ver complicada con la existencia de dos tipos de ceguera involuntaria: la ceguera por falta de atención y la ceguera por cambio.

En 1999 Christopher Chabris y Daniel Simons publicaron su famoso experimento, donde a una serie de sujetos se les muestra un breve vídeo de dos equipos de baloncesto pasándose la pelota unos a otros, uno con camisetas blancas y otro con camisetas negras[3]. A dichos sujetos se les pide una tarea tan simple como que cuenten el número de veces que se pasan la pelota los jugadores del equipo blanco. Pero hacia la mitad del vídeo, una mujer disfrazada de gorila camina lentamente hacia el centro de la pantalla, golpea su pecho y luego abandona la escena. Si uno solo está viendo el vídeo, detectar este cambio es lo más sencillo del mundo. Pero cuando a los sujetos se les pide que cuenten el número de pases que se llevan a cabo entre los jugadores del equipo blanco, para la mitad de ellos, la escena del gorila pasa desapercibida. Ocurre que, cuando el sujeto dirige su foco de atención a los pases de baloncesto, deja en la oscuridad el resto de detalles. Incluso muchos de los sujetos para los que pasaba desapercibida la escena del gorila, aunque miraran directamente al gorila, con frecuencia no lo veían porque no era lo que estaban buscando. En esencia, este estudio revela que cada vez que fijamos la atención en un aspecto de nuestro entorno solemos desatender otros detalles evidentes de dicho entorno. Y esto es lo que se conoce como "ceguera atencional".

3 El video original puede consultarse en CHABRIS, C. y SIMONS, D., "Selective Attention Test, form Simons y Chabris (1999)": https://www.youtube.com/watch?v=vJG698U2Mvo

Ver consume muchos más recursos que mirar o contemplar y lo que vemos está mediatizado, en gran medida, por lo que esperamos ver o por lo que estamos buscando. Los seres humanos no vemos lo que no estamos buscando con la mirada. En 2010, en otro famoso experimento[4], Daniel Simons planteaba que si somos conocedores, a priori, de las escenas del vídeo sobre atención selectiva (Simons y Chabris, 1999), o alguien nos ha informado de lo que ocurre en dichas imágenes, es muy probable que estemos pendientes de buscar al gorila y que dicha búsqueda nos distraiga del control de otros cambios o detalles. Es decir, cuando tenemos información a priori de lo que va a pasar la búsqueda de ese elemento puede cegarnos para ver otros cambios relevantes, como el número de pases que suceden entre los jugadores de camiseta blanca, el que haya desaparecido un jugador de la escena o que se haya cambiado el fondo del decorado. Hablaríamos entonces de "ceguera al cambio".

Hallinan (2009) habla de "ceguera al cambio" para referirse al fallo para detectar cambios en una escena (desaparición de un jugador), después de una interrupción breve del campo visual (aparición del gorila). Es por ello que si se produce un pequeño cambio en la escena, aunque sea crucial, este pase desapercibido.

Este y otros estudios demuestran que no existe garantía de que percibamos el mundo con precisión y que, prestar atención a un evento concreto, reduce nuestra capacidad para prestar atención a otras actividades. Por tanto, el problema radicará en cómo dirigir nuestros recursos atencionales hacia donde obtengamos la ganancia más útil (Chabris y Simons, 2010, pág. 39). Tanto la ceguera por falta de atención como la ceguera al cambio, suponen un riesgo para quienes realizan tareas de vigilancia. Ambas están relacionadas con no ver lo que tienen delante, ya sea por estar centrados en otra actividad, por exceso de confianza, por rutina o por disponer de información previa respecto a la previsión de que ocurra un determinado evento.

Por muy tranquilo que parezca estar el entorno y por muy controlada que se crea tener la situación, siempre habrá que estar alerta. Pero la capacidad de estar alerta ante lo inesperado disminuye. Si alguien que realiza tareas de vigilancia está buscando algo y no lo encuentra, su nivel de alerta irá descendiendo y acabará dándose por vencido. Su umbral de abandono estará en parte relacionado con su índice de éxito en encontrar algo en otras ocasiones anteriores.

Ya que nuestros recursos atencionales son limitados y todas las personas emitimos continuamente mensajes a través de los distintos canales no verbales (gestos, posturas, expresión facial, oculésica, háptica, paralenguaje, apariencia), habrá que tener en cuenta que no todos los canales resultarán igualmente relevantes para una situación concreta. Un observador entrenado debe saber centrarse en los comportamientos importantes y eliminar los intrascendentes. La detección de cambios es fundamental para detectar una amenaza y la cantidad de información que nos llega por las distintas vías puede ser enorme. Pero para aquellas personas que posean formación y experiencia en el análisis del comportamiento no verbal, la elección de los mensajes verdaderamente relevantes será más clara que para aquellas personas que carezcan de dicha formación y experiencia. Podríamos afirmar que la "ceguera involuntaria", es decir, la capacidad de mirar algo directamente y no verlo (Hallinan, 2009), sería mayor en los casos de individuos no formados ni entrenados.

4 "The Monkey Business Illusion, Daniel J. Simons (2010)": https://www.youtube.com/watch?v=IGQmdoK_ZfY

3. VIGILANCIA EN AEROPUERTOS: BIOMETRÍA VERSUS OBSERVACIÓN MINUCIOSA DEL ROSTRO

La biometría es una tecnología empleada para la identificación de la persona, que se basa en características físicas intransferibles, como la huella digital, patrones de voz, patrones faciales o el escaneo de retina. En los últimos años diversos países, como Estados Unidos, Australia o Brasil, han llevado a cabo importantes inversiones para implantar tecnologías en los aeropuertos internacionales, que les permitan mejorar la seguridad a través de software para la identificación de rostros en tiempo real.

Dichos sistemas, no intrusivos, se basan en las imágenes captadas por cámaras de seguridad de alta definición que cotejan rápidamente con bases de datos de fotografías de individuos sospechosos o en búsqueda y captura (Figura 1). Además, dichos sistemas podrían emplearse para mejorar la eficiencia de los procesos de aduanas y acelerar el paso de los pasajeros por los aeropuertos, al no tener que mostrar ningún tipo de tarjeta de embarque o pasaporte.

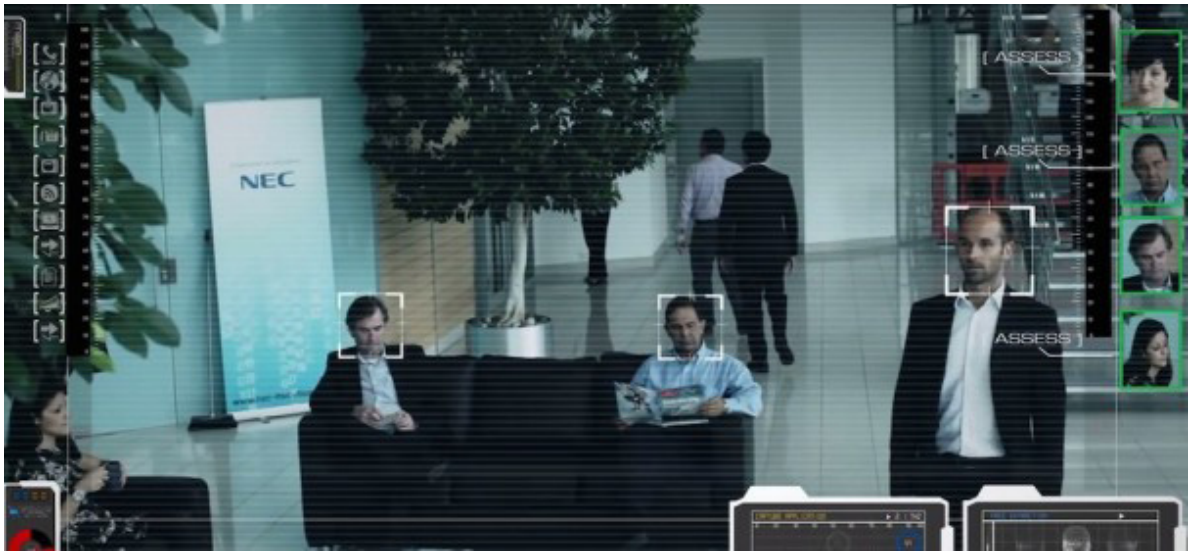

Figura 1. Tecnologías de reconocimiento facial empleadas en muchos aeropuertos internacionales[5].

Pero disponer de este tipo de tecnologías no está al alcance de todos y ocurre que tampoco es un sistema totalmente fiable. Pensemos en los casos en los que la variabilidad entre individuos sea muy pequeña, como sucede con algunos familiares (sobre todo gemelos), o en el caso de sujetos con rasgos similares. Otro inconveniente sería la variabilidad entre distintas imágenes de un mismo individuo, al ser tomadas en diferentes condiciones de iluminación o posición (las condiciones ambientales de luces y sombras de cualquier habitáculo cambian a lo largo del día). Además, en entornos donde hay mucho trasiego de gente se pueden producir ocultaciones de unas personas sobre otras. Y a ello, habría que añadir la dificultad para disponer de una base de datos de caras actualizada y donde todas las imágenes de referencia (base de datos de caras) deberían haber sido adquiridas en condiciones equivalentes para todos los individuos. Por no hablar de la robustez que tendrán estos sistemas frente a determinados ataques fraudulentos.

5 Fuente: http://www.digitalsecuritymagazine.com/2015/07/30/aeropuertos-internacionales-de-brasil-implantan-la-tecnologia-de-reconocimiento-facial-de-nec/

Por todo ello, dichos sistemas claramente podrán complementar, pero nunca sustituir, la inestimable labor de los agentes de seguridad de dichos aeropuertos. Por tanto, parece que sigue siendo evidente la necesidad de formación de dichos agentes en temas vinculados a la detección temprana de amenazas. Y, en ese sentido, conocer las posibilidades de información que puede expresar el rostro humano parece fundamental.

3.1. LA COMPLEJIDAD DE LA EXPRESIÓN FACIAL HUMANA

Para empezar, la expresión facial nos puede aportar información de cuatro tipos diferentes (Fernández-Abascal y Chóliz Montañés, 2001):

- *Signos estáticos*, que contribuyen a la apariencia de un individuo y representan los rasgos relativamente permanentes de la cara (como su estructura ósea y la masa de los tejidos).
- *Signos lentos*, ya que ocurren gradualmente con el paso del tiempo y que representan cambios en la apariencia de la cara (como arrugas y cambios en la textura de la piel).
- *Signos artificiales,* que pueden modificar, disimular o distorsionar los signos anteriores (como el empleo de cosméticos, botox y lentes oculares).
- *Signos rápidos,* que se traducen en cambios visibles en la expresión facial.

Está claro que los cuatro tipos de signos contribuyen al reconocimiento facial humano, pero ¿qué comunican los signos faciales rápidos? Pues bien, a este respecto sigue habiendo una enorme controversia sobre si los movimientos faciales expresan emociones o comunican motivos.

En este sentido, podríamos afirmar que existen dos perspectivas diferentes sobre la vinculación del rostro humano y la emoción: una que podemos denominar “clásica” y otra “ecológico-conductual”. Según la perspectiva clásica, representada por autores como Ekman, Izard o Matsumoto, las expresiones faciales tienen una base innata, son fijas y establecen una relación necesaria y suficiente con las emociones. Sin embargo, la perspectiva ecológico-conductual, representada por autores como Fridlund, Russell o Fernández-Dols, mantiene que las expresiones son pautas fijas de acción que no denotan emociones, sino que sirven para establecer comunicación e interacción social. Fridlund asume que existe cierta asociación entre rostro y emoción, pero plantea el interrogante de cuál es la naturaleza de esa asociación y qué papel representa la cultura en dicha asociación. Para él las conductas faciales de exhibición pueden ser entendidas sin recurrir a la emoción y los rostros pueden expresar *motivos* y *contextos* en lugar de emociones. Así plantea que la expresión de ira de un sujeto sirve de advertencia para que quienes le rodean den marcha atrás en caso de ataque (disposición a atacar), independientemente de cuál sea la emoción que estuviese experimentando ese sujeto (Fridlund, 1994). En cambio la sonrisa iría más encaminada al apaciguamiento, a jugar o a afiliarse; la tristeza a la búsqueda de ayuda (petición de socorro); la expresión de temor como disposición a ceder, a rendirse; y la expresión de menosprecio como declaración de superioridad. En definitiva, plantea que “las conductas faciales de exhibición emocional son manifestaciones de la intencionalidad social” (Fridlund, 1994, pág. 212). Para la Ecología de la conducta, los rostros exhiben motivaciones sociales, que únicamente son comprensibles para el *contexto* en el que surge la motivación.

Parkinson (2005) plantea que aunque muchos movimientos faciales connotan emociones involuntarias o automáticas, ello no implica que los movimientos faciales sean dependientes por completo de la emoción y nada más. Y las últimas investigaciones al respecto parecen indicar que ni siquiera sea la emoción el referente para explicarlos. En este sentido, Fridlund y Gilbert (1985) afirman que el principal papel de las exhibiciones faciales no es emocional, sino *paralingüístico*, acompañando, complementando y suplementando al lenguaje. En definitiva es importante tener en cuenta que no todas las expresiones faciales (signos rápidos) muestran emociones, también muestran señales de comunicación, ilustradores, actos manipuladores y emblemas. Fridlund (1994) menciona que de unas 6.000 conductas tabuladas por Ekman y Friesen de grabaciones de 30 entrevistas psiquiátricas de 10 minutos, solo pudieron clasificar movimientos faciales como "expresiones de la emoción" en menos de 1/3 (pág. 331). También cita un estudio de Chovil, quien indicó que dicha tasa se reduce a un 18% de las expresiones faciales.

Por tanto, el rostro es una de las zonas de nuestro cuerpo con mayor potencial comunicativo (Petisco, 2014, pág. 98), pero siguiendo la evidencia convergente de las investigaciones llevadas a cabo en la última década, parece razonable afirmar que las expresiones faciales no pueden definirse como señales nítidas y "verdaderas" de una emoción (Fernández-Dols y Crivelli, 2013). Para Fernández-Dols y Crivelli un solo episodio emocional puede incluir movimientos faciales simultáneos o sucesivos vinculados a reacciones afectivas, valoraciones, motivos sociales o estrategias de regulación, pero también a procesos cognitivos o convenciones culturales. Ello complica enormemente su "lectura", máxime cuando el rostro puede ser la parte más engañosa del cuerpo, ya que podemos controlar a voluntad la mayoría de los músculos que controlan la expresión facial.

Entonces, si la mayoría de los movimientos faciales que llevamos a cabo están más vinculados a la comunicación que a la expresión de emociones ¿qué utilidad pueden tener en al ámbito de la seguridad las tecnologías de reconocimiento de emociones?

Las inversiones en software de reconocimiento de emociones a través de la expresión facial han ido proliferando en los últimos años, dando como resultado sistemas muy similares con denominaciones distintas (Facet, Avatar, FaceSense, FaceReader, Affectiva, Automatic Face Recognition, etc). Casi todos ellos se basan en los trabajos de Ekman y Friesen (1978), que dieron como resultado la creación de un riguroso sistema de codificación facial denominado FACS (Facial Action Coding System); pero la mayoría de estos sistemas lo que facilitan es exclusivamente información referida a las seis o siete -denominadas por los defensores del modelo clásico- emociones básicas o primarias (alegría, ira, tristeza, asco, sorpresa, miedo y desprecio).

Algunas de estas tecnologías, como AVATAR[6] (Figura 2), son más complejas y utilizan diversos indicadores, como los cambios en los ojos, la voz, los gestos y la postura, para detectar un riesgo potencial. No obstante, dicha tecnología podrá ofrecer cierta utilidad a modo de filtro inicial, ya que los casos significativos seguirán requiriendo la inestimable labor de los agentes de seguridad.

6 El proyecto AVATAR (Automated Virtual Agent for Truth Assessments in Real Time) ha comenzado a ser probado en 2017 por la Agencia de Servicios Fronterizos de Canadá.

Figura 2. El Proyecto AVATAR tiene como objetivo identificar viajeros con malas intenciones y determinar su riesgo potencial.

Otras de esas tecnologías, como la diseñada por Emotient, toman como base las famosas *microexpresiones* para, según afirman, descubrir los sentimientos más profundos de la gente. En palabras de Mariam Bartlett, cofundadora y científica principal de Emotient, el software de la compañía llamado *Facet* puede rastrear las fortalezas de la emoción a lo largo del tiempo, e incluso capturar microexpresiones, llegando a afirmar que "incluso cuando alguien quiere mantener una cara neutral, se obtienen microexpresiones"[7]. Sin embargo, como citan Durán, Reisenzein y Fernández-Dols (2017), los escasos estudios empíricos que se han publicado hasta la fecha sobre microexpresiones, sugieren que, de producirse, lo hacen de manera muy escasa: 18 de 1.711 expresiones mostradas por sujetos a los que se les presentó algún estímulo *elicitador* de emociones (Porter, ten Brinke, y Wallace, 2012), o 109 entre más de 1.000 expresiones faciales provocadas (Yan, Wu, Chen, Liang, y Fu, 2013) fueron clasificadas como microexpresiones.

Por tanto, el *profesional de seguridad* sigue siendo importante en este proceso y cuanta mejor preparación tenga en todos los ámbitos de la seguridad, más eficientemente podrá realizar su trabajo.

Si el uso de la tecnología no es un medio suficiente y su precisión se pone en entredicho, ¿por qué no potenciar la capacitación de quienes velan por nuestra seguridad? Centrémonos, por tanto, en la observación minuciosa del rostro, ya que puede llegar a aportar algunos indicadores de utilidad para la detección de amenazas. En este sentido, los cambios que provoca el Sistema Nervioso Autónomo son difíciles de ocultar y así ocurre con el rubor y el *empalidecimiento* (Petisco, en prensa). Ekman mantiene que el rubor es un signo de turbación o de embarazo, que también puede aparecer cuando hay vergüenza, culpa o ira. Si la cara enrojece de ira, es porque la ira ha quedado fuera de control o porque el sujeto trata de ocultar una rabia a punto de explotar (Ekman, 2009, pág. 148). La expresión de lo que comúnmente denominamos *ira*, unida al enrojecimiento de la piel, podrían ser precursores de una inminente agresión

7 Fuente: https://www.livescience.com/42975-facial-recognition-tech-reads-emotions.html

física, lo que para la Ecología de la conducta sería interpretado como "disposición a atacar" (intención social). Por su parte, el *empalidecimiento* aparecería más en situaciones de *ira controlada*, sirviendo a motivos sociales de "apaciguamiento" o vinculada a ciertas actitudes para "guardar las apariencias". Pero el *empalidecimiento* también puede acompañar a un rostro que muestra *temor* y, en este caso, la lectura sería más de "disposición a ceder, o rendirse".

Por tanto, siguiendo el modelo de la Ecología de la conducta, la observación minuciosa del rostro humano podría proporcionarnos ciertos indicadores de las intenciones de una persona y prever los movimientos o reacciones amenazantes ante una situación específica.

Otro canal de información importante, que atañe al rostro, es la acción ocular. A través de la mirada, en conjunción con otros canales no verbales, se pueden comunicar actitudes interpersonales, sentimientos, muestras de interés, atención, excitación, características de la personalidad y un largo etcétera. Además, en determinadas ocasiones, la *oculésica* puede ser el único canal no verbal visible del rostro; pensemos en vestimentas que cubren el rostro casi por completo, como el pasamontañas o el turbante de los tuareg (casos más extremos serían el burka o el niqab).

La *dirección de la mirada* suele mantenerse baja cuando sentimos tristeza, vergüenza o culpa y se suele mirar a lo lejos (mirada perdida) en situaciones de rechazo. No obstante, resulta sencillo controlar voluntariamente la dirección de la mirada y ello ha podido dar lugar a crear ciertos estereotipos erróneos de validez universal. Así la creencia popular de que el mentiroso aparta la mirada, que también han difundido algunas publicaciones (por ej. Lieberman, 1998), es totalmente falsa (Masip, 2005). También es falsa, por muy difundida que esté, la afirmación de los defensores de la PNL que relacionan mirar a la izquierda o a la derecha con decir la verdad o mentir (Mann, y otros, 2012). No existe ningún patrón de movimiento ocular asociado al engaño (Wiseman, y otros, 2012).

Por su parte, el *parpadeo* puede ser voluntario, pero de manera involuntaria puede aumentar su frecuencia cuando el sujeto se siente nervioso. La frecuencia normal de parpadeo de una persona es de unos 15-20 parpadeos por minuto o, lo que es lo mismo, un parpadeo cada 3-4 segundos. La velocidad de parpadeo es un parámetro biométrico observable que puede indicarnos actividad normal, pero también la presencia de nerviosismo, estrés o ansiedad. Así, cuando un sujeto parpadea rápidamente puede ser un indicador de que siente algún tipo de amenaza. Si el parpadeo vuelve a su frecuencia normal, podríamos inferir que la amenaza percibida, o la situación incómoda, ha pasado para el sujeto. Pero además, por los estudios de Andreassi (1973), o de Bauer y otros (1985), sabemos que los parpadeos responden a las demandas cognitivas, en el sentido de que se inhiben bajo altas demandas cognitivas y aumentan cuando las demandas son bajas. Pero solo nos percataremos de ello mediante una minuciosa observación.

De menor utilidad puede resultar la *dilatación pupilar,* ya que normalmente pasará desapercibida. Hoy sabemos que el tamaño de las pupilas se modifica con los cambios de luz, el estrés, el ejercicio, la exposición al calor o al frío, los bajos niveles de glucosa en sangre y con otros retos medioambientales. Pero los estudios iniciales de Hess y Polt mostraron la existencia de un vínculo entre excitación emocional y dilatación pupilar (Hess y Polt, 1960), así como entre dilatación pupilar y esfuerzo cognitivo

(1964). Con posterioridad son muchos los trabajos que han puesto de manifiesto la vinculación entre la dilatación pupilar y la carga cognitiva durante el desempeño de una amplia variedad de actividades mentales, como el recuerdo y transformación de cadenas de dígitos, la multiplicación mental, la memorización de palabras, el procesamiento de letras, etc.

4. LA DISTANCIA A MANTENER ES IMPORTANTE

Otra importante fuente de información es la interpretación de la distancia espacial que alguien mantiene al interactuar con los demás. El antropólogo Edward T. Hall (1976) acuñó el término de proxemia (o proxémica) para referirse al "estudio de la percepción y el uso del espacio por parte de la humanidad". Dicho autor desarrolló, en su obra "The Silent Lenguage" (1959), su teoría sobre las distancias que utilizan las personas mientras interactúan entre sí, describiendo cuatro niveles diferentes de espacio: espacio íntimo, espacio personal, espacio social y espacio público (Figura 3).

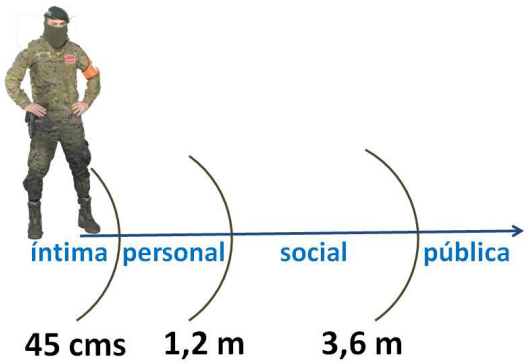

Figura 3. Diagrama de las distancias proxémicas según Edward Hall.

Su estudio fue llevado a cabo con población americana de clase media, por lo que es importante mencionar que el propio Hall reconoció que diferentes culturas mantienen estándares diferentes de espacio interpersonal. Hoy sabemos que las culturas latinas y árabes se sienten cómodas estando cerca unos de otros y que estas distancias relativas, propuestas por Hall, se reducen. En cambio, las culturas nórdicas y los anglosajones prefieren mantener mayores distancias con los demás.

También descubrió que las personas que tienden a ocupar mayor espacio suelen ser personas seguras de sí mismas y que, por lo general, a mayor posición socioeconómica y jerárquica, más espacio exigimos. Pero, independientemente de su tamaño, todos nos sentimos celosos de nuestro espacio personal y no nos agrada que un desconocido lo invada (y menos aún si se trata de nuestro espacio íntimo). De hecho, cuando un desconocido invade nuestro espacio personal, se activa nuestro sistema límbico, experimentando una reacción emocional negativa (tensión) intensa e inmediata: nos ponemos en alerta, nuestro pulso se acelera y nos enardecemos (Knapp y Hall, 2002).

En ese uso del espacio, los seres humanos (al igual que otros animales) cuando se sienten amenazados, o en una situación de confrontación, cuando tratan de intimidar

a otro, llevan a cabo exhibiciones territoriales. De esta forma tratan de establecer el control y dominio de la situación (Figura 4).

Figura 4. Vladimir Putin y Donald Trump durante la reciente cumbre del G-20.

Para el *profesional de seguridad* el espacio personal es crítico, ya que dentro de los parámetros de un potencial agresor es la distancia óptima para iniciar una agresión: no invade la distancia íntima (alertándole) y a la vez está a la distancia prácticamente de su brazo para llegar al contacto. Además, es la distancia que habitualmente se mantiene cuando se conversa con un desconocido, por lo que será muy difícil reaccionar a tiempo ante la acción violenta de un agresor, máxime si va armado. Por ello, en los casos en los que se detecte un potencial agresor, aparentemente no armado, la distancia de seguridad debe oscilar entre los 3 y 5 metros; y es a esa distancia a la que convendría observar cualquier tipo de detalle para contrarrestar una posible agresión. Detectar detalles como bultos debajo de la ropa, movimientos para estirarse el jersey, ladearse para ocultar dicho bulto, o el gesto de separar el pulgar para empuñar un arma, pueden resultar vitales para reaccionar a tiempo.

5. EL CUERPO NO PARA DE HABLAR

La expresión corporal puede darnos información relacionada con las actitudes, intenciones y motivaciones de un sujeto. Bajo este epígrafe incluimos tanto posturas y gestos, como orientación y movimientos corporales.

La investigación sobre comportamiento no verbal se ha descuidado bastante, en cuanto al estudio de la postura y el gesto, en comparación con áreas como la expresión facial o la proxemia (Petisco y Sánchez, 2016). Postura y gesto están íntimamente relacionados, ya que pueden implicar a las mismas partes del cuerpo. No obstante, se suele referir a la postura como posición estática, puesto que una postura dotada de movimiento sería tratada como gesto.

Aunque la lectura del comportamiento no verbal no debe buscarse en los componentes aislados, sino en la información combinada que nos llega por los diferentes canales, vamos a desglosar la expresión corporal en sus distintos componentes.

5.1. LA POSTURA CORPORAL ADOPTADA

A través de las posturas corporales podemos obtener información sobre la *actitud* del sujeto hacia una posible interacción y también información sobre su *estatus* o *poder*. Así, posturas con brazos relajados, orientación frontal, pies dirigidos hacia nosotros y contacto ocular directo, serían indicadores de una actitud abierta hacia una interacción; posturas con los brazos cerrados, cuerpo ladeado y mirada huidiza serían indicadores de una actitud de cierre o rechazo; posturas expansivas (tratando de ocupar mayor espacio), posturas arrogantes (barbilla hacia arriba) y posturas orgullosas (pecho hinchado, espalda hacia atrás), podrían darnos información sobre la actitud, poder y estatus de esa persona.

Mehrabian (1968) agrupó en cuatro categorías las distintas posturas que puede mantener un individuo: *posturas de acercamiento* (inclinación del cuerpo hacia adelante), que denotan atención o interés; *posturas de retirada* (retroceso o vuelta hacia otro lado), que denotan rechazo o repulsa; *posturas de expansión* (expansión del pecho con tronco recto o hacia atrás y cabeza erecta), que denotarían arrogancia, orgullo, altivez o desprecio; y *posturas de contracción* (tronco hacia adelante con cabeza y pecho hundidos, hombros abatidos), que denotarían abatimiento, desgana o tristeza.

Para el *profesional de seguridad* es importante la lectura postural adoptada por la persona con la que interactúa, no obstante, los indicadores y categorías posturales citadas dependerán principalmente del contexto en el que se producen, mediando otras variables como sexo, edad, raza o cultura (Petisco & Sánchez, 2016, pág. 69).

El combatiente que permanece en un checkpoint o en un control de accesos, o el agente de policía, para dar muestras de autoridad, confianza y control, puede adoptar una postura con los pies separados y las manos en las caderas o en el cinturón que porta su arma. Ocupando más espacio muestra cierta actitud agresiva, pero también transmite un mensaje claro de que está listo para entrar en acción a alguien que se dirija hacia él (Figura 5).

Figura 5. Al llevarse las manos a las caderas este soldado ocupa mayor espacio y se hace más visible. La separación de sus piernas le da mayor estabilidad y seguridad.

En el caso de un sujeto que interactúa con un *profesional de seguridad*, llevarse las manos a las caderas, puede ser una muestra de seguridad, de enfado o de miedo. Los gatos y perros erizan su pelo y las aves hinchan sus plumas, cuando se sienten amenazados, para parecer más grandes; pero el ser humano no tiene nada que erizar. Quizás por ello, el ser humano se ha inventado un gesto que contribuye a conseguir parecer de mayor tamaño: el gesto de llevarse las manos a las caderas (Pease y Pease, 2006, pág. 256).

5.2. LA ORIENTACIÓN DEL CUERPO

La orientación corporal puede aportarnos información sobre las relaciones entre dos personas, ya sean de colaboración, amistad o jerarquía (Ricci y Cortesi, 1980). Cuando la relación es de jerarquía, el sujeto superior se suele situar enfrente del sujeto de inferior rango o estatus. En cambio, cuando la relación es de colaboración o amistad íntima, los sujetos suelen adoptar una orientación lateral (lado con lado). No obstante, si observamos a dos personas hablando cara a cara, ello puede ser indicador de intimidad o de no querer que se les interrumpa en una conversación.

El adoptar una orientación frontal o lateral, también está condicionado por la cultura a la que se pertenece. Los árabes suelen adoptar una orientación de frente para mantener una conversación y, según algunos autores (Ingham, 1971), los suecos tienden a evitar posicionarse con ángulos de noventa grados.

Mehrabian (1971), puso de manifiesto la relación entre la orientación del cuerpo en una interacción y las actitudes o estatus de los sujetos. Afirma que, en el caso de las mujeres que están sentadas, cuanto más directa es la orientación del cuerpo hacia un individuo, más positiva es su actitud hacia él (no teniendo trascendencia este hecho en el caso de seres muy queridos).

En un checkpoint, en un control de acceso, o en una aduana, la orientación corporal de la persona con la que se interactúa puede dar pistas al *profesional de seguridad* sobre la conveniencia o no de pasar a una revisión más exhaustiva. Si mientras se mantiene la conversación, los pies de la persona en cuestión están apuntando hacia otro lugar dicho profesional podría tener un indicador de que esa persona preferiría estar en otra parte; desearía abandonar ese lugar; aunque el torso orientado hacia quien le plantea las preguntas intente ocultar ese deseo.

5.3. MOVIMIENTOS CORPORALES

Otra aportación importante de Mehrabian (1971), con aplicación a la detección de amenazas, fue el principio que estableció según el cual “la gente se siente atraída hacia las personas y cosas que les gustan, evalúan altamente y prefieren, y evitan o se alejan de las cosas que no les gustan, evalúan negativamente o no prefieren”. Dicho de otra manera, los seres humanos suelen alejarse de las situaciones o personas que les desagradan, o perciben como amenazantes, y se vuelven hacia las personas con las que están de acuerdo, o les resultan agradables. La respuesta humana más normal, cuando perciben a otra persona como amenazante o desagradable, será la de crear distancia física. Pero si no es posible alejarse, usarán el torso y la parte superior del cuerpo para “distanciarse” del individuo. Este comportamiento, sutil, pero observable

y relevante, podría ser una señal para un vigilante, un funcionario de aduanas o un binomio que patrulla por una zona confluida de gente.

5.3.1. La observación de comportamientos de comodidad e incomodidad

Según Navarro y Karlins (2008), nuestro cerebro y nuestro cuerpo colaboran para confortarnos y darnos confianza en nuestra seguridad personal. En esencia, existen dos indicadores universales que se reflejan a través de la expresión corporal y que son de suma importancia: la *comodidad* (bienestar) y la *incomodidad* (malestar).

Cuando un sujeto experimenta una sensación de comodidad, su sistema límbico "filtra" esa información en forma de expresión corporal en consonancia con sus sentimientos positivos. Así, si una persona está relajada tomando el sol, su cuerpo refleja la sensación de bienestar que experimenta su cerebro. En cambio, cuando un individuo experimenta una sensación de incomodidad, si está angustiada, su sistema límbico expresará un comportamiento no verbal de malestar (por ejemplo cambiando de postura). Además, en muchas ocasiones, ante una experiencia amenazadora o negativa, se suceden una serie de gestos, que como veremos más adelante se denominan "adaptadores" (por ejemplo tocarse la cara, atusarse el pelo, apretar una mano contra otra, etc.).

Si un individuo, al que se ha dirigido un *profesional de seguridad*, le identifica como una posible amenaza, se activará su sistema límbico para tratar de dar respuesta a dicha amenaza. En situaciones de peligro nuestro sistema límbico trata de oxigenar la musculatura de mayor tamaño para que podamos reaccionar adecuadamente (lucha o huida). Si la emoción sentida es de *rabia* o *ira,* el mayor aporte sanguíneo irá hacia los brazos (lucha). Goleman (1996) mantiene que la ira aumenta el flujo sanguíneo hacia las manos, haciendo más fácil empuñar un arma o golpear a alguien; y que para poder acometer tales acciones, se genera la necesaria energía aumentado la tasa cardiaca y los niveles de adrenalina. En cambio, cuando surge el *miedo*, la sangre se retira del rostro y afluye a los grandes músculos de las piernas, preparándonos para la huida. Ello no significa que vayamos a huir, sino que la evolución nos ha preparado para hacer lo que ha contribuido a una mejor adaptación en la historia pasada de nuestra especie (Goleman, 1996). Pero además, cuando la persona detecta una posible amenaza, su tórax puede expandirse más de lo normal, llenando los pulmones de aire para que la sangre sea oxigenada lo máximo posible.

La observación minuciosa debe permitir, al personal que trabaja en ámbitos de la seguridad, detectar los comportamientos de bienestar y malestar, para así poder inferir algún tipo de reacción poco adecuada por parte de la persona con la que interacciona.

5.4. GESTOS

El gesto incluye no solo los movimientos de las manos y brazos, sino también de otras partes del cuerpo como la cabeza, el tronco, las piernas o los pies (Petisco y Sánchez, 2016, pág. 76).

Ekman y Friesen establecieron cinco categorías distintas de gestos: emblemas, ilustradores, expresivos de afecto, reguladores y adaptadores (Ekman y Friesen, 1969). La de mayor interés, para el tema que nos ocupa, es la que engloba a los adaptadores, que son

gestos que se llevan a cabo para manejar y gestionar emociones, o como reacción a un estado físico o fisiológico (aunque también para satisfacer necesidades corporales, como hurgarse la nariz). En definitiva, sirven para tranquilizarnos tras haber experimentado algo molesto para nosotros. Además, se realizan de manera inconsciente y sin intención de comunicar, pero pueden aportar mucha información útil de cara a la detección de amenazas.

Interpretar adecuadamente los gestos que muestra una persona, puede ayudar al *profesional de seguridad* a inferir lo que esa persona está sintiendo, sus actitudes o intenciones y anticipar cómo podría actuar en esa situación concreta. Una evaluación precisa y un enfoque proactivo pueden resultar vitales para salvar su vida.

Valga como ejemplo, el incidente ocurrido en 1998 en Georgia (Estados Unidos), cuando un ayudante de sheriff procedió a parar a una camioneta blanca tras la comisión de una infracción de tráfico. El ayudante del sheriff (que estaba solo), tras detenerse la camioneta, paró su coche patrulla detrás de la misma. Mientras, una cámara colocada en el salpicadero grababa toda la escena.

Tras un pequeño análisis de dichas imágenes, se pueden detectar al menos seis indicadores de peligro para la vida del agente:

1. El conductor infractor abre la puerta y sale del vehículo (se aparta del vehículo, lo que puede indicar que esconde algo en el vehículo o tiene intención de atacar al agente).
2. El agente le da indicaciones de que vuelva al vehículo, pero este duda (tiene algo en su cabeza) y lo que hace es cerrarse el abrigo (lo que podría indicar nerviosismo por lo que pretende hacer en breve).
3. Se mete las manos en los bolsillos (otro indicador de peligro, ya que puede guardar algún tipo de arma).
4. El agente le grita que saque las manos de los bolsillos y este las pone en alto, pero iniciando un baile (Figura 6) a modo de burla (intimida al agente, otra señal de peligro).

Figura 6. Instantánea del incidente con fatal desenlace para el agente[8].

8 Instantáneo tomada del documental “Los secretos del lenguaje corporal” emitido por el Canal Historia.

5. El ayudante del sheriff sale del coche patrulla para hablar con el conductor y, en un momento dado, durante su danza, el infractor da un puñetazo a la palma de su propia mano (señal de agresión inminente).

6. Se va hacia el agente y se produce un enfrentamiento fuera de cámara. El agente apuntándole con su arma reglamentaria le permite volver a su vehículo; allí busca algo en su interior (señal de peligro inminente), saca un arma de fuego (situación ya fuera de control) y comienza un tiroteo entre ambos que acaba con la vida del agente.

Dichas imágenes son un ejemplo real de los peligros que puede conllevar, para un *profesional de la seguridad*, el no tener en cuenta, o no saber "leer", lo que comunica el comportamiento no verbal del sujeto con el que se interactúa. Este agente no supo detectar una potencial amenaza, en este caso, contra su propia seguridad personal. No tuvo en cuenta las señales de peligro que comunicaba el comportamiento no verbal mantenido por el conductor. La más clara y que anunciaba una inminente agresión, fue el gesto que empleó para activarse aún más, para subir sus niveles de adrenalina. Algo similar a lo que hacen los velocistas antes de iniciar una carrera. Los atletas, se golpean en las piernas preparándolas para la acción que van a llevar a cabo: correr. Este sujeto se golpeó en su propia mano, preparando sus manos para otro tipo de acción: luchar. El agente no hizo otra cosa más que apuntarle con su arma, arma que solo llegó a disparar cuando se inició el tiroteo por parte del infractor. El desenlace final fue trágico para el agente.

6. CONCLUSIONES FINALES

La mayoría de las personas desconoce la cantidad de información que podemos transmitir y recibir a nivel no verbal. En el caso de la detección temprana de amenazas, la observación minuciosa y la búsqueda de anomalías pueden ser vitales.

En tareas de vigilancia de alto riesgo, donde peligra nuestra integridad física, podemos padecer la denominada "visión de túnel". Saber de su existencia puede ser ventajoso, ya que en tales situaciones es probable que al adversario también le esté afectando. Movernos rápido a la izquierda o derecha, para salir de su campo de visión, puede salvarnos la vida.

Cuando realizamos actividades de vigilancia rutinarias, o excesivamente familiares, la búsqueda de cualquier tipo de cambio se puede ver complicada con la aparición de dos tipos de ceguera involuntaria: la ceguera por falta de atención y la ceguera por cambio. Si en una escena, fijamos la atención en un aspecto de nuestro entorno, solemos desatender otros detalles evidentes de dicho entorno (ceguera atencional) y cuando esperamos ver lo que estamos buscando, pueden pasarnos desapercibidos otros eventos que pueden ser relevantes (ceguera al cambio).

Las tecnologías de reconocimiento facial son sistemas, no intrusivos, que se basan en las imágenes captadas por cámaras de seguridad de alta definición que cotejan rápidamente con bases de datos de fotografías de individuos sospechosos, o en búsqueda y captura. Su utilidad es clara en el campo de la detección de amenazas en lugares como aduanas y aeropuertos, pero dichas tecnologías no están exentas de limitaciones y posibles errores. Por ello, como complemento a dichos recursos

tecnológicos, parece evidente la necesidad de formación de los agentes de seguridad en temas vinculados a la detección temprana de amenazas, tomando como base la observación minuciosa del comportamiento no verbal de los sujetos.

Esa observación minuciosa debe tener siempre en cuenta el rostro humano, ya que, según investigaciones recientes, más que aportar significados afectivos, el rostro humano es una herramienta que empleamos para comunicar motivos sociales. De acuerdo con este punto de vista, una expresión de ira –independientemente de la emoción que el individuo estuviese experimentando- habría que interpretarla como una advertencia. La expresión de lo que comúnmente denominamos *ira*, unida al enrojecimiento de la piel, podrían ser precursores de una inminente agresión física, lo que para la Ecología de la conducta sería interpretado como "disposición a atacar" (intención social). Por su parte, el *empalidecimiento* aparecería más en situaciones de *ira controlada*, sirviendo a motivos sociales de "apaciguamiento", o vinculada a ciertas actitudes para "guardar las apariencias". Pero el *empalidecimiento* también puede acompañar a un rostro que muestra *temor* y, en este caso, la lectura sería más de "disposición a ceder, o rendirse".

Respecto a la dirección de la mirada, no existe ningún patrón de movimiento ocular asociado al engaño.

En cuanto al aumento del parpadeo, puede ser un indicador de nerviosismo, estrés o ansiedad. Así, cuando un sujeto parpadea rápidamente, ello puede ser un indicador de que siente algún tipo de amenaza. Pero la frecuencia del parpadeo también responde a las demandas cognitivas (se inhiben bajo altas demandas y aumentan cuando las demandas son bajas).

Para el *profesional de seguridad* el espacio personal es crítico, ya que es la distancia óptima para llegarse al contacto y es la distancia que habitualmente se mantiene cuando se conversa con un desconocido. Ello hace muy difícil que pueda reaccionarse a tiempo ante una acción violenta. Por ello, la distancia de seguridad debe oscilar entre los 3 y 5 metros, ya que dicha distancia permite observar cualquier tipo de detalle para contrarrestar una posible agresión. Entre dichos detalles, conviene observar cualquier bulto bajo de la ropa, movimientos para ocultar dicho bulto o el gesto de separar el pulgar para empuñar un arma.

A través de las posturas corporales podemos obtener información sobre la *actitud* de un sujeto hacia una posible interacción y también sobre su *estatus* o *poder.* Para el profesional de seguridad es importante la lectura postural adoptada por la persona con la que interactúa. No obstante, la interpretación de la postura dependerá principalmente del contexto en el que se produzca, mediando variables como el sexo, la edad, la raza o la cultura. También es notoria la influencia de esas variables a la hora de interpretar la orientación corporal adoptada.

Respecto a los movimientos corporales, cuando una persona percibe a otra como amenazante o desagradable, la respuesta humana más habitual, será la de crear distancia física con ella.

La observación minuciosa debe permitir, al personal que trabaja en ámbitos de la seguridad, detectar los comportamientos de bienestar y malestar, para así poder inferir algún tipo de reacción poco adecuada por parte de la persona con la que interacciona.

Cuando un individuo experimenta una sensación de incomodidad, su sistema límbico expresará un comportamiento no verbal de malestar (por ejemplo cambiando de postura). Además, en muchas ocasiones, ante una experiencia amenazadora o negativa, suelen aparecer gestos "adaptadores" que denotan tal incomodidad.

En definitiva, una observación minuciosa y un enfoque proactivo pueden resultar vitales para el profesional de seguridad. Disponer de las últimas tecnologías en detección de amenazas es importante, pero no lo es menos la formación en comportamiento no verbal de quienes deben manejar dichas tecnologías. Dicha formación puede ayudar a inferir el estado emocional, los pensamientos y las intenciones de un sujeto y a anticipar cómo podría actuar dicho sujeto en una determinada situación. Si el *profesional de seguridad* sabe "leer" una amenaza, podrá reaccionar en consecuencia y contrarrestar o mitigar dicha amenaza. Pero la correcta "lectura" de comportamiento no verbal, como cualquier otra habilidad, requiere además de formación, entrenamiento y práctica continua. Leer las señales producidas por el sistema límbico es crítico para poder llevar a cabo cualquier acción anticipatoria. Pero, si no hemos adquirido determinada competencia en ese campo, puede que tampoco tengamos la debida percepción de peligro y que nuestra amígdala no envíe una respuesta instantánea ante esa potencial amenaza.

BIBLIOGRAFÍA

Andreassi, J. L. (1973). Alpha and problem solving: a demonstration. *Perceptual and Motor Skills, 36*, 905-906.

Bauer, L., Strock, B., Goldstein, R., Stern, J. y Walrath, L. (1985). Auditory discrimination and the eyeblink. *Psychophysiology, 22*, 629-635.

Chabris, C. y Simons, D. (2010). *The Invisible Gorilla.* New York: Crown Publishers.

Durán, J. I., Reisenzein, R. y Fernández-Dols, J. M. (2017). Coherence Between Emotions and Facial Expressions. En J. M. Fernández-Dols, y J. A. Rusell (Edits.), *The Science of Facial Expression* (págs. 107-132). New York: Osford University Press.

Ekman, P. (2009). *Cómo detectar mentiras. Una guía práctica para utilizar en el trabajo, la política y la pareja* (Segunda ed.). (L. Wolfson, Trad.) Barcelona: Paidós.

Ekman, P. y Friesen, W. (1978). *Facial Action Coding System: A Technique for the Measurement of Facial Movement.* Palo Alto: Consulting Psychologists Press.

Ekman, P. y Friesen, W. V. (1969). The Repertoire of Nonverbal Behaviour: Categories, Origins, Usage and Coding. *Semiotica, 11*, 49-98.

Fernández-Abascal, E. G. y Chóliz Montañés, M. (2001). *Expresión facial de la emoción.* Madrid: UNED.

Fernández-Dols, J. M. y Crivelli, C. (2013). Emoction and Expression: Naturalistic Studies. *Emotion Review, 5*(1), 24-29.

Fridlund, A. J. (1994). *Expresión facial humana. Una Visión Evolucionista.* (J. Cerdas Ibañez e I. Cardas Ibánez, Trads.) Bilbao: Desclée De Brouwer.

Fridlund, A. y Gilbert, A. (1985). Emotions and facial expressions. *Sciencie, 230*, 607-608.

Goleman, D. (1996). *Inteligencia emocional.* (D. González Raga y F. Mora, Trads.) Barcelona: Kairós.

Grossman, D. y Christensen, L. (2014). *Sobre el combate.* New York: Melusina.

Hall, E. (1959). *The Silent Language.* New York: Anchor Books.

Hall, E. (1976). *La dimensión oculta.* (F. Blanco, Trad.) México: Siglo Veintiuno.

Hallinan, J. T. (2009). *Why We Make Mistakes: How We Look Without Seeing, Forget Things in Seconds, and Are All Pretty Sure We Are Way Above Average.* New York: Broadway Books.

Hess, E. H. y Polt, J. M. (1960). Pupil size as related to interest value of visual stimuli. *Science, 132*, 349-350.

Ingham, R. (1971). Cultural differences in social behavior. En *Tesis doctoral.* Universidad de Oxford.

Knapp, M. y Hall, J. (2002). *Nonverbal communication in human interaction* (5ª ed.). New York: Harcourt Brace Jovanovich.

Lieberman, D. J. (1998). *Never be lied to again.* New York: St. Martin's Press.

Mann, S., Vrij, A., Nasholm, E., Warmelink, L., Leal, S. y Forrester, D. (2012). The Direction of Deception: Neuro-Linguistic Programming as a Lie Detection Tool. *Journal of Police and Criminal Psychology, 27*, 160-166.

Masip, J. (2005). ¿Se pilla antes a un mentiroso que a un cojo? Sabiduría popular versus conocimiento científico sobre la detección no-verbal del engaño. *Papeles del Psicólogo, 26*, 78-91.

Mehrabian, A. (1968). Inference of attitudes from the posture, orientation and distance of a comunicator. *Journal of Consulting and Clinical Psychology, 32*, 296-308.

Mehrabian, A. (1971). *Silent messages.* Belmont, CA: Wadsworth.

Navarro, J. y Karlins, M. (2008). *El cuerpo habla.* Málaga: Editorial Sirio.

Parkinson, B. (2005). Do Facial Movements Express Emotions or Communicate Motive? *Personality and Social Psychology Review, 9*(4), 278-311.

Pease, A., & Pease, B. (2006). *El lenguaje del cuerpo. Cómo interpretar a los demás a través de sus gestos.* Barcelona: Amat, S.L.

Petisco, J. M. (2014). *La comunicación en el aula. Cuando la postura y el gesto toman la palabra.* Madrid: Dykinson.

Petisco, J. M. (en prensa). Detección del engaño. Indicios no verbales. En J. M. Petisco y A. Manzanero (Edits.), *Credibilidad del testimonio y detección del engaño.* Delta Publicaciones.

Petisco, J. M. y Sánchez, N. (2016). Expresión corporal. Movimientos corporales, posturas, orientación corporal y gestos. En R. M. López Pérez, F. Gordillo León y M. Grau Olivares, *Manual de Análisis de Comportamiento no Verbal: más allá de la comunicación* (págs. 67-84). Madrid: Pirámide.

Porter, S., ten Brinke, L. y Wallace, B. (2012). Secrets and lies: Involuntary leakage in deceptive facial expressions as a function of emotional intensity. *Journal of Nonverbal Behavior, 36*, 23–37.

Ricci, P. E. y Cortesi, S. (1980). *Comportamiento no verbal y comunicación.* Barcelona: Gustavo Gili S.A.

Simons, D. y Chabris, C. (1999). Gorilas en nuestro medio: Ceguera por inatención sostenida para eventos dinámicos. *SAGE Publications Ltd STM, 28*(9), 1059 - 1074.

Wiseman, R., Watt, C., Ten Brinke, L., Porter, S., Couper, S. y Rankin, C. (2012). The Eyes Don't Have It: Lie Detection and Neuro-Linguistic Programming. *PLoS One, 7*(7).

Yan, W.-J., Wu, Q., Chen, Y.-H., Liang, J. y Fu, X. (2013). How Fast Are the Leaked Facial Expressions: The Duration of Microexpression. *Journal of Nonverbal Behavior, 37*, 217-230.

Fecha de recepción: 20/03/2018. Fecha de aceptación: 25/06/2018

SUMISIÓN QUÍMICA
USO DE SUSTANCIAS PARA REALIZACIÓN DE DELITOS SEXUALES

JOSÉ MANUEL QUINTANA TOUZA

CAPITÁN DE LA GUARDIA CIVIL. SECCIÓN DE ANÁLISIS DE COMPORTAMIENTO DELICTIVO. UTPJ

OLGA MORENO RODRÍGUEZ

SARGENTO DE LA GUARDIA CIVIL. EMUME CENTRAL. UTPJ

MANUEL RAMOS ROMERO

SARGENTO DE LA GUARDIA CIVIL. SECCIÓN DE ANÁLISIS DE COMPORTAMIENTO DELICTIVO. UTPJ

RESUMEN

En los últimos tiempos los delitos contra la libertad sexual y los nuevos modos de perpetración han tenido una gran relevancia mediática y de movilización social, generando un gran debate que ha afectado a todas las estructuras sociales y políticas. A nivel policial, no debemos mantenernos al margen de estos casos y la Guardia Civil tiene el deber inexcusable de atender y responder a las demandas de los ciudadanos en general y a las víctimas de delitos en particular, además de adaptar los medios y procedimientos de investigación a estos nuevos modos de agresión y abuso. Desde hace años, desde la Unidad Técnica de Policía Judicial se viene prestando especial atención a los casos en los que se utilizan sustancias para anular la voluntad de una víctima potencial y realizar una conducta delictiva de tipo sexual minimizando la posibilidad de defensa de la víctima y el recuerdo de aspectos de la agresión que son cruciales para la investigación. En el presente artículo presentamos los principales aspectos que caracterizan este tipo de delitos y una serie de recomendaciones para su investigación policial.

Palabras clave: sumisión química, delito sexual, abuso, agresión, anulación de la voluntad, víctima vulnerable.

ABSTRACT

In recent times, sexual offenses and new modes of perpetration, like *drug-facilitated sexual assault,* have had great media and social mobilization relevance, generating a great debate that has affected all social and political structures. As enforcement law agencies, we must not stay out of these cases and the Civil Guard has an inexcusable duty to attend and respond to the citizens and victims demands, in addition to adapt investigation tools and procedures to these new sexual aggression and abuse modes. For years, Intelligence Criminal Unit of the Civil Guard has been paying special attention to cases in which substances are used to annul the will of a potential victim and

carry out a sexual type of criminal conduct, minimizing the possibility of the victim's defense and her memory of aspects of the aggression that are crucial for the investigation. In this article we present the main aspects that characterize this type of crime and some recommendations for investigators.

Keywords: drug-facilitated sexual assault, sexual offense, sexual abuse, aggression, annulment of the will, vulnerable victim.

1. INTRODUCCIÓN

Entendemos comúnmente por "sumisión química" la administración de algún tipo de sustancia química a una víctima con el objetivo de incapacitarla y anular su resistencia, con el fin de lograr el objetivo propuesto por el autor. Incluye todas las figuras delictivas asociadas a esta práctica, si bien cabe destacar su asociación principalmente al delito sexual.

En los últimos años son varios los casos que han saltado a los medios de comunicación relativos a víctimas que han sufrido distintos delitos, habiendo sido alteradas sus facultades físico-psíquicas para lograr su comisión. Desde 1990 se viene observando un incremento en el número de estos casos, lo que ha llevado a un aumento del interés por este tipo de sucesos que, debido a la indefensión que se provoca en la víctima, generan gran alarma social. La mayoría de los autores definen la sumisión química como el uso o la administración de una o varias sustancias psicoactivas a una persona con fines delictivos o criminales, de forma que se pueda manipular o modificar la voluntad o el comportamiento de la misma, alterando su grado de vigilancia, su capacidad de juicio o su estado de consciencia (García-Caballero, Cruz-Landeira & Quintela-Jorge, 2012; García-Repetto & Soria, 2013). En esta situación, los efectos de dicha sustancia o sustancias, con el fin de causar a la víctima –aquella persona a la que le es suministrada el fármaco o la droga– un perjuicio secundario, impiden que sea capaz de prestar su consentimiento legal o, en su caso, de oponer resistencia a un posible agresor.

Son varios los organismos que han fijado su atención en este fenómeno en crecimiento y que se han pronunciado, dictando una serie de recomendaciones a los Estados de la Unión Europea. Así, la Comisión de Estupefacientes aprobó la Resolución sobre Cooperación Internacional para combatir la administración subrepticia de sustancias psicoactivas relacionadas con la agresión sexual y otros actos delictivos en 2010 (Resolución 53/7; E/CN.7/2010/18). En España recientemente se han introducido cambios en la legislación al respecto, pero si hay un hecho que destaca es la elaboración del primer protocolo de actuación para casos de agresión sexual con sospecha de intoxicación y su publicación por parte del Instituto Nacional de Toxicología y Ciencias Forenses (INTCF), dependiente del Ministerio de Justicia, en 2012 (Orden JUS/1291/2012, de 13 de mayo).

Aunque su uso se ha extendido a multitud de delitos, uno de los que generan mayor inquietud, debido tanto al bien jurídico protegido como a la dificultad de su detección para el personal sanitario, es la agresión sexual facilitada por drogas o, en su acrónimo inglés, DFSA (*drug-facilitated sexual assault*), si bien no es el único (Cruz-Landeira, Quintela-Jorge & López-Rivadulla, 2008). Este acrónimo se refiere

a aquellas relaciones sexuales no consentidas, abusos o agresiones sexuales que se llevan a cabo mientras las víctimas se encuentran bajo los efectos de sustancias psicoactivas como alcohol, psicofármacos o drogas ilícitas, generalmente incapacitadas o en estado de inconsciencia (Payne-James & Rogers, 2002). El organismo público británico experto en drogas de abuso (*Advisory Council on the Misuse of Drugs*)[1], en el año 2007, llevó esta definición un paso más allá, puntualizando que el delito abarca "toda actividad sexual con penetración no consentida, tanto si implica la administración forzosa o encubierta por parte del agresor de una sustancia con el objeto de realizar un asalto sexual –DFSA premeditada o proactiva[2]–, como si se trata de una actividad sexual realizada por el mismo con una víctima incapacitada, tras el consumo voluntario de las mencionadas sustancias –DFSA oportunista[2]–" (García-Repetto & Soria, 2013).

En cualquier caso, la literatura científica al respecto señala que la principal diferencia entre estos delitos mediados por sumisión química y otros del mismo tipo en los que no existe tal sumisión, es la pérdida de poder y control –de la voluntad, de sus actos…– de las víctimas por el efecto de las sustancias consumidas, situación que es aprovechada por el agresor o abusador (García-Caballero, Cruz-Landeira & Quintela-Jorge, 2013).

En nuestro país, la legislación no considera la sumisión química como un agravante del delito de abusos sexuales (Berenguer, Suárez & Rodríguez, 2011), si bien en España sí que disponemos de instrucciones de actuación para los casos de agresión sexual con sospecha de intoxicación, publicadas por el Ministerio de Justicia en 2012[3], y de la guía de actuación médico-forense elaborada por un grupo de investigación en esta materia, del Instituto de Medicina Legal de Cataluña[4] (García-Repetto & Soria, 2013). Ambos, además de dar las pautas de actuación en este tipo de delitos, aportan algunos datos sobre la situación española, señalando que un 20-30% de las agresiones sexuales se producen por medio de la sumisión química y que, de ello, menos de un 20% se denuncia, debido a la pérdida o disminución de memoria por parte de la víctima, a consecuencia de los efectos de las sustancias facilitadas por el agresor (Ministerio de Justicia, 2012). Así, numerosos autores coinciden en que la prevalencia real de este fenómeno nunca podrá ser conocida, debido a que muchos casos no se denuncian –por no quedar claro el suceso, por vergüenza que sufre la víctima…– o la denuncia se presenta tan tarde que entorpece las labores de investigación (García-Repetto & Soria, 2011). A ello se le suma la complejidad para diagnosticar como sumisión química aquellos casos que llegan al centro sanitario con indicadores de sospecha –la detección de los casos de sumisión química supone un reto para los laboratorios de toxicología,

1 Operation Matisse: Investigating Drug Facilitated Sexual Assault. London: Association of Chief Police Officers; 2006.

2 Clasificación propuesta en: Horwath, M. & Brown, J. Drug assisted rape and sexual assault: definitions, conceptual and methodological developments. Investigative Psychology Offender Profiling. 2005; 2: 203-10.

3 Vega P (coord.). Instrucciones de actuación en casos de agresión sexual con sospecha de intoxicación. Madrid: Ministerio de Justicia; 2012 [consultado 21 Feb 2018]. Disponible en: http://institutodetoxicologia.justicia.es/

4 Xifró, A., Barbería, E., Pujol, A., Arroyo, A., Bertomeu, A., Montero, F., et al. *Sumisión química: guía de actuación médico-forense*. Revista Esp. Medicina Legal. 2013; 39: 32-6.

ya que requiere la determinación de sustancias que estarán presentes en concentraciones muy bajas en una buena parte de las muestras analizadas– o la falta de colaboración de la víctima debido a los efectos del tóxico, la relación con el autor de los hechos, etc.

No conocemos estudios que se hayan llevado a cabo en nuestro país acerca de la sumisión química desde una perspectiva de investigación policial y los que se han hecho, en su mayoría, están más orientados a aspectos puramente toxicológicos (ver, por ejemplo, Cruz-Landeira, Quintela-Jorge & López-Rivadulla, 2008; García-Repetto & Soria, 2013; o García-Caballero, Cruz-Landeira & Quintela-Jorge, 2013). Por otro lado, y a tenor de la repercusión mediática de algunos casos y la alarma e indignación social que han provocado, es esperable que próximamente abunden artículos de orientación más bien jurídica.

2. MODUS OPERANDI

El denominado *modus operandi* en los casos de sumisión química se suele caracterizar por un contexto en el que la víctima potencial tiene una percepción de seguridad, al estar en un ambiente distendido de ocio: una fiesta, un pub, una discoteca, una cena de trabajo, en casa de un amigo, etc., en la cual consume, voluntariamente, bebidas u otras sustancias. Tiempo después de la ingesta sufre la pérdida de conciencia y, al despertar, la víctima toma conciencia de que han pasado varias horas, no recuerda nada de lo que ha ocurrido, tiene la sensación de haber mantenido relaciones sexuales e incluso puede estar en algún lugar desconocido para ella.

Por lo que respecta a la administración de sustancias nocivas, esta puede realizarse disuelta en una bebida o alimento (sin que la víctima lo sepa o con engaño, caso en que se administra la sustancia diciéndole que se trata de otra); mezclada con tabaco u otro producto, en cigarrillos, pastillas, etc., que la víctima acepta creyendo saber la sustancia que está tomando; o por la inhalación de la sustancia mediante engaño.

Así, la agresión sexual por sumisión química se diferencia de la violación, en la que la víctima es forzada a mantener relaciones sexuales con el agresor mediante amenaza, violencia o intimidación, lo que puede evidenciarse en los análisis forenses al constatar la presencia de agresiones físicas o lesiones defensivas en la víctima. La ausencia de estas evidencias del delito en los supuestos de sumisión química provoca que, en ocasiones, surja la duda sobre la existencia del consentimiento de la víctima.

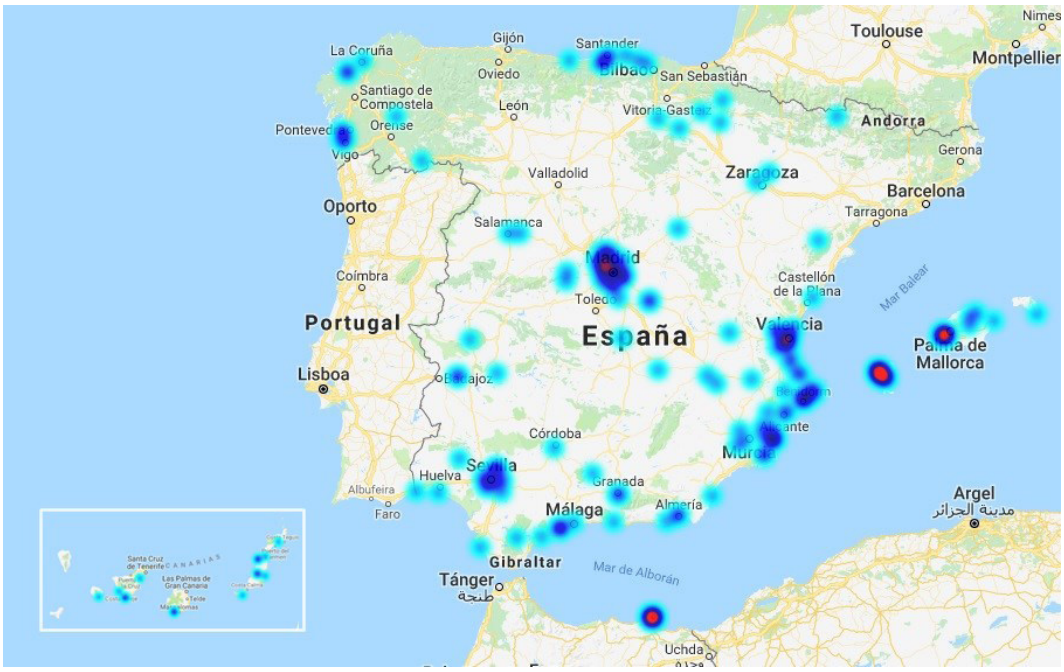

Imagen 1. *Mapa de calor de los hechos de sumisión química (2008-2017). Puede observarse una mayor incidencia de estos casos en aquellas zonas vinculadas con lugares de turismo y grandes zonas de ocio. Fuente: Unidad Técnica de Policía Judicial de la Guardia Civil.*

3. LA VÍCTIMA

El trazo que se le da a la víctima es el de una mujer joven, menor de 30 años, que en un entorno social, laboral o de ocio, especialmente, consume bebidas alcohólicas de forma voluntaria, perdiendo la noción del espacio y del tiempo y despertando en un lugar desconocido, sin saber qué ha ocurrido, pero con la sensación o signos de haber mantenido relaciones sexuales sin su consentimiento (McGregor, Ericksen, Ronald, Janssen, Van Vliet & Schulzer, 2004). Sin embargo, el análisis toxicológico de las sustancias que puede haber consumido involuntariamente es muchas veces infructuoso, dada la rápida desaparición de estos tóxicos del organismo, bien a través de la orina o de otros medios, dificultando que la toma de muestras biológicas llegue a suponer una prueba científica y de certeza de que se ha producido sumisión química (Cruz-Landeira, Quintela-Jorge & López-Rivadulla, 2008).

Así, haciendo uso de la Victimología –ciencia que se encarga del estudio de la víctima-, se puede realizar una clasificación siguiendo a B. Mendelsohn, autor de una de las sistematizaciones más valoradas y completas:

- Víctima ideal o víctima inocente: es el caso de menores de corta edad y/o personas con discapacidad, que por su vulnerabilidad se encuentran en una situación de indefensión. El menor destaca por su debilidad física, inmadurez e inexperiencia, estando en un proceso de formación biológica y mental; no tiene aún la capacidad de resistencia corporal, ni intelectual ni moral para oponerse en igualdad de condiciones a un agresor adulto o, en el caso de los supuestos de sumisión química sorpresivos, mediante el uso de sustancias de inhalación.
- Víctima por ignorancia: es aquella que no es consciente del riesgo que corre. En el caso de la sumisión química sería aquella víctima a la que, por descuidar

su bebida, le ponen alguna sustancia química en la misma o la persona que abusando del alcohol u otras sustancias es victimizada al tener su capacidad psíquico-física alterada.

- Víctima "voluntaria": en el sentido en que su participación es determinante, ya que conscientemente se pone o acepta una determinada situación de posible peligro sin prever las consecuencias. En este caso sería aquella que conscientemente consume la sustancia, aunque no anticipa que otras personas puedan aprovechar sus efectos para cometer una agresión sexual sobre ella.

Más adelante se describen y analizan los datos obtenidos en el presente estudio, realizando un perfil aproximativo de la víctima tipo de sumisión química con motivación sexual.

4. EL AGRESOR

Estudios previos coinciden en que el perfil del agresor, en casos de agresión sexual mediados por sustancias, es el de un varón, conocido de la víctima[5], amigo, ex-pareja o vecino, siendo incluso algunas veces un completo desconocido (Read, Kufera, Jackson & Dischinger, 2005). Este asaltante se aprovecha del estado de embriaguez de la víctima –que presenta mayor vulnerabilidad–, o bien le suministra de modo subrepticio el propio tóxico en la bebida para ocasionar dicha vulnerabilidad, incluyendo la amnesia total o parcial de los hechos por parte de aquella –la amnesia anterógrada o pérdida de memoria, donde los acontecimientos más recientes no se guardan en la memoria a largo plazo, es síntoma característico del abuso de alcohol o benzodiacepinas– (Kuhn, Swatzwelder & Wilson, 2011). Así pues, en los casos de sumisión química el autor no suele utilizar la fuerza ni la amenaza para obligar a la víctima a realizar el acto sexual.

El autor de una agresión mediante sumisión química se diferencia respecto del violador "tradicional" porque aquel busca, principalmente, satisfacer el deseo sexual, en tanto que este, según los estudios parecen demostrar, suele estar motivado por el poder, el control, el sadismo sexual u otro tipo de motivos patológicos (Groth y Birnbaum, 1979).

Los agresores, mediante uso de productos químicos que anulan la voluntad y/o conocimiento de la víctima, pueden clasificarse en:

- Agresor "oportunista", se aprovecha de la situación de indefensión de la víctima sin haber contribuido a crearla.
- Agresor "ocasional", el que, sin haber contribuido a crear la indefensión de la víctima, actúa ante circunstancias desinhibitorias: en momentos de euforia, después de una ingesta excesiva de alcohol, tras el consumo de sustancias estupefaciente, etc.
- Agresor "propio", el que voluntaria y conscientemente, con el fin de agredir sexualmente a la persona elegida, provoca mediante el uso de sustancias químicas la sumisión de la víctima.

5 Cruz-Landeira, Quintela-Jorge & López-Rivadulla (2008), señalan en su estudio que en el 70% de los casos, el agresor es un conocido de la víctima.

5. LAS SUSTANCIAS

Finalmente, en lo que respecta a las sustancias empleadas, la literatura científica señala una serie de características que las hace idóneas para la finalidad de los autores de los hechos: son fáciles de obtener y de disimular –inoloras, insípidas, incoloras…– en bebidas, para su administración discreta por vía oral, de acción rápida y corta duración, en dosis bajas, y que producen síntomas poco característicos pero suficientes para que el agresor pueda tener a la víctima bajo su control (Cruz-Landeira, Quintela-Jorge & López-Rivadulla, 2008). Son sustancias depresoras y estimulantes del sistema nervioso central, psicoactivas, como el alcohol etílico, las benzodiacepinas, la gammahidroxibutirato –GHB, llamada también "*droga de la violación*"–, o de otro tipo, como la cocaína, el zolpidem, la ketamina o el LSD.

En definitiva, las sustancias psicoactivas que son utilizadas con la finalidad de facilitar la comisión de una agresión sexual son aquellas que producen en la víctima un estado de incapacidad o inconsciencia, alterando su facultad para tomar decisiones, disminuyendo su capacidad para identificar una situación peligrosa o para resistirse a una agresión. Por tanto no hablamos solamente de la conocida escopolamina o *burundanga*, sino que debemos tener presente que cualquier sustancia que consiga estos efectos es susceptible de ser usada para obtener el fin perseguido.

Ya hemos visto que en algunos casos estas sustancias son consumidas por las víctimas de forma voluntaria, pero en otros se les proporciona de forma furtiva; en estos casos los agresores buscan en la droga las cualidades siguientes:

- La sustancia ha de permitir su administración discreta, por ello se realiza normalmente por vía oral, mezclándola con bebidas, café, zumos de fruta, cerveza, bebidas alcohólicas, etc., o alimentos. Ocasionalmente el excipiente puede aumentar los efectos.

- Debe ser de difícil detección por la víctima. Así, ha de ser soluble, insípida, incolora e inodora, que presente una importante actividad a dosis bajas (para que pasen inadvertidas), de acción rápida, para facilitar el control sobre la víctima e impedir que el cambio de las circunstancias pueda frustrar sus objetivos, y de corta duración, para no levantar sospechas. Es por esto que la Comisión de Estupefacientes de Naciones Unidas, en su resolución 52/8 (2010), invitó al sector farmacéutico a que cooperara en la elaboración de preparados que comprendieran elementos de seguridad, como colorantes y saborizantes, a fin de advertir a las posibles víctimas de la adulteración de sus bebidas, sin afectar la disponibilidad de los ingredientes activos para los preparados farmacéuticos legítimos (Comisión de Estupefacientes, 2010). Respondiendo a esto, el fabricante del Rohypnol (Roche) modificó su composición añadiendo un colorante azul que burbujea cuando entra en contacto con líquidos[6].

- La fácil disponibilidad de la droga es también un criterio importante para el agresor a la hora de elegirla para la comisión del delito. Así, aquellas que se encuentran fácilmente en la calle, vía Internet o incluso aquellas que son legales en el ámbito de la medicina son las más usadas en estos casos. Es el caso por

6 Garcia-Repetto& Soria 2011.

ejemplo del Rohypnol, que en países como Estados Unidos se ha prohibido su distribución debido a su alta implicación en delitos de este tipo[7].

- La sustancia debe provocar indefensión en la víctima durante la agresión sexual, lo que además la hace sentir desamparada durante la investigación judicial.

Dependiendo del tipo de droga o de la cantidad administrada, la víctima puede experimentar:

- Amnesia anterógrada o pérdida de memoria: es la incapacidad de memorizar hechos nuevos. En el caso de la sumisión química se produce el síndrome amnesia-automatismo, con problemas de comportamiento y signos de confusión. La amnesia es un efecto favorable para el agresor, al incapacitar a la víctima para recordar lo sucedido durante el curso del efecto de la sustancia química, limitando la información de esta en su testimonio y retrasando la denuncia del hecho, lo que dificulta la toma precoz de muestras biológicas o, incluso algunas veces, impidiéndolo, sobre todo cuando la amnesia se asocia a un sentimiento de culpa.

- Sedación: para perturbar la capacidad de vigilia, de atención y de respuesta ante una agresión. El grado de sedación será ligero en casos de abusos sexuales. En ocasiones la víctima recupera la conciencia durante la agresión sexual, pero vuelve a desmayarse, incluso varias veces. Esto provoca *somnolencia*, *parálisis corporal* e *imposibilidad de articular palabras*.

- Efectos alucinógenos: con desorientación temporal y espacial de la víctima, con lo que se invalida su testimonio. A veces se superponen a los recuerdos aislados que tiene la víctima, de modo que puede ser difícil diferenciar ambos, lo cual dificulta todavía más la investigación.

- Desinhibición: que constituye una ventaja para el agresor en el curso de la agresión sexual, ya que la víctima puede aceptar situaciones que hubiera considerado intolerables en un estado de consciencia normal.

De este modo, las sustancias que presentan estas cualidades, y que frecuentemente se utilizan en la sumisión química, son:

- Alcohol etílico: el alcohol es la principal sustancia que actúa como depresor del sistema nervioso. El alcohol tiene la capacidad de afectar la voluntad, reducir las inhibiciones y causar la pérdida del control de funciones cognitivas y de la conciencia.

- Benzodiacepinas: son depresores del sistema nervioso central y están normalmente controladas como fármacos legales, siendo por lo tanto sencilla su obtención. Entre sus efectos secundarios se encuentran el automatismo, la desinhibición y la amnesia anterógrada. Las benzodiacepinas que se usan para este fin suelen ser el Triazolam y el Oxazepam. Pero la benzodiacepina comúnmente asociada con las agresiones sexuales es el Flunitrazepan o Rohypnol. Este, autorizado como un potente sedante hipnótico en muchos países europeos, es insípido, inodoro y se disuelve en líquido. Sin embargo,

7 Cruz Landeira, Quintela Jorge, & López Rivadulla, 2008

aunque en menos ocasiones, también se han presentado casos de sumisión con Lorazepam, Bromazepam, Clonazepam y Alprazolamentre, entre otros. Los efectos de la mayoría de drogas con propiedades ansiolíticas, sedantes o hipnóticas se incrementan significativamente cuando se toman con alcohol.

- ÁcidoGamma-hidroxibutírico (GHB): es también un depresor del sistema nervioso, autorizado con receta médica como agente anestésico. Sirve como un producto medicinal para tratar a personas con narcolepsia y cataplexia. El GHB produce sedación y anestesia, e incluso en pequeñas dosis puede causar pérdida de control y de conciencia. Tiene un efecto muy rápido y corto y se elimina rápidamente, impidiendo su detección.
- La Atropina, Escopolamina o Burundanga actúa como depresor de las terminaciones nerviosas y del cerebro. Es una sustancia inolora, incolora e insípida, que provoca la pérdida de la voluntad y del recuerdo de lo que sucede mientras dura su efecto. Es factible su ingreso por vía inhalatoria, por la piel o en líquidos. Esta sustancia ha sido la que ha dado publicidad en España a este tipo delictivo, pero realmente solo se administra en uno de cada cien casos.
- Otros estimulantes del sistema nervioso como la Cocaína y los Cannabinoides (las drogas de abuso detectadas con mayor frecuencia), las Anfetaminas, la Ketamina, sustancias como el Zolpidem, Clonazepam, Zopiclona, derivados de la Metilendioximetanfetamina, el Hidrato de cloral, Fentanilo, LSD (Dietilamida del Ácido Lisérgico) o, incluso, distintos disolventes orgánicos son también utilizados, entre otros, para estos fines.

Ante la falta de estudios centrados en las principales variables que afectan a la investigación de estos delitos de agresión sexual mediante sumisión química, tales como un perfil detallado de la víctima y del agresor, la situación espacio-temporal en la que se producen, o las circunstancias que rodean el caso, se planteó por parte de la Unidad Técnica de Policía Judicial la realización de un trabajo de investigación de cara a describir la situación actual de la casuística conocida en su demarcación, de cara a conocer las principales características de estos delitos, así como aportar recomendaciones que faciliten su abordaje policial y su investigación.

6. LA SUMISIÓN QUÍMICA EN LA LEGISLACIÓN ESPAÑOLA

En nuestro Código Penal, las agresiones sexuales se recogen en los artículos 178, 179 y 180, pero la sumisión química no encaja en estos tipos al ser requisito indispensable la existencia de violencia o intimidación. Actualmente nos encontramos en un intenso debate acerca de la pertinencia de actualizar y modificar estos aspectos con el fin de que determinados delitos contra la libertad e indemnidad sexual sean considerados agresiones sexuales y no abuso, para ajustar de modo más adecuado las penas correspondientes. En tanto en cuanto no se produce tal modificación, al hablar de sumisión química deberíamos hablar de abusos sexuales y no de violación, recogidos en los artículos 181 y 182 del citado Código, sin que exista un tipo agravado para los casos de sumisión química.

El artículo 181, después de su última modificación, establece en su punto 2: "*A los efectos del apartado anterior, se consideran abusos sexuales no consentidos*

los que se ejecuten sobre personas que se hallen privadas de sentido o de cuyo trastorno mental se abusare, así como los que se cometan anulando la voluntad de la víctima mediante el uso de fármacos, drogas o cualquier otra sustancia natural o química idónea a tal efecto." Lo que equipara el abuso sobre una persona que se halle privada de sentido por motivos propios con los casos en los que su incapacidad haya sido provocada.

7. RECOMENDACIONES PARA LA INVESTIGACIÓN

La investigación de este tipo de delito viene dificultada por la tardanza en la interposición de la denuncia, la inconsistencia en la declaración de la víctima y la ausencia de signos de defensa propios de las agresiones sexuales.

La mayoría de las drogas utilizadas para facilitar el asalto sexual producen síntomas como dificultad motora, falta de coordinación, somnolencia, falta de memoria, etc. Por ello es importante documentar en la manifestación de la víctima las sensaciones, referencias temporales y detalles de lo que recuerda y no recuerda; es imprescindible que cuente lo sucedido desde el principio hasta el final con sus propias palabras, en un ambiente seguro y libre de prejuicios. Estos son los principales obstáculos que tienen las víctimas a la hora de presentar denuncia por estos hechos:

1. Ausencia de resistencia. La ausencia de lesiones consecuencia de la no resistencia a la agresión puede tener su origen en que:

    - Muchas de las sustancias que se utilizan para lograr la sumisión química son fármacos depresores del sistema nervioso central, que pueden dar lugar a síntomas como la incapacidad en habilidades motoras, el deterioro en el juicio o la pérdida de conciencia, lo que provoca su falta de resistencia ante la agresión.

    - La confusión, el miedo o el estado de shock son otros tantos motivos, junto al uso de drogas, por los que la víctima puede verse incapacitada para ofrecer resistencia.

2. Inconsistencias o declaraciones no válidas. El recuerdo de estas víctimas sobre lo sucedido es especialmente difícil, debido a que tendrán una percepción inexacta de la cronología de los hechos y, además, pueden sentirse culpables de lo sucedido, ambas consideraciones darán lugar a inconsistencia o contradicciones en la denuncia. Ante lo expuesto, hay que tener en cuenta:

    - La víctima se siente incómoda al dar información sobre el uso de drogas al investigador. Por lo que, con el fin de facilitar la declaración de la víctima sobre su experiencia, hay que lograr un entorno en el que se sienta segura. Es necesario que el agente disipe, cuanto antes, sus temores respecto de la finalidad de la investigación, que no es otra que detener al agresor.

    - La víctima pudo denunciar haber sido drogada y su prueba toxicológica dar resultado negativo. Este resultado no desvirtúa la denuncia por cuanto la mayoría de los medicamentos utilizados en la sumisión química son metabolizados rápidamente por la orina y la sangre, lo que impide que la prueba toxicológica tenga carácter determinante en caso de resultado negativo.

- La víctima, debido al estado deteriorado de la memoria, puede rellenar inconscientemente los vacíos de su memoria con información ajena a los hechos, por lo que las preguntas han de ser claras y no sugestivas.

3. Retraso en la denuncia. La tardanza en la denuncia puede producirse porque en ocasiones:

   - La víctima de sumisión química se siente desorientada o bajo los efectos de la sustancia durante un periodo variable, que puede ser de varios días, por lo que puede sentirse incapacitada durante el mismo para denunciar el delito.
   - Al haber participado la víctima voluntariamente en el consumo de alcohol u otras drogas en los momentos previos al suceso, puede albergar sentimientos de culpabilidad que le impiden, al menos inicialmente, denunciar los hechos.
   - La víctima se resiste a presentar denuncia por vergüenza o temor ante las posibles reacciones de la familia.

Por lo tanto, el retraso en la denuncia no debe considerarse indicio de denuncia falsa, sino una consecuencia normal de este tipo de agresiones.

En los casos en los que esta denuncia llegue muy tarde, ni las pruebas toxicológicas ni el examen médico de la víctima serán de utilidad para el esclarecimiento de la investigación, por lo que esta deberá centrarse en entrevistas con la víctima, el autor, los testigos y otras personas que puedan tener información de los hechos próximos al suceso.

La herramienta más importante del investigador será una meticulosa recogida de información, evidencias y documentación, que incluirá las evidencias físicas, las entrevistas a la víctima, testigos y sospechosos, la escena del crimen y la investigación.

Teniendo en cuenta todo lo anterior, debemos:

- Calificar los hechos correctamente, determinar si los actos sexuales cumplen con la definición legal de agresión sexual o de otro tipo.
- Averiguar si la víctima estaba bajo la influencia de las drogas o alcohol y en qué medida, para determinar la existencia de consentimiento valido y la capacidad de resistencia.
- Establecer en qué grado la víctima consumió voluntariamente las sustancias o si su ingesta se produjo de manera subrepticia.
- Identificar al presunto autor y determinar si tuvo acceso a los medicamentos o drogas que fueron identificados por los análisis toxicológicos (en caso de haberlos y de haber dado un resultado positivo) o los que puedan ser por la descripción de los efectos de estos sobre la víctima.

7.1. ENTREVISTA CON LA VÍCTIMA

La entrevista, para ser eficaz, debe desarrollarse en un clima de confianza y seguridad, en el que la víctima no se sienta culpabilizada ni objeto de persecución policial/judicial, de privacidad y de comodidad para ella, lo que le permitirá proporcionar información

honesta de lo ocurrido y del contexto en el que sucedió el asalto. La declaración deberá ser contrastada con las evidencias recogidas, los testigos y sospechoso.

Se realizará el menor número posible de entrevistas, con el fin de evitar aumentar su victimización.

Cuando la denuncia se produce muy próxima a la agresión y dependiendo de las circunstancias de esta, puede ser conveniente programar la entrevista de seguimiento para el día siguiente. La víctima puede presentar algunos o todos de los siguientes síntomas: pérdida de memoria, mareos, confusión, somnolencia, dificultad para hablar, deterioro de las habilidades motoras, alteraciones en el juicio, inhibición reducida o una variedad de otros síntomas. Puede parecer ebria o con resaca, pero no por ello debe tenerse menos en cuenta. Retrasar la entrevista en estos casos hace que generalmente mejoren la investigación y la calidad de la información obtenida.

El lenguaje empleado debe ser sencillo y no inquisitorial, estimulando la conversación preferiblemente frente al interrogatorio. Debe dejarse a la víctima describir lo que ocurrió con sus propias palabras sin ninguna interrupción por parte del investigador.

Hay que asegurarse de que la víctima entienda que no será culpada o perseguida por el consumo de drogas, así como que ese consumo no afecta a su condición de víctima.

Durante la entrevista, el investigador debe estar alerta ante nueva información o acontecimientos que pudieran ser importantes. Si la historia de la víctima difiere de los hechos originalmente denunciados el investigador deberá pedir, después del relato libre de la víctima, las aclaraciones que procedan. Es necesario preguntar a la víctima si había alguien más presente en cualquiera de los momentos del suceso que pueda corroborar su declaración.

Si la denuncia se presenta dentro de los tres días siguientes a la agresión, advertir a la víctima de que no se duche, ni realice actividad que pueda destruir evidencias. Activar el protocolo de actuación.

Informar a la víctima que es necesario que entregue las prendas que llevaba puestas en el momento de la agresión para su análisis.

Cuando alcohol y drogas están involucrados, la víctima suele recordar muy poco, puede que nada, sobre la agresión que ha sufrido. El relato de la víctima puede tener grandes lagunas que dificultan la descripción de los hechos, por ello, el encargado de la entrevista debe tener paciencia y la mente abierta ante la narración de la víctima.

Hay que tener en cuenta que la víctima puede rellenar inconscientemente las lagunas de la memoria a partir de los falsos recuerdos generados por las preguntas del investigador, por lo que se deben evitar las preguntas sugestivas y las directas sobre aspectos que la víctima no recuerda.

Es muy importante que las víctimas expresen cómo se sintieron y qué estaban haciendo antes de perder la conciencia. Los síntomas narrados por la víctima pueden ayudar a identificar la sustancia utilizada, caso de no contar con el análisis toxicológico.

No hay que olvidarse de preguntar a la víctima si han podido realizarle fotos, grabar los hechos o si le falta algún objeto personal.

7.2. ENTREVISTAS CON LOS TESTIGOS

Aunque la declaración de la víctima es crucial para la investigación, la declaración de personas que vieron a la víctima o que hablaron con ella antes, durante o después del suceso es muy importante, debiéndose averiguar quién fue la primera persona que la vio después del incidente y quién fue la primera persona a la que se lo contó. Hay que procurar entrevistar a todos los testigos de la agresión y de las situaciones previa y posterior a esta.

Los investigadores, además de entrevistar a las personas que pudieron haber presenciado algo relacionado con el suceso, también deben entrevistar a tantos amigos y conocidos de la víctima y del sospechoso como sean posibles. Normalmente, son los testigos los que ponen un orden cronológico a los hechos, notan conductas inusuales y proporcionan datos o fuentes de información fundamentales para la investigación. Por ello, es importante entrevistar a camareros, personal del local, clientes, personal de seguridad o vecinos que puedan ser capaces de confirmar el relato de la víctima. Así como buscar otras posibles víctimas del autor, mujeres que hayan tenido contacto o relación con el sospechoso y que quizá hayan podido ser también víctimas.

Hay que tener en cuenta que, aunque los testigos declaren que han visto a la víctima irse voluntariamente con el sospechoso, las acciones de la víctima pudieron haber sido el resultado de los efectos de la droga administrada.

El investigador se interesará también por revisar los vídeos que considere oportunos; siempre se debe identificar a la/s persona/s a las que la víctima ha relatado en primer lugar lo sucedido y documentarlo con el máximo detalle.

7.3. ENTREVISTA CON EL SOSPECHOSO

Para identificar al autor de una sumisión química es necesario realizar una minuciosa investigación del sospechoso, pues en la mayoría de las ocasiones este admitirá que tuvo relaciones sexuales con la víctima pero que fueron consentidas e, incluso, intentará culpabilizarla diciendo que fue ella quien lo provocó.

Los investigadores deberán evaluar las circunstancias de la agresión e intentar encontrar los indicios que guíen la estrategia de investigación. Indicios como la relación que pudiera unir a la víctima con el sospechoso, si algo le vincula con la escena donde ocurrieron los hechos, si existen testigos que puedan relacionarle con el lugar de comisión o con la víctima, o si estos son capaces de corroborar la falta de consentimiento por parte de la víctima. Además, al igual que con la víctima, se debe averiguar la rutina habitual del sospechoso, tratando de descubrir lo que realmente sucedió antes, durante y después del asalto sexual.

7.4. RECOPILACIÓN DE INDICIOS.

La *Société Française de Toxicologie Analytique* ha elaborado un protocolo con tres muestras que deben tomarse de modo sistemático: sangre, orina y cabello. La asociación de toxicólogos norteamericanos recomienda, además de las muestras anteriores, el uso de parches de sudor.

En España, debido al aumento de casos que se han registrado en los últimos años en relación con este tipo de delito, el Instituto Nacional de Toxicología y Ciencias Forenses (INTCF), en colaboración con profesionales de los Institutos de Medicina Legal, han publicado un protocolo con las *Instrucciones de actuación en caso de agresión sexual con sospecha de intoxicación.* Entre estas instrucciones de actuación contempla la recogida de determinadas muestras para el estudio toxicológico, entre ellas:

- La sangre es una muestra biológica que informa del consumo reciente de la sustancia y además puede permitir establecer la correlación entre la concentración y el efecto clínico. Como principal desventaja de su uso para este tipo de casos figura la rápida eliminación de las sustancias de este medio biológico, por lo que en el caso de existir cierto retraso en solicitar ayuda médica, es probable que la sustancia administrada haya desaparecido de la sangre.
- La orina es una muestra que también informa del consumo reciente, pero ofrece ventajas de detección superiores a las de la sangre para las sustancias químicas, ya que pueden llegar a ser de varios días en algunas sustancias concretas.
- También se recomienda tomar muestras de cabello, pero solo en aquellos casos en los que no se pudo hacer una toma de muestra inmediata o se estima que se ha producido la eliminación de la sustancia en la sangre y la orina.

Para preservar las evidencias, la víctima no debería ducharse, bañarse, orinar, comer, beber, lavarse los dientes, fumar o masticar chicle, si no se han recogido todavía las muestras biológicas, pues posiblemente con ello pueda contaminar o destruir indicios del agresor, ya sea semen, saliva, pelo, etc.

El paso del tiempo es determinante en la detección de algunos tóxicos, ya que se suelen emplear sustancias con una acción rápida y de corta duración, que rápidamente son eliminadas del organismo. Así, de cara a una correcta interpretación de los resultados, habrá que tener en cuenta que un resultado negativo no implica necesariamente que no se haya administrado una sustancia química, sino que puede haber desaparecido del organismo por el tiempo transcurrido. Para que el informe toxicológico sea correcto, la víctima debe comunicar si toma algún tipo de droga recreativa recetada o cualquier otro medicamento sin receta.

También se aconseja recoger muestras no biológicas relacionadas con los hechos denunciados. Estos indicios podemos encontrarlos en casa del sospechoso, en su vehículo, en su lugar de trabajo (taquilla, escritorio), etc. Puede que este se haya llevado algo de la víctima o esta haberse dejado algo en el lugar de los hechos. Si la agresión tuvo lugar en el vehículo, habrá que procesarlo.

Hay que buscar además de los indicios habituales: utensilios utilizados cuando la víctima y el agresor se encontraban juntos, como máscaras, objetos extraños, lubricantes, preservativos, cuerdas u otros para atar, armas, trofeos, fetiches, etc., la droga en sí, los ingredientes para su fabricación, fármacos, literatura sobre drogas para violaciones y sus efectos, recetas, correos o conversaciones, historial de internet, bebidas o alimentos sospechosos, envases para drogas o botellas, vasos, recipientes donde se haya podido mezclar la bebida, fotografías o vídeos de las víctimas. También buscar fotografías en cámaras digitales o móviles, vídeos en móviles y cualquier otra grabación que se haya podido realizar.

En todos los casos en los que media un delito sexual, se debe tener en cuenta lo largo y arduo que se presenta el proceso para la víctima. Es por esto que hay que tenerla presente como protagonista principal a la hora de estipular las recomendaciones más adecuadas.

Como medio de prevención de este tipo de agresiones en nuestro país, es preciso aceptar el uso de la sumisión química en relación con los delitos sexuales, por lo que se debe informar de manera seria a todos los segmentos de la sociedad y realizar campañas de prevención, dirigidas a aquellas personas más vulnerables. Hay que mostrar el problema tal como es y advertir a las víctimas de los lugares y situaciones en los que tienen mayor riesgo de victimización y las precauciones que deben tomar.

Los casos relacionados con agresiones y abusos sexuales son delicados y tienen unas consecuencias "especiales" para las víctimas: son numerosas las secuelas que producen, en especial psicológicas, y citando a Ángel Bajo "*hay que insistir en que no es culpa de ellas. Se encuentran mal creyendo que son las responsables de lo que ha sucedido; por eso los profesionales debemos explicarles que han sido expuestas a sustancias tóxicas y agredidas. Tratamiento médico necesitan poco, lo que precisan es apoyo social y psíquico*"[8]. Por ello, es necesario concienciar y facilitar formación específica a los profesionales que intervienen con la víctima, con el fin de proporcionarle un trato adecuado y minimizar su victimización secundaria, además de establecer protocolos adecuados.

Es conveniente contar con un método universal de recogida de datos relativos a estas agresiones, que facilite su intercambio y estudio a distintos niveles, desde el local hasta el internacional.

Como se ha constatado, este tipo de víctima es propensa a ocultar los hechos por distintos temores, por lo que la cifra oscura en estos delitos es alta, siendo la única forma de aproximarnos a ella la realización de encuestas anónimas.

Finalmente, es necesaria la actuación coordinada entre todos los intervinientes en estos hechos, la intervención de urgencias, de la policía, del médico asistencial, del psicólogo, del jurista, del educador social y del médico forense, entre otros, para conseguir el esclarecimiento de este tipo de delitos.

8. CONCLUSIONES

La comisión de delitos contra la libertad sexual usando métodos de sumisión química está de gran actualidad, debido a ciertos casos mediáticos; no obstante, hace años que este modus operandi se utiliza en España y, en los últimos años, se ha detectado un aumento exponencial. Además, es necesario tener en cuenta la existencia de una cifra negra en hechos de esta índole abundante, bien porque la víctima no denuncia, bien porque no se detectan, bien porque se encuadran erróneamente en otro tipo de delitos.

Las zonas costeras de nuestro país son las más afectadas, junto con Madrid y las islas, coincidiendo con los lugares que suelen concentrar mayor cantidad de turistas extranjeros, así como mayores lugares de ocio y festivos, que acogen grandes

8 González, 2010.

afluencias sociales en las que la víctima está más expuesta a su agresor. De hecho, las discotecas y los locales de recreo nocturnos son uno de los principales focos de acción en estos delitos sexuales mediante sumisión química, junto con la vía urbana y los propios domicilios de víctimas, agresores o desconocidos. En este sentido, las Fuerzas y Cuerpos de Seguridad encargadas de investigar y hacer frente a este tipo de hechos, deben centrar su atención en estos lugares en los momentos más vulnerables a que se produzcan transgresiones en las que medien sustancias, si bien es cierto que resulta imposible controlar la circulación de muchos de estos tóxicos, debido a su facilidad de obtención y disimulación en prácticamente cualquier ambiente y situación.

Es necesario, y en este sentido se está trabajando actualmente en la Unidad Técnica de Policía Judicial de la Guardia Civil, realizar una aproximación seria y exhaustiva al problema, ahondando en el conocimiento de diferentes variables implicadas en este fenómeno que redunden tanto en la persecución de este tipo de delitos como en la prevención a partir del análisis del contexto en el que se produce, así como de las características de víctima y autor. Así, a partir de los perfiles aproximados de las partes que suelen estar implicadas en delitos de este tipo, debe advertirse a mujeres jóvenes de nacionalidad española –más del 60% de los casos conocidos– que frecuenten espacios sociales de carácter nocturno, especialmente en los periodos temporales indicados anteriormente (estivales, fines de semana), de aquellos lugares y situaciones en los que tienen mayor riesgo de victimización, proporcionando las precauciones que deben tomar y las pautas de actuación en caso de sufrir hechos de esta índole –pues las denuncias constituyen el pilar fundamental para conocer y poder perseguir la sumisión química de manera efectiva–.

También debe formarse de forma especializada a los profesionales que atienden a estas víctimas, bien recogiendo las declaraciones o iniciando las diligencias de investigación de los hechos, pues son muchos los padecimientos –tanto físicos como psicológicos– que ya de por sí sufre la persona a la que drogan para cometer una agresión sexual, y conviene minimizar a toda costa su victimización secundaria. Conocer el perfil del autor puede facilitar las labores de indagación y averiguación en estos casos, pues en muchas ocasiones permite acotar el número de sospechosos, facilitando su identificación temprana y detención.

Con todas estas pautas, las instancias policiales, en colaboración con los servicios sanitarios y especialistas de la materia –peritos, forenses…–, deben tratar de dar respuesta a la elevada cifra negra que se esconde tras estos delitos, aumentando progresivamente su visualización –como recogen los datos de los últimos años–, para de esta forma encontrar los métodos más eficaces –y menos dañinos para la víctima– que den una respuesta al problema y reduzcan su prevalencia. Asimismo, sería necesaria una puesta en común entre todos los organismos encargados de recibir e investigar el fenómeno de la delincuencia sexual mediante sumisión química –coordinación entre todos los cuerpos policiales con competencia en esta materia–, para poseer un método universal de recogida de estos datos que hiciese posible su análisis e intercambio a diferentes niveles, tanto a nivel nacional como internacional. Se vuelve así de vital importancia la realización de estudios nacionales que abarquen las estadísticas al completo en poder de todas las fuerzas policiales españolas –únicamente con los datos de la Guardia Civil, se cuenta con alrededor de 240 casos denunciados en nueve años, por lo que es de esperar que esta cifra sea mucho mayor si se incluyen también los registros de Policía Nacional y Cuerpos Autonómicos para estos años,

por ejemplo–, de cara a poder conocer con total exactitud la magnitud del problema, y poder elaborar así pautas más precisas que ayuden a contenerlo.

El presente artículo pretende constituir una primera aproximación al fenómeno, ahondando en las variables más relevantes para la investigación de estos casos, tratando de relacionar lo encontrado con la escasa literatura científica existente hasta el momento y, en su mayoría, centrada en estudios toxicológicos más que en aspectos puramente delincuenciales.

Es de vital importancia que las Fuerzas y Cuerpos de Seguridad responsables de investigar estos delitos se centren en el momento y en el lugar de comisión, de cara a su prevención o temprana identificación, ya no solo por la propia gravedad del acto para quien lo sufre, sino para darle mucha más visibilidad de la que tiene actualmente. No obstante, anticiparse a estos delitos implica una elevada dificultad, ya que, a pesar de poder dilucidar un perfil para víctima y autor, como se ha expuesto en este trabajo, e incluso los lugares más proclives para su comisión, existen otras variables relacionadas con las propias sustancias empleadas –su facilidad de obtención y disimulación para la víctima, su acción rápida y corta duración…– que hacen prácticamente imposible poder controlar cuándo y en qué situación se van a producir hechos de este tipo. Análisis conjuntos de factores delincuenciales y toxicológicos, característicos de los delitos de sumisión química, podrían resultar de gran utilidad para atenuar su prevalencia y contribuir así de manera positiva a la lucha contra este fenómeno en la sociedad actual.

BIBLIOGRAFÍA

315/2011 (Tribunal Supremo. Sala de lo Penal 24 de Marzo de 2011).

831/2010 (Tribunal Supremo. Sala de lo Penal 23 de Septiembre de 2010).

833/2009 (Tribunal Supremo. Sala de lo Penal 28 de Julio de 2009).

861/2010 (Tribunal Supremo. Sala de lo Penal 13 de Octubre de 2010).

Bañón González, R., Bravo Serrano, B., García Repetto, R., Martín Castillo, A., Quintela Jorge, O., & Soria Sánchez, M. (2012). *Instrucciones de actuación en casos de agresión sexual con sospecha de intoxicación*. Ministerio de Justicia.

Bañón González, R., Bravo Serrano, B., García Reppetto, R., Martín Castillo, A., Quintela Jorge, O., & Soria Sánchez, M. (2012). *Instrucciones de actuación en casos de agresión sexual con sospecha de intoxicación.* Ministerio de Justicia.

Berenguer, E., Suárez, C., & Rodríguez, M. (2001). *Los delitos contra la libertad e indemnidad*. Valencia: Tirant Lo Blanch.

Butler, B., & Welch, J. (2009). *Drug-facilitated sexual assault*. CMAJ, 180: 4-493.

Cadena COPE. (9 de Octubre de 2012). *Ivoox. audioKiosco.* Recuperado el 10 de Noviembre de 2012, de http://www.ivoox.com/130-agresiones-sexuales-sumision-quimica-al-ano-audios-mp3_rf_1482275_1.html

Comisión de Estupefacientes. (2010). Cooperación internacional para combatir la administración subrepticia de sustancias psicoactivas relacionadas con la agresión

sexual y otros actos delictivos. *53º período de sesiones* (págs. 1-4). Viena: Consejo Económico y Social. Naciones Unidas.

Comisión de Justicia. (21 de Abril de 2010). *Diario de Sesiones del Congreso de los Diputados(522)*, 31-33. Madrid, España.

Cruz Landeira, M., Quintela Jorge, O., & López Rivadulla, M. (2008). Sumisión química: epidemiología y claves para su diagnóstico. *Revista de Medicina Clínica, 131*(20), 783-789.

Cruz Landeira, M., Quintela Jorge, O., & López Rivadulla, M. (2008). *Sumisión química: epidemiología y claves para su diagnóstico*. Revista de Medicina Clínica, 131(20): 783-789.

García-Caballero, C., Cruz-Landeira, A., & Quintela-Jorge, Ó. (2014). *Sumisión química en casos de presuntos delitos contra la libertad sexual analizados en el Instituto Nacional de Toxicología y Ciencias Forenses (Departamento de Madrid) durante los años 2010, 2011 y 2012*. Revista Española de Medicina Legal, 40(1): 11-18.

García-Repetto, R., & Soria, M. (2011). Sumisión Química: reto para el toxicólogo forense. *Revista Española de Medicina Legal, 37*(3), 105-112.

García-Repetto, R., & Soria, M. (2011). *Sumisión química: reto para el toxicólogo forense*. Revista Española de Medicina Legal, 37(3): 105-112.

García-Repetto, R., & Soria, M. (2013). *Consideraciones toxicológicas sobre supuestos casos de sumisión química en delitos de índole sexual en el sur de España entre los años 2010-2012*. Revista Española de Medicina Legal, 40(1): 4-10.

González, M. (20 de Junio de 2010). En dos de cada diez agresiones sexuales a mujeres se utilizan drogas para someter a la víctima. *Diario de Noticias*, pág. 6.

Horwath, M., & Brown, J. (2005). *Drug assisted rape and sexual assault: definitions, conceptual and methodological developments*. Investigative Psychology Offender Profiling, 2: 10-203. http://www.erowid.org/psychoactives/assault/assault_article3.shtml

Hurley, M., Parker, H., & Wells, D.L. (2006). *The epidemiology of drug facilitated sexual assault*. Clinical Forensic Medicine, 13: 5-181.

Instituto Nacional de Toxicología y Ciencias Forenses (2012). Protocolo de actuación para casos de agresión sexual con sospecha de intoxicación. (Orden JUS/1291/2012, de 13 de mayo).

Instituto Nacional de Toxicología y Ciencias Forenses (2012). *Protocolo de actuación para casos de agresión sexual con sospecha de intoxicación* (Orden JUS/1291/2012, de 13 de mayo).

Instituto Vasco de Medicina Legal. (2011). Anulación de la voluntad de la víctima mediante el uso de fármacos, drogas o cualquier otra sustancia natural o química. En G. Portero Lazcano, A. E. Abasolo Tellería, M. De Francisco Maiz, A. Sudupe Moreno, A. Hidalgo Ocaña, & S. C. Vasco (Ed.), *Agresiones y abusos sexuales en Bizkaia. Víctimas Bienio 2009-2010* (1ª ed., pág. 252). Vitoria: Gráficas Ulzama.

International Association of Chiefs of Police, I. (2004). Investigating Sexual Assaults Part II: Investigative Procedures. En *Training Key* (págs. 1-6). Alexandria, Estados Unidos.

International Association of Chiefs of Police, I. (2004). *Investigating Sexual Assaults Part II: Investigative Procedures*. En Training Key (págs. 1-6). Alexandria, Estados Unidos.

López Rivadulla, M., Cruz, A., Quintela, O., De Casto, A., Concheiro, M., Bermejo, A., & Jurado, C. (2005). Sumisión química: antecedentes, situación actual y perspectivas. Protocolos de actuación para estudios multicéntricos. *Revista de Toxicología Asociación Española de Toxicología, 22*(1), 119-126.

López Rivadulla, M., Cruz, A., Quintela, O., De Casto, A., Concheiro, M., Bermejo, A., & Jurado, C. (2005). *Sumisión química: antecedentes, situación actual y perspectivas. Protocolos de actuación para estudios multicéntricos*. Revista de Toxicología, Asociación Española de Toxicología, 22(1): 119-126.

M. Pittel, S., & Spina, L. (27 de Marzo de 2009). Recuperado el 10 de Noviembre de 2012, de The Vaults of Erowid:

Olszewski, D. (2008). *Sexual assaults facilitated by drugs or alcohol.*Recuperado el 2012, de European Monitoring Centre for Drugs and Drug Addiction: http://www.emcdda.europa.eu/

Operation Matisse: Investigating Drug Facilitated Sexual Assault (2006). London: Association of Chief Police Officers.

Organización Panamericana de la Salud. (2003). La violencia sexual. En E. Krug, L. Dahlberg, J. Mercy, A. Zwi, & R. Lozano (Edits.), *Informe Mundial sobre la violencia y la salud* (págs. 161-197). Washington D.C., Estados Unidos .

Ortiz De La Tierro, Z. (1 de Octubre de 2012). Recuperado el 10 de Noviembre de 2012, de sitio Web diariovasco.com: http://www.diariovasco.com/20121001/mas-actualidad/sociedad/sumision-quimica-violaciones-impunes-201210011000.html

Payne-James, J., & Rogers, D. (2002). *Drug-facilitated sexual assault, "ladettes" and alcohol*. JR Society Medicine, 95: 7-326.

Read, K.M., Kufera, J.A., Jackson, M.C., & Dischinger, P.C. (2005). *Population-based study of police-reported sexual assault in Baltimore, Maryland*. A.M. Emergency Medical, 23: 8-273.

Sancho de Salas, M., Xifró Collsamata, A., Bertomeu Ruiz, A., & Arroyo Fernandez, A. (2012). Sumisión química con finalidad sexual: nuevos aspectos legales. *Revista Española de Medicina Legal*.

Sanders, J. (Septiembre de 1998). Training bulletin. Drug facilitated sexual assault investigations. (S. D. Department, Ed.) San Diego, EE.UU.

Sanders, J. (Septiembre de 1998). T*raining bulletin. Drug facilitated sexual assault investigations* (S. D. Department, Ed.). San Diego, EE.UU.

Serie A: Proyectos de Ley. (18 de Marzo de 2010). *Boletín Oficial de las Cortes Generales(52-9)*, 156. Madrid, España.

The National Center for Women and Policing. (2001). Assault, Successfully Investigating Acquaintance Sexual. A National Training Manual for Law Enforcement. Estados Unidos.

Tiffon Nonis, B.-N. (16 de Diciembre de 2009). *Directorio de profesionales Togas.* Recuperado el 10 de Noviembre de 2012, de http://www.togas.biz/articulos/Peritaje/Peritaje/La-Sumision-Quimica.html

Torres, Y., Aler, M., Pata, A., Dominguez, A., Sanz, P., & Gisbert, M. (Enero de 2007). Factores que afectan al análisis biológico de las muestras de agresiones sexuales. *Cuadernos de Medicina Forense, 13*(47), 48-49.

Welner, M. (2001). *The perpetrators and their modus operandi*. En: LeBeau, M.A., Mozayani, A. (2009). *Drug-facilitated sexual assault – A forensic handbook*. London: Academic Press, pp. 39-71.

Fecha de recepción: 25/05/2018. Fecha de aceptación: 25/06/2018

HISTORIA DEL TERRORISMO YIHADISTA: DE AL QAEDA AL DAESH

JUAN AVILÉS FARRÉ

Editorial Síntesis, Madrid, 2017, 248 páginas.

ISBN: 9788491710578

El profesor Juan Avilés Farré nos presenta una obra de obligada lectura para quienes investigan bien desde posiciones académicas, bien desde aquellas otras de corte más operativo, el fenómeno del terrorismo yihadista. El autor efectúa un brillante recorrido cronológico por su trayectoria, analizándolo dentro del contexto histórico concreto en el que se produce. Asimismo, consciente de la complejidad de su objeto de estudio, facilita la comprensión del mensaje a través de una narración dinámica y la presentación de un resumen al inicio de cada capítulo en el que anticipa las cuestiones principales que abordará, todo ello sin olvidar un respeto escrupuloso hacia el método científico y aportando abundante bibliografía y fuentes.

El doctor Avilés enfatiza algunos hechos conocidos pero que revisten la máxima transcendencia. En primer lugar, desde una perspectiva general, la preocupación existente en la sociedad ante la posibilidad de un ataque terrorista, incrementándose aquella en los momentos posteriores a la comisión de un atentado: *"el terrorismo suicida presenta dos ventajas: una en el plano operativo, ya que facilita el acercamiento del terrorista a su objetivo sin ser detectado; y otra en el plano psicológico, ya que demuestra la total entrega y determinación de quien lo protagoniza, con el consiguiente impacto negativo en la moral del enemigo"* (p.225).

En segundo lugar, de una manera particular subraya dos rasgos complementarios del terrorismo yihadista. Por un lado, que ya existía antes del 11-S, en particular en Asia y en África (sobresaliendo al respecto los atentados cometidos contra las embajadas de Estados Unidos en Tanzania y Kenia en 1998). Asimismo, en la década de los años noventa del pasado siglo la yihad actuaba en Bosnia (en el contexto de la guerra de los Balcanes) y Chechenia (desafiando a la "recién nacida" Federación rusa). Por otro lado, señala que la mayor parte de sus víctimas son ciudadanos musulmanes: *"la prioridad informativa que los medios de comunicación occidentales dan a los atentados que se producen en Estados Unidos o la Unión Europea puede generar la falsa percepción de que el terrorismo yihadista se dirige sobre todo contra Occidente. En realidad la mayoría de sus víctimas son musulmanas, suníes o chiíes"* (p. 187).

No obstante, el mundo occidental tiene razones poderosas para preocuparse. En efecto, como recoge el profesor Avilés Farré, el fenómeno de la radicalización (y la auto-radicalización) permea sobre sus sociedades, en particular entre los inmigrantes musulmanes de segunda y tercera generación.

Ideas, personajes y organizaciones

¿Por qué el terrorismo yihadista atenta contra poblaciones musulmanas? ¿No supone ello, en teoría, una contradicción? Para responder a estos complejos interrogantes Juan Avilés explica la tergiversación del Islam llevada a cabo por los primeros teóricos de la yihad, para quienes la lucha armada suponía el único camino para que

la citada religión volviera a sus orígenes. En consecuencia, la yihad no solo debía dirigirse contra ateos o cristianos sino también contra gobernantes musulmanes, puesto que *"que habrían abandonado la senda marcada por Dios a Mahoma"* (p.12).

Esta última idea hace referencia a una dialéctica fundamental: enemigo lejano (Occidente, Rusia) vs enemigo cercano (países musulmanes). Al respecto, los yihadistas conciben la democracia como una forma de gobierno impía, porque atribuye al pueblo una soberanía que corresponde únicamente a Dios (p.25). Consecuentemente *"el odio hacia occidente que profesa el islamismo radical se basa en un rechazo hacia valores esenciales de nuestra cultura, como las libertades, la emancipación femenina y la independencia de la moral pública y privada respecto a las imposiciones religiosas"* (p. 27).

Por tanto, quienes propagan el terrorismo yihadista parten de la existencia de dos conceptos contradictorios: Islam vs democracia. Esto se observa en los formuladores iniciales de la yihad, quizás desconocidos para el gran público, pero cuyas doctrinas asumieron posteriormente Al Qaeda o el Daesh, y a los que el autor dedica varias páginas para explicar sus ideas. Se trata de Sayyid Qutb (sostenía que las sociedades musulmanas han entregado el poder legislativo a los hombres, cuando pertenece a Dios en exclusiva), Muhammad Abd al Salam Faraj (partidario de combatir al enemigo cercano antes que al lejano para *"establecer las leyes de Alá en nuestra tierra y hacer que domine la palabra de Alá"* (p. 218-219) y Abdullah Azzam (efectuó un llamamiento a los musulmanes de todos los países para que se unieran y combatieran contra la URSS en la guerra de Afganistán).

A partir de ahí, profundiza en organizaciones y personajes sobradamente conocidos, como es el caso de Al Qaeda y Bin Laden (cuyo perfil biográfico nos traza), rechazando un mantra que ha penetrado en el imaginario colectivo: la CIA no creó Al Qaeda, ni tampoco otorgó un rol dirigente en dicha organización terrorista a Bin Laden, subraya Juan Avilés.

Sin embargo, Al Qaeda sí que significó un cambio en la estrategia terrorista desarrollada hasta entonces, pues su objetivo radicó en asesinar al mayor número de personas para aparecer en los medios. Este fenómeno lo explica en los siguientes términos el autor: *"si había más de un atentado simultáneo, su impacto se multiplicaría y el empleo de terroristas suicidas no solo resultaría útil en el terreno operativo, sino que incrementaría la sensación de amenaza, al demostrar de manera irrefutable la convicción profunda de quienes estaban dispuestos a dar su vida en la lucha. En el ambiente fanatizado de los campos yihadistas de Afganistán no faltaban los aspirantes al martirio y algunos consideraban incluso que una misión suicida era el más alto honor que se les podía encomendar"* (p.80).

En íntima relación con esta idea, el autor se detiene en la influencia desempeñada por la guerra de Irak a la hora de incentivar el terrorismo yihadista. En este sentido, el profesor Avilés de nuevo se muestra políticamente incorrecto puesto que descarta que el control del petróleo fuera la razón fundamental de la intervención norteamericana, otro mantra sobradamente consolidado entre amplios sectores de la opinión pública. Por el contrario, el factor que llevó a la Administración Bush a introducirse en un escenario como el de Irak residió en la búsqueda del binomio estabilidad-seguridad en Oriente Medio, siguiendo las tesis defendidas por el sector "neocon" cercano a George W. Bush (p.109).

Sin embargo, Estados Unidos fue incapaz de ofrecer una respuesta eficaz a los problemas que generaba ese Irak post-Saddam Hussein. Igualmente, el recurso sistemático a la represión favoreció una mayor adscripción a la causa yihadista, lo que multiplicó la inestabilidad regional, como corroboró el protagonismo adquirido por el Daesh en los últimos años de gobierno de Barack Obama.

Entre el ocaso (relativo) de Al Qaeda y el éxito (inicial) del Daesh irrumpieron las denominadas "Primaveras Árabes", las cuales disecciona el autor de manera sobresaliente, partiendo de un hecho fundamental: en el origen de aquellas, el yihadismo tuvo una influencia marginal. En efecto, fueron los factores económicos (pobreza de amplias capas sociales y ausencia de expectativas profesionales para la juventud) y políticos (corrupción de sus gobiernos que si bien durante las décadas previas dotaron de estabilidad a sus países, ello había sido a costa de eliminar cualquier atisbo de democracia) los que las posibilitaron. Haciendo balance, solo en Túnez han triunfado las "Primaveras Árabes".

Daesh: protagonismo, crisis y cautelas necesarias

Con la irrupción y consolidación del Daesh a partir de 2014 se inició un nuevo incremento de atentados terroristas. Con respecto a Al Qaeda, introdujo ciertas novedades que multiplicaron la letalidad sus acciones liberticidas, destacando al respecto la financiación vía secuestros y petróleo o la férrea centralización organizativa. Además, el carácter rudimentario de sus atentados encerraba una ventaja mayúscula: *"la facilidad de alquilar un vehículo y lanzarlo contra una multitud ha convertido este método en uno de los más letales en Europa, donde no es tan fácil procurarse explosivos"* (p. 201). Todo ello sin olvidar que "*se trató de ataques fáciles de organizar y realizados por residentes locales. Ello supone una amenaza difusa, preocupante por la dificultad que implica identificar a los agresores potenciales, que pueden mantener un perfil muy bajo hasta el momento del crimen"* (p. 202). Lejos del triunfalismo, Juan Avilés advierte que, aunque pierda el territorio del califato, ello no supone necesariamente su desaparición *"porque puede mantenerse como una organización puramente terrorista"* (p.189).

En conclusión

Una obra sobresaliente y rigurosa que disecciona con precisión un fenómeno tan complejo como el terrorismo yihadista, rechazando toda equidistancia o condescendencia en el tratamiento hacia el mismo. El doctor Avilés Farré descompone los diferentes elementos que lo integran, lo que le permite determinar las características de las organizaciones que se han constituido en exponentes de este tipo de terrorismo, mostrando sus diferencias y semejanzas.

Alfredo Crespo Alcázar

Profesor del Máster de Relaciones Internacionales, Universidad Antonio de Nebrija, Madrid.

LA SOCIEDAD ARMADA

SALVADOR GINÉ

Ediciones Corona Borealis, 2017, 251 páginas.

ISBN: 9788494606175

He de reconocer que cuando me invitaron a leer y escribir mi análisis sobre este libro no pensé, ni por asomo, que encontraría en su interior un repaso exhaustivo de la historia de los Estados Unidos, dado su manejable formato y su tamaño de letra, muy agradable para la lectura. La cantidad de fechas, datos y detalles que aporta resulta abrumadora, por lo que hay que destacar la capacidad de síntesis su autor.

Apunta como posible semilla del *"derecho a portar armas"* una obligación instaurada en Inglaterra, allá por el año 605, y hace un repaso de cómo ha evolucionado la relación entre la sociedad americana y las armas de fuego, dependiendo del momento de su historia, desde que en 1791 la segunda enmienda de la Constitución de los Estados Unidos reconociera este derecho a la ciudadanía, cuya mala redacción no parece aclarar realmente si existe limitación alguna al derecho a llevar armas. Lo cierto es que esa lectura, convenientemente interpretada, ha convertido a Estados Unidos en el país de las armas, con un total de 4.436.096 permisos concedidos en 2016 según la ATF.

Esta relación con las armas tan estrecha afecta transversalmente a todos los aspectos de la vida de los americanos: socialmente se acepta y convive con normalidad el hecho de portar o poseer armas, siempre desde la escusa del derecho a la autodefensa, hasta extremos que para los europeos resultan aberrantes, como la posibilidad de adquirir un arma de fuego casi en cualquier tipo de establecimiento abierto al público. La incidencia de las armas entre las causas de muerte de la población americana se sitúa en el rango de las víctimas mortales de accidentes de tráfico, ambas con algo más de 30.000 fallecimientos. No en vano, según se indica en el libro, el ratio de armas por cada 100 habitantes es de 88,8.

Resulta significativo cómo la preocupación de la sociedad por su seguridad provocó que se duplicaran las ventas de armas cortas tras el 11-S.

En el plano criminológico y policial, el autor nos descubre el *modus operandi* de los cárteles mejicanos para proveerse ilegalmente de armas muy peligrosas, bien por su calibre, bien por su capacidad de fuego, como son los fusiles AR15 (versión civil del M16) y el AK-47 (Kalashnikov), o la conocida pistola belga FN 5.7, cuya munición, por su forma abotellada, hace que su proyectil ojival agudo de pequeño calibre (poco mayor que un .22) consiga atravesar los chalecos de uso policial.

Esta actividad supone un quebradero de cabeza para la ATF, no solo por el hecho en sí del tráfico de armas, sino porque estas pueden volver a ser utilizadas en contra de los propios policías americanos. Siendo este otro de los aspectos recogidos en este libro, no solo en lo relativo a cárteles mejicanos, sino en términos generales, desvelando que entre 2006 y 2015, fallecieron un total de 454 agentes de policía por arma de fuego, a pesar de que 311 de ellos iban equipados con chalecos antibala.

Otra perspectiva del máximo interés que presenta es la evolución de la normativa, que en ocasiones ha tratado de regular de manera restrictiva el uso de las armas, sin lograr un acuerdo entre republicanos y demócratas, recibiendo además las presiones de la Asociación Nacional del Rifle (NRA), y es que parece que no todo son desventajas, la industria armamentística en Estados Unidos reporta pingües beneficios a los que no resulta fácil renunciar.

Se trata de un libro interesante, bien documentado y que facilita una amplia bibliografía sobre el tema, que permite al lector tomar perspectiva sobre la problemática de la proliferación de las armas en Estados Unidos, su génesis y consecuencias, a pesar de los esfuerzos por legislar de una manera más eficiente, al objeto de disminuir la prevalencia de incidencias con el uso de armas de fuego.

Manuel Jesús Ruano Rando

Cabo 1º, experto en Balística Forense y Criminólogo

OBTENCIÓN Y VALORACIÓN DEL TESTIMONIO PROTOCOLO HOLÍSTICO DE EVALUACIÓN DE LA PRUEBA TESTIFICAL (HELPT)

JOSÉ LUIS GONZÁLEZ Y ANTONIO L. MANZANERO

Ediciones Pirámide (Grupo Anaya S.A.),2018, 295 páginas.

ISBN: 9788436839289

El libro Obtención y valoración del testimonio, ofrece un protocolo holístico de evaluación de la prueba testifical (HELPT), como bien reflejan sus autores, José Luis González y Antonio L. Manzanero, en el título de este manual que, editado por Ediciones Pirámide, nace con vocación de ayudar a diferentes profesionales en esos difíciles quehaceres diarios de las investigaciones criminales.

Policías, fiscales, abogados, jueces y psicólogos forenses, además de todos los que participan de una u otra manera en actividades relacionadas con la investigación, van a encontrar a lo largo de los nueve capítulos que componen esta propuesta, junto a los cinco apéndices y numerosísimas referencias, una guía más que detallada de lo que se pueden encontrar y cómo afrontarlo. Y es que los mismos autores, en el prólogo, ya nos anticipan sus intenciones a la hora de afrontar las líneas que siguen poniendo “el foco en lo más práctico, proporcionando, hasta donde se puede, guías y sugerencias de intervención de cómo hacer las cosas para conseguir los mejores testimonios posibles, tanto de los testigos y de las víctimas como de los inculpados”.

En este sentido, no solo trabajan ese enfoque holístico que nos anticipan, sino que nos enseñan cómo recopilar y analizar la información para la evaluación pericial de la validez de la prueba testifical, además de todos los factores y procedimientos de la entrevista de investigación, desde las que se realizan a víctimas vulnerables, al interrogatorio de inculpados, pasando por la identificación de agresores, a los factores de influencia sobre la exactitud de las declaraciones, la evaluación de las habilidades para testificar de los testigos, por ejemplo, y las habilidades de comunicación interpersonal, entre otros.

Sus perfiles profesionales refrendan este manual. No en vano Antonio Manzanero es doctor en Psicología y profesor titular del Grado en Criminología y del Grado en Psicología en la Universidad Complutense de Madrid, además de director del Grupo de Investigación UCM en Psicología del Testimonio, director del Anuario de Psicología Jurídica y del Grupo oficial UCM de Investigación sobre Psicología del Testimonio, mientras que José Luis González es doctor en Psicología y máster en Ciencias Forenses y en Psicología Clínica, así como teniente coronel de la Guardia Civil con veinte años de servicio en Policía Judicial y fundador de la Sección de Análisis del Comportamiento Delictivo, en 1995, y de los Equipos Mujer Menor en 1996. Durante esos años, ha podido trabajar con numerosos testigos, víctimas e inculpados, probando sobre el terreno las recomendaciones que nos trasladan y que han visto que son efectivas. Actualmente es jefe de área en el Gabinete de Coordinación y Estudios de la Secretaría de Estado de Seguridad del Ministerio del Interior.

Su específica formación y su vocación docente hace que también hayan enfocado estas páginas a sus alumnos, sobre todo los del Máster de la Universidad Autónoma de Madrid, de la Universidad Complutense y de la Universidad a Distancia, a los que agradecen que les hayan ayudado con su interés y preguntas. Sin duda encontrarán un manual útil, pragmático y minucioso, hasta en el más mínimo detalle, que va a "contribuir a la mejora de los procedimientos de obtención de testimonios y de valoración de las pruebas testificales", pero que sigue en constante evolución, pues sus autores están abiertos a recibir críticas constructivas, para seguir trabajando y actualizando los contenidos que nos presentan, según se vayan produciendo avances significativos.

Los autores nos comentan en el prólogo su lógica a la hora de estructurar en nueve capítulos el manual. No ha sido en absoluto al azar. Nos señalan que en el capítulo 1 analizan la importancia que tiene la prueba testifical, además de la necesidad de obtenerla y valorarla con las máximas garantías científicas posibles. Es ahí donde proponen la aproximación holística (HELPT) y explican con detalle los fundamentos y fases de este protocolo, sobre todo en lo referente a la valoración de la prueba, que detallan en el capítulo 2, ejemplificando la tarea de revisión de los antecedentes documentales de cada caso en uno de abuso sexual infantil, uno de los escenarios más difíciles para los investigadores.

Para ello, recuerdan los factores de influencia que suelen afectar a todo testimonio en el capítulo 3, por la importancia de conocerlos y documentarlos antes de obtener los testimonios, pues el entrevistador tendrá criterios que le ayudarán posteriormente a la evaluación de lo relatado. En este sentido, el capítulo 4 valora las habilidades para testificar y, con casos difíciles, muestra cómo es posible obtener un buen testimonio manejando bien los escenarios que correspondan. Y en el capítulo 5 encontramos las primeras recomendaciones prácticas para obtener los testimonios, que ya en el capítulo 6 se materializan en "un procedimiento de entrevista de investigación fundamentado en las aportaciones científicas sobre la Entrevista Cognitiva" en base a la guía de entrevista de investigación probada con éxito en la Guardia Civil.

A continuación, el capítulo 7 ayuda a perfeccionar las destrezas investigadoras (correspondientes a las habilidades comunicativas básicas y a los fundamentos generales de la entrevista de investigación), con más recomendaciones en casos de víctimas vulnerables y especiales, incluyendo las de violencia sexual y/o las de violencia de pareja.

El capítulo 8 se centra en la identificación de los inculpados que, en el siguiente y último capítulo, seguirán siendo protagonistas, pues se realiza un extenso repaso de las técnicas de interrogatorio para la obtención de su testimonio, entre otras cuestiones.

Finalmente, los cinco anexos que aportan sus autores, tremendamente prácticos, además de las referencias, facilitan a los lectores que lo deseen la capacidad de ampliar todo lo señalado.

En definitiva, una excepcional cita con la Criminología, desde el punto de vista más pragmático y útil, de cara a la obtención y valoración del testimonio, no solo interesante para los profesionales, sino también para todos aquellos que sienten interés por esta materia y por conocer cómo se realizan este tipo de entrevistas.

Ana María Ruano

Periodista del CAP

DATOS SOBRE LOS AUTORES DE ESTE VOLUMEN POR ORDEN ALFABÉTICO

José María Blanco Navarro es director de Ciberinteligencia Estratégica, en Prosegur Ciberseguridad, desde enero de 2018. Previamente, durante casi 10 años, fue director del Centro de Análisis y Prospectiva de la Guardia Civil. Licenciado en Derecho y en Ciencias Empresariales. Master en Análisis de Inteligencia, Dirección de Recursos Humanos y Prevención de Riesgos Laborales. Experto en Gestión del Conocimiento. Codirector del Área de Inteligencia y Estudios Estratégicos del Instituto de Ciencias Forenses y de la Seguridad de la Universidad Autónoma de Madrid, y codirector del título de Experto en Análisis de Inteligencia. Investigador en proyectos financiados por la Comisión Europea (FP7 y H2020) en materias como terrorismo, radicalización y crimen organizado. Profesor, conferenciante y autor de numerosas publicaciones en materia de seguridad e inteligencia. jose-maria.blanco-navarro@prosegur.com

José Leandro Martínez-Cardós está especializado en Derecho Administrativo, Derecho Procesal–Arbitral y en Derecho Mercantil del Transporte, Marítimo y Aeronáutico. Abogado en Ejercicio. Letrado Mayor del Consejo de Estado. Del Cuerpo Jurídico Militar. Doctor en Derecho y en Geografía e Historia. Licenciado en derecho y en Ciencias Políticas y Sociología. Diplomado en Contabilidad Pública y en Derecho Comunitario Europeo. Profesor titular de la Escuela de Práctica Jurídica de la Universidad Complutense de Madrid. Es árbitro de la Corte Civil y Mercantil de Arbitraje desde su fundación en 1988; de la Corte de Arbitraje del Colegio de Abogados de Madrid; del Tribunal Arbitral de la Construcción y del Tribunal Arbitral de la Contratación Pública de la Asociación Europea de Arbitraje (AEADE). También es Académico correspondiente de la Real Academia de Jurisprudencia y Legislación desde 1987. jlmcruiz@gmail.com

Olga Moreno Rodríguez, sargento de la Guardia Civil. Licenciada en Psicología por la Universidad de Granada. Diplomada en Policía Judicial. Especialista EMUME (Mujer y Menor), realizando investigaciones criminales en casos de malos tratos graves, abusos y agresiones sexuales, abusos y agresiones sexuales a menores y personas con discapacidad psíquica, abandono y sustracción de menores, trata de seres humanos con fines de explotación sexual, laboral o mendicidad, pornografía infantil, delincuencia juvenil, así como cualquier intervención e investigación policial con víctimas sensibles. Destinada en la actualidad en la Unidad Técnica de Policía Judicial-Grupo de Análisis Criminal de delitos contra las Personas-Sección EMUME Central, donde realiza el seguimiento y coordinación a nivel nacional de los casos que investigan los EMUMES territoriales, así como funciones de asesoramiento y formación a los mismos. omoreno@guardiacivil.es

Jesús Narciso Núñez Calvo, coronel de la Guardia Civil, jefe de la Comandancia de Cádiz desde 2015, es doctor en Historia por la UNED y autor y coautor de una decena de libros, monografías e innumerables artículos sobre Historia Militar y de la Guardia Civil en diferentes medios y revistas especializadas. En este sentido, ha sido ponente y conferenciante en medio centenar de cursos y jornadas académicas y universitarias, tanto en España como en el extranjero. De hecho ha participado en operaciones internacionales de cooperación policial y asistencia técnica en

Venezuela, Nicaragua y Guatemala, así como de mantenimiento de la paz en Bosnia-Herzegovina, Irak y Líbano, lideradas por la Unión Europea, Naciones Unidas y la OTAN. jenunez@guardiacivil.es

Joaquín Mariano Pellicer Balsalobre es capitán en el Departamento de Química y Medio Ambiente del Área de Espectroscopia del Servicio de Criminalística de la Guardia Civil. Es licenciado en Ciencias Biológicas por la Universidad de Murcia y también en Bioquímica, por la Universidad de Zaragoza, además de máster en Paz, Seguridad y Defensa, por el Instituto Universitario Gutiérrez Mellado-UNED, y magister universitario en Seguridad y Defensa, por la UCM-CESEDEN, entre otros. Cuenta con multitud de publicaciones de diversa índole y ha participado en numerosos seminarios y conferencias, por ejemplo de formación en toma de muestras de ADN para equipos EMUME de Policía Judicial de la Guardia Civil o en actividades formativas y de reciclaje de personal de la Administración de Justicia y de las Fuerzas Armadas. jmpellicer@guardiacivil.es

José Manuel Petisco Rodríguez es comandante jefe del Área Docente de la Escuela Militar de Ciencias de la Educación (EMCE) de la Academia Central de la Defensa (ACD). Licenciado en Psicología por la UAM, posee entre otros el diploma en Aptitud Pedagógica, Formación de Evaluadores de la Enseñanza Militar, Comunicación Social, Diseño de Planes de Estudio, certificado en Formación de Auditores Internos AUDIT, Técnicas Estadísticas y de Aptitud en Formación de tutores on-line. Es Profesor Honorífico Investigador de la Universidad de Alcalá desde el curso académico 2016-17. Ha colaborado como profesor en distintos programas de postgrado, como en el “Experto universitario en comportamiento no verbal” de la Universidad Camilo José Cela, o en el “Máster en comportamiento no verbal y detección de la mentira”, de la Universidad a Distancia de Madrid (UDIMA). También ha sido profesor en la primera edición del “Máster en Inteligencia Económica y Análisis Experto” de la Universidad Francisco Vitoria/Atenea, entre otros. Recientemente ha codirigido un manual sobre criminología y es autor de diversos libros, capítulos de libro, artículos y blogs relativos al comportamiento no verbal, la comunicación en el aula, la detección psicofisiológica del engaño, la memoria de testigos oculares, o la tutoría on-line. comportamiento.no.verbal@gmail.com

José Manuel Quintana Touza, capitán de la Guardia Civil destinado en la Unidad Técnica de Policía Judicial desde 2008, en la Sección de Análisis de Comportamiento Delictivo (SACD). Licenciado en Psicología, y Diplomado en Criminología por la Universidad de Santiago de Compostela. Máster en Terapia de Conducta por la Universidad Nacional de Educación a Distancia; Máster en Ciencias Forenses por la Universidad Autónoma de Madrid y Máster en Intervención Psicológica en el Desarrollo y la Educación por la UNED. En la Sección realiza apoyos técnico-operativos a las Unidades de Policía Judicial del Cuerpo de todo el territorio nacional (UCO y UOPJ,s), en ámbitos como la realización de indagatorias con víctimas o implicados sensibles en delitos violentos o graves, con especiales circunstancias, como niños de muy corta edad, testigos o menores traumatizados, personas con algún tipo de alteración psíquica o discapacidad intelectual, etc. para facilitar la obtención de testimonios extensos y fiables y la valoración posterior de la credibilidad de estas declaraciones; intervención con detenidos de características peculiares (trastornos mentales, psicópatas, pederastas, etc.) a fin de facilitar su toma de declaración; realización de perfiles criminológicos de sospechosos en el marco de investigaciones, tanto en los

supuestos de sospechosos conocidos como no conocidos, así como la elaboración de informes criminológicos acerca de diferentes tipos de delitos contra las personas. También realiza actividades de formación en cursos de especialización del cuerpo de diferente naturaleza. jmqtouza@guardiacivil.es

Manuel Ramos Romero es sargento de la Guardia Civil y miembro de la Sección de Análisis del Comportamiento Delictivo de la Unidad Técnica de Policía Judicial. Licenciado en Criminología, Máster en Análisis del Comportamiento y Especialista en Psicología Criminal. Formador en el Curso de especialización de Policía Judicial y en jornadas y actividades formativas de la Especialidad. Profesor del Máster de Ciencias Forenses: Análisis e investigación Criminal de la Universidad Autónoma de Madrid y del Máster de Perfilación Criminal de la Universidad a Distancia de Madrid (UDIMA). Ponente en multitud de Congresos y Jornadas relacionadas con las Ciencias del Comportamiento. manuelrr@guardiacivil.es

NORMAS PARA LOS AUTORES

Los trabajos que se remitan para su publicación en la Revista "Cuadernos de la Guardia Civil" deberán ser inéditos y no estar pendientes de publicación en otra revista. No obstante, previa solicitud al Centro de Análisis y Prospectiva, podrán ser publicados en otro medio, una vez otorgada autorización escrita en tal sentido por el Director de la revista.

Los criterios para la presentación de textos son los siguientes:

EXTENSIÓN. Un mínimo de 6.000 palabras y un máximo de 9.000 a espacio y medio, en DIN A-4.

TÍTULO, AUTORÍA Y AFILIACIÓN. En la primera página constará el título, en mayúsculas y negrita, y, debajo, el nombre del autor (en mayúsculas), indicando puesto de trabajo y profesión.

Se adjuntará adicionalmente breve CV del autor de 10 o 15 líneas y dirección de correo electrónico.

RESUMEN Y PALABRAS CLAVE. Precedido de la palabra "Resumen" se incluirá a continuación un extracto en castellano de unas 10-15 líneas. A continuación, en otro párrafo, un "Abstract", traducción al inglés del resumen anterior. En el párrafo siguiente se incluirán las palabras clave, en un máximo de cinco, precedidas por la expresión "Palabras clave". A continuación, en párrafo nuevo, esas palabras clave en inglés precedidas de la expresión "Keywords".

ESTRUCTURA. Los trabajos se dividirán en apartados y secciones (2 niveles), con su propio título, numerados. Se titularán en mayúscula negrita en el primer nivel de jerarquía y con mayúscula redondo en el segundo (sin negrita). Si fuera necesario un tercer nivel se escribiría en minúscula y negrita, y el cuarto en minúscula y cursiva.

TIPO DE LETRA. Arial 12 puntos. Las notas y afiliación serán de la misma letra, tamaño 10 puntos.

CUADROS Y FIGURAS. Serán numerados e incluirán una breve titulación.

PÁRRAFOS. Sangrado de 5 espacios. Espacio sencillo.

Se evitará la utilización de negrita y palabras subrayadas en el cuerpo del texto. Se utilizará letra cursiva para los títulos de libros y otras fuentes o para la inclusión dentro del texto de palabras o expresiones en otro idioma diferente al del artículo.

NOTAS. Serán las imprescindibles y se situarán al final de la página de forma numerada.

REFERENCIAS Y CITA BIBLIOGRÁFICA. Se utilizará el sistema APA (http://www.apastyle.org/ http://normasapa.com/)

- En el texto

Se utilizará el sistema APA, en el texto del artículo, para citar autoría y fecha, evitando en todo caso el uso de notas a pie de página. Ejemplo: (García, 2014) o "según García (2014) las condiciones…."

- Bibliografía

Se limitará a las fuentes bibliográficas utilizadas y referenciadas en el texto. Sigue orden alfabético de apellido de autores.

Ejemplos:

1. Libro:

Mansky, C. (2013). Public Policy in an Uncertain World. London: Harvard University Press.

2. Artículo o capítulo de libro:

Antaki, C. (1988). Explanations, communication and social cognition. En C. Antaki (Ed.), Analysing everyday explanation. A casebook of methods (pp. 1-14). London: Sage.

3. Artículo:

Moskalenko, S.; McCauley, C. (2010). Measuring Political Mobilisation: The Distinction Between Activism and Radicalisation. Terrorism and Political Violence, vol. 21, p. 240.

4. Artículo de revista on-line:

Blanco, J. M.; Cohen, J. (2014).The future of counter-terrorism in Europe. The need to be lost in the correct direction. European Journal of Future Research, vol. 2 (nº 1). Springer. Extraído el 1 de enero de 2015 de: http://link.springer.com/article/10.1007%2Fs40309-014-0050-9

5. Contenidos on-line:

Weathon, K. (2011). Let's Kill the Intelligence Cycle. Sources and Methods. Extraído el 1 de enero de 2015 de: http://sourcesandmethods.blogspot.com/2011/05/lets-killintelligence-cycle-original.html

6. Artículos o noticias de periódico:

Schwartz, J. (10 de septiembre de 1993). Obesity affects economic, social status. The Washington Post, pp. B1, B3, B5-B7

ORGANISMOS Y SIGLAS. Siempre que sea posible se utilizarán las siglas en castellano (OTAN, y no NATO; ONU y no UNO). La primera vez que se utilice una sigla en un texto se escribirá primero la traducción o equivalencia, si fuera posible, y a continuación, entre paréntesis, el nombre en el idioma original, y la sigla, separados por una coma, pudiendo posteriormente utilizar únicamente la sigla:

Ejemplo: Agencia Central de Inteligencia (Central Inteligencia Agency, CIA).

Se acompañará en soporte informático, preferentemente Microsoft Word. Las fotografías y ficheros se remitirán también en ficheros independientes. Se podrá remitir por correo electrónico a esta dirección: CAP-cuadernos@guardiacivil.org

Los trabajos se presentarán, precedidos por una ficha de colaboración en la que se hagan constar: título del trabajo, nombre del autor (o autores), dirección, NIF, número de teléfono y de fax, situación laboral y nombre de la institución o empresa a la que pertenece. Igualmente se presentará una ficha de cesión de derechos de autor, que se facilitará oportunamente.

Los artículos serán evaluados por el Consejo de Redacción. Se enviarán a los autores las orientaciones de corrección que se estimen pertinentes, salvo aquellas de carácter menor, que no afecten al contenido y que puedan ser realizadas por el equipo de redacción (correcciones de tipo ortográfico, de puntuación, formato, etc.).

Los autores de los trabajos publicados en la Revista serán remunerados en la cuantía que establezca el Consejo de Redacción, salvo aquellos casos en que se trate de colaboraciones desinteresadas que realicen los autores.

A todos los autores que envíen originales a la Revista "Cuadernos de la Guardia Civil" se les remitirá acuse de recibo. El Consejo de Redacción decidirá, en un plazo no superior a los seis meses, la aceptación o no de los trabajos recibidos. Esta decisión se comunicará al autor y, en caso afirmativo, se indicará el número de la Revista en el que se incluirá, así como fecha aproximada de publicación.

Los artículos que no se atengan a estas normas serán devueltos a sus autores, quienes podrán reenviarlos de nuevo, una vez hechas las oportunas modificaciones.

Los trabajos que se presenten deberán respetar de forma rigurosa los plazos que se indiquen como fecha máxima de entrega de los mismos.

Ni la Dirección General de la Guardia Civil ni "Cuadernos de la Guardia Civil" asume las opiniones manifestadas por los autores.

CENTRO UNIVERSITARIO GUARDIA CIVIL

Marco Legal

- Ley 39/2007 de la Carrera Militar
- Real Decreto 1959/2009 de creación del Centro Universitario de la Guardia Civil (CUGC)
- Orden PRE /422/2013 de servicios centrales de la DGGC
- Ley 29/2014 de Régimen de Personal de la Guardia Civil

Capacidades

- Titularidad del Ministerio del Interior a través de la Dirección General Guardia Civil.
- Ente público diferente de la Administración General del Estado.
- Adscrito a una o varias universidades públicas que expiden titulos oficiales universitarios del EEES: Actualmente UC3M y UNED (pendiente de desarrollo).
- Impartir titulaciones universitarias oficiales (grado, máster, doctor) y desarrollar líneas de investigación de interés para la Guardia Civil.
- Acuerdos de cooperación con otras instituciones a nivel nacional e internacional.

Oferta Académica

Actualmente el CUGC está adscrito a la Universidad Carlos III de Madrid (UC3M) e imparte las Titulaciones Académicas oficiales de:

- Máster en Dirección Operativa de la Seguridad.
- Máster en Seguridad Vial y Tráfico.
- Grado en Ingeniería de la Seguridad.
- Grado en Gestión de Seguridad Pública.
- Curso experto universitario en reconstrucción de siniestros viales.

Para prestar un mayor apoyo en las asignaturas y facilitar el contacto con los alumnos, el CUGC dispone de un Aula Virtual cuyo acceso se realiza desde la página web (www.cugc.es).

Además desarrolla otras actividades:

- Apoyo institucional para desarrollo de doctorados.
- Investigación Académica.
- Reconocimiento Carta Erasmus 2014-2020.
- Línea Editorial del CUGC.
- Extensión Universitaria.

El **Instituto Universitario de Investigación sobre Seguridad Interior** se creó mediante la firma de un convenio de colaboración suscrito entre el Ministerio del Interior, la Dirección General de la Guardia Civil y la Universidad Nacional de Educación a Distancia, el 17 de octubre de 2002, pues la Guardia Civil y la UNED llevaban vinculadas por distintos acuerdos de colaboración desde 1988 y precisaban de un centro especializado en la investigación, enseñanza y asesoramiento en materias relacionadas con la seguridad.

IUISI pretende desarrollar y promover la investigación científica de alta calidad en materias de seguridad que sean de interés para instituciones públicas y privadas, impulsar y promover la difusión de obras científicas, y crear un marco de reflexión y diálogo.

Las actividades previstas para este año se irán anunciando en su página web: www.iuisi.es