Cuadernos de la Guardia Civil

Revista de Seguridad Pública

Núm. 49-2014

GOBIERNO DE ESPAÑA
MINISTERIO DEL INTERIOR
GUARDIA CIVIL
DIRECCIÓN GENERAL

CUADERNOS DE LA GUARDIA CIVIL

REVISTA DE SEGURIDAD PÚBLICA

3ª ÉPOCA

SECRETARÍA:

Centro de Análisis y Prospectiva

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: 126-14-006-3

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://bit.ly/1Fdw213

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

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 mayo y el 1 de noviembre. El primer número de cada año se publica durante el mes de enero, y el segundo durante el mes de julio. 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?viewshelf=59&sortfield=

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

DOSSIER: CIBERSEGURIDAD

CIBERSEGURIDAD; RESPUESTA GLOBAL A LAS AMENAZAS CIBERNÉTICAS DEL s.XXI *6*
Luis Fernando Hernández García

HACKTIVISMO *37*
Jose Luis Mayorga Martín

PANOPTICON DIGITAL *55*
Centro De Análisis y Prospectiva. Guardia Civil

ARTÍCULOS

LA GESTIÓN DE LA I+D+i EN LA GUARDIA CIVIL *76*
Miguel Cañellas Vicens

LA ESTRUCTURA DE SEGURIDAD PÚBLICA DURANTE LA SEGUNDA REPÚBLICA (1931-1936) *95*
Jesús Narciso Núñez Calvo

A VECES LA VOZ DICE MÁS QUE LAS PALABRAS *122*
José Manuel Petisco Rodríguez y Rafael Manuel López Pérez

LA MUJER EXTRANJERA EN ESPAÑA Y LA VIOLENCIA DE GÉNERO *142*
Francisco Miguel Rodríguez Rodríguez

LA RESPUESTA POLÍTICA A LOS TRÁGICOS SUCESOS DE LAMPEDUSA *164*
Francisco Javier Vélez Alcalde

RESEÑA DE LIBROS

LA AMENAZA TERRORISTA ¿HACIA LA TERCERA GUERRA MUNDIAL? *186*
Ángel García-Fraile Gascón

INTELIGENCIA Y ANÁLISIS RETROSPECTIVO. LECCIONES DE HISTORIA Y LECTURAS RECOMENDADAS *189*
Diego Navarro Bonilla

LA SEÑAL Y EL RUIDO *191*
Nate Silver

DATOS SOBRE LOS AUTORES DE ESTE VOLUMEN POR ORDEN ALFABÉTICO *194*

NORMAS PARA LOS AUTORES *196*

INSTITUTO UNIVERSITARIO DE INVESTIGACIÓN SOBRE SEGURIDAD INTERIOR *198*

CIBERSEGURIDAD; RESPUESTA GLOBAL A LAS AMENAZAS CIBERNÉTICAS DEL s.XXI
LAS CIBERAMENAZAS, UN NUEVO RETO PARA LA JEFATURA DE INFORMACIÓN DE LA GUARDIA CIVIL

LUIS FERNANDO HERNÁNDEZ GARCÍA

RESUMEN

Las nuevas tecnologías de la información y las comunicaciones han supuesto una revolución tecnológico-social sin precedentes, que se ha traducido en la globalización del conocimiento y su acceso universal, así como en la creación de nuevos marcos de relación en lo social, lo cultural, lo económico, lo político y lo militar, en lo que viene a denominarse Ciberespacio.

Esta monografía, articulada en seis bloques temáticos íntimamente relacionados entre sí, que cuestionan la seguridad, la ciberseguridad, las ciberamenazas, las ciberrespuestas, las estrategias de seguridad y ciberseguridad, además de las iniciativas de la Guardia Civil en esta materia, pretende esbozar una visión actualizada, amplia y desde distintos enfoques de cómo desde las diferentes organizaciones de investigación e inteligencia se afronta el reto de luchar contra la delincuencia más especializada, el terrorismo y otras amenazas. Y más en concreto desde aquellas unidades de Investigación Tecnológica de la Guardia Civil integradas en las Jefaturas de Información y Policía judicial, con especial énfasis en el ámbito de responsabilidad del Servicio de Información de la Guardia Civil (SIGC).

Palabras clave: cibercrimen, ciberdelito, ciberdelincuencia, ciberterrorismo, hacktivismo, ciberespionaje, ciberguerra, ciberrespuestas, ciberresiliencia.

ABSTRACT

The new information and communication technologies have been an unprecedented social revolution that has led to the globalization of knowledge and its universal access, as well as creating new frameworks for relationships in the social, cultural, economic, political and military fields, in what comes to be called Cyberspace. I

This monograph, in six themes closely interrelated, questions the security in the cyberspace (cyber security), cyber threats, the measures adopted to face new risks, security strategies, and the initiatives of the Civil Guard in this area. It aims to outline a comprehensive updated vision, and several existing approaches from different research organizations in order to combat organized crime, terrorism and other threats, and more specifically from those units for technological research of the Guardia Civil.

Keywords: Cyberspace, cyber security, cybercrime, cyberterrorism, cyberwar, cyber security strategies.

1. INTRODUCCIÓN

A lo largo de los últimos años la generalización del uso de las Tecnologías de la Información y las Comunicaciones (TIC) ha propiciado un hecho trascendental y con profunda influencia en lo político, social y económico. Es cierto que el fenómeno de Internet ha traído consigo una gran revolución tecnológica que ha vivido la humanidad; más allá de los aspectos meramente técnicos y productivos ha tenido y sigue teniendo una significada repercusión en la forma de moldear nuevos hábitos y comportamientos sociales. La denominada "globalización" representa un marco de grandes oportunidades, pero lleva parejo riesgos, la mayoría a priori intangibles y por lo tanto de difícil percepción y que, en una imparable escalada, están llegando a tener trascendentales repercusiones. Internet ha pasado de ser un sueño de visionarios allá por los años 70, un valioso instrumento de investigación en los 80 o un insustituible elemento en el crecimiento económico en los 90, a irrumpir con fuerza de la mano del nuevo siglo para convertirse en el mayor fenómeno social conocido, con marcada influencia en lo cotidiano.

Es seguro que esta revolución tecnológico-social ha aportado aspectos muy positivos, como lo es la globalización del conocimiento y su acceso universal. Con la extensión de la red se ha proporcionado interoperabilidad a millones de usuarios de todo el mundo en un abanico de servicios hasta ahora impensables -navegación y acceso a contenidos web tanto abiertos como restringidos, correo electrónico, redes sociales, información compartida, transferencia y salvaguarda de datos, tanto personales como profesionales, etc.- y de forma casi instantánea; así pues, a través de la Red de redes, estamos siendo testigos de excepción de una total transformación de las relaciones humanas. Pero como con demasiada frecuencia ocurre, esta creación humana también ha sido y está siendo utilizada para satisfacer los ilícitos intereses de individuos y grupos faltos de escrúpulos que han visto en Internet una oportunidad para saciar sus oscuros e ilegítimos intereses y, con ello, términos tales como cibercrimen, ciberdelitos, ciberdelincuencia, ciberterrorismo, hacktivismo, ciberespionaje o ciberguerra se están haciendo un hueco en lo cotidiano, hasta tal punto que los ciudadanos están aprendiendo a convivir con esta nueva realidad, ya que cada vez está siendo más frecuente hallar noticias sobre algún hecho ilícito que se ha producido a través de la red; de igual manera, las relaciones entre Estados se están viendo profundamente distorsionadas y en algunos casos gravemente alteradas.

Estos nuevos marcos de relación en los social, cultural, económico, político y militar dependen cada vez en mayor medida de lo que acontece en lo que viene en denominarse Ciberespacio y han hecho más que necesario articular un Sistema de Seguridad Nacional[1], que gestione los riesgos que amenazan su funcionamiento y que

1 El año 2013 trajo consigo aportaciones fundamentales a la política de Seguridad Nacional en forma de nuevos documentos estratégicos y de una estructura integral orientada a la mejor organización del Sistema de Seguridad Nacional. En cuestión de meses se aprobaron tres estrategias y se constituyeron órganos interministeriales con poder de decisión, coordinación y apoyo en materia de Seguridad Nacional. La aprobación de dichos instrumentos vino precedida de cambios en la estructura de la Presidencia del Gobierno. Al comienzo de la presente legislatura se detectó la necesidad de dotar al Gabinete de la Presidencia del Gobierno de un órgano eficaz que sucediera al Departamento de Infraestructura y Seguimiento de Situaciones de Crisis (DISSC) en la función de prestar asesoramiento y apoyo técnico en materia de Seguridad Nacional a la Presidencia del Gobierno. Ello se materializó en la creación del Departamento de Seguridad Nacional del Gabinete de la Presidencia del Gobierno (DSN) mediante el Real Decreto 1119/2012, de 20 de julio, de mo-

ha tenido su más clara aproximación hasta la fecha con la aprobación por el Gobierno de España de la Estrategia de Seguridad Nacional (ESN) de 31 de mayo de 2013, ahondando y concretizando con la Estrategia de Ciberseguridad Nacional (ECSN), de 5 de diciembre de 2013.

No existe una unidad de criterio a la hora de definir qué es o qué se entiende por ciberespacio, máxime cuando aún no está claro el alcance del mismo más allá de la descriptiva conformación de medios, tanto físicos como lógicos, que dan lugar a las denominadas infraestructuras TIC. Para el Departamento de Defensa de los Estados Unidos (DoD), el ciberespacio es:

«Un dominio global dentro del entorno de la información que consiste en una red interdependiente de infraestructuras de tecnologías de la información, incluyendo Internet, redes de telecomunicaciones, sistemas informáticos, procesadores embebidos y controladores»[2].

La presente monografía se estructura en seis bloques temáticos, que aunque se presenten relativamente diferenciados no dejan de ser partes de un todo, con niveles de interrelación (imbricación) tales que en todo momento están interrelacionados; Iniciando la exposición con un bloque introductorio de lo que hoy en día engloba el término SEGURIDAD, seguido por un segundo en el que se pretende evidenciar los problemas y retos que una «sociedad digital» como la actual tiene que afrontar desde la perspectiva de la CIBERSEGURIDAD, el tercero comprenderá una sucinta exposición sobre las nuevas CIBERAMENAZAS, para enlazar con una visión descriptiva de capacitación y respuesta coordinadas desde el Gobierno de España en lo que podríamos bautizar como CIBERRESPUESTAS, resultando obligado recoger en el texto un breve estudio de las diferentes ESTRATEGIAS DE SEGURIDAD Y CIBERSEGURIDAD, nacionales y europeas que nos son de aplicación y, por último, las principales INICIATIVAS de la Jefatura de Información de la Guardia Civil en materia de ciberseguridad.

La pretensión del presente artículo no es otra que la de esbozar una visión actualizada, con una perspectiva amplia -nacional e internacional- y desde diferentes enfoques de cómo desde las distintas organizaciones de investigación e inteligencia son afrontados los nuevos retos para combatir la delincuencia especializada, el terrorismo y otras amenazas; concretando aún más en aquellas unidades de Investigación Tecnológica del Cuerpo, integradas en las Jefaturas de Información y Policía judicial, enfatizando aquellos que afectan al ámbito de responsabilidad del SIGC.

El binomio Ciberamenaza & Ciberseguridad es una realidad en permanente metamorfosis y, a pesar de los constantes esfuerzos, tanto gubernamentales como del sector privado, cada día resulta más evidente que las acciones hostiles dirigidas contra los sistemas informáticos, especialmente aquellos vinculados de alguna manera a Internet, son algo más que una amenaza y se han transformado en un riesgo emergente.

dificación del Real Decreto 83/2012, de 13 de enero, por el que se reestructura la Presidencia del Gobierno. [Resulta recomendable la lectura del capítulo «El Sistema de Seguridad Nacional» del Informe Anual de Seguridad Nacional 2013]

2 Maria José Caro Bejarano, en el capítulo segundo -Alcance y ámbito de la Seguridad Nacional en el Ciberespacio-, recoge una serie de definiciones y realiza un amplio estudio del concepto Ciberespacio. [Cuaderno de Estrategia nº149 del IEEE - Ciberseguridad. Retos y Amenazas a la Seguridad Nacional - diciembre 2010].

Las TIC han coadyuvado al bienestar y progreso de las sociedades de forma que gran parte de las relaciones públicas y privadas no sólo dependen de estas tecnologías sino que ya no se conciben sin ellas. Con el tiempo y la evolución de las TIC han aparecido riesgos que hacen necesario gestionar de una forma lo más eficiente posible su Seguridad.

Inicialmente, la Ciberseguridad se ocupó de proteger la información de una manera reactiva, pero posteriormente ha evolucionado hacia una posición proactiva que identifica y gestiona los riesgos que amenazan el ciberespacio a través del ya referido sistema de seguridad nacional, que fomenta la integración de todos los actores e instrumentos, públicos o privados, para aprovechar las oportunidades de las nuevas tecnologías y hacer frente a los retos que presentan.

2. SEGURIDAD EN EL SIGLO XXI

Y es que el nuevo concepto de SEGURIDAD surge en la década de los ochenta del pasado siglo XX. Una vez que se hace realidad la distensión Este-Oeste, donde el empleo de la fuerza, incluida la nuclear, era el eje principal del concepto tradicional de seguridad, emerge la realidad de considerar la seguridad bajo un prisma más amplio que incardine entre otros los riesgos económicos, medioambientales, delincuencia transnacional o que surgen de cuestiones de identidad social. Se ha pasado de un periodo de bipolaridad de la guerra fría a una multipolaridad. La globalización provocada por la revolución de la tecnologías de la información ha invadido exponencialmente los espacios de todas las actividades humanas, conformando un concepto de seguridad más heterogéneo de multipolaridad que contrasta con la unipolaridad que ejerció Estados Unidos desde la distensión de la guerra fría hasta los atentados del 11 de septiembre de 2001 (11-S). Se ha evidenciado, desde tan fatídica fecha, que el poder militar por sí sólo, aunque siendo un gran potencial, no es determinante ante los conflictos asimétricos actuales para conseguir combatirlos adecuadamente. Los problemas globales de seguridad afectan a toda la comunidad internacional, el terrorismo yihadista, el tráfico encubierto de armas de destrucción masiva, la delincuencia internacional organizada –narcotráfico, tráfico clandestino de seres humanos o de armas, blanqueo de dinero, etc.− crecientes problemas medioambientales, pandemias, hambrunas… configuran un escenario de seguridad con un enfoque más novedoso, donde el motivo no sólo es el Estado, sino que el individuo es también un elemento fundamental en cuanto sujeto a proteger y como actor imprescindible para colaborar en la prevención y la respuesta -concienciación-.

Desde el 11-S, y hasta la fecha, la barbarie y la sinrazón del terrorismo de corte yihadista ha experimentado un dramático recrudecimiento; ha sacudido los cinco continentes y golpeado a multitud de países, incluida España aquel fatídico 11 de marzo del 2004 en Madrid, con sus casi dos centenares de víctimas mortales, que le convirtió en el atentado más grave en suelo europeo hasta la fecha o Londres el 7 de julio del 2005 con 56 muertos. El 2 de octubre de ese mismo año atentaron en Bali-Indonesia y el 13 de septiembre del 2008 en Nueva Delhi, por recordar algunos de los más significativos, aunque resulta de justicia rememorar otros muchos, casi ignorados o incluso olvidados, pero igualmente terribles, acontecidos en Irak, Paquistán, Afganistán, Chechenia, Egipto, Kenia, etc. porque si en algo se igualan todos ellos es en las víctimas, siempre inocentes y mayoritariamente anónimas, pues no hay víctimas de primera o de segunda.

Pero dicho esto, no debemos caer en el error de infravalorar o dejar en el olvido otras amenazas terroristas aun presentes en nuestra sociedad, como el mal adjetivado terrorismo “doméstico”, no menos brutal e irracional. Terrorismos son todos los que prostituyendo los más básicos principios de la democracia pretenden imponer -siempre desde una minoría sin representación alguna- su aberrante visión del mundo y de la sociedad que les rodea a una mayoría legítima, democrática y pacífica, mediante la imposición del terror. En el caso de nuestra Nación y a lo largo de más de cuatro décadas ha causado cerca de un millar de muertos y más de una decena de millar de heridos, cercenando la ilusión y el futuro a muchas familias españolas; y aún hoy sigue causando dolor y desasosiego a muchos conciudadanos. Pues bien, muchas de sus tácticas y objetivos pueden ser perfectamente trasladables a la Red, como más adelante se concretará.

3. CIBERSEGURIDAD

Y es precisamente a raíz de los atentados del 11-S, cuando en los diferentes entes gubernamentales, tanto de los Estados Unidos como de los países occidentales, se generalizó la percepción de la amenaza desde el ciberespacio; inicialmente orientada hacia la potencial actuación de organizaciones terroristas, de ahí que tomara fuerza el concepto de ciberterrorismo como una amenaza global. Trascurrido ya más de un decenio, la realidad se ha mostrado muy diferente, ya que el concepto de ciberterrorismo se ha visto desplazado del todo a una parte de un nuevo concepto globalizador, el de ciberamenaza y, frente a ésta, como antagonista, el ya mencionado de la ciberseguridad.

Para entender este nuevo escenario y estar en condiciones de entenderlo resulta fundamental adquirir una conciencia de ciberseguridad, tanto en lo profesional como en lo personal, faceta que se convierte en vertebral, ya que la seguridad es una percepción que permite al ser humano y a las organizaciones desarrollar de una forma armónica sus relaciones. Y es que las relaciones sociales se desarrollan en marcos conceptuales definidos, en los que la seguridad jurídica y el cumplimiento de la ley y de las normas establecidas permiten una ordenación estable, definida. El problema surge en los espacios donde esas relaciones no están aún reguladas porque la velocidad de los cambios son significativamente superiores al de su marco de referencia racionalmente establecido.

«Existe un fenómeno creciente, el de los “nativos en Internet”, con patrones de comportamiento e incluso patologías muy características, que les llevan con frecuencia a no encontrar razonables determinadas limitaciones que son reclamadas por aquellos que han visto el nacimiento de este nuevo modelo de interacción social. Las iniciativas sobre materias de ciberseguridad que están siendo desarrolladas en todos los países ante este entorno de cambio y en el ciberespacio configuran un reto de entendimiento de este “nuevo mundo”. Un mundo que permite grandes oportunidades y presenta grandes retos, una experiencia fascinante para el investigador social donde, transformado en analista de inteligencia, debe interpretar los datos, ver más allá de lo evidente y concluir que, desde un punto de vista interpretativo y otro prospectivo, el papel que desarrollan los individuos, las empresas, las organizaciones públicas y los Estados está sometido a cambios y revisión»[3].

3 ¿Por qué una conciencia nacional de ciberseguridad? introducción a la Monografía del CESEDEN nº137 - Necesidad de una conciencia nacional de ciberseguridad. La ciberdefensa: un reto prioritario - (abril 2013).

En el marco de la ESN se plantea como un objetivo estratégico la implantación de una cultura de ciberseguridad sólida que traslade tanto a los ciudadanos como a profesionales y empresas la importancia de la seguridad de la información y del uso responsable de las nuevas tecnologías y de los servicios de la sociedad del conocimiento.

Para la ESN, España, al igual que el resto de países de nuestro entorno sociocultural, está expuesta a los ciberataques, que no solo generan elevados costes económicos sino también, y lo que es más importante, la pérdida de confianza de los ciudadanos en unos sistemas que, en la actualidad, resultan críticos para el normal funcionamiento de la sociedad.

El tercer capítulo de la Estrategia de Seguridad Nacional describe «los riesgos y amenazas para la Seguridad Nacional: los conflictos armados, el terrorismo, las amenazas cibernéticas, el crimen organizado, la inestabilidad económica y financiera, la vulnerabilidad energética, la proliferación de armas de destrucción masiva, los flujos migratorios irregulares, el espionaje, las emergencias y catástrofes, la vulnerabilidad del espacio marítimo y la vulnerabilidad de las infraestructuras críticas y los servicios esenciales. También se contemplan factores potenciadores como el cambio climático, la pobreza, la desigualdad, los extremismos ideológicos, los desequilibrios demográficos o la generalización del uso nocivo de las nuevas tecnologías que, sin ser en sí mismos un riesgo o una amenaza, pueden desencadenarlos o agravarlos».

El factor humano[4] «es el eslabón más débil de la cadena de seguridad y del que se pueden explotar tres rasgos presentes en el ser humano: el miedo, la confianza y la inconsciencia (o inadvertencia). Se utilizarán tres vías principalmente para crear una conciencia nacional de ciberseguridad: la educación, la enseñanza y la concienciación. La conciencia de ciberseguridad se alcanza paulatinamente, según ciertos grados; no todas las personas pueden llegar a alcanzar el mismo grado. La edad también influye: cada grado de madurez de la persona permite alcanzar un grado de conciencia de ciberseguridad. Podemos establecer cuatro grados, de los que los tres primeros podrían ser alcanzados por una parte significativa de la población. Desde el nivel más básico al más avanzado se pueden establecer los siguientes grados: ciberhigiene, ciberconciencia, ciberciudadanía y ciberespecialistas. Siendo los sujetos primarios los que deben crear conciencia de ciberseguridad en los sujetos últimos, es decir, en la población».

«En efecto, falta el eslabón principal de todo el sistema: las personas. Es necesario formar a las personas en seguridad informática o ciberseguridad. No todo el mundo puede ni debe tener la misma formación. Los usuarios deben estar formados en buenas prácticas, algo así como ciberurbanidad o cibereducación.

Esta ciberurbanidad o buenas prácticas[5] de seguridad informática debe ser algo que se repita con frecuencia hasta que la sociedad lo tenga interiorizado como tiene interiorizadas normas de buena educación o buenas maneras».

4. CIBERAMENAZAS

Y es que las nuevas amenazas para nuestra seguridad, tanto individual como colectiva son múltiples, diversas y cambiantes, e Internet y su tecnología asociada están

4 Ibid.

5 Consultar estas buenas prácticas en: Monografía del CESEDEN nº137 - Necesidad de una conciencia nacional de ciberseguridad. La ciberdefensa: un reto prioritario - (abril 2013).

contribuyendo, de una forma cada vez más determinante en ello -Ciberamenazas-; ya que están siendo utilizadas con profusión como soporte para la ejecución de tradicionales acciones ilícitas pero con novedosos modus operandi; y no sólo empleados por los grupos delincuenciales al uso -que se han adaptado y rápido a los nuevos tiempos- sino que lo están siendo también por otras formas de delincuencia grave y organizada, tales como grupos y organizaciones terroristas, colectivos antiglobalización y antisistema -preferentemente a través del denominado hacktivismo- o que tienen como fin último la desestabilización de un estado en particular, atacando su estructura social, económica y política, sin olvidar organizaciones clandestinas e, incluso, las estructuras de inteligencia de algunos estados.

Al hablar de delincuencia vinculada a organizaciones terroristas o afines, debemos contemplar Internet y las TIC desde una óptica amplia, verlo como parte de su "negocio", su forma de obtener ilícitos beneficios o saciar sus instintos. Para ellos representa una oportunidad sin precedentes de organizarse, comunicarse y coordinarse, compartir, proclamar, intoxicar y difamar, reclutar, financiarse, etc. Y, todo ello, con unas condiciones de seguridad y anonimato sin precedentes.

Desde que la organización terrorista Al Qaeda cometió los brutales atentados del 11-S, retransmitidos en directo a través de los medios de comunicación audiovisuales, la percepción del mundo en el que vivimos ha cambiado drásticamente y muchas miradas se han vuelto hacia este entorno y han descubierto el sinfin de perversas posibilidades que ofrece a todos aquellos que optan por el terror como forma de vida -nuevas ciberamenazas-.

Ya la extinta Estrategia Española de Seguridad del 2011 (EES) abordaba cinco factores considerados como potenciadores de riesgo que «propician la propagación o transformación de las amenazas y riesgos e incrementan nuestra vulnerabilidad». Estos factores transnacionales eran: «las disfunciones de la globalización, los desequilibrios demográficos, la pobreza y la desigualdad, el cambio climático, los peligros tecnológicos, y las ideologías radicales y no democráticas.». Estos peligros tecnológicos se han visto nuevamente reflejados y concretados en la vigente ESN de modo que se presentan como auténticos potenciadores de riesgo. En definitiva, la tecnología aparece como parte del problema y a la vez de la solución.

Recientes acontecimientos han constatado que las amenazas de ataques, sabotajes y espionaje a través de Internet son una realidad de graves e impredecibles consecuencias, la tradicional dialéctica de la diplomacia ha terminado y son constantes las denuncias y acusaciones entre estados. De estos quizás el más relevante haya sido el protagonizado entre Estados Unidos y la República Popular de China durante el primer semestre del año 2013 y que estuvo presente en la intervención del presidente Barak Obama ante el Capitolio, en el discurso del estado de la Unión -13 de febrero del 2013-, en el que anunció la promulgación de una Orden Ejecutiva en la que en aras de la seguridad buscaba mejorar la protección de las infraestructuras nacionales contra ataques cibernéticos. A continuación se recupera una breve pero significativa parte de esta alocución:

«EE. UU. también debe hacerle frente a la amenaza real y creciente de ciberataques. Sabemos que los piratas informáticos roban las identidades de personas y se infiltran en correos electrónicos privados. Sabemos que empresas extranjeras sustraen nuestros secretos corporativos. Y nuestros enemigos buscan la capacidad de sabotear nuestra red de energía eléctrica, nuestras instituciones

financieras, y nuestros sistemas de control del tráfico aéreo. No podemos mirar hacia atrás en años venideros y preguntarnos por qué no hicimos nada ante las serias amenazas a nuestra seguridad y nuestra economía (...). Es por eso que hoy, más temprano, firmé un nuevo decreto ejecutivo que fortalecerá nuestras defensas cibernéticas aumentando el intercambio de información y desarrollando normas que protejan nuestra seguridad nacional, nuestros empleos y nuestra privacidad. Ahora bien, el Congreso también debe actuar, aprobando las leyes que otorguen a nuestro Gobierno una mayor capacidad para proteger nuestras redes y disuadir los ataques».

Y resulta evidente que esta petición ha calado en el legislador estadounidense, puesto que se han aprobado diversas iniciativas desde entonces; sin duda la más relevante o de mayor alcance llegó en mayo de 2014, cuando un portavoz del Pentágono anunció a los medios de comunicación que, a partir de ese momento, los sabotajes informáticos provenientes de otros países podrían ser catalogados como constitutivos de actos de guerra, lo que ha abierto la puerta a que los EE.UU. respondan a sabotajes informáticos con la fuerza militar[6].

Podemos decir que las nuevas ciberamenazas comprenden cinco áreas fundamentales y perfectamente diferenciadas que, si bien comparten técnicas y procedimientos, obedecen a motivos, fines u objetivos perfectamente diferenciados y premeditados, estas son: **ciberdelincuencia, ciberterrorismo, hacktivismo, ciberespionaje y ciberguerra.**

Quizás antes de continuar con la exposición, resulte oportuno adelantar una de las que pudieran considerar como conclusiones de la exposición, y es el hecho de considerar algunas de las ideas que a lo largo de este artículo se exponen como parte de una visión fatalista y alejada de la realidad; es por ello que se debe desmitificar pero no subestimar el riesgo creciente que supone Internet como medio e instrumento de lo que se viene denominando “Ciberterrorismo”.

Siempre se ha dicho que en el arte de la guerra es esencial el conocimiento de tu enemigo, sin el cual cualquier campaña está destinada al fracaso. En el campo de la ciberseguridad el conocimiento de los «ciberenemigos o ciberatacantes»[7], y de sus «técnicas y procedimientos de ataque[8], obviamente resulta así mismo fundamental.

6 Noticia publicada por el Wall Street Journal en su edición del 31 de mayo del 2014.

7 Como comenta el general José Manuel Roldán Tudela, al hablar de acciones hostiles en el ciberespacio en sus diferentes modalidades nos enfrentamos a un primer problema, que es el de la atribución o la capacidad de poder identificar quién ha atacado un determinado objetivo y desde dónde. Se trata de un problema con trascendencia legal que plantea un fuerte reto técnico, ya que los orígenes de los ataques emplean medios y técnicas muy elaborados para ocultar sus huellas. A veces, es muy difícil incluso determinar el verdadero objetivo del ataque, debido al empleo de técnicas de decepción. En cualquier caso, la persona debe estar atenta y precaverse contra tres orígenes genéricos de ataques: causas fortuitas, personas próximas y amenazas en la red.

8 La infección mediante código (o software) dañino (o malicioso), conocido en inglés como malware, es, en general, la amenaza más conocida y a la que se atribuyen los peores efectos. Sin quitarle la importancia que merece, no es la única y, a veces, tampoco es la más dañina. Se llama código dañino o malware a un programa o a una pieza de código ejecutable que produce cambios en el funcionamiento correcto de un equipo informático, dañándolo o apoderándose de él con intención maliciosa. La característica fundamental del código dañino es que causa un funcionamiento incorrecto del sistema infectado porque produce cambios en el entorno (sistema operativo, memoria, datos, sistema de archivos) o en los programas instalados. Otra característica del código dañino es su tendencia generalizada a extenderse, infectando nuevos sistemas por diversos procedimientos. Una clasificación general del código dañino sigue el criterio de si tiene existencia autónoma y puede ejecutarse por sí mismo (independiente) o si necesita para ejecutarse de un programa u objeto anfitrión (código dañino embebido). Fuente: Juan Antonio Gómez Bule

Como es lógico, el Ciberdelito[9] conforma uno de los cinco grandes bloques de las ciberamenazas del siglo XXI, pero no está previsto ser tratado con profundidad en el presente artículo, ya que éste se orienta hacia las responsabilidades que recaen en el ámbito competencial de la Jefatura de Información y, como es lógico, el ciberdelito entendido como tal recae plenamente en el marco de actuación de la Jefatura de Policía Judicial; no obstante, sí se considera oportuno realizar ciertos apuntes sobre la materia. La globalización de la delincuencia y la indeterminación del ámbito geográfico en el que viene actuando la delincuencia organizada transnacional en las últimas dos décadas, donde el lucro obtenido por el ciberdelito se estima supera ya el del tráfico de drogas, armas y seres humanos juntas -cifrado por las autoridades de los EE.UU en 2012 en 1,3 billones de dólares (Dólar USA), el 1,7% del PIB mundial- genera constantes conflictos de jurisdicción entre estados o en el peor de los casos impunidad. Pero en este sombrío panorama se llegó a un acuerdo histórico, el conocido como Convenio de Budapest, promovido por el Consejo de Europa y aprobado el 23 de noviembre del 2001 en Budapest. El Convenio es, sin lugar a duda, un acuerdo nacido con vocación universal y transatlántica, que supuso y es el máximo referente para la lucha contra la ciberdelincuencia, y sigue siendo el único tratado que tiene por objeto la armonización normativa del derecho penal de las naciones o estados que lo ratifican. Nuestro país lo hizo en el año 2010 y se unió así a los restantes estados miembros de la UE que lo han ratificado -23 países-. A través de la Estrategia de Ciberseguridad de la UE se ha solicitado a los cinco estados que aún no lo han ratificado -Grecia, Irlanda, Luxemburgo, Polonia y Suecia- que así lo hagan y lo incorporen al ordenamiento jurídico propio, buscando con ello la homogeneización normativa o su universalización cuando menos en el espacio común europeo.

A comienzos del año 2013 se creó, en el seno de la organización de cooperación policial europea EUROPOL, el Centro Europeo de la Lucha contra la Ciberdelincuencia o EC3, como punto focal para el tratamiento de los ciberataques y constituyendo en su seno un Centro de Respuesta ante Incidentes Cibernéticos (CERT) y de ámbito europeo -CERT-EU-.

Retomando el concepto de Ciberterrorismo y haciendo una interpretación extensiva del término que, vinculado al uso de las TIC en general y de Internet en particular, vienen haciendo las organizaciones terroristas y grupos afines para la consecución de sus objetivos, siempre enmarcados en el uso de las TIC e Internet como medio o instrumento, más que como objetivo de la acción ilícita -momento en que en puridad sí nos encontraríamos ante una acción pura del denominado ciberterrorismo-; el ciberterrorismo, en su concepción estricta, estaría orientado a la realización de acciones ofensivas contra los sistemas de información y comunicaciones que sustentan el normal funcionamiento de las denominadas Infraestructuras Críticas (IC,s) y Estratégicas, así como cualquier otro servicio esencial para la ciudadanía -lo que viene en denominarse Internet como objetivo-.

9 Legislación de interés cibercrimen/ciberterrorismo. Quizás, de entre todas las definiciones de delito informático o cibercrimen, la que goza de mayor aceptación, por el consenso alcanzado, ha sido la realizada por el Consejo de Europa a través de su Convenio de Ciberdelincuencia. Éste, fue promulgado, el 23 de noviembre del 2001 en Budapest, y ratificado por España en el año 2010. Posteriormente, en enero de 2003, se añadió al Convenio un Protocolo Adicional para penalizar los actos de racismo y xenofobia cometidos a través de sistemas informáticos.

Si miramos a otros se evidencia la existencia de tantas definiciones válidas sobre el concepto ciberterrorismo como enfoques de análisis se planteen, desde conceptos simples -pero no por ello desatinados– como:

«La convergencia del ciberespacio con el terrorismo»[10]

Acuñado en los EE.UU en los años 80, y que ha evolucionado en sintonía con la transformación de la amenaza hacia conceptos tales como los siguientes:

«El ciberterrorismo es el ataque premeditado y políticamente motivado contra información, sistemas, programas y datos informatizados no combatientes, por parte de grupos terroristas o agentes encubiertos de potencias extranjeras»[11]

Una de las definiciones más elaboradas es:

«El ciberterrorismo es la ejecución de un ataque sorpresa por parte de un grupo (o persona) terrorista, extranjero subnacional, con objetivo político, utilizando tecnología informática e Internet para paralizar o desactivar las infraestructuras electrónicas y físicas de una nación, provocando de este modo la pérdida de servicios críticos, como energía eléctrica, sistemas de emergencia telefónica, servicio telefónico, sistemas bancarios, Internet y otros muchos (...). El objeto de un ataque ciberterrorista no es solo impactar sobre la economía de una región o país, sino amplificar los efectos de un ataque terrorista físico tradicional provocando confusión y pánico adicionales en la población en general (...). El ciberterrorismo existe porque es en el reino cibernético donde son más débiles la mayoría de las naciones industrializadas»[12].

En el seno de la Unión Europea ya en el año 2002 y a través de la DM 173/2002[13], al analizar la amenaza de ataques terroristas contra los sistemas de información vitales de la UE, se vislumbró la naturaleza del riesgo de ciberataques empleando expresamente el término ciberterrorismo.

Los incidentes más serios que han acontecido en los últimos años se han centrado en acciones de espionaje (económico, militar y político); el sabotaje, la desobediencia civil e incluso la guerra han sido otras de sus manifestaciones más recientes y es por ello que, bajo el denominador común del prefijo “Ciber”, se están acuñando diversas acepciones, catalogadas y diversificadas por los fines cuya consecución se persigue, aunque compartiendo todas ellas las tecnologías de ataque y centrando sus objetivos en Internet o, más bien, a través de éste.

Concretando aún más el concepto, se pueda hablar del:

- Uso con fines terroristas: las diferentes organizaciones terroristas, vienen utilizando las TIC e Internet como Instrumento[14] para la consecución de sus

10 Ciberterrorismo: La convergencia del ciberespacio con el terrorismo [Barry Collin – Instituto de Inteligencia y Seguridad – California USA 1984].

11 Mark M Pollitt – E.A.FBI – Proccedings of the 20th National Information Systems Security Conference, oct.1997.

12 Dan Verton –periodista especializado en seguridad informática y ex oficial de inteligencia Naval de los Estados Unidos– Washington, D.C. 2003.

13 Decisión Marco del Consejo, Bruselas 19.04.2002 COM(2002)173 final 2002/0086 (CNS).

14 Ante la cuestión de si se ha materializado de alguna manera la amenaza ciberterrorista, significar que del empleo de Internet y las TIC como instrumento existen pruebas evidentes de que las organizaciones terroristas vienen aprovechando las posibilidades que les ofrecen las TIC en su propio beneficio. Es una realidad que ya no existen operaciones contra cédulas, taldes o grupos terroristas en las que no se intervengan medios informáticos, es más, la presencia de estos ha experimentado un crecimiento exponencial, no tanto en el número sino en la capacidad de almacenamiento de los mismos, lo que ha obligado a afrontar nuevos retos en todo lo relativo a la informática forense; tanto por su complejidad como por los cada vez más sofisticados procedimientos y sistemas

objetivos y, en este sentido, utilizan en su beneficio las posibilidades que las nuevas tecnologías les ofrecen para ocultar sus comunicaciones o blindar la información contenida en los ordenadores que les son incautados; de hecho, en los últimos años se ha realizado un gran esfuerzo a fin de dotar humana y materialmente a los departamentos de Informática Forense, para poder dar respuesta al aumento, casi exponencial, tanto del número de dispositivos incautados como de la complejidad de su análisis. Así mismo, destacar el uso de Internet y las TIC como Medio[15], a través de su utilización para la recluta, financiación, difusión de ideas, comunicados o reivindicaciones y localización de información esencial para la planificación de acciones contra potenciales objetivos; este uso resulta más evidente en la actividad de la Ciber-Yihad.

- Internet como medio para llegar a objetivos tecnológicos u objeto directo de acciones hostiles: el grave incidente acaecido en Estonia[16] en la primavera del 2007 supuso el punto de inflexión entre la especulación a la constatación de una realidad, por primera vez se producía un ciberataque "a gran escala", y con éxito, contra un estado, inutilizando o colapsando una parte más que considerable de sus infraestructuras TIC. Internet había sido algo más que el medio, había sido el Objetivo de las acciones ilícitas. Este incidente obligó a la OTAN a replantear toda su estrategia de Ciberseguridad y Ciberrespuesta, o más bien a definirla, concretándose en dos hechos de evidente relevancia, como son, por un lado la Creación del Centro de Excelencia de Ciberdefensa Cooperativa (CCD CoE) en Tallín, capital de Estonia, y por otro la nueva Estructura de la Alianza surgida de la Cumbre de Lisboa en octubre del 2010.

---

informáticos que den soporte a las necesidades de las unidades de lucha antiterrorista. En este sentido destacar el éxito obtenido con el modelo de informática forense-operativa, haciendo salir a los analistas forenses de sus laboratorios, transformar éstos en elementos móviles y fusionar la actividad técnica con la operativa de obtención sobre el terrero, con más que notables resultados.

15 Como medio reseñar que el empleo de las TIC está facilitando las relaciones y colaboraciones entre diferentes organizaciones, favorece sus objetivos de guerra psicológica, al posibilitar la desinformación y difusión de amenazas, identifica canales de financiación, fomenta la recluta y sirve de base para todo su aparato de propaganda. En la memoria colectiva han quedado grabadas las horrendas imágenes de rehenes asesinados por decapitación o acciones terroristas filmadas y posteriormente difundidas a través de la Red. Los videos con mensajes propagandísticos del propio Osama Bin Laden o comunicados de la organización terrorista ETA son técnicas que mejoran y optimizan la consecución de sus objetivos, ya que impiden la "censura y/o valoración" a que mayoritariamente son sometidos por los medios de comunicación en el momento de su difusión, amedrentan la moral de sus objetivos y víctimas y enaltecen la sinrazón de sus adeptos. Finalmente constituyen una inestimable fuente de información de todo tipo sobre potenciales objetivos tanto personales como de infraestructuras.

16 Algunos de ustedes se estarán preguntando si la alarma que existe alrededor de las Infraestructuras Críticas y Estratégicas responde a una amenaza real o nos encontramos ante un ejercicio de informática-ficción para justificar modificaciones en el marco legal y normativo que, en aras de la seguridad, restrinjan o limiten derechos individuales. La realidad es que el supuesto que se está planteando es perfectamente viable ya que en la actualidad las TIC están diariamente comprometidas por la acción anónima de hackers, algunas con bastante éxito por la relevancia de los sistemas comprometidos, el número de ordenadores afectados o incluso por los daños económicos causados; pues bien, lo único que le faltaría a cualquiera de estas acciones para convertirse en una acción "ciberterrorista" es la motivación y reivindicación por parte de una organización terrorista. Los acontecimientos que entre el 27 de abril y 11 de mayo de 2007 tuvieron lugar en Estonia han hecho que la percepción del problema cambie de una forma radical, al encontrarnos ante el primer ciberataque a gran escala dirigido contra infraestructuras TIC de un país, vía Internet.

Igualmente resulta muy significativa la constitución, por parte del DoD, del denominado Mando de Defensa Cibernética (CYBERCOM ó USCMBERCOM) el año 2010.

Y en analogía al anterior, así como clara inspiración en éste, el día 26 de febrero de 2013, y mediante la Orden Ministerial 10/2013, vio la luz en el seno de las Fuerzas Armadas Españolas del Mando Conjunto en Ciberdefensa (MCCD).

Como ya se indicó con anterioridad, desde el episodio de Estonia la escalada de "incidentes" presenta una peligrosa tendencia creciente, contabilizándose múltiples vulneraciones de sistemas de información sensibles, algunas de ellas de extrema gravedad, que van desde conflictos bélicos y sabotajes industriales a espionaje en todas sus vertientes, político, económico o militar y terminando en actos de desobediencia civil organizada; todo ello sin olvidar la amenaza siempre presente de grupos y organizaciones terroristas y siempre orientado hacia las que han sido denominadas y catalogadas como Infraestructuras Críticas (IC,s).

Aunque el caso Estonia, por ser considerado el primer ciberataque de grandes dimensiones, es tomado como referente, sucedió otro aún más grave si cabe entre julio y agosto de 2008, fue el denominado caso Georgia ya que un enquistado conflicto en el Cáucaso, entre los estados de Rusia y Georgia, por el control del enclave estratégico de Osetia del Sur, llevó a que el 21 de julio se iniciaran una serie de oleadas de ataques DDoS (Distributed Denial of Service) procedentes de suelo ruso y que precedieron a una incursión militar sobre el territorio de Georgia. Para la mayoría de analistas no cabe duda de que se trató de un escenario de Ciberguerra[17].

Finalmente **Internet como objetivo** es la razón última del **ciberterrorismo**; y a la pregunta de cuáles serían los objetivos propios del terrorismo a través de Internet la respuesta resulta obvia: los mismos que ya lo son en la actualidad, telecomunicaciones, infraestructuras, economía y empresa, servicios públicos en general y Administración y Estado; en suma, aquellas que se encuadran en el concepto de Infraestructura Crítica, entendiendo como tal:

«instalaciones, redes, servicios, equipos físicos y de tecnología de la información cuya interrupción o destrucción tendría un impacto mayor en la salud, la seguridad o el bienestar económico de los ciudadanos o en el eficaz funcionamiento de los gobiernos»

(COM (2004) 702 final, 20 octubre).

La debilidad de las IC,s, además de su naturaleza intrínseca, viene amplificada en el hecho de la interconexión e interdependencia que existe entre ellas, propiciando efectos encadenados, también conocidos como "en cascada" o "dominó", que posibilitarían que la pérdida directa de uno de ellos conlleve a su vez la pérdida, inoperatividad o inaccesibilidad de otros; no sólo con los consiguientes perjuicios y daños en servicios esenciales, sino también, y muy especialmente, efectos psicológicos en la

17 El concepto y casos reales son quirúrgicamente diseccionados y analizados por el Richard A. Clarke -responsable de seguridad con cuatros presidentes de los EE.UU- quien prestó servicio durante 30 años en la Casa Blanca, el Departamento de Estado y el Pentágono. [GUERRA En la RED - Los nuevos campos de batalla, Editorial Ariel].

población. No perdamos de vista que nuestra cada vez mayor dependencia tecnológica nos hace más débiles y vulnerables[18].

«La primera reivindicación de un presunto ataque ciberterrorista tuvo lugar el día 19 de febrero de 2004 cuando la autodenominada "brigada Abu-Nafsa" se atribuyó la autoría de un supuesto ciberataque contra la infraestructura energética de EE.UU., que derivó en el mayor apagón de su historia (verano de 2003); a este comunicado no se le dio credibilidad por lo extemporáneo si bien la causa real del incidente sigue siendo un misterio»[19].

Realmente existen elementos tangibles de la amenaza, aunque a nivel nacional aún no se podría hablar de proyección real de una amenaza concreta, pero a nivel internacional y más concretamente de EE.UU. sí, toda vez que existen evidencias reales de que algunos sistemas informáticos de administración remota de infraestructuras críticas están comprometidos, concretamente los denominados sistemas Scada (Supervisión,Control y Adquisición de Datos):

«los ataques con éxito sobre los sistemas SCADA podrían producir terror a gran escala. En las cuevas de Afganistán, las tropas de EE.UU. encontraron planes de Al Qaeda para atacar esos sistemas»[20].

Sin duda son las denominadas infraestructuras críticas las que están en el ojo del huracán ya que cualquier interferencia grave en su normal funcionamiento acarrearía graves problemas a una sociedad cada vez más dependiente de la tecnología y de sus prestaciones; así mismo la actividad económica también es objetivo; de hecho, se estima que una acción ciberterrorista de gran calado no se materializaría de forma aislada sino que sería el complemento o refuerzo de otra acción terrorista convencional.

Y llegados a este punto podríamos preguntarnos si realmente los terroristas son conscientes de esta situación y pretenden aprovecharla o se está ante un mero ejercicio de informática-ficción; pues a modo de respuesta unas breves citas cargadas de gran significación dada su naturaleza, el contexto en el que se citan y sus autores:

«Es muy importante concentrarnos en golpear a la economía de EE.UU. de todas las formas posibles (...), buscando los pilares clave de la economía de EE.UU. deberían golpearse los pilares clave del enemigo (...) »

***Osama Bin Laden**, entrevistado en un medio de difusión árabe el 27 de diciembre de 2001.*

«Dividid su nación, rompedla en pedazos, destruid su economía, quemad sus empresas, arruinad su bienestar, hundid sus barcos y matadles en tierra, mar y aire (...)»

*Cita atribuida a **Muhammad Atef**, antiguo comandante militar de Al Qaeda.*

«(...) Salah había recibido cursos de programación, cifrado y otras técnicas de hacking y vigilancia electrónica realizadas con la inteligencia en una casa de huéspedes perteneciente a Osama Bin Laden en Hyatabad, un barrio de Peshawar, Pakistán (...)»

*Testimonio de **L'Houssaine Kherchtou** ante un tribunal de Nueva York el 7 de febrero de 2001.*

18 La población mundial en general, y en particular los más jóvenes, cada vez es más dependiente del uso de la tecnología y consecuentemente vulnerable a su carencia. Psiquiatras surcoreanos ya han desarrollado el concepto de "demencia digital" y han identificado la sintomatología de este cuadro clínico de trastorno mental. Dr. Manfred Spitzer [Demencia Digit@l - El peligro de las nuevas tecnologías - editorial B grupo Zeta]

19 Informe de Andrey Belousov del Centro de Investigación de Delitos Informáticos de los EE.UU [Computer Crime Research Center].

20 Cita de Mark Rasch, antiguo jefe de la Unidad de delitos informáticos del Departamento de Justicia de EE.UU.

«El FBI cree que el ciberterrorismo, la utilización de ciberherramientas para parar, degradar o denegar el acceso a infraestructuras críticas nacionales, como la energía, el transporte, las comunicaciones o los servicios gubernamentales, con el propósito de coaccionar o intimidar a un gobierno o a la población civil, es claramente una amenaza emergente para la que debemos desarrollar habilidades de prevención, disuasión y respuesta».

***Louis Freeh**, antiguo director del FBI (Federal Bureau of Investigation) en una declaración ante un Comité del Senado de los EE.UU., mayo 2001.*

«Aunque todavía no hemos visto a estos grupos emplear ciberherramientas como arma contra infraestructuras críticas, su dependencia de las tecnologías de la información y la adquisición de pericia informática son claros indicadores de alerta».

***Leslie G Wiser**, jefe de la Sección de Estrategia, Prospectiva y Formación del NIPC –FBI- Manifestaciones realizadas ante un Comité de la Cámara de Representantes sobre la investigación de Ramzi Yousef, cerebro del ataque con bomba al Wold Trade Center, agosto 2001.*

El supuesto que se está planteando es perfectamente viable ya que en la actualidad las TIC están diariamente comprometidas por la acción anónima de hackers y organizaciones delictivas, algunas con bastante éxito por la relevancia de los sistemas comprometidos, el número de ordenadores afectados o incluso por los daños económicos causados. Pues bien, lo único que le faltaría a cualquiera de estas acciones para convertirse en una acción ciberterrorista es la motivación o reivindicación por parte de una organización terrorista.

Y en esta línea, el 2 de febrero de 2012, el director del FBI, Robert Mueller, aseguró que «el ciberterrorismo igualará o superará a las amenazas que suponen el modelo de terrorismo actual en un futuro no muy lejano». Tal afirmación la realizó durante su declaración en audiencia ante el Comité de Inteligencia del Senado estadounidense sobre las amenazas mundiales, advirtiendo que el FBI y las agencias de inteligencia deberían cambiar su estructura para hacer frente a este tipo de amenaza, cada vez más fuerte. «Es muy poco lo que hacemos hoy en día con los asuntos relacionados con Internet. El robo de propiedad intelectual, el robo de investigación y desarrollo, el robo de planes y programas empresariales para el futuro, todo ese tipo de asuntos son vulnerables de ser explotados por atacantes». En segundo lugar, señaló que las agencias de inteligencia «han de compartir información, (...) tenemos que construir un colectivo para hacer frente a esa amenaza, de la misma manera que lo hicimos y rompimos las barreras tras el 11 de septiembre».

Alcanzado este punto, ha llegado el momento de identificar y realizar una somera descripción de los mecanismos de Ciberrespuesta que han sido articulados, tanto a nivel nacional como europeo e internacional.

En los últimos años los esfuerzos para la protección, prevención y respuesta, en torno a las catalogadas como IC,s tanto nacionales como europeas, han sido constantes y crecientes. El máximo exponente de ello es la creación en noviembre del 2007 del **Centro Nacional de Protección de Infraestructuras Críticas** (CNPIC)[21], Órgano

21 Nota de Prensa: Centro Nacional de Protección de las Infraestructuras Críticas (CNPIC). El Consejo de Ministros aprobó mediante Acuerdo de 2 de Noviembre de 2007 el marco estructural que permitirá dirigir y coordinar las actuaciones precisas para proteger las infraestructuras críticas en la lucha de España contra el terrorismo. Tiene su base en la Comunicación de la Comisión Europea de 20 de octubre de 2004 sobre protección de las infraestructuras críticas, que contiene propuestas para mejorar la prevención, preparación y respuesta de Europa frente a atentados terroristas que la amenacen.

Ministerial encuadrado en la Secretaría de Estado para la Seguridad del Ministerio del Interior, como responsable de impulsar, coordinar y supervisar los esfuerzos nacionales de adecuación al Plan Europeo de Protección de Infraestructuras Críticas (PEPIC) y su traslación a la normativa nacional, a través del Plan Nacional de Protección de Infraestructuras Críticas (PNPIC), poniendo en marcha importantes iniciativas para alcanzar los objetivos para los que ha sido creado. Estos planes preventivos y medidas de protección se han ido transponiendo de su concepción teórica a su plasmación real a través del Catálogo de Infraestructuras Críticas (CIC); en la actualidad se encuentran incluidos en el precitado CIC la Red Energética, Instalaciones Nucleares, las grandes operadoras y gestoras TIC, Transportes, Agua y Alcantarillado, Alimentación, Salud, Sector Financiero y Bancario, Industria Química, Industria Espacial, Centros de Investigación y Desarrollo y por último la Administración General del Estado. El marco competencial del Centro ha quedado regulado a través de la Ley 8/2011 y el Real Decreto 704/2011.

La actividad desarrollada desde el CNPIC se vio reforzada con la firma, el 5 de marzo de 2013, de un convenio de colaboración entre las Secretarías de Estado de Seguridad (SES-Ministerio del Interior) y la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información (SETSI-Ministerio de Industria), acuerdo que ha permitido que el Instituto para las Tecnologías de la Comunicación (INTECO) se convierta en el (CERT) de las Infraestructuras Críticas nacionales y por extensión del Ministerio del Interior, rebautizado como CERT de Seguridad e Industria.

Asimismo, y con el objetivo de reforzar las capacidades en ciberseguridad y mejorar la coordinación de las acciones de las Fuerzas y Cuerpos de Seguridad del Estado en este ámbito, el 25 de octubre de 2013 fue creada la Oficina de Coordinación Cibernética (OCC), integrada dentro del CNPIC, que servirá de punto de contacto del Ministerio de Interior para todo lo relativo a la ciberseguridad.

Pero las nuevas ciberamenazas no se circunscriben exclusivamente al ámbito de las IC,s ya que el riesgo a una agresión de motivación esencialmente económica, mediante la sustracción de información, campañas de desinformación o sencillamente alterando la normal continuidad de negocio, que afecten gravemente la capacidad competitiva de nuestras empresas y más en estos momentos de crisis económica.

Un nuevo concepto ha surgido en los últimos años de la imbricación de la inteligencia competitiva tradicional con el empleo de las TIC en el ciclo de planeamiento empresarial. Estamos hablando de la inteligencia económica (IE -también conocida como guerra económica en algunos estados como p.ej. Francia-), que no es más que la adaptación de viejos conceptos económicos a nuevas técnicas. Una de ellas, antigua como el arte mismo de la guerra, es la utilización de los servicios de inteligencia en el medio económico. Se ha dado así un nuevo giro a las actividades de inteligencia, naciendo el concepto de IE como el «conjunto de acciones coordinadas de investigación, tratamiento y distribución de la información para tomar decisiones en el orden económico. Acciones que se dirigen tanto al ámbito de la economía nacional como en el dominio empresarial, pues la globalización de los mercados pone también en riesgo a las propias empresas. La defensa de los intereses económicos, por un lado, y, por otro, la necesidad de lograr ventajas respecto de los competidores -a nivel empresarial o estatal- ha sido el motor decisivo del desarrollo de potentes instrumentos de inteligencia económica al servicio de los intereses nacionales y de importantes

empresas transnacionales de muchos países que hoy dominan la escena económica mundial»[22]. La defensa de los intereses nacionales ha de incluir también los aspectos económicos, claves hoy en el mundo global en el que vivimos. Un hecho largamente olvidado en España, que solo desde hace relativamente poco tiempo se ha ocupado de la importancia que tienen los servicios de inteligencia económica, más allá de dotar de seguridad a personas o instalaciones críticas. «La globalización económica -proceso aún en curso - es un movimiento, quizás espontáneo, por el que las naciones se han ido haciendo más interdependientes».

Y encontramos en el **ciberespionaje**, un elemento perturbador y desestabilizador en el legítimo desarrollo económico de las sociedades modernas, los incidentes de esta naturaleza -orientados sobre objetivos económicos- han experimentado un crecimiento viral, afectando a la práctica totalidad del tejido productivo de los países occidentales. Los daños patrimoniales infligidos por esta ciberamenaza se estima que ocasionan unas pérdidas anuales superiores a los 300.000 millones de euros, aunque no existe una cuantificación o estadística fiable a nivel nacional; no así en otros países de nuestro entorno y, por ejemplo, en el 2013 estos daños en el Reino Unido han sido cuantificados en 27.000 millones de libras esterlinas y en la República Federal de Alemania en 45.000 millones de euros.

5. RESPUESTAS A LAS CIBERAMENAZAS

Con respecto a las medidas y planes de protección puestos en marcha destacar la constitución del Centro de Respuesta ante Incidentes de Seguridad Informática de ámbito gubernamental, también conocido como CCN-CERT y dependiente del Centro Criptológico Nacional –Centro Nacional de Inteligencia– Ministerio de la Presidencia; este servicio se creó en el año 2006 como CERT Gubernamental/Nacional español y sus funciones quedaron recogidas en la Ley 11/2002 reguladora del Centro Nacional de Inteligencia, el RD 421/2004 de regulación del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad. De acuerdo a todas ellas, el CCN-CERT tiene responsabilidad en ciberataques sobre sistemas clasificados y sobre sistemas de las Administraciones Públicas y de empresas y organizaciones de interés estratégico para el país. Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopera y ayuda a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas.

Para hacerse una idea más aproximada de la magnitud del problema que suponen las nuevas ciberamenazas, bastan algunos datos estadísticos facilitados por el Centro en su Informe mensual de Ciberseguridad CCN-CERT IS-06/14:

«En el acumulado en los cinco primeros meses del año se ha trabajado sobre un total de 5.300 incidentes. De ellos, 668 tuvieron una criticidad entre muy alta y crítica. Por categorías, los incidentes más detectados fueron aquellos con código dañino (el 80%), intrusiones (17%) y recogida de información (2,13%). Los incidentes son detectados a través de distintas vías, entre ellas el Sistema de Alerta Temprana, SAT, implantado tanto en la red SARA como en Internet (SAT-SARA y SAT-INET). De este modo, al ser detectados, se notifican a los distintos organismos adscritos a este servicio (AGE, Comunidades Autónomas, Ayuntamientos y empresas de interés estratégico).

22 Eduardo Olier Arenas. Cuaderno de Estrategia nº162 del IEEE - La inteligencia económica en el mundo globalizado (mayo 2013).

No obstante, si ampliamos los datos al total de eventos analizados por el CCN- CERT, la cifra se dispara hasta cifras cercanas a los 50 millones. De ellos, 31.827.140 provienen del servicio del SAT-INET y 17.928,576 de SAT SARA. En este sentido conviene reseñar que el Sistema de Alerta Temprana en Internet, tras la incorporación en el mes de mayo de nuevos organismos, está desplegado en un total de 59 organizaciones públicas y privadas (69 sondas).

Por su parte, en el SAT-SARA cuenta con 49 áreas de conexión».

Podríamos también añadir al catálogo de riesgos potenciales, una serie de vulnerabilidades extra que presentan este tipo de infraestructuras:

- Amplia interconexión entre ellas, la caída de una puede acarrear la imposibilidad de operar correctamente otras.
- La gran dependencia tecnológica que de ellas tiene nuestra sociedad, que basa parte de su "modelo del bienestar" en ellas.
- Potencial objeto de ataque directo.
- Potencial objeto de ataque concertado con un atentado convencional.
- Posibilidad de efectos en cascada entre ellas (interdependencia).
- Efectos psicológicos amplificadores.

Toda esta actuación se ve reforzada con la activa y directa participación en foros y grupos de trabajo e instituciones de vigilancia, como son la Agencia Europea de Seguridad de las Redes y de la Información (ENISA), la Red de Centros de Emergencia europeos (CERT,s y CSIRT,s) y de los EE.UU. (US-CERT) o el Centro de Ciberdefensa de la OTAN (CCD-CoE) entre otros.

También contamos con el Convenio Marco de colaboración en materia de Ciberseguridad, entre la Secretaría de Estado de Seguridad del Ministerio del Interior y la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información del Ministerio de Industria, Energía y Turismo, firmado el 4 de octubre de 2012, con el objetivo de mejorar nuestras capacidades de ciberseguridad.

En este sentido la Estrategia de Ciberseguridad de la Unión Europea (ECUE), de 7 de febrero de 2013, «Un ciberespacio abierto, protegido y seguro», representa la visión de conjunto de la UE sobre cómo prevenir y resolver mejor las perturbaciones de la red y los ciberataques. El objetivo consiste en impulsar los valores europeos de libertad y democracia y velar por un crecimiento seguro de la economía digital. Evidencia una creciente preocupación por el más que notable incremento de la delincuencia económica; y es que el tradicional espionaje industrial/económico, dirigido contra grandes corporaciones industriales, preferentemente del ámbito de la Defensa, de corte más bien artesanal, ha cedido el testigo a ciberataques indiscriminados que afectan a todo el tejido industrial básico, formado por las PYMES y los autónomos.

«Cuanta más gente dependa de Internet, más gente dependerá de que la red sea segura. Una red segura protege nuestros derechos y libertades y nuestra capacidad de ejercer actividades económicas. Ha llegado el momento de coordinar nuestra acción: el coste de la inacción es mucho más elevado que el de la acción»[23].

23 Neelie Kroes, vicepresidenta de la Comisión Europea responsable de la Agenda Digital, con ocasión de la presentación de la Estrategia de Ciberseguridad de la UE, rueda de prensa en Bruselas el 7 de febrero de 2013.

La Comisión Europea, junto con la alta representante de la Unión para Asuntos Exteriores y Política de Seguridad, acompañó la presentación de la ECUE de una propuesta de Directiva de la Comisión sobre la seguridad de las redes y de la información (SRI). La Directiva sobre la SRI propuesta es un elemento central de la estrategia de conjunto; exige a todos los estados miembros, facilitadores clave de Internet y operadores de infraestructuras críticas —plataformas de comercio electrónico, redes sociales y operadores de servicios de energía, transportes, banca y sanidad—velar por un entorno digital seguro y fiable en toda la UE.

«Para que el ciberespacio no deje de ser abierto y gratuito, deben aplicarse las mismas normas, los mismos principios y los mismos valores que rigen fuera de él en la UE. Debemos proteger los derechos fundamentales, la democracia y la primacía del Derecho en Internet. La UE está trabajando con sus socios internacionales, así como con la sociedad civil y el sector privado, para promover esos derechos desde una perspectiva global»[24].

La política internacional del ciberespacio de la UE promueve el respeto de los valores europeos esenciales, define las normas sobre comportamiento responsable, impulsa la aplicación al ciberespacio de la legislación internacional vigente, ayudando a los países de fuera de la UE mediante la creación de capacidades de ciberseguridad, y fomenta la cooperación internacional en este ámbito.

«La estrategia pone de relieve nuestras iniciativas concretas para reducir drásticamente la ciberdelincuencia. Muchos países de la Unión carecen de las herramientas necesarias para rastrear y combatir la delincuencia organizada en Internet. Todos los estados miembros deben establecer unidades nacionales de ciberdelincuencia efectivas que puedan beneficiarse de la experiencia y el apoyo del Centro Europeo de Ciberdelincuencia (EC3)»[25].

El documento Estrategia de Ciberseguridad de la Unión Europea propone una visión articulada en cinco prioridades estratégicas:

1. Lograr la ciberresiliencia.
2. Reducir drásticamente la ciberdelincuencia.
3. El desarrollo de la política de ciberdefensa y las capacidades relacionadas con la Política Común de Seguridad y Defensa (PCSD).
4. Desarrollar los recursos industriales y tecnológicos para la ciberseguridad.
5. Establecer una política internacional coherente para la Unión Europea en el ciberespacio y promover valores esenciales de la UE.

Como puede apreciarse deja bien sentada su prioridad: ciberespacio abierto y libre; pero la libertad en línea requiere también protección y seguridad. El ciberespacio debe ser protegido de los incidentes, las actividades maliciosas y el mal uso; y los gobiernos tienen un papel importante para garantizar este «ciberespacio libre y seguro» como salvaguardar el acceso y apertura de respeto y protección de los derechos fundamentales en línea y para mantener la fiabilidad y la interoperabilidad de Internet.

24 Catherine Ashton, alta representante de la Unión para Asuntos Exteriores y Política de Seguridad y vicepresidenta de la Comisión, con ocasión de la presentación de la Estrategia de Ciberseguridad de la UE, rueda de prensa en Bruselas el 7 de febrero de 2013.

25 Cecilia Malmström, comisaria de la UE responsable de los Asuntos de Interior, con ocasión de la presentación de la Estrategia de Ciberseguridad de la UE, rueda de prensa en Bruselas el 7 de febrero de 2013.

Sirvan de ejemplo dos datos relacionados con sendos países de la Europa Occidental y con economías saneadas, como son Alemania y Holanda. Las autoridades de la RFA publicaron un cálculo del «valor intelectual» aportado por sus PYMES en 2013, próximo a los 55.000 millones de euros anuales, estimando a su vez que las pérdidas por ataques cibernéticos de diversa índole supusieron un 40% del total; se está hablando de unas pérdidas anuales de unos 22.000 millones de euros. Mientras que Holanda vino a considerar materialmente imposible hacer frente a todas las amenazas procedentes del ciberespacio, por lo que decidió focalizar sus esfuerzos en ese año tan solo en dos de ellas, centrándose fundamentalmente en la amenaza económica y la amenaza yihadista.

Estas referencias evidencian que la seguridad económica es requisito esencial y parte integral de la Seguridad Nacional, como así se manifiesta en la ESN al hablar de la inestabilidad económico-financiera. Todo estado moderno necesita disponer de capacidad de reacción para evitar los colapsos financieros, tanto públicos como privados, y en ello la integridad económica es un pilar fundamental en la gestión de lo que viene en llamarse resiliencia -entendiendo como tal la capacidad de afrontar una situación crítica con flexibilidad y fortaleza tales que permitan minimizar daños y recuperar estructuras y capacidades-.

En el caso de los EE.UU, La Estrategia Nacional para asegurar el Ciberespacio fue promulgada durante el mandato del presidente George W. Bush, concretamente en el año 2003 y, con posterioridad, vio la luz el Plan Nacional de Protección de Infraestructuras en 2006, que designa hasta 18 sectores críticos que requieren planes de protección específicos e individualizados; prolífica legislatura en esta materia, cerró el círculo con la publicación en 2008 de la Iniciativa Nacional Integral de Ciberseguridad. La Administración del presidente Barak Obama inició sus esfuerzos en ciberseguridad con la publicación en 2009 del estudio «Los sesenta días de examen de las políticas sobre el ciberespacio», que presenta una revisión sólida de dónde estaba el gobierno en relación con la ciberseguridad. La principal recomendación fue que el presidente debería nombrar a un solo coordinador central de los esfuerzos nacionales y del gobierno para las políticas de ciberseguridad. En cuanto a los posicionamientos de los dos partidos en Estados Unidos, tanto republicanos como demócratas convergen en el reconocimiento de que existe una importante amenaza de naturaleza cibernética contra la seguridad nacional y en la necesidad de la cooperación público-privada y del intercambio de información. El presidente Obama ha declarado que la «amenaza cibernética es una de los más graves desafíos de la seguridad económica y nacional al que nos enfrentamos como nación» y que «la prosperidad económica de EE.UU. en el siglo XXI dependerá de la seguridad cibernética». Además, el señor Panetta, que ha sido director de la CIA y secretario de Defensa, advirtió seriamente que EE.UU. se enfrenta a la posibilidad de un «Pearl Harbor cibernético» y que cada día eran más vulnerables ante piratas informáticos extranjeros que podrían desmantelar la red nacional de energía eléctrica, el sistema de transporte, la red financiera o la del gobierno, incluso dijo que «una nación agresora» o grupo extremista podría causar una catástrofe nacional.

Los estadounidenses están muy sensibilizados ante la posibilidad -plausible- de que sus infraestructuras de suministro energético sean objeto de un sabotaje a gran escala y que, como consecuencia de ello y por efecto del conocido como «efecto cascada», otros servicios esenciales queden inoperativos tras la pérdida del primero;

es lo que los analistas denominan «Blackout» o el gran apagón, que de producirse podría desencadenar la destrucción total del modelo social y económico imperante, acarreando impredecibles pero en cualquier caso catastróficas consecuencias.

Más de una docena de organizaciones internacionales –incluyendo las Naciones Unidas, el G-8, la OTAN, el Consejo de Europa, OSCE, el foro Cooperación Económica Asia-Pacifico, la Organización de los Estados Americanos, la Organización para la Cooperación y el Desarrollo Económicos, la Unión International de Telecomunicaciones (UIT) y la Organización Internacional de Normalización (ISO)– están involucradas en seguridad cibernética.

Los **ciberataques** son potentes instrumentos de agresión contra instituciones públicas y privadas, e incluso contra particulares, siendo un fenómeno en auge por los bajos costes y mínimo riesgo para los atacantes, y es que las fronteras físicas han sido rebasadas y aun existe una falta total de consenso en cuanto a la legislación internacional concerniente.

Aunque ya ha sido precintada en varias ocasiones, porque así lo ha exigido la lógica de la secuencia argumental del presente documento, ha llegado el momento de realizar una exposición más pormenorizada de la Estrategia de Seguridad Nacional (ESN), aprobada en Consejo de Ministros el 30 de mayo de 2013, pues es un instrumento que refleja los riesgos y amenazas que son necesarios afrontar, siempre bajo sus principios informadores: Unidad de Acción, Anticipación y Prevención, Eficiencia y Sostenibilidad en el uso de los recursos y Resiliencia o capacidad de resistencia y recuperación.

«La seguridad es un fundamento esencial para el desarrollo y el progreso de una sociedad libre. Por eso, resulta imprescindible un entendimiento básico y generalizado de la importancia de la seguridad como garantía de bienestar de los ciudadanos y de la estabilidad del propio Estado.

Esta visión solo se puede articular a través de una Estrategia que defina un marco de referencia global y omnicomprensivo en materia de seguridad. Una Estrategia que contemple las singularidades de los riesgos y amenazas a los que nos enfrentamos en un mundo que experimenta cambios tan profundos como constantes. Una Estrategia que oriente la acción del Estado de cara a dar respuesta a los desafíos actuales utilizando los recursos disponibles de forma flexible y eficaz. Una Estrategia que potencie nuestras capacidades de prevención, protección y respuesta en un entorno de complejidad creciente como es el actual.

A los riesgos y amenazas tradicionales se suman, en efecto, otros nuevos de naturaleza generalmente transnacional, que se interconectan y potencian su peligrosidad, a la vez que aparecen nuevos espacios abiertos que facilitan su expansión e impacto. El ciberespacio es hoy el ejemplo más claro de un ámbito accesible, poco regulado y de difícil control, y en consonancia, la ciberseguridad es uno de los principales ámbitos de actuación de esta Estrategia (...).

(…) La Estrategia de Seguridad Nacional 2013 ofrece una visión integral de la Seguridad Nacional. Una sociedad responsable y concienciada de su seguridad está en mejores condiciones para hacer frente a los desafíos actuales y ganar en términos de desarrollo y prosperidad...

(…) Las posibilidades de una España segura y de una sociedad fuerte y determinada son ilimitadas. Con esta Estrategia de Seguridad Nacional 2013 avanzamos todos en la dirección adecuada» [26].

Resulta crucial conseguir el objetivo marcado en el ámbito de la Ciberseguridad pues es prioritario por la repercusión que tiene en el resto de los ámbitos, como es la seguridad económica y financiera.

26 Fragmentos del preámbulo de la Estrategia de Seguridad Nacional 2013, firmado por el presidente del Gobierno de España, Mariano Rajoy Brey.

La ESN se articula en torno a cinco capítulos, en los que se ofrece un concepto de Seguridad Nacional, se sitúa la seguridad de España en el mundo, se identifican los riesgos y amenazas actuales, se traza a partir de esta base los objetivos y las líneas de acción estratégicas en los ámbitos de actuación prioritarios para España y se configura un nuevo Sistema de Seguridad Nacional.

Los riesgos y amenazas para la Seguridad Nacional describe los riesgos y amenazas que afectan singularmente a la Seguridad Nacional: los conflictos armados, el terrorismo, las ciberamenazas, el crimen organizado, la inestabilidad económica y financiera, la vulnerabilidad energética, la proliferación de armas de destrucción masiva, los flujos migratorios irregulares, el espionaje, las emergencias y catástrofes, la vulnerabilidad del espacio marítimo y la vulnerabilidad de las infraestructuras críticas y los servicios esenciales. También se contemplan los factores potenciadores como el cambio climático, la pobreza, la desigualdad, los extremismos ideológicos, los desequilibrios demográficos o la generalización del uso nocivo de las nuevas tecnologías, que, sin ser en sí mismos un riesgo o una amenaza, pueden desencadenarlos o agravarlos.

Entre las líneas de acción para alcanzar los objetivos descritos en la ESN destaca: la implantación de una adecuada Cultura de Ciberseguridad, (las sociedades que se hacen responsables de su seguridad son sociedades más libres).

Con la ESN nos encontramos ante lo que se denomina estrategia de primer nivel. El 5 de diciembre de ese mismo año el Consejo de Seguridad Nacional (CSN) aprobó dos nuevas estrategias de segundo nivel y focalizadas a dos de los riesgos identificados en la primera: la Ciberseguridad y la Seguridad Marítima. Ambas estrategias comparten muchos aspectos comunes, aunque sin duda uno de los más destacados es la coincidencia de contemplar las ciberamenazas como una de las principales amenazas. Cronológicamente, la más reciente de las doce amenazas identificadas se ha convertido a su vez en una de las más preocupantes; ya que si bien el ciberespacio es un nuevo ámbito de relación que ha proporcionado el desarrollo de las TIC, también ha diluido las fronteras, permitiendo una globalización sin precedentes que propicia nuevas oportunidades, pero que a su vez conlleva nuevos y preocupantes riesgos y amenazas. Resulta evidente que las ciberamenazas son consideradas como amenaza trasversal y que sin duda estarán presentes en las estrategias que pudieran ser aprobadas en el futuro.

Como ya se ha dicho, en la reunión del 5 de diciembre de 2013 del CSN[27], y en cumplimiento del mandato recogido en la ESN[28], se reunió por segunda vez desde su constitución y aprobó las Estrategias de Ciberseguridad Nacional (ECSN) y de Seguridad Marítima Nacional (ESMN).

La ECSN debe ser considerada como el documento estratégico que sirve de fundamento al gobierno para desarrollar las previsiones de la ESN en materia de protección

27 La estructura del Sistema de Seguridad Nacional se asienta sobre dos organismos de nueva creación: el Consejo de Seguridad Nacional y los Comités especializados. El Consejo es un órgano colegiado de composición amplia y flexible, con reuniones periódicas, y como órganos de apoyo se conformarán los Comités especializados.

28 El 31 de mayo de 2013, el Consejo de Ministros aprobó el documento “Estrategia de Seguridad Nacional. Un proyecto compartido”, una actualización de la anterior ESN de junio de 2011, que articula la Seguridad Nacional como Política de Estado y contiene una serie de directrices a fin de optimizar los recursos estado en aras de la Seguridad Nacional.

del ciberespacio, con el fin último de desarrollar y optimizar un modelo de acciones encaminadas a la prevención, defensa, detección y respuesta frente a las ciberamenazas[29]; dado el carácter transnacional de la ciberseguridad, la cooperación con la Unión Europea y con otros organismos de ámbito internacional o regional con competencias en la materia forma parte esencial de este modelo.

La ECSN debe enmarcarse en el ámbito de la lucha contra las nuevas ciberamenazas[30], entendiendo éstas en sus diferentes vertientes de cibercrimen, ciberterrorismo, hacktivismo, ciberespionaje y ciberguerra, todo ello en línea con los esfuerzos que en materia de Ciberseguridad se vienen impulsando desde el gobierno[31] y la Unión Europea.

Estos ataques ilícitos a las TIC pueden proceder tanto de grupos y organizaciones terroristas, redes de crimen organizado, empresas o estados, como de individuos aislados[32] con motivaciones y cualidades excepcionales. También la ciberseguridad se puede ver comprometida por causas técnicas o fenómenos naturales.

Estas circunstancias son las que explican que sea un objetivo prioritario para el gobierno[33] el garantizar la integridad, confidencialidad y disponibilidad de los sistemas que soportan la prestación de servicios ampliamente utilizados, así como la gestión de las IC,s.

Para contrarrestar estas ciberamenazas se define en la ECSN un ámbito de actuación con un objetivo y unas líneas de acción estratégicas.

Y éste no es otro que el de la ciberseguridad, entendiéndola en su acepción más amplia, cuyo objetivo es el de garantizar un uso seguro de las redes y los sistemas de información a través del fortalecimiento de nuestras capacidades nacionales en la prevención, detección y respuesta a los ciberataques.

29 La Estrategia de Ciberseguridad Nacional es el marco de referencia de un modelo integrado basado en la implicación, coordinación y armonización de todos los actores y recursos del estado, en la colaboración público-privada, y en la participación de la ciudadanía (IEEE - A65 2013).

30 La creciente presencia y dependencia de la sociedad occidental del ciberespacio y su fácil accesibilidad hacen que cada vez sean más frecuentes y preocupantes las intromisiones en este ámbito. En buena medida, el ciberespacio es un medio para la materialización de otros riesgos y amenazas. Los ciberataques, en sus diversas modalidades de ciberterrorismo, ciberdelito, ciberespionaje o hacktivismo en la red, se han convertido en un potente instrumento de agresión contra particulares e instituciones tanto públicas como privadas. El bajo coste, dificultad para imputar autoría y mínimo riesgo que suponen para el atacante y su fácil empleo, efectividad y accesibilidad, son factores que explican la extensión del fenómeno.

31 El borrador de Líneas de Acción de la Guardia Civil en el Exterior 2014, según propuesta de la Jefatura de Información, y siempre en el marco de la ciberseguridad, recoge como reflexión, entre otras cuestiones, que en el combate contra las formas especiales de delincuencia con conexiones internacionales la mayor parte de los analistas internacionales han identificado como parte de las futuras amenazas que pueden poner en riesgo la paz y estabilidad en el mundo el terrorismo, el crimen organizado y las ciberamenazas.

32 La Estrategia de Ciberseguridad Nacional recoge mención expresa a los ciberataques procedentes de la acción de individuos aislados, o lobos solitarios, dentro del catálogo de nuevas ciberamenazas.

33 Desde el Gabinete de Coordinación y Estudios de la Secretaría de Estado de Seguridad, en el marco de la actividad desarrollada por el Grupo de Trabajo de Coordinación de la Ciberseguridad, se afirma que esta amenaza y su adecuada respuesta es una de las tres máximas prioridades del Ministerio del Interior para la presente legislatura.

Este objetivo ambiciona ser conseguido a través del desarrollo de seis líneas de acción que enmarcarán las actuaciones concretas necesarias para la preservación de la denominada Ciberseguridad Nacional.

El documento se estructura en un resumen ejecutivo y cinco capítulos; desarrollándose a continuación un sucinto resumen:

- **"El ciberespacio y su seguridad"**, define el ciberespacio y sus características como un nuevo dominio global y dinámico que está compuesto por las infraestructuras vinculadas a las TIC. Identifica como riesgos y amenazas a la ciberseguridad nacional un amplio espectro proveniente de una multiplicidad de orígenes (individuos aislados, hacktivistas, amenazas internas, delincuencia y criminalidad organizada, terrorismo, espionaje, estados extranjeros, conflictos entre estados, problemas técnicas o fenómenos naturales adversos), pero que comparten técnicas y escenario.

- **"Propósito y principios rectores de la ciberseguridad en España"**, establece el propósito de la ECSN, promovido por el CSN, fija las directrices del uso seguro del ciberespacio con una visión integradora a través de la adecuada coordinación y cooperación de todas las Administraciones Públicas (AA.PP.), contando además con el sector privado y con los ciudadanos.

  Como principios rectores se recogen cuatro que están en sintonía con los principios informadores de la ESN (unidad de acción, anticipación y prevención, eficiencia y sostenibilidad en el uso de los recursos y resiliencia o capacidad de resistencia y recuperación). Estos principios rectores son: el liderazgo nacional y la coordinación de esfuerzos, la responsabilidad compartida, la proporcionalidad, racionalidad y eficacia, así como la cooperación internacional.

  Todo esto desarrollado con la premisa del máximo respeto al ordenamiento jurídico interno e internacional y alentando la presencia española en los organismos y foros de carácter internacional que canalizan las iniciativas y esfuerzos en defensa del ciberespacio.

- **"Objetivos de la ciberseguridad"**, define un objetivo global y seis objetivos específicos. Este objetivo global recoge el ya planteado en la ESN en el ámbito de la ciberseguridad "Garantizar un uso seguro de las redes y los sistemas de información a través del fortalecimiento de nuestras capacidades de prevención, detección y respuesta a los ciberataques". Este fin será recogido en una futura Política de Ciberseguridad Nacional.

  Esta Política estará alineada con iniciativas similares a las de los países de nuestro entorno, así como con las organizaciones europeas e internacionales competentes, en particular, con la ECUE[34]. Para garantizar la protección de los sistemas y la resiliencia de los servicios de las AA.PP,s y las IC,s; así como la disponibilidad de productos, herramientas y desarrollos TIC confiables, para lo que será necesario potenciar, impulsar y reforzar las capacidades nacionales de investigación y desarrollo en ciberseguridad de las TIC. Para ello se velará por

34 La Estrategia de Ciberseguridad Europea fue aprobada por la Comisión Europea el pasado 2 de febrero de 2013.

la utilización de componentes que estén certificados conforme a normas internacionalmente y nacionales reconocidas.

Los otros seis objetivos específicos se vinculan a:

1. Administraciones Públicas, garantizar que los Sistemas de Información y Telecomunicaciones utilizadas por las AA.PP,s posean el adecuado nivel de seguridad y resiliencia, mediante la implantación de un marco nacional, coherente e integrado, de políticas, procedimientos y normas técnicas.
2. Empresas en general y operadores de IC,s en particular, impulsar la seguridad y la resiliencia de las redes y los sistemas de información usados por el sector empresarial en general y los operadores de infraestructuras críticas en particular, como principio garante de la adecuada protección del "Patrimonio Tecnológico de España".
3. Ámbitos Judicial y Policial, potenciar las capacidades de prevención, detección, respuesta, investigación y coordinación frente a las actividades del terrorismo y la delincuencia en el ciberespacio. Para ello se estima como imprescindible el fortalecimiento de la cooperación judicial y policial internacional, articulando los instrumentos adecuados de colaboración e intercambio de información y la armonización de las legislaciones nacionales.
4. Sensibilización, concienciar a los ciudadanos, profesionales, empresas y AA.PP,s españolas de los riesgos derivados del ciberespacio.
5. Capacitación, alcanzar y mantener los conocimientos, habilidades, experiencia y capacidades tecnológicas que necesita España para sustentar todos los objetivos de la ciberseguridad, fomentando una actividad en I+D+i efectiva.
6. Colaboración internacional, contribuir a la mejora de la ciberseguridad, apoyando el desarrollo de una política de ciberseguridad coordinada en la Unión Europea y en las organizaciones internacionales[35], así como colaborar en la capacitación de estados que lo necesiten a través de la política de cooperación al desarrollo.

- "**Líneas de acción de la ciberseguridad Nacional**", se centra en detallar las líneas de acción que habrán de articularse para alcanzar los objetivos señalados en el capítulo precedente.

  ♦ LA-1: Capacidad de prevención, detección, respuesta y recuperación ante las ciberamenazas.

  1. Ampliar y mejorar las capacidades de detección y análisis de ciberamenazas.

35 Se fomentará la cooperación en el marco de la UE y con organizaciones internacionales y regionales como la Agencia Europea de Defensa (EDA), la Agencia Europea de Seguridad de las Redes y de la Información (ENISA), el Centro Europeo de Ciberdelincuencia, adscrito a Europol, la Organización de Naciones Unidas (ONU), la Organización para la Seguridad y la Cooperación en Europa (OSCE), la Organización del Tratado del Atlántico Norte (OTAN) y la Organización para la Cooperación y Desarrollo Económicos (OCDE), entre otras.(Extracto literal de la ECSN).

2. Fortalecer las capacidades de detección y respuesta ante ciberataques, garantizar la coordinación, la cooperación y el intercambio de información entre los diferentes actores, asegurar la cooperación de los organismos con responsabilidades en ciberseguridad, en especial entre el CERT de la Administración Pública del Centro Criptológico Nacional (CCN-CERT), el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas (MCCD) y el CERT de Seguridad e Industria (CERT-SI).
3. Desarrollar procedimientos de respuesta frente a situaciones de crisis y planes de contingencia específicos.
4. Desarrollar y ejecutar un Programa de Ejercicios de Simulación de Incidentes de Ciberseguridad, ampliar y mejorar permanentemente las capacidades de Ciberdefensa de las Fuerzas Armadas que permitan una adecuada protección de sus Redes y Sistemas de Información y Telecomunicaciones, así como de otros sistemas que afecten a la Defensa Nacional y potenciar las capacidades militares y de inteligencia para ejercer la respuesta oportuna, legítima y proporcionada en el ciberespacio ante amenazas o agresiones que puedan afectar a la Defensa Nacional.

- LA-2: Seguridad de los Sistemas de Información y Telecomunicaciones que soportan las Administraciones Públicas.

1. Asegurar la plena implantación del Esquema Nacional de Seguridad, ampliar y mejorar las capacidades del CERT de las Administraciones Públicas (CCN-CERT).
2. Optimizar el modelo de interconexión de los organismos de las Administraciones Públicas.
3. Reforzar la implantación y seguridad de la infraestructura común y segura en la Administración Pública española (Red SARA), potenciando su uso y sus capacidades de seguridad y resiliencia.

- LA-3: Seguridad de los Sistemas de Información y Telecomunicaciones que soportan las Infraestructuras Críticas.

1. Asegurar la implantación de la normativa sobre Protección de las Infraestructuras Críticas.
2. Ampliar y mejorar las capacidades del CERT de Seguridad e Industria (CERT-SI), potenciando la colaboración y coordinación del CNPIC con los diferentes órganos con capacidad de respuesta ante incidentes y con las unidades operativas de las Fuerzas y Cuerpos de Seguridad del Estado.
3. Impulsar la participación del sector privado en los Programas de Ejercicios de simulación de incidentes de Ciberseguridad.
4. Desarrollar modelos de simulación.

- LA-4: Capacidad de investigación y persecución del ciberterrorismo y la ciberdelincuencia.

1. Integrar en el marco legal español las soluciones a los problemas que surjan relacionados con la ciberseguridad para la determinación de los tipos penales y el trabajo de los departamentos competentes.
2. Ampliar y mejorar las capacidades de los organismos con competencias en la investigación y persecución del ciberterrorismo y la ciberdelincuencia así como asegurar la coordinación de estas capacidades con las actividades en el campo de la ciberseguridad, a través del intercambio de información e inteligencia por los canales de comunicación adecuados.
3. Fortalecer la cooperación policial internacional y fomentar la colaboración ciudadana, articulando los instrumentos de intercambio y transmisión de información de interés policial.
4. Asegurar a los profesionales del derecho el acceso a la información y a los recursos que les proporcionen el nivel necesario de conocimientos en el ámbito judicial para la mejor aplicación del marco legal y técnico asociado. En este sentido, es especialmente importante la cooperación con el Consejo General del Poder Judicial, la Abogacía del Estado, la Fiscalía General del Estado, la Fiscalía Coordinadora de la Criminalidad Informática y el Consejo General de la Abogacía Española.

♦ LA-5: Seguridad y resiliencia de las TIC en el sector privado.

1. Impulsar la cooperación entre los sectores público y privado.
2. Promover la cooperación entre sectores con el fin de mejorar conjuntamente las capacidades de detección, prevención, respuesta y recuperación frente a los riesgos de seguridad del ciberespacio.
3. Impulsar el desarrollo de estándares en ciberseguridad.

♦ LA-6: Conocimientos, Competencias en I+D+i.

1. Desarrollar un marco de conocimientos de ciberseguridad en los ámbitos técnico, operativo y jurídico, programas de captación de talento, investigación avanzada y capacitación en ciberseguridad en cooperación con universidades y centros especializados.
2. Fomentar el desarrollo industrial de productos y servicios en materia de ciberseguridad.
3. Impulsar la dinamización del sector industrial y las actividades de certificación de ciberseguridad.
4. Impulsar modelos y técnicas de análisis de riesgos cibernéticos.

♦ LA-7: Cultura de ciberseguridad.

1. Impulsar las actividades de sensibilización entre ciudadanos y empresas con acceso a información relativa a vulnerabilidades, ciberamenazas e información sobre cómo proteger mejor su entorno tecnológico.
2. Propiciar el desarrollo de programas de concienciación en ciberseguridad.

3. Fomentar los mecanismos para apoyar a empresas y profesionales en el uso seguro de las TIC.

4. Asesorar y dar soporte al desarrollo de módulos educativos de sensibilización en ciberseguridad dirigidos a todos los niveles de la enseñanza.

♦ LA-8: Compromiso Internacional.

1. Potenciar la presencia de España en organizaciones y foros internacionales y regionales sobre ciberseguridad.

2. La implantación de la Estrategia de Ciberseguridad de la UE.

3. Fomentar la cooperación con la OTAN en materia de Ciberdefensa.

- **"La ciberseguridad en el Sistema de Seguridad Nacional"**, establece la estructura orgánica al servicio de la ciberseguridad que responde a la visión integral del documento con objeto de dar una respuesta conjunta y adecuada para preservar la ciberseguridad. Esta estructura orgánica está formada por tres componentes, los dos últimos de nueva creación, bajo la dirección del presidente del Gobierno: a) el Consejo de Seguridad Nacional; b) el Comité Especializado de Ciberseguridad; c) el Comité Especializado de Situación, único para el conjunto del Sistema de Seguridad Nacional.

  ♦ El Comité Especializado de Ciberseguridad dará apoyo al presidente del Gobierno y al propio CSN para coordinar la Política de Seguridad Nacional en el ámbito de la ciberseguridad. Se encargará, además, de reforzar las relaciones de coordinación, colaboración y cooperación entre las distintas AA.PP,s con competencias en materia de ciberseguridad, así como entre los sectores públicos y privados, y facilitará la toma de decisiones del propio CSN mediante el análisis, estudio y propuesta de iniciativas tanto en el ámbito nacional como en el internacional.

  Este Comité estará compuesto por representantes de los distintos ámbitos de las Administraciones Públicas afectados, amén de otros actores pertenecientes al sector privado y especialistas en ciberseguridad.

  La presidencia de este Comité será rotatoria y tendrá periodicidad anual. La rotación se hará entre altos representantes de los ministerios de la Presidencia, del Interior, de Industria, Energía y Turismo, de Defensa y de Asuntos Exteriores y de Cooperación; para este primer periodo ha sido designado el director del CNI.

  ♦ Por otra parte el Comité Especializado de Situación, único para el conjunto del Sistema de Seguridad Nacional, será convocado para gestionar las situaciones de crisis de ciberseguridad que, por su transversalidad o su dimensión, desborden las capacidades de respuesta de los mecanismos habituales. Contará con el apoyo del Centro de Situación del Departamento de Seguridad Nacional para garantizar su interconexión con los centros operativos implicados y dar una respuesta adecuada en situaciones de crisis, facilitando su seguimiento y control y la trasmisión de las decisiones.

Los dos Comités Especializados actuarán de forma complementaria, cada uno en su ámbito de competencias, con una misma dirección estratégica y política del Consejo de Seguridad Nacional presidido por el presidente del Gobierno.

La última iniciativa, a nivel nacional, que por su relevancia se estima importante reseñar en este documento, es la constitución, en septiembre de 2012, del Centro Nacional de Excelencia en Ciberseguridad (CNEC) que, bajo los auspicios de la UE y de su programa ECTEG (European Cybercrime Training and Education Group) e integrado en la Red Europea de Centros de Excelencia -2CENTRE- coordinados por el EC3 de EUROPOL, pretende facilitar la más alta capacitación en ciberseguridad e informática forense a los miembros de las Fuerzas y Cuerpos de Seguridad del Estado, a través del desarrollo de cursos específicos que posibiliten la ampliación y mejora de las capacidades de prevención, detección y análisis de ciberamenazas, detección y respuesta ante ciberataques, lucha contra el ciberdelito, creación de programas de certificación y acreditación -desarrollado a través de la Agencia de Certificación de Seguridad (ACS)- y el apoyo a la potenciación de las capacidades de I+D+i de las PyMEs.

Ambos -el CNEC y la ACS- operan bajo el manto del Instituto de Ciencias Forenses y de la Seguridad (ICFS) de la Universidad Autónoma de Madrid. En diciembre de 2010 el ICFS y la SES firmaron un convenio de colaboración para la investigación y cooperación educativa, reportando evidentes beneficios a ambos.

Una muestra palpable de la creciente preocupación y alta sensibilización con la que se vive la problemática de la ciberseguridad, desde el Gobierno de España y en lo que a Fuerzas de Seguridad del Estado concierne, se vivió en las jornadas previas y durante los actos de Proclamación de SAR Don Felipe de Borbón y Grecia como Rey de España, pues por primera vez en nuestra historia se contempló y activó un dispositivo específico y concreto de ciberseguridad. La Instrucción núm. 11/2014 de la SES así lo contempló, ordenando cometidos concretos al CNPIC y la OCC, así como a las unidades especializadas de los Cuerpos.

6. CIBERSEGURIDAD Y GUARDIA CIVIL

La amenaza del uso de Internet y de las Tecnologías de la Información y Comunicaciones (TIC) por parte de organizaciones terroristas o afines, y la adecuación de los procedimientos de actuación y respuesta ante la misma por parte de la Guardia Civil, se convirtieron en una de sus prioridades desde el año 2000, como así lo atestiguan informes y estudios del entonces Servicio de Información.

Estos estudios y planes iniciaron su materialización en noviembre del 2002, con la incorporación al Servicio del primer personal expresamente seleccionado para conformar el embrión del entonces Subgrupo de Ciberterrorismo; desarrollando su primera actuación de apoyo especializado, en beneficio de una Unidad de Investigación de la Jefatura de Información, en febrero de 2003.

Una constante, desde entonces y hasta la actualidad, ha sido la firme apuesta por este proyecto y el decidido empeño de los sucesivos mandos del entonces Servicio y actual Jefatura de Información, con la lógica “complicidad” de las más altas instancias de la Institución.

De esta forma en 2007 se conformó como **Grupo de Ciberterrorismo**; pero sin duda la fecha más emblemática la encontramos en el 31 de marzo de 2011, cuando el entonces Grupo de Ciberterrorismo se incorporó, junto con otras unidades de claro perfil tecnológico como son los Grupos Técnico Informático y de Interceptación de las Telecomunicaciones, al nuevo y ambicioso proyecto de integrar capacidades y esfuerzos bajo el manto de la creada Área Técnica de la Jefatura de Información, al mando de un coronel.

Paralelamente, en diciembre del 2012 se constituyó la Unidad de Ciberseguridad, como otra ambiciosa apuesta ante la creciente preocupación por esta amenaza.

En la actualidad lo integra un equipo humano polivalente y multidisciplinar de muy alta cualificación, dotado de novedosos sistemas tecnológicos y herramientas informáticas, todo ello con muy significativas inversiones económicas y evidentes esfuerzos y sacrificios de otras unidades de la Jefatura para atender la constante demanda de incremento de recursos humanos.

Se puede afirmar con absoluta certeza y rotundidad que son Unidades pioneras a nivel nacional y con dilatada experiencia, tanto en el apoyo a la investigación y represión de la actividad terrorista en Internet como en la labor divulgativa y de sensibilización, sobre un concepto ahora en auge como es el de la Ciberseguridad y las Ciberamenazas. Sirvan para ilustrar esta afirmación los siguientes datos:

- En enero de 2005 se llevó a cabo la primera operación contra una intrusión en sistemas informáticos del Departamento de Defensa de los Estados Unidos y, en marzo de 2007 (y tras diez meses de investigación), se culminó con éxito la primera operación, desarrollada en Europa, contra una cédula de la denominada Yihad Informativa o Global Islamic Media Front.

- En 2006 la Jefatura de Información inició su actividad divulgativa y de sensibilización, que la ha llevado a participar activamente en un sinfín de cursos, seminarios y conferencias organizados por el Consejo General del Poder Judicial, la Fiscalía General del Estado, la Escuela Superior de las Fuerzas Armadas, la Agencia Estatal de Seguridad Aérea o universidades tanto públicas como privadas (Universidad Internacional Menéndez Pelayo, Complutense, Autónoma de Madrid, Politécnica de Madrid, de Alcalá, Carlos III, de Murcia, de Granada, de Sevilla, de Santiago, de la Rioja, de Navarra, Universidad Nacional de Educación a Distancia, Francisco de Vitoria, Camilo José Cela y Rey Juan Carlos, entre otras), así como en infinidad de eventos organizados por colegios oficiales y asociaciones profesionales, fundaciones o empresas, además de los organizados por la propia Institución, la SES, el CNPIC o INTECO, entre otros.

- En el ámbito internacional destacar que la Jefatura de Información ha sido pionera en este campo, pues ha hablado de la problemática del Ciberterrorismo y de la Protección de Infraestructuras Críticas, antes incluso que la creación de instituciones y organismos tan de actualidad como el CNPIC, el INTECO o el propio Centro Criptológico Nacional. Y, en esta línea, integrantes de la Unidad de Ciberseguridad han participado en multiplicidad de eventos en Europa (Alemania, Francia, Inglaterra, Irlanda, Italia, Holanda, Bélgica, Polonia, Rumanía, Albania, Grecia, Turquía y Rusia), en América (Estados Unidos, Canadá, México, Colombia, Uruguay, Perú, Chile y Argentina), en el Magreb (Marruecos,

Argelia y Egipto) y Oriente Medio (Israel y Líbano), en Asia (Corea y Singapur) y Oceanía (Australia).

También es destacable que fue en mayo de 2007 cuando se inició este ya largo periplo en Colombia, de la mano de la Agencia Española de Cooperación Internacional. En noviembre de ese mismo año fueron los Estados Unidos, de la mano del Comité contra el Terrorismo de la Organización de Estados Americanos y del propio Servicio Secreto de los Estados Unidos, donde se llevaron a cabo nuevas actividades. El último, y más reciente encuentro, ha sido Argelia, en junio de 2014 donde, de la mano de la Oficina de las Naciones Unidas contra la Droga y el Delito, se han impartido cursos completos de capacitación en investigación en Internet y nuevas tecnologías, así como informática forense.

- Desde 2009, la Unidad de Ciberdelincuencia ha participado en los cuatro Ejercicios Nacionales en Ciberdefensa, organizados por la División de Seguridad CIS del Estado Mayor Conjunto del Ministerio de Defensa, así como en dos Ejercicios CDX de Ciberdefensa de la OTAN, integrada en el equipo nacional seleccionado por la precitada DIVCIS-EMACON (el primero bajo el nombre “Locked Shields 2013” CDX13, organizado por el Centro de Excelencia en Ciberseguridad (CCD-CoE) desde Tallín (Estonia), y, el segundo CDX14, organizado por el mando Conjunto de Ciberdefensa (MCCD) del Ministerio de Defensa).

BIBLIOGRAFÍA

VV.AA. (2010) Ciberseguridad. Retos y amenazas a la Seguridad Nacional en el ciberespacio. Cuaderno de Estrategia del Instituto Español de Estudios Estratégicos, 149.

Clarke, R. A., y Knake, R. K. (2011). Guerra en la red. Los nuevos campos de batalla. Barcelona: Ariel.

Comisión Europea. Estrategia de Ciberseguridad de la Unión Europea. 7/02/2013.

Departamento de Seguridad Nacional y Presidencia del Gobierno. Estrategia de Seguridad Nacional. 31/05/2013.

Departamento de Seguridad Nacional y Presidencia del Gobierno. Estrategia de Ciberseguridad Nacional. 5/12/2013.

Departamento de Seguridad Nacional y Presidencia del Gobierno. Estrategia de Seguridad Marítima Nacional. 5/12/2013.

Departamento de Seguridad Nacional y Presidencia del Gobierno. Informe Anual de Seguridad Nacional 2013. Julio 2014.

VV.AA. (2012) El Ciberespacio. Nuevo escenario de confrontación. Monografía del Centro Superior de Estudios de la Defensa Nacional, 126.

VV.AA. (2014) Energía y Geoestrategia 2014. Cuaderno de Estrategia del Instituto Español de Estudios Estratégicos, 166.

VV.AA. (2014) Informe Mensual de Ciberseguridad. Centro Criptológico Nacional Computer Emergency Response Team, IS-06/14.

VV.AA. (2013) La inteligencia económica en un mundo globalizado. Cuaderno de Estrategia del Instituto Español de Estudios Estratégicos, 162.

VV.AA. (2013) Los Potenciadores del riesgo. Cuaderno de Estrategia del Instituto Español de Estudios Estratégicos, 159.

VV.AA. (2013) Necesidad de una conciencia nacional de ciberseguridad. La ciberdefensa: un reto prioritario. Monografía del Centro Superior de Estudios de la Defensa Nacional, 137.

Spitzer, M. (2013). Demencia Digit@l. El peligro de las nuevas tecnologías. Barcelona: B.

Unión Internacional de Telecomunicaciones. Aspectos generales de la ciberseguridad. Recomendación UIT-T X.1205. 18/04/2008.

Fecha de recepción: 14/05/2014. Fecha de aceptación: 24/06/2014

HACKTIVISMO

JOSE LUIS MAYORGA MARTÍN

RESUMEN

Las nuevas tecnologías y el ciberespacio han propiciado la aparición de nuevos modos de realizar acciones reivindicativas. El hacktivismo, como conjunción de la acción política directa con el empleo de técnicas de hacking, es uno de ellos. Además del hacktivismo existen otras formas similares de cometer acciones a través del ciberespacio con un marcado trasfondo político y que las diferencian claramente del cibercrimen, pero es necesario analizarlas para no confundirlas con otras acciones perpetradas por grupos hacktivistas. Este es el caso del ciberactivismo, el ciberespionaje, el ciberterrorismo o la ciberguerra.

Dentro de los grupos hacktivistas se encuentra el colectivo Anonymous, quizás el más conocido y singular. Colectivo sin organización ni estructura, lo que le ha permitido obtener un éxito y una repercusión sin precedentes gracias a la fascinación que despiertan en el público en general y la facilidad de colaboración con ellos.

Palabras clave: Hacktivismo, Anonymous, hacking, acción política, ciberespacio, ciberterrorismo, ciberespionaje, ciberguerra.

ABSTRACT

The new technologies and the cyberspace have promoted the existence of new ways of recognition actions. “Hacktivism”, known as the direct political action by hacking strategies, is one of these ways. Besides “hacktivism” there are other similar paths to commit such actions through cyberspace. These paths are also characterized by the political action and are quite differenciated from the “cybercrime”. Nevertheless, it is compulsory to analyze them in order to avoid possible confusions with “hacktivist groups” actions. This is the case of the “ciberactivism”, “cyberespionage”, “cyberterrorism” or the “cyberwar”.

Within the activist groups we may find “Anonymous”. This might be the most known and also the most peculiar one. This group doesn’t have any type of organization or structure, which has let them to gain great success and an unprecedented repercussion as a consequence of the general public fascination and the easiness to collaborate with them.

Key words: Hacktivism, Anonymous, hacking, political action, cyberspace, cyberterrorism, cyberespionage, cyberwarfare.

1. INTRODUCCIÓN

Es indudable que el cambio tecnológico experimentado desde mediados del siglo pasado ha calado profundamente en la sociedad. La tecnología se ha infiltrado en todas las facetas de nuestra vida cotidiana. Términos como correo electrónico,

Internet, smartphone, ordenador, redes sociales, etc. se han incorporado a nuestro lenguaje diario y a nuestra forma de vida; es más, para muchos de nosotros resulta difícil imaginarse como podíamos vivir hace unos años sin este tipo herramientas tecnológicas. Al igual que el fuego era indispensable en la sociedad prehistórica, las Tecnologías de la Información y la Comunicación (TIC) se han convertido en un elemento esencial dentro de nuestra sociedad, incorporándose a todo tipo de facetas como la educación, la comunicación, la industria, el comercio y, por supuesto, la acción política. No hay sector donde no se hayan introducido con fuerza y hayan supuesto un cambio importante a tener en cuenta, tanto que muchos las definen como una auténtica revolución.

El término hacker[1] (Raymond, 1996) ha pasado a formar parte de nuestra vida cotidiana y, de una forma simplista, para la inmensa mayoría de nosotros denota a una persona que utiliza sus conocimientos informáticos para acceder de forma ilegal a sistemas informáticos, ya sea sólo para demostrar su valía o porque tenga alguna motivación económica, política o simplemente destructiva o lúdica. Nada más lejos de la realidad, la comunidad hacker está formada por un conjunto de familias que, agrupadas en motivaciones más o menos comunes, no tienen que realizar siempre acciones al margen de la ley.

En realidad, los hackers han sido fundamentales en el desarrollo de Internet y de las nuevas tecnologías, en muchas ocasiones de forma totalmente altruista y desinteresada (Castells, 2001), y en otras obteniendo pingües beneficios gracias a la comercialización de sus descubrimientos (Himanen, 2004).

Por otro lado, no es menos cierto que todos conocemos noticias de intrusiones, robos de información confidencial, ataques DDoS (Distributed Denial of Service), virus, troyanos, etc., también cometidos o desarrollados por supuestos hackers.

Desde luego el submundo hacking no es homogéneo y el hecho de intentar clasificar a personas siempre es una tarea difícil. Newbies, Black hackers, White hackers, Lamers, Phreakers, Crakers, Carders, Piratas software, Ciberokupas, Ciberpunks, Carders, Phisers, Samurais, Ubecrackers, Geeks, etc. forman parte de la comunidad que, a modo de simplificación (y normalmente por desconocimiento), identificamos como Hackers, aunque cada una de estas familias tiene sus signos distintivos unidos por el común denominador de la utilización de unas técnicas y procedimientos parecidos para la consecución de sus objetivos, todo ello sin que se haya puesto el foco en la motivación que les empuja a la realización de actos que, en muchas ocasiones, pueden considerarse como delito.

En este sentido, aunque los motivos para realizar actos utilizando técnicas hacking pueden ser muy dispares, se podría simplificar englobándolos en tres grandes grupos: los que tienen un trasfondo económico, principal motor de la mayoría de estas acciones, sea desde un punto de vista positivo, ayudando a las empresas y gobiernos a fortalecer sus medidas de seguridad, o negativo, donde se persigue el lucro a través del delito y es lo que comúnmente denominamos ciberdelincuencia; también existen motivaciones totalmente altruistas, que persiguen el conocimiento y que el mismo fluya sin ataduras; aquí estarían las acciones de los seguidores de la denominada ética Hacker; y por último estarían los que realizan sus acciones por cuestiones

1 http://dictionary.cambridge.org/dictionary/american-english/hack

políticas/reivindicativas de diferente índole, incluidas las acciones de los denominados ciberactivistas, hacktivistas, ciberterroristas, ciberespías o cibersoldados.

Esta clasificación por genérica y amplia no pretende ser absoluta ni estanca pues, como en muchas otras facetas de la vida, a una persona pueden moverla varias motivaciones a la vez y con diferente intensidad, alimentando el motor de sus actos individuales, o ir pasando de unas a otras en función de sus condicionantes personales.

Actor	Intención	Objetivo principal	Recursos	Volumen	Visibilidad
Estados	Mejorar su posición geopolítica (mejorar su posición de poder en el ámbito interno)	Organismos del gobierno, multinacionales, ciudadanos (en el caso de regímenes específicos)	Alto	Medio	Baja
Organizaciones privadas	Mejorar su posición informativa	Sus competidores	Alto	Bajo	Bajo
Criminales profesionales	Lucro económico	Empresas y ciudadanos	Media a alta	Alto	Media a baja
Terroristas	Infundir terror, objetivos políticos	Objetivos de alto impacto, objetivos seleccionados por motivaciones ideológicas	Pocos para promediar	Bajo	Alto
Hacktivistas	Propagar una ideología	Objetivos seleccionados por motivaciones ideológicas	En la media	En la media	Alto
Script kiddies	Para comprobar si es posible realizarlo, por diversión	Cualquiera	Baja	Alta	En la media
Ciber investigadores	Para revelar debilidades, para mejorar sus habilidades	Cualquiera	En la media	Baja	Alta
Actores internos	Venganza, incompetencia, falta de cuidado	Entorno de trabajo anterior o actual	Alta (fácil acceso a recursos internos)	Baja	Baja

Actores con sus motivaciones y características.

(National Cyber Secutity Centre, 2012)

2. HACKTIVISMO: DEFINICIÓN Y ANTECEDENTES HISTÓRICOS

Realizar una definición de hacktivismo[2] es relativamente simple, es la fusión del hacking y el activismo, la utilización de las técnicas hackers para una causa política (Garaizar, 2004). El término hacker se utiliza en referencia a su significado original, es decir, una persona que disfruta explorando los detalles de sistemas programables y cómo ampliar sus funcionalidades, mientras que activismo se define como la práctica de la acción directa y militante para conseguir una meta social o política.

El hacktivismo, al igual que otras familias dentro del submundo hacker, se podría dividir en dos movimientos diferenciados (Lizama, 2005):

2 En algunas publicaciones se puede ver escrita la palabra como hactivismo.

- El hacktivismo digitalmente correcto. Que antepone el valor tecnológico al político-social, buscando remediar en Internet el problema de los códigos de software que restringen la información[3]; una labor que fundamentalmente es llevada a cabo por una élite de hackers con amplios conocimientos de programación (como ejemplo los colectivos Cult of The Dead Cow y Hacktivismo[4]).

Imagen representativa del hacktivismo digitalmente correcto

- El hacktivismo digitalmente incorrecto. Que privilegia los efectos político-sociales sobre los tecnológicos que usa Internet como un medio publicitario y de presión semántica para promover la justicia social, que se organiza a partir de una élite con un conocimiento no experto de la programación (p.ej. Electronic Disturbance Theater, los yippies[5], Etoy, etc.) y que requiere el apoyo estratégico de los usuarios de Internet.

Aunque nos parezca un término nuevo que ha surgido a raíz de la aparición principalmente de Anonymous, el hacktivismo se remonta a los orígenes de la red, los yippies, la Free Software Foundation (FSF) o los primeros cypherpunks (entre ellos Philip Zimmermann, creador del software de cifrado PGP). Los ideales de acceso universal a las computadoras, libre flujo de información y derecho a la privacidad son una constante de la cultura hacker del "do it yourself" o el "information wants to be free". Pero el término hacktivismo no surgirá hasta mucho más tarde (no obstante, existen discrepancias de cuando exactamente se utilizó por primera vez el término que podríamos situar sobre la segunda mitad de la década de los noventa (Paget, 2012)).

Desde ese momento, el hacktivismo siempre ha estado muy vinculado con movimientos de izquierdas, extrema izquierda o incluso anarquista, aunque, como uso mediático de la tecnología que precisan sus acciones, está al servicio de cualquier ideología[6].

3 Como caballo de batalla emblemático es su defensa a ultranza del software de código libre (en inglés "Open Source") y el fomento del copy left.

4 http://centrodeartigo.com/articulos-revista-digital/contenido-revista-36328.html

5 http://es.urbandictionary.com/define.php?term=yippie

6 Morrocan Ghost o Syrian Electronic Army son dos ejemplos de grupos hacktivistas nacionalistas (con un cierto corte islamista) que no se ajustarían al perfil de los grupos hacktivistas normalmente militantes de izquierdas.

A modo de resumen, se exponen las fechas y acciones más relevantes realizadas por el movimiento hacktivista en sus orígenes (Paget, 2012):

Fechas	Acciones destacadas
12/09/1981	Se funda en Berlín la organización Chaos Computer Club.
1984	Se publica el libro Hackers: Heroes of the Computer Revolution (Hackers, los héroes de la revolución informática), de Steven Levy.
08/01/1986	Se publica por primera vez el manifiesto The Hacker Manifesto, de Loyd Blankenship (alias "The Mentor").
16/10/1989	Mediante el uso del protocolo DECNET, un gusano llamado WANK (del inglés, Worms Against Nuclear Killers, gusanos contra los asesinos nucleares) se propaga por la red informática de la NASA en Maryland. Uno de sus objetivos era difundir un mensaje denunciando los peligros de los ensayos nucleares.
05/11/1994 (Día de Guy Fawkes)	Los Yippies lanzan un ataque de denegación de servicio distribuida (DDoS) y una campaña de envío masivo de correo a los servidores del gobierno británico para protestar contra una ley que prohíbe los conciertos de música con un ritmo repetitivo al aire libre.
21/12/1995	En Italia, el grupo Strano Network decide bloquear sitios web franceses para protestar contra los ensayos nucleares en Mururoa.
09/02/1996	John Perry Barlow publica A Declaration of the Independence of Cyberspace (Una declaración de independencia del ciberespacio).
30/06/1997	El grupo de hackers portugués UrBan Ka0s ataca cerca de 30 sitios web del gobierno indonesio para llamar la atención sobre la opresión que sufren los habitantes de Timor.
29/01/1998	En apoyo a las guerrillas zapatistas, se celebra una manifestación virtual en respuesta a una masacre cometida por fuerzas paramilitares en un pueblo de Chiapas, México.
Noviembre de 1999	Toywar: un acto de resistencia contra el distribuidor de juguetes eToys Inc., que había demandado a un grupo de artistas con el pretexto de que su nombre de dominio era demasiado parecido al de ellos.
03/12/1999	El grupo Electrohippies Collective organiza una sentada virtual, en la que todos sus seguidores deben visitar las páginas web de la Organización Mundial del Comercio para bloquear el comunicado final de la conferencia de Seattle, Washington, con el fin de impedir su difusión.
10/06/2001	Para protestar contra el uso de los aviones de la compañía Lufthansa con el fin de deportar a inmigrantes sin papeles de Alemania, dos redes humanitarias alemanas organizan una protesta virtual para bloquear el sitio web de la aerolínea mediante el envío masivo de mensajes de correo electrónico.

A partir de 2003 se experimenta un salto cualitativo en el movimiento hacktivista. La aparición en escena de Anonymous (colectivo que se analizará más adelante) y las filtraciones publicadas por WikiLeaks, revolucionaron Internet y la manera en que estos movimientos llevaban a cabo sus acciones, las cuales pasaron de estar centradas en la disponibilidad de la información (normalmente con ataques DDoS o Defacement[7] de páginas web), a centrarse en los últimos años en el acceso y difusión de datos confidenciales.

7 Según el CCN, "el ataque de denegación de servicio (conocido como DoS, por sus siglas en inglés Denial Of Service) es un tipo de ataque informático orientado a interrumpir la disponibilidad de un servicio provocando que usuarios legítimos no dispongan de acceso al mismo" (CCN-CERT, 2013). El ataque DoS más común ocurre cuando un atacante "inunda" de peticiones de información al servidor que aloja el sitio web de destino. Los servidores sólo pueden procesar un número determinado de solicitudes concurrentes; con este tipo de ataques se sobrecarga de peticiones al servidor, provocando que se ralentice o se vea incapaz de responder a las mismas y deje de funcionar. Una variante del DoS es la denegación de servicio distribuida, también conocido como DDoS por sus siglas en inglés Distributed Denial of Service, donde no existe un único equipo atacante, sino que el ataque es perpetrado por múltiples asaltantes de forma simultánea. El método tradicional de ejecución de este tipo de ataques era mediante el empleo de las denominadas botnets o redes zombies (con la aparición de Anonymous, este procedimiento se ha generalizado gracias al empleo de herramientas automáticas como LOIC, HOIC, RefRef o WebHive y la participación masiva de colaboradores coordinados a través de Internet, por lo tanto para sus ataques ya no es necesario el empleo de botnets aunque se sigan utilizando). Por último, el Defacement o Desfiguración Web

3. HACKTIVISMO Y FIGURAS AFINES

Es indudable que el hacktivismo tiene características afines con otros colectivos del ciberespacio que persiguen un objetivo político/reivindicativo, pero también hay que resaltar que existen diferencias importantes que lo singularizan y distinguen de los demás.

En este apartado trataremos de diferenciar el hacktivismo de otros movimientos, de tal manera que nos facilite la clasificación de los diferentes grupos. No se va a tratar el cibercrimen porque su motivación es meramente lucrativa y por tanto carece de la motivación política que caracteriza al resto de colectivos, sin que esto quiera decir que en el hacktivismo, como en el resto, no pueda existir algún tipo de interés económico siempre supeditado a su objetivo político/reivindicativo principal.

3.1. ACTIVISMO DIGITAL O CIBERACTIVISMO

Quizás el activismo digital o ciberactivismo sea el movimiento más afín al hacktivismo[8] y más difícil de diferenciar junto con el ciberterrorismo.

En el activismo digital o ciberactivismo, como con el hacktivismo (sea digitalmente correcto o incorrecto), se ejercita la acción política no convencional en el contexto de las TIC, pero a diferencia del hacktivismo sólo se emplean las nuevas tecnologías como herramienta comunicativa con una gran capacidad de difusión y una audiencia global, aprovechando las características propias que posee Internet, entre otras la facilidad de producción de contenidos y su distribución, la viralidad y el alcance a un público cada vez mayor no limitado por las barreras comunicativas que normalmente afectan al mundo físico. Además, como fin último, lo que se pretende es la movilización de masas, en un principio restringiéndose su acción a los ciberciudadanos, con la expectativa de que sus acciones trasciendan del mundo virtual al físico.

En este sentido existen tres diferencias fundamentales entre el ciberactivismo y el hacktivismo:

La primera y más clara es que en el ciberactivismo no se utilizan técnicas hacking[9]. Aunque los resultados puedan parecer similares, por ejemplo, un ataque Distribuido de Denegación de Servicio (DDoS), mientras que en el hacktivismo se realizaría mediante herramientas informáticas que simularan miles de accesos a una página web, en una acción de ciberactivismo se haría mediante la acción coordinada de miles de usuarios que simultáneamente intentasen acceder a los contenidos del sitio web objetivo, consiguiéndose en ambos casos que se produzcan los mismos efectos, es decir, el colapso y la caída del servidor web y de las páginas web alojadas en él debido a la petición de acceso simultánea y masiva.

consiste en explotar con éxito una vulnerabilidad en los sistemas de alojamiento (servidor web) o en las aplicaciones que permiten a un atacante modificar contenidos y páginas web. Estos ataques pueden involucrar la inserción de enlaces a sitios maliciosos y/o añadir contenidos con contienen el mensaje del atacante (políticos, difamatorios, etc.) (CCN-CERT, 2012).

8 Algunos autores incluso incardinan el hacktivismo dentro del activismo digital (Barandiaran, 2003; Aceros Gualdrón, 2006), aunque creo que existen elementos diferenciadores suficientes para realizar dicha distinción.

9 Elemento necesario para que se hable de hacktivismo.

En el ciberactivismo se emplean Internet y las nuevas tecnologías como un instrumento no como un objetivo, al contrario que en el hacktivismo, cuyas acciones tienen como objetivo Internet y las nuevas tecnologías.

Por último, en el ciberactivismo se requiere la participación de multitud de personas o ciberciudadanos para que sus acciones tengan éxito. Debemos recordar que en activismo digital es más importante la movilización de las masas que la consecución de un objetivo concreto, mientras que en el hacktivismo la movilización de masas no es necesaria ni requerida al suplirse mediante el empleo de técnicas de hacking.

El ciberactivismo ha ganado fuerza en los últimos años gracias a la aparición de la Web 2.0 (algunos autores la llaman Activismo 2.0) y las posibilidades de comunicación que se han abierto gracias a las redes sociales, convirtiéndose en foco de atención tanto de gobiernos como de partidos o movimientos políticos tradicionales que se han visto sobrepasados por la aparición de nuevos partidos o movimientos con un amplio despliegue en Internet y en las redes[10].

	Activismo 1.0	**Activismo 2.0**
Web	1.0 (Página web)	2.0 (Redes sociales: Facebook y Twitter especialmente)
Utilización	Información y coordinación	Debate y acción
Reacción de los gobiernos	Reprime en el mundo real	Reprime en el mundo real y virtual (censura de Internet)
Comunicación de los activistas	Eminentemente vertical en la web (uso pocos expertos)	Básicamente horizontal en las redes sociales
Consecuencias	Sensibilización	Transformación (caída de gobiernos…)
Ejemplos	Movimientos altermundista o antiglobalización (1999 -)	Revolución democrática árabe y Spanish revolution: (2010 -)

Cuadro comparativo de la transformación sufrida por el ciberactivismo gracias a la Web 2.0. (Fernández, 2012)

3.2. CIBERTERRORISMO

El ciberterrorismo se puede definir como la conjunción del terrorismo con el ciberespacio utilizado como instrumento, medio u objetivo, entendiendo que con el terrorismo[11] se busca un objetivo político mediante el empleo de acciones que infundan miedo a la población. Si analizamos esta definición en la parte que nos atañe, que es

10 http://politica.elpais.com/politica/2014/05/28/actualidad/1401305050_166293.html

11 Según el artículo 1 de la Decisión marco del Consejo 2002/475/JAI, de 13 de junio de 2002, sobre la lucha contra el terrorismo, se consideran delitos de terrorismo "los actos intencionados a que se refieren las letras a) a i) tipificados como delitos según los respectivos Derechos nacionales que, por su naturaleza o su contexto, puedan lesionar gravemente a un país o a una organización internacional cuando su autor los cometa con el fin de: intimidar gravemente a una población, obligar indebidamente a los poderes públicos o a una organización internacional a realizar un acto o a abstenerse de hacerlo, o desestabilizar gravemente o destruir las estructuras fundamentales políticas, constitucionales, económicas o sociales de un país o de una organización internacional; a)…… d) destrucciones masivas en instalaciones gubernamentales o públicas, sistemas de transporte, infraestructuras, incluidos los sistemas informáticos, plataformas fijas emplazadas en la plataforma continental, lugares públicos o propiedades privadas, que puedan poner en peligro vidas humanas o producir un gran perjuicio económico; …… i) amenaza de ejercer cualesquiera de las conductas enumeradas en las letras a) a h)."

sus nexos con el ciberespacio, se puede ver que existen tres posibles vías de utilización por parte de grupos terroristas[12]: como instrumento, como vía o como objetivo, lo cual pasaremos a explicar a continuación de forma breve.

En el primer caso, el uso del ciberespacio como instrumento por grupos terroristas, se suele realizar para proporcionar una plataforma para publicitar sus acciones y recabar adeptos y recursos (los delitos típicos se corresponden con la apología[13], publicidad[14], reclutamiento[15] y la financiación ilícita[16] de grupos terroristas).

En el segundo, la utilización de medios tecnológicos se emplea para facilitar las acciones físicas del grupo, este es el caso del uso de programas de cifrado, comunicaciones entre los miembros del grupo a través de buzones de correo electrónico compartidos, recolección de información de posibles objetivos, etc.

Por último lugar, se encuentra el ciberespacio o sus "habitantes" como objetivo del grupo terrorista, ya sean webs de empresas o gobiernos, infraestructuras críticas, particulares, etc., es lo que en puridad se consideraría ciberterrorismo.

Como se puede comprobar hacktivismo y ciberterrorismo (en sus tres interpretaciones) son muy similares en cuanto a su funcionamiento, no así en cuanto al objetivo que se pretende con sus acciones[17]. En sus últimas motivaciones, el hacktivismo aspira como mucho a lograr la desobediencia civil para conseguir un triunfo político o reivindicativo, ganándose la simpatía y el apoyo de los ciudadanos, en ningún caso provocarles miedo o terror para obligarles a adoptar una idea política con la cual no comulgan. Éste es el elemento diferenciador con el ciberterrorismo y el cual debemos analizar a la hora de clasificar una acción como hacktivista o ciberterrorista.

3.3. CIBERESPIONAJE.

El ciberespionaje se define como "la realización de cualquier acto clandestino o con falsos pretextos que utiliza capacidades cibernéticas para recopilar (o intentar recopilar) información con la intención de comunicarla a la parte contraria." (Schmitt, 2013)

Como en las dos figuras anteriores, es la conjunción del espionaje con el mundo cibernético. Este ciberespionaje puede ser promovido tanto por empresas como por gobiernos y puede tener unas motivaciones económicas o políticas, o ambas a la vez (U.S. Office of the Secretary of Defense, 2013). Desde luego el único ciberespionaje que puede ser confundido con hacktivismo es el promovido/ejecutado por el Estado (Klimburg, 2012), ya que el empresarial sólo persigue beneficios económicos y no políticos.

Tradicionalmente las acciones hacktivistas no iban encaminadas a obtener información de los sistemas atacados sino a realizar acciones de protesta mediante DDoS, defacement de páginas web, Cross-site scripting, etc., con el objetivo de que tuvieran una repercusión rápida (normalmente hasta que se terminaba el ataque o se eliminaba el error por parte de los administradores de los sistemas atacados). Sin embargo,

12 http://observatorio.cisde.es/?p=2019
13 Art. 18.1 del CP.
14 Art. 578 del CP.
15 Art. 575 del CP
16 Art. 576 bis del CP.
17 http://www.edshare.soton.ac.uk/8762/2/whatishacktivism.pdf

en los últimos años se ha experimentado un cambio de tendencia en los ataques sufridos, incrementándose significativamente los robos de información para su posterior difusión pública con el doble propósito de ganar publicidad y poner en entredicho a la víctima (gobierno, empresa o particular)[18] (Advisen Insurance Intelligence, 2012). Es significativo que en el año 2011, individuos o grupos hacktivistas consiguieron acceder y robar más de cien millones de registros que ascienden a casi el doble de lo robado por motivos económicos. (Verizon, 2012)

	Todas		Grandes empresas	
Delincuencia organizada	83%	35%–	33%	36%
Se desconoce	10%	1%	31%	0%
Personas sin afiliación	4%	0%	10%	0%
Grupo activista	2%	58%+	21%	61%
Ex-empleado (ya no tiene acceso)	1%	0%	6%	0%
Pariente o conocido del empleado	0%	0%	2%	0%

Variedades de agentes externos por porcentaje de brecha dentro de la categoría de externos y porcentaje de registros (en rojo). (Verizon, 2012)

Es indudable que la recolección de información procedente de elementos no cooperantes es un trabajo típico de espionaje, de aquí la similitud de estas acciones hacktivistas con el ciberespionaje. Sin embargo, existen tres grandes diferencias a tener en cuenta:

El fin que se pretende con las acciones hacktivistas es promover la desobediencia civil o un cambio de escenario político sin beneficio para un país tercero, mientras que en el ciberespionaje (promovido por otro Estado) se persigue la mejora de sus propias capacidades (militares, económicas, técnicas, etc.) frente al Estado víctima o terceros.

La segunda gran diferencia es la publicidad. En una acción hacktivista resulta inherente a su objetivo final, que no es otro que una movilización de masas, la necesidad de publicidad, tanto de la acción en sí misma como de los datos obtenidos con ella, con el consiguiente sacrificio de un posible acceso futuro; en cambio, en el ciberespionaje la discreción es necesaria y total, ya que una vez descubierto el acceso ilícito se corta la fuente de información y la ventaja informativa ganada.

Consecuencia de lo anterior, existe otra gran diferencia respecto al momento temporal de la obtención del beneficio gracias a la acción de hacking. Mientras que en el ciberespionaje el beneficio se obtiene mientras dure el acceso a los datos comprometidos, en las acciones de hacktivismo el beneficio se obtiene cuando ha finalizado la misma y se ha conseguido publicitar tanto la acción como los datos obtenidos.

18 Un ejemplo de lo expuesto es la bien conocida colaboración entre el colectivo Anonymous y otros grupos hacktivistas con la organización WikiLeaks.

3.4. CIBERGUERRA

Para el Departamento de Defensa de Estados Unidos, el ciberespacio se ha convertido en un campo de operaciones de igual entidad que la tierra, el mar, el aire o el espacio y por tanto susceptible de ser escenario tanto de maniobras defensivas como ofensivas, lo que podría incluir ataques preventivos y represalias. (U.S. Department of Defense, 2011)

En este campo de operaciones es donde transcurriría la ciberguerra, definida como el conjunto de acciones que se realizan para producir alteraciones en la información y los sistemas del enemigo, a la vez que se protege la información y los sistemas del atacante. (Benedicto, 2013)

Es cierto que denominar guerra a una serie de acciones que no pueden generar, en principio, ningún tipo de daño humano directo[19] puede resultar un tanto aventurado, pero no es menos cierto que a día de hoy los daños económicos causados por acciones de hacking pueden ser mucho mayores que los que se pudieran producir por un bombardeo[20] y, por tanto, causar más perjuicio a un Estado enemigo que los de un ataque convencional. También hay que tener en cuenta que, aunque un ataque cibernético no puede ocasionar daños humanos directamente, de forma indirecta se podrían conseguir victimas mortales si el objetivo es alguna de las denominadas infraestructuras críticas, pudiendo llegar a ser incluso más destructivo que un ataque militar convencional (p.ej. atacando los sistemas de control de una vía férrea, los dispositivos de seguridad de una central nuclear, los sistemas que gestionan el tráfico aéreo, etc.).

Llegado a este punto hay que significar que el lugar donde se realizan estas acciones de hacking, el ciberespacio, no facilita la labor de identificar a los agresores, así que se han denominado como actos de ciberguerra a determinadas acciones que han infligido daños generalizados en cualquiera de las dimensiones sociales, económicas, o políticas de ciertas naciones[21] y que han excedido lo que se podría denominar como un simple perjuicio. Esta circunstancia puede ser comprensible por el hecho de que el término ciberguerra es fácil de recordar y por ello suele emplearse alegremente al observar cualquier experiencia negativa que se produzca en el ciberespacio, sin analizar en profundidad su alcance (Gordo, 2012). Por ello es necesaria una delimitación apropiada del término que facilite su correcta utilización.

Vista la dificultad de identificar a los agresores (en el ciberespacio no se viste uniforme, no hay banderas y no hay una franja de terreno que pueda llamarse campo de batalla), hay que diferenciar que es hacktivismo y que es ciberguerra:

La ciberguerra se produce entre Estados que tienen un conflicto declarado conforme a la normativa nacional[22] e internacional[23]. Por lo tanto, un grupo o individuo no

19 Por supuesto se podrían producir bajas si el ataque cibernético llega a causar daños a los elementos de seguridad de determinadas instalaciones o infraestructuras, p.ej. presas hidráulicas, centrales nucleares, redes de suministro eléctrico, etc., pero el posible daño humano sería subsidiario y nunca directo como pudiera ser con un ataque militar.

20 http://economia.elpais.com/economia/2013/03/01/actualidad/1362156981_076595.html

21 http://id.tudiscovery.com/ciberguerras-las-batallas-del-futuro-hoy/

22 En el caso de España el artículo 63.3 de la Constitución Española establece que “Al Rey corresponde, previa autorización de las Cortes Generales, declarar la guerra y hacer la paz”.

23 A nivel internacional hay que tener como referencia la Carta de Naciones Unidas artículo 2.4 (prohibición de la amenaza y el uso de la fuerza), artículo 51 (legítima defensa individual o colectiva) y Capítulo VII (sistema de seguridad colectiva).

puede entablar una guerra contra un Estado (Benedicto, 2005). Así que, por mucho que Anonymous, Afghan Cyber Army, Syrian Electronic Army o cualquier otro grupo hacktivista publicite que está en guerra[24], sus acciones son acciones hacktivistas o, a lo sumo, de ciberterrorismo y no de ciberguerra.

Otra circunstancia a tener en cuenta es que la ciberguerra se realiza por fuerzas combatientes en el conflicto, por lo tanto no pueden ser enjuiciados por sus acciones siempre que respeten el Derecho Internacional Humanitario (Schmitt, 2013), mientras que las acciones hacktivistas (aunque se autodenominen cibersoldados) son perpetradas por no combatientes y, por tanto, enjuiciables en cualquier momento.

Por último, en la ciberguerra las acciones de hacking se realizan por las fuerzas combatientes involucradas en el conflicto que obviamente están vinculadas a los Estados a los que pertenecen; en cambio, el hacktivismo se caracteriza porque los colectivos que lo integran no están vinculados directamente a ningún Estado (aunque en ocasiones se intuya un cierto apoyo gubernamental como en el caso de los ataques a Taiwan, Estonia o Georgia) y, por tanto, no se incluyen dentro de sus estructuras de defensa.

Una vez hecho el repaso de estas figuras parecidas o afines al hacktivismo, a modo de resumen y antes de pasar a analizar al grupo hacktivista por antonomasia, se podría determinar la diferenciación entre estos términos en función de cuatro parámetros fundamentales: el uso de técnicas hacking, la intención de causar temor en la población, la inclusión de los grupos actuantes dentro de las estructuras de seguridad o defensa de un Estado y la necesidad de publicitar las acciones llevadas a cabo.

	TÉCNICAS HACKING	MIEDO POBLACIÓN	APARATO ESTATAL	PUBLICIDAD
CIBERACTIVISMO	NO	NO	NO	SI
HACKTIVISMO	SI	NO	NO	SI
CIBERTERRORISMO	SI	SI	NO	SI
CIBERESPIONAJE	SI	NO	SI	NO
CIBERGUERRA	SI	SI/NO	SI	SI/NO

Diferencias entre el hacktivismo y figuras afines (elaboración propia)

4. ANONYMOUS

Si hay un grupo que ha captado la atención de los medios de comunicación en los últimos tiempos este es Anonymous. Armado con el poder de Internet, una voz generada por ordenador y una máscara de Guy Fawkes[25] han causado una gran alarma y hecho volar la imaginación de periodistas, manifestantes cibernéticos y ciudadanos en general.

Anonymous es probablemente el grupo más conocido por todos, pero existen multitud de grupos hacktivistas activos en la actualidad. Sean de ideología de izquierdas como X-Blackerz INC., St0rmyw0rm, etc., nacionalistas como Red Hackers Alliance, China Eagle Union, Green Army, Syrian Electronic Army, Afghan Cyber Army,

24 http://hilf-ol-fozoul.blogspot.com.es/2013/07/afghan-cyber-army-declare-war-on-israel.html o http://actualidad.rt.com/actualidad/view/78537-anonymous-declara-guerra-israel-escapara-ira

25 http://documentalium.foroactivo.com/t378-la-historia-de-guy-fawkes

Kosova Hackers Group, Moroccan Ghosts, Moroccan Team Evil, etc., islamistas como Cyber-Jihidi, Izz ad-din al-Qassam Cyber Fighters, etc., ninguno de ellos, aunque algunos sean muy activos y con una elevada cualificación técnica, llegan a tener el reclamo mediático que tiene Anonymous. Por ello trataremos de analizar únicamente este grupo, siempre teniendo en cuenta que se existen muchos y que algunos son más peligrosos que Anonymous.

Emblema de Anonymous.

4.1. ORÍGENES

Mientras que los miembros de Anonymous se mantienen así, anónimos, el grupo es asunto de interés público. Nacidos en el seno del foro de imágenes 4chan.org, dedicado en sus comienzos para los amantes del anime y manga, Anonymous es fruto del tablón de imágenes "/b/" cuyas reglas de funcionamiento se reducen a un anonimato absoluto y a una total libertad de expresión, con la única limitación de la pornografía infantil (e incluso así se bromeaba sobre el tema). En este sitio no hay ningún sistema de registro de entrada. Cualquiera puede escribir en él y la mayoría de los participantes publican sus comentarios sin utilizar un nombre de usuario, con lo que se les asigna el nombre predeterminado: anonymous.

Anonymous, nacido de /b/, siguió sus mismas reglas, es decir, no había reglas, no había lista de miembros y no había una estructura organizativa como tal. Y así en 2006 Anonymous asestó su primer gran golpe, conocido como ataque Habbo. Coordinándose en 4chan y utilizando avatares que representaban a americanos de color vestidos con trajes grises, el grupo bloqueó el acceso de los avatares de los adolescentes a la piscina en el mundo virtual de Habbo Hotel. Ya entonces sus motivaciones no estaban del todo claras. Para algunos se trataba simplemente de diversión; sin embargo, para otros era una forma de recalcar la falta de personajes de raza negra en las redes sociales.

No obstante, Anonymous se hizo realmente famoso a partir de 2008 a través del proyecto Chanology, que aún sigue activo y con los mismos objetivos. El proyecto protesta, de manera no violenta, contra los mitos en los que se basa la Iglesia de la Cienciología y denuncia su oscurantismo y los riesgos para sus miembros que quedan aislados del mundo exterior. Este proyecto se caracterizó porque por primera vez

Anonymous salió al mundo físico mediante convocatoria de concentraciones a las puertas de algunos de los centros de la Iglesia de la Cienciología[26].

Desde ese momento hasta la fecha, casi un centenar de acciones "globales" han sido llevadas a cabo por el colectivo Anonymous o por individuos que decían actuar en su nombre[27], y aunque la mayoría de sus acciones se realizan mediante ataques DDoS y otras técnicas hacking, también realizan campañas no de hacking. Recientemente, por ejemplo, se anunció la operación "No Manifiesto" en la que se alienta a las personas a modificar las copias del manifiesto escrito por el noruego asesino de masas Anders Breivik, creando versiones que ridiculizan su ideología. Al inundar la web con estas copias modificadas, cualquier persona que busque el manifiesto no puede estar segura de la veracidad del mismo.

4.2. CARACTERÍSTICAS

"Somos Anonymous.

Somos Legión.

No perdonamos.

No olvidamos.

¡Esperadnos!"[28]

Anonymous se suele identificar con una máscara de Guy Fawkes rememorando al combatiente por la libertad V, de la película V de Vendetta, y una silueta de un hombre con chaqueta y corbata pero sin la cabeza, con la intención de representar al anonimato de Internet y a una organización que no tiene líderes.

Escena de la película V de Vendetta donde se muestra a su protagonista con la máscara de Guy Fawkes.

Con un lenguaje claramente revolucionario, según su video-presentación "I am one Anonymous"[29], Anonymous dice proteger la libertad de expresión en Internet, además de luchar contra la corrupción y la opresión; sin embargo algunas acciones

26 El 10 de febrero de 2008 alrededor de 7.000 personas se manifestaron en más de 93 ciudades en todo el mundo. Muchos de los manifestantes llevaban máscaras de Guy Fawkes para ocultar su identidad y evitar las posibles represalias por parte de la Iglesia de la Cienciología.

27 http://en.wikipedia.org/wiki/Timeline_of_events_associated_with_Anonymous

28 Traducción del lema de Anonymous.

29 http://www.youtube.com/watch?v=aEcvaoDIKtU

perpetradas por el colectivo se podrían incardinar dentro del vandalismo o la comisión por pura diversión.

Anonymous declara no tener líder ni una estructura organizativa y que cualquier persona puede participar en una campaña o proponer una propia bajo su nombre. Esto en parte es cierto, pero existen indicadores, como la gestión de las cuentas de Twitter, la producción de videos de YouTube (de una gran calidad), el control de los canales IRC (algunos cerrados al público en general) o el manejo de algunas técnicas avanzadas de hacking por parte de ciertos miembros, que indican que existe un núcleo duro dentro del colectivo (U.S. Department of Justice, 2011).

Pero, ¿qué hace a Anonymous un referente del nuevo hacktivismo? El modelo colectivo de protesta creado por Anonymous parece ser el indicador más importante del futuro de la desobediencia civil cibernética. Pertenencia sin ningún requisito significa posibilidades ilimitadas para la protesta política a escala global. Además, la posibilidad de uso de su nombre[30] tipo franquicia, al estilo de Al Qaeda, lo convierte en un conglomerado de grupos, individuos, colectivos, etc., de difícil definición y lucha. Anonymous es un meme, una idea fácilmente reproducible y asumible por otros y, al estilo de la Hidra de Lerna, cualquier intento de desarticulación de alguno de sus corpúsculos hace aparecer otros o simplemente su lugar es ocupado por otros miembros del colectivo, por lo que la desarticulación completa de Anonymous se antoja imposible.

País	Total
Estados Unidos	107
Turquía	32
Reino Unido	16
Italia	15
Alemania	10
España	7
Chile	6
Países Bajos	6
Colombia	5
Francia	2
Grecia	2
Polonia	1

Detenciones de miembros de Anonymous entre diciembre de 2010 y abril de 2012 (Paget, 2012)

Y todo ello basado, como se ha adelantado anteriormente, en tres pilares:

- Comunicaciones. En un doble sentido, por un lado la comunicación "institucional" con una penetración en redes sociales[31] como Twitter (Paget, 2012) o Facebook[32] muy elevada y una difusión audiovisual de sus operaciones con una altísima calidad, pareciendo en muchas ocasiones más una campaña de marketing promocional que una alocución informativa. Por otro, la seguridad de las

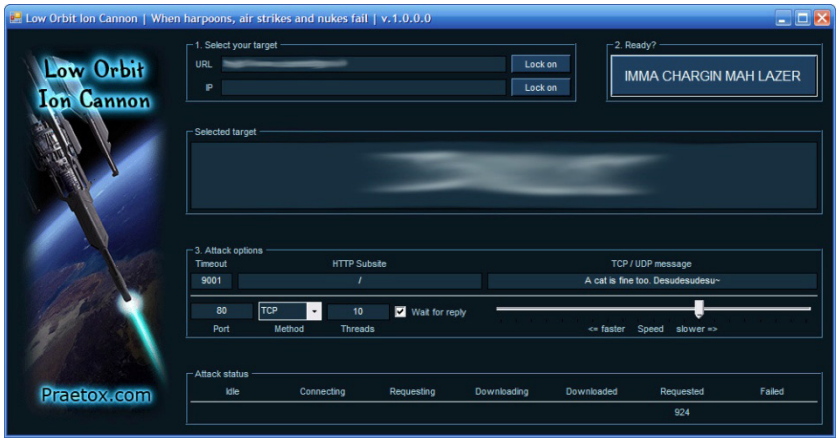
30 Existen multitud de franquicias de Anonymous, p.ej. Anonymous Latinoamérica, Anonymous España, Anonymous Portugal, Anonymous Francia, Anonymous Marruecos, Anonymous Egipto, etc.

31 Debido a que alguno de sus miembros han sido expulsados de Facebook y Google+, otros de sus miembros han creado su propia red social llamada Anonplus (www.anonplus.com) que, a día de hoy, está parcialmente operativa.

32 http://www.concepto05.com/2013/07/estadisticas-usuarios-redes-sociales-en-espana-2013/

mismas mediante el empleo de canales IRC para la discusión y coordinación de los miembros del colectivo utilizando redes TOR (The Onion Router) y conexiones SSL (Secure Sockets Layer) para evitar ser localizados[33].

- Anonimato. Por propia idiosincrasia del colectivo que establece la norma de nunca utilizar un nombre real y amparado por la seguridad que les proporcionan las comunicaciones cifradas y torificadas[34].
- Hacking de masas. Existen miembros de Anonymous con elevado conocimientos de técnicas hacking, las cuales requieren pericia, dedicación y entrenamiento para poder ser empleadas, lo que no es la norma dentro de Anonymous. La mayoría de los miembros del colectivo desconocen estas técnicas por lo que se han puesto a su disposición unas herramientas de fácil uso. LOIC (Low Orbit Ion Canion)[35], HOIC (Hight Orbit Ion Canion), RefRef o WebHive son herramientas diseñadas para realizar los ataques más utilizados por Anonymous, DDoS y DoS. De tal manera que cualquiera puede "sentirse hacker" y pertenecer a Anonymous sin necesidad de tener ningún conocimiento técnico, ampliando la capacidad del colectivo de asumir nuevos miembros a virtualmente todo el que tenga disponible un ordenador, una conexión a Internet y unos minutos de tiempo libre.



Pantalla de inicio de LOIC.

4.3. ANONYMOUS EN ESPAÑA

Como ya se había adelantado anteriormente, Anonymous es un fenómeno global que extiende sus filiales por todo en el mundo y donde España no es una excepción. Las filiales españolas no se diferencian del resto de filiales de Anonymous, caracterizadas por una gran labor de comunicación sobre todo en las redes sociales, anonimato y acciones de amplio calado en la opinión pública y que aseguran un gran número de simpatizantes.

33 Existen multitud de manuales en la Red para pertenecer a Anonymous con la seguridad de no ser detectado.

34 Referente al empleo del software de navegación anónima TOR (The Onion Router), proyecto cuyo objetivo principal es el desarrollo de una red de comunicaciones en la que el encaminamiento de los mensajes intercambiados entre los usuarios no revela su identidad.

35 Existen varias versiones de LOIC para varias plataformas y dispositivos: IRCLOIC, LOIQ, JSLOIC y LOIC Mobile.

Imagen tomada durante las manifestaciones del 15-M en Madrid.

En nuestro territorio existen actualmente tres grupos particularmente activos llamados Anonymous España (como no podía ser de otra manera), AnonSpain y La Novena Legión[36].

*Imagen-icono de Anonymous España en su perfil de Facebook (*www.facebook.com/pages/ANONYMOUS-ESPAÑA/190938564305930*)*

Estos grupos han llevado a cabo multitud de acciones aunque la respuesta policial ha sido realmente tenue. Hasta el momento sólo se ha practicado la detención de siete supuestos integrantes de Anonymous. Esta baja actividad policial es debida, en gran parte, a la falta de concienciación social sobre este tipo de acciones (inclusive la policial), también a la escasa cuantía de los daños causados y, por último, a los posibles perjuicios reputacionales que pueden llevar aparejados si se les dota de una significación excesiva. Por lo tanto, a día de hoy existe una gran cifra negra en el ámbito de las denuncias de las acciones hacktivistas que fomenta la inacción de los cuerpos policiales.

En cuanto a la afinidad política de los grupos que componen Anonymous en España, en teoría no cuentan con ninguna (o al menos así se declaran), pero sin embargo se puede comprobar que las acciones de los últimos años tienen como objetivo en su gran mayoría a instituciones públicas a cargo de miembros del Partido Popular (Arbor Networks, 2013), aunque ni PSOE ni Izquierda Unida[37] se han librado de sus ataques.

36 Supuestamente en honor de la Legio IX denominada “Hispana” formada por Pompeyo en el año 62 a.C.
37 http://www.eldiario.es/sinsentidocomun/Izquierda-Unida-Indignada_6_80901931.html

5. CONCLUSIÓN

El mundo se mueve y cambia al abrigo de las nuevas tecnologías dando lugar al nacimiento de nuevos actores del escenario político entre los que se encuentran los grupos hacktivistas, los cuales conjugan la acción política con el uso de técnicas hacker para el logro de sus objetivos políticos/reivindicativos.

Al igual que otros movimientos sociales, el hacktivista no es un movimiento con unas fronteras claras y definidas, existen otras figuras que pueden ser confundidas con el hacktivismo. Para no caer en este error hay que tener en cuenta los tres elementos definitorios claros del hacktivista[38]: la necesidad de publicitar sus acciones (incluso los fallos suponen un reclamo publicitario importante), sus acciones no están promovidas por un Estado y, por último, que no pretende infundir miedo en la población sino causar simpatía y adherirla a su causa. Estos tres elementos, junto con el empleo de técnicas hacker para el ejercicio de la acción política, delimitan por completo al hacktivismo y lo diferencian con figuras muy próximas como el activismo digital, el ciberterrorismo, el ciberespionaje o la ciberguerra.

Acorde con las características expuestas, en España existen grupos que podríamos clasificar como hacktivistas, empezando por las filiales españolas de Anonymous, colectivo hacktivista de carácter global que es sin duda el que cuenta con un mayor renombre. Nótese que no se ha utilizado el término grupo para denominarlo, ya que no tiene esa estructura, sino que es un conglomerado de grupos independientes, aunque se supone que existe un grupo de iniciados con unas funciones directivas que utilizan el nombre de Anonymous para declarar su afinidad con los principios del colectivo y para aprovechar el tirón mediático y de simpatizantes de la marca matriz (al igual que hace el grupo terrorista Al Qaeda).

Con la aparición en escena de Anonymous, el hacktivismo ha experimentado un renacimiento en gran parte por sus especiales características de anonimato, uso de formas de comunicación segura, gran despliegue mediático y propagandístico de sus acciones y facilidad de participación de cualquiera, aunque carezca de conocimientos técnicos, gracias al empleo de herramientas informáticas diseñadas al efecto. Y he aquí el porqué del éxito de Anonymous y la atracción que despierta en el público en general: cualquiera puede pertenecer a Anonymous, desde una persona sin conocimientos informáticos que está aburrida en su casa y le atrae hacer de hacker durante un rato para contárselo a sus amigos, pasando por trabajadores (o extrabajadores) descontentos con su empresa y que ven una oportunidad para vengarse de ella, hasta auténticos hackers que ponen al servicio de una causa sus conocimientos informáticos. Esto ha provocado la aparición de un sinfín de filiales e imitadores de Anonymous (en España hay activas varias de ellas, como por ejemplo Anonymous España, AnonSpain o La Novena Legión), que pueden participar en las campañas globales orquestadas desde la matriz, al igual que el resto de filiales de otros países, y a su vez promover operaciones propias. Por otro lado cualquiera puede realizar una acción, hacktivista o no, y atribuírsela a Anonymous; primero porque “sus miembros” no se conocen entre sí y segundo porque, al no haber una dirección ni estructura organizativa, nadie puede decir que la acción no está respalda por la cúpula de la organización.

38 Siempre teniendo en cuenta que el leitmotiv de sus acciones debe ser político/reivindicativo y no económico para que no sean clasificados como ciberdelincuentes.

BIBLIOGRAFIA

Advisen Insurance Intelligence. (2012). Hacktivism: The growth and implication of this 21st century method of protest.

Arbor Networks. (2013). Monitorización activa #Ops Internet. 2013.

Benedicto, R. A. (2005). Teorías y conceptos para entender formas actuales de hacer la Guerra. Universitat Autònoma de Barcelona.

Benedicto, M. A. (2013). EEUU ante el reto de los ciberataques. Instituto Español de Estudios Estratégicos, 37/2012

Castells, M. (2001). Internet, libertad y sociedad: una perspectiva analítica. Universitat Oberta de Catalunya.

Fernández, J. S. (2012). Ciberactivismo: Conceptualización, hipótesis y medida. ARBOR Ciencia, Pensamiento y Cultura, 188 (756), 631-639.

Garaizar, P. (2004). El Software Libre como herramienta del hacktivismo contra el cibercontrol social. Universidad de Deusto.

Gordo, F. (2012). Ciberinquietud o Ciberindiferencia: ¿es la ciberguerra un auténtico desafío a la seguridad y la defensa? Red Safe World.

Himanen, P. (2004). La ética del hacker y el espíritu de la era de la información. Destino.

Klimburg, A. (2012). National Cyber Security. Framework manual. Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence.

Lizama, J. A. (2005). Hackers en el contexto de la sociedad de la información. Ciudad de México: Universidad Nacional Autónoma de México.

National Cyber Security Centre. (2012). Cyber Security Assessment Netherlands. The Hague, Netherlands.

Paget, F. (2012). Hacktivismo. El ciberespacio: nuevo medio de difusión de ideas políticas. Alcobendas, Madrid, España: McAfee Labs.

Raymond, E. S. (1996). The New Hacker's Dictionary. Paperback.

Schmitt, M. N. (2013). Tallinn Manual on the International Law Applicable to Cyber Warfare. New York: Cambridge University Press.

U.S. Department of Justice. (2011). Psychological Profiles of Anonymous Leadership.

U.S. Department of Defense. (2011). Department of Defense Strategy for Operating in Cyberspace.

U.S. Office of the Secretary of Defense. (2013). Annual Report on Military and Security Developments Involving the People's Republic of China.

Verizon. (2012). Informe sobre investigaciones de brechas en los datos de 2012.

Fecha de recepción: 05/05/2014. Fecha de aceptación: 24/06/2014

PANOPTICON DIGITAL
INTERNET: REVOLUCIÓN, PRIVACIDAD Y VIGILANCIA

CENTRO DE ANÁLISIS Y PROSPECTIVA. GUARDIA CIVIL

RESUMEN

Los avances tecnológicos, y especialmente el desarrollo y evolución de Internet y los medios sociales, han posibilitado la democratización del conocimiento, la mejora de las comunicaciones entre los ciudadanos, la posibilidad de realizar transacciones y gestiones sin necesidad de desplazamientos, además de facilitar la movilización de ciudadanos en defensa legítima de multitud de causas. Pero a su vez también ha llevado hacia un fenómeno que podríamos denominar de “sociedades bajo vigilancia”. Internet y las redes sociales son vías que pueden ser utilizadas para espiar, desinformar o manipular. Regímenes totalitarios, por otra parte, tratan de censurar la Red con objeto de evitar la movilización social. La protección de los datos personales, empresariales o gubernamentales se convierte en estos momentos en una cuestión urgente.

Palabras clave: Internet, privacidad, espionaje, redes sociales

ABSTRACT

Technological advances, particularly the development and evolution of the Internet and social media have enabled the democratization of knowledge, improved communication between citizens, the ability to conduct transactions without the need to travel and also facilitate the mobilization of citizens in self-defense in many causes. But it has also led to a phenomenon that we could call “under surveillance societies”. Internet and social networks are pathways that can be used to spy, mislead or manipulate. Totalitarian regimes, on the other hand, try to censor the web in order to avoid social mobilization. The protection of personal, corporate or government data now becomes an urgent issue.

Keywords: Internet, privacy, spying, social media

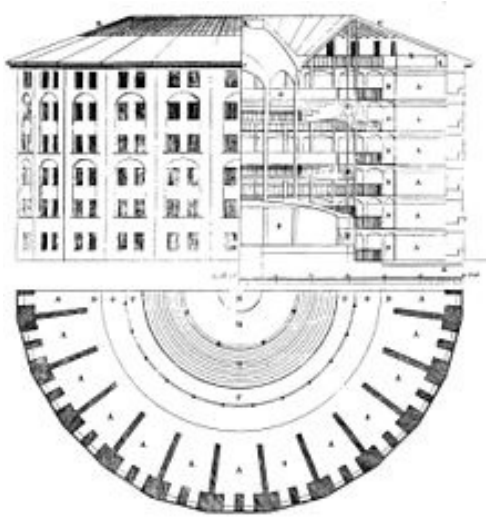
"La privacidad es uno de los mayores problemas en esta nueva era electrónica. En el corazón de la cultura de Internet existe una fuerza que quiere saberlo todo acerca de ti. Y una vez que sabe todo de ti y de otros cientos de millones de personas tiene un activo muy valioso y la gente tendrá la tentación de comerciar con ese activo. Esta no es la información que la gente tenía en mente cuando llamaron a esto la Era de la Información."

Andrew Grove. Ejecutivo y cofundador de Intel Corporation.

1. INTRODUCCIÓN

Los filósofos aman la sabiduría y la verdad por encima de todas las cosas, algunos tienen además la modesta pretensión de cambiar el mundo para mejorarlo. Entre las varias teorías éticas que nos ha proporcionado la filosofía, el utilitarismo pretende proporcionar la mayor felicidad posible al conjunto de los seres humanos. Jeremy

Bentham (1748-1832) fue uno de sus fundadores y entre sus múltiples y variadas aportaciones se incluye el diseño del centro penitenciario perfecto. Denominado Panopticon, estaba pensado de forma que los vigilantes pudieran observar (-opticon) a todos (pan-) los internos sin que éstos pudieran saber si estaban siendo observados o no. Su diseño implica ejercer el control sobre los prisioneros, incluso si realmente nadie los vigilaba, por el hecho de que desconocían en todo momento si estaban siendo observados. Este desconocimiento del alcance real de la vigilancia inhibiría los comportamientos antisociales y aumentaría la seguridad.



Panopticón de Bentham. Willey Reveley, 1791.

Este artículo pretende abordar el tema de la vigilancia en Internet -de actualidad por las recientes revelaciones de Edward Snowden- pero no como algo novedoso, porque realmente no lo es, sino en el contexto de la transformación que ha experimentado la red en los últimos años.

Esta transformación ha convertido Internet en un medio de activismo social y en una herramienta que afecta profundamente a la privacidad de sus usuarios. No se trata ya de un medio donde no sabemos si alguien nos ve, sino de uno donde muchos usuarios quieren observar y ser observados. Esto transforma los sistemas de vigilancia y crea nuestro particular Panopticon digital.

2. LA RED DE REDES

El pasado 6 de agosto de 2014, celebrábamos el vigésimo tercer aniversario de la puesta en línea del primer servidor web y de la publicación de la primera página web en Internet. Esto nos aporta un dato importante: una gran mayoría de los ciudadanos de los países desarrollados en su cuarta década de vida no han conocido un mundo sin Internet. ¿Cómo era aquel viejo mundo de los primeros tiempos de la World Wide Web?

A principios de los noventa, tanto el número de páginas como de servidores se multiplicó exponencialmente y se popularizó el concepto de Internet como una "superautopista de la información"[1], como un lugar que podía crear sus sistemas de gober-

1 Getting Your Feet Wet In a Sea Called Internet. L. R. Shannon. The New York Times. 26/10/1993.

nanza propios y que trascendían al "mundo real". Se trataba de un lugar virtual al que algunos llamaban ciberespacio y que inicialmente no estaba centrado en la compra de libros, las reservas de vuelos o el comercio en general. Las cualidades físicas parecían realmente irrelevantes y muchos de sus usuarios pensaban que este mundo podía y debía ser dirigido por sus integrantes. Sin espacio físico que controlar, parecían haber surgido las primeras comunidades verdaderamente liberadas de la historia.

Sin embargo, desde los primeros tiempos surgió el problema de la libertad de expresión, la privacidad y la vigilancia en la red. La Electronic Frontier Foundation (EFF) se creó en 1990 como una organización sin ánimo de lucro, con el objetivo de defender los derechos de libertad de expresión en Internet a raíz del caso de registro y embargo que la empresa estadounidense Steve Jackson Games sufrió por parte del servicio secreto de Estados Unidos a principios de 1990 (Sterling, 1992).

En 1996 se produjo el primer ataque contra la concepción de una red que se gobernaba a sí misma. La Communications Decency Act (Ley de Decencia en las Telecomunicaciones) fue el primer gran intento del Congreso de los Estados Unidos para regular el material pornográfico en Internet basado en la protección a los menores de edad[2]. Sin embargo, la "indecencia" podía afectar a gran cantidad de contenidos no relacionados con el acceso a los mismos por menores de edad -desde discusiones sobre control de natalidad o información sobre métodos anticonceptivos a los efectos de las violaciones en las prisiones, etc.-. En 1997 la Corte Suprema de los Estados Unidos rechazó la ley por atentar contra la libertad de expresión.

Internet fue diseñado para ser resiliente y resistir interrupciones e interferencias. Se trataba de una arquitectura abierta -cualquier dispositivo puede conectarse-, minimalista -los requerimientos para conectarse son mínimos- y neutral -porque trata a todas las aplicaciones por igual-. Esto, por supuesto, mostró algunas características colaterales: el sistema descentralizado de enrutamiento de la red estaba diseñado para llevar mensajes de punto a punto incluso si las rutas intermedias de acceso estaban deshabilitadas, dañadas o destruidas. No era fácil de censurar pues "la red interpreta la censura como daño y está diseñada para circunnavegar las zonas dañadas" (Goldsmith y Wu, 2006).

Los ingenieros que la diseñaron crearon instituciones que salvaguardaran estas características. La más importante se denominó Internet Engineering Task Force (IETF), encargada de las propuestas y los estándares de Internet y que pronto se convirtió en una forma de gobierno "de facto" de la red en el que las decisiones surgían de abajo a arriba mediante la discusión y el consenso. En principio, ningún gobierno se inmiscuía en sus decisiones. Hubo quien llegó a afirmar que los gobiernos territoriales se convertirían en irrelevantes.

La autoridad raíz o de nombres y numeración en Internet se encarga de decidir quién obtiene qué direcciones numéricas de Internet, qué nombres de dominio como www.google.es y cuántos dominios de alto nivel ".com", ".org", etc. existirán y quién los administrará. Esta autoridad decide en nombre de todos los usuarios de Internet del mundo, tiene el poder de dar forma a la red y aplicar su poder en ella. Sin embargo, desde el principio, la autoridad operó sin una idea clara de quién tenía el poder real

2 Communications Bill Signed, and the Battles Begin Anew. Edmund L. Andrews. The New York Times. 08/02/1996.

sobre el servidor raíz ni por qué. Los ingenieros fundadores de la red eran la autoridad operativa y se encargaban del control ordinario si bien no tenían ningún derecho legal para hacerlo. Uno de ellos, el informático Jonathan Bruce Postel, se había encargado de administrar el servidor raíz desde 1977 en el Stanford Research Institute (SRI), donde se registró el primer dominio ".com" en 1985 de forma gratuita. Esta atribución del SRI se hacía bajo un contrato del Departamento de Defensa de Estados Unidos.

En 1990 el contrato fue renovado y asignado a la empresa Network Solutions Inc., aunque Jon Postel siguió conservando la autoridad de decisión principal mientras la empresa se encargaba de los detalles de gestión. Sin embargo, por primera vez en la historia de Internet, parte del sistema de nombres, estaba en manos de una compañía privada cuyo objetivo era la obtención de beneficios y que, además, se encargaba de la custodia física del servidor raíz. "El Arca había dejado el Templo y nunca volvería"[3]. En 1995 Network Solutions obtuvo el derecho de cobrar por registrar los nombres de dominio y, con la burbuja de Internet, se trataba de millones de nombres y de ingentes beneficios.

El contrato de Network Solutions expiraba en 1998 y los pioneros de Internet, a través de la Internet Society (ISOC) consideraron que el crecimiento de la red y su carácter internacional requería un acuerdo sobre su gobernanza global "a través de un agente gubernamental que sirviera a toda la comunidad". Pero el gobierno estadounidense consideró que había estado virtualmente detrás de cada desarrollo y de cada aspecto de Internet y esto le otorgaba el derecho de propiedad sobre el sistema y de ser el custodio último de la red -un propietario in absentia-. Para el gobierno de Estados Unidos se trataba de una prioridad indiscutible: sus empresas no invertirían miles de millones de dólares sin la garantía de la seguridad y la estabilidad de su infraestructura. Debía ser Estados Unidos, no la ISOC o Jon Postel, quien decidiera sobre los nombres y la numeración en Internet.

El 28 de enero de 1998 Jon Postel solicitó por correo a ocho operadores de servidores raíz -de los 12 existentes en el mundo- que reconocieran a su servidor como raíz central; en esencia, como el ordenador que controla Internet. Los ocho operadores accedieron direccionando sus sistemas al servidor de Postel. Ese día la autoridad raíz quedó dividida: cuatro servidores -NASA, Ejército de EE.UU, Ballistic Research Laboratory y Network Solutions Inc.- siguieron reconociendo al gobierno estadounidense como autoridad raíz, el resto del mundo reconocía al ordenador de Postel situado en la Universidad del Sur de California. Aunque los usuarios no apreciaran ningún problema, Internet se convirtió en dos gigantescas redes. Jon Postel estaba en situación de modificar o escindir la red, podía hacer inaccesibles los dominios ".com", admitir dominios nuevos de alto nivel según su criterio, etc. porque "si falla la raíz, todo lo demás falla". Network Solutions controlaba el "com", pero Postel todavía controlaba el "punto".

Jon Postel pretendía demostrar que él podía controlar la autoridad raíz por encima de Network Solutions, quisiera Estados Unidos o no. Lo que ocurriría sería todo lo contrario. El gobierno estadounidense presionó y amenazó inmediatamente con acciones legales a Postel y a la Universidad del Sur de California. En una semana Jon Postel había finalizado su "test" y cedió la autoridad al gobierno. A partir de entonces cualquier cambio en el servidor raíz sería un delito criminal (Froomkin, 2000). Desde

3 Goldsmith y Wu. op. cit.

febrero de 1998, la autoridad de Internet para la asignación de nombres y números ha permanecido sin interrupción en manos del gobierno de EE.UU. Jonathan Bruce Postel falleció nueve meses después de un ataque al corazón. “El dios de Internet estaba muerto y con él había muerto una era”[4].

3. LAS FRONTERAS

Así pues, a finales de los noventa, en Internet parecía estar librándose una lucha relativa a las fronteras nacionales que ponía en cuestión la relación entre gobiernos y ciudadanos. Por un momento la relevancia del estado-nación pareció diluirse en el ciberespacio. Nada más alejado de la realidad.

Las fronteras nacionales reflejan diferencias reales e importantes entre las personas. La importancia de la separación fronteriza viene dada por las diferencias de idioma, idiosincrásicas y prácticas. Un ciudadano portugués que compra un producto de Apple necesita un manual en su idioma y una dirección y un teléfono locales para su servicio técnico. La información no quiere ser libre; quiere ser etiquetada, clasificada y filtrada para que sea útil al usuario local. La personalización de servicios en Internet responde a las diferencias entre las personas, el lugar en el que se está situado determina el contenido y la calidad de la experiencia en la red. La propia popularidad de la red hace que, al haber más usuarios, cada vez sean menos los políglotas o los bilingües, convirtiéndose en mayoritario el sector que quiere una Internet en su propio idioma. Es cierto que Internet es una “red de redes”, pero de redes nacionales y regionales.

Uno de los primeros en apreciar esta circunstancia fue la compañía estadounidense de comercio electrónico Amazon.com, Inc. Principalmente cuando, en sus comienzos, el servicio al cliente o el atender numerosos pedidos locales hizo necesaria la construcción de múltiples almacenes físicos a lo largo de todo el mundo y fuertes inversiones en distribución real. El intermediario en el mundo físico resultaba fundamental para las transacciones sin intermediarios del mundo virtual.

Aunque Internet comparte la infraestructura y el protocolo, en muchos sentidos se ha convertido en una red de redes estatales separadas. La gente, en los distintos países, tiene diferentes lenguajes y culturas distintas. Sus preferencias, sus deseos y necesidades difieren y su historia y geografía marcan fronteras virtuales. Tecnológicamente, los países están construyendo redes cerradas mediante cortafuegos, en lo que se conoce como splinternet (o ciberbalcanización)[5].

La cuestión fundamental es si el discurso en Internet debe ser regulado global o localmente[6] y si nuestra privacidad se ve comprometida cuando lo hacemos. Un Internet con fronteras es valioso porque permite a gente con valores diferentes coexistir en un mismo espacio. Una legislación de la red que intentara satisfacer a todo el mundo en las diferentes culturas no sería efectiva -regular asuntos como el divorcio o el aborto es ya suficientemente complicado dentro de las fronteras nacionales-. Podemos pensar que se puede estar de acuerdo en algo como la Primera Enmienda

4 Goldsmith y Wu. Ibid.

5 Término acuñado por Forrester Research en 2010. The Web Is Turning Into The ‘Splinternet’. Josh Bernoff. Forbes. 29/03/2010.

6 Cierta pornografía en Japón se considera pederastia en Estados Unidos, mientras que lo que puede ser considerado obscenidad en Tennessee puede ser perfectamente legal en Holanda, etc.

a la Constitución de los Estados Unidos que asegura la libertad de culto, de expresión, de prensa, de reunión, etc., pero en la realidad no refleja valores globales. De hecho, ninguna otra nación del mundo se adhiere plenamente a esos valores y desde luego no están inscritos en la infraestructura de Internet.

Sí es posible, en cambio, que se produzca una "carrera hacia el fondo" en la que empresas e instituciones ajusten sus contenidos a los menos problemáticos en la jurisdicción más restrictiva. Es algo conocido en el mundo anglosajón como el "efecto California". Cuando este estado norteamericano reguló las emisiones de los coches en su territorio provocó que General Motors adecuara toda su producción a esa regulación porque era más eficiente económicamente hacerlo que fabricar coches personalizados para cada estado o región del mundo.

En realidad, los grandes problemas de la red se están convirtiendo en problemas entre naciones -al final EE.UU. nunca ha cedido el control, ni la propiedad ni la autoridad, del servidor raíz[7], actualmente en manos de la Internet Corporation for Assigned Names and Numbers, ICANN[8]-. Si se crea una gobernanza en Internet es poco probable que venga de una institución supranacional, sino que será una combinación de la práctica, el poder de mercado y la regulación de una entidad territorial.

4. LA RED Y EL ACTIVISMO

La información es poder. La desinformación es abuso del poder.

Newton Lee. Informático teórico. 2012.

Hasta aquí hemos visto una aproximación a quién ejerce el control sobre Internet y cómo ésta no es aquella red sin fronteras y autogobernada que una vez pretendió ser. Trataremos en este contexto el tema actual del ciberactivismo, especialmente de la oposición a los regímenes autoritarios a través de las plataformas de comunicación online conocidas como redes sociales. Un fenómeno que ha sufrido una explosión en los últimos cinco años.

En primer lugar, deben aclararse dos términos fundamentales porque pretenden dar una importancia a Internet y las redes sociales en las revueltas ciudadanas de los últimos tiempos que tal vez resulte desmesurada, aún reconociendo su importancia. Ambos priorizan la herramienta sobre el entorno. Por "doctrina Google" se entiende la creencia entusiasta en el poder liberador de la tecnología y la información para la promoción de la democracia. Del mismo modo, el "Internet centrismo" responde a cualquier cuestión sobre cambio democrático, replanteándola en términos de Internet, más que del contexto en que se presenta (Morozov, 2012).

En junio de 2009, tras las elecciones presidenciales iraníes, se produjeron protestas ciudadanas. La República Islámica cortó teléfonos y redes de telefonía móvil, pero el servicio de mensajería Twitter permaneció abierto. Inmediatamente las protestas fueron denominadas "la Revolución de Twitter", atribuyéndose a la tecnología el protagonismo de la revuelta, especialmente por gente que usaba esos servicios para informarse[9].

7 Europa quiere que Internet se libre del control de EEUU. Miguel Ángel Criado. Público. 19/06/2009.
8 ICANN Awarded Renewal Of IANA Contract By US Department of Commerce. Michael Berkens. TheDomains. 03/07/2012.
9 Iran's Twitter revolution. The Washington Times. 16/06/2009.

Pero la tecnología no lo era todo. Al fin y al cabo Al Qaeda era tan prolífica en Internet como las democracias occidentales. Tal vez resultara que más que las redes sociales habría que mirar los contextos económicos y sociales de los países en cuestión. Lo que ocurrió tras las protestas fue que el gobierno iraní formó un equipo contra el cibercrimen entre cuyas funciones estaba la identificación de opositores al régimen en las redes sociales -se produjeron cientos de identificaciones y al menos 40 detenidos-. En los aeropuertos la policía comenzó a examinar las cuentas en redes sociales de los pasajeros iraníes. Los bloggers, twitteros y usuarios de Facebook fueron encarcelados[10]. Como alguien dijo: "los analistas occidentales van a debates, los bloggeros iraníes o los twitteros egipcios van a prisión"[11].

A raíz de la ola de protestas revolucionarias en el mundo árabe producidas tras 2010, o de las movilizaciones ciudadanas mundiales de 2011, nadie puede negar la importancia que tiene Internet como herramienta en estos fenómenos. Es más dudoso afirmar que las redes sociales y los dispositivos móviles son la causa de los mismos. Un mensaje en Twitter no convierte a nadie en un revolucionario y el futuro de la democracia no puede depender de una empresa de nueva creación creada en Silicon Valley en 2006. Si un árbol cae en medio de un bosque y todo el mundo lo "twittea" no implica que Twitter haya movido el árbol.

Es evidente que las redes sociales y las nuevas tecnologías son capaces de alterar la probabilidad y la magnitud de las protestas -el simple hecho de saber que 20 amigos acudirán a manifestarse hace más probable que el usuario acuda-. Pero la dispersión de la información y su descentralización puede ser un inconveniente. En la República Democrática Alemana no existían cientos de canales de televisión, ni decenas de miles de páginas web, ni millones de emails. Bastó una confusa conferencia de prensa, retransmitida en directo por la televisión de Alemania Oriental, para que el Muro de Berlín se abriera en cuatro horas.

Internet es un medio efectivo para el activismo cívico y para la promoción democrática. Pero la realidad es que lo que predomina en la red es entretenimiento y relaciones sociales. Las búsquedas más populares en China o Rusia no son sobre libertades, sino sobre métodos para adelgazar. Las protestas iraníes fueron populares en Twitter, pero la muerte de Michael Jackson las eclipsó al momento.

Para un gobierno autoritario mantener a los jóvenes alejados de la política con YouTube (o RuTube) es más efectivo que la censura. "El sistema más efectivo de control de Internet no es el que tiene el sistema de censura más sofisticado y draconiano, sino aquel que no tiene necesidad de censura de ninguna clase". En los países del llamado Bloque del Este, los ciudadanos estaban expuestos a noticias políticas porque no había otra cosa. Cuando llegó la televisión por cable, el satélite e Internet la gente tuvo la opción de elegir y la mayor parte de la población se desentendió de ellas. En los países autoritarios se ha documentado el fenómeno denominado "escapismo", por el que la vida se hace más llevadera para la población con unas horas al día de televisión, noticias de sociedad y programas de entretenimiento. Salvo en circunstancias excepcionales, durante mucho tiempo ocurre que en las dictaduras, la población está despolitizada.

10 From protest to prison. Iran one year after the election. Amnesty International. 09/06/2010.
11 Evgeny Morozov. op. cit.

Lo que la población reclama en primer lugar en los países autoritarios es bienestar económico y no una idea abstracta de democracia. El consumismo refuerza a los gobiernos de estos países en vez de debilitarlos –China-. Tampoco se hará la revolución cuando todo el mundo está en un centro comercial comprando coches o televisores de plasma -Arabia Saudita-.

Este consumismo y esta búsqueda del entretenimiento puede provocar que en vez de "rebeldes digitales" lo que traiga Internet sea una generación de "cautivos digitales" que buscan el placer online, cualquiera que sea la realidad política del mundo real. Y los gobiernos son perfectamente conscientes de ello, como lo demostró el hecho de que el gobierno chino levantara las prohibiciones a la pornografía antes de que las protestas se politizaran o el gobierno de Vietnam, que configura su cortafuegos de modo que un menor puede acceder a contenidos pornográficos, pero no a los de un informe de Amnistía Internacional.

5. INTERNET Y CENSURA

Internet completó un círculo en 2005. Fue el resultado de una batalla que comenzó en 1999. Hace tan sólo una década la empresa Yahoo! era "El Señor de los Portales"; el punto de entrada a la red de la mayoría de los usuarios. A principios del año 2000 la compañía se enfrentó a una demanda ante los tribunales franceses por traficar con parafernalia nazi. Esto era ilegal en territorio francés, pero se permitía en territorio estadounidense donde, en principio, estaban situados físicamente los servidores de Yahoo!. La compañía se defendió vehementemente argumentando que un tribunal francés pretendía imponer su criterio en un área sobre la que no tenía ningún control y advirtió del precedente que supondría permitir a los gobiernos nacionales el control de Internet. Si las leyes francesas podían imponerse a servidores de EE.UU. también podían hacerlo las alemanas, japonesas, las chinas o las saudíes. "Hay muchas legislaciones y muchos países, pero solo existe un Internet".

Para Yahoo!, la naturaleza de su actividad económica impedía determinar la procedencia de sus clientes o el destino de sus productos. A diferencia de una compañía de venta de coches o lavadoras -que deben cumplir las normas medioambientales y las leyes de seguridad del país en el que venden sus productos-, en Internet era imposible realizar una trazabilidad exacta de cualquier negocio. La red, sencillamente, no estaba diseñada en base a la geografía; no se encontrarían fronteras físicas en el ciberespacio.

Sin embargo, al profundizar en el caso, se advirtieron algunos puntos disonantes: en primer lugar, resultó que los servidores de Yahoo! no estaban situados en EE.UU. y, por tanto, bajo la protección de la Primera Enmienda de la Constitución de ese país. Estaban en Estocolmo. Además, la página web de la empresa saludaba a sus usuarios en francés, si este era su origen, y la publicidad que les proporcionaba hablaba en el mismo idioma. Con esto se demostraba una cierta capacidad de selección de contenidos en función de la ubicación del usuario.

Finalmente, el tribunal galo falló en contra de Yahoo! que, en última instancia, cumplió la sentencia presionada por el riesgo de confiscación por la justicia de sus activos en suelo francés.

Poco tiempo después, tras la expansión de la compañía en la República Popular China, Yahoo! accedía a filtrar los contenidos o materiales dañinos o amenazantes para el Partido Comunista chino, adhiriéndose voluntariamente al Public Pledge on Self Discipline for the Chinese Internet Industry (Liang y Lu, 2010).

En 2005, Yahoo! había pasado de ser el defensor de la libertad absoluta en Internet a ser el censor del Partido Comunista en China; un agente de control del gobierno chino. Es una historia que habla de la transformación de la red. Del cambio desde una tecnología sin leyes territoriales a una tecnología que impone su implementación.

Pero un régimen autoritario no sobrevive exclusivamente por el establecimiento de barreras o de sistemas de censura. Tal vez el sistema ni siquiera se perciba como ilegítimo por sus ciudadanos: su legitimidad puede proceder del jingoísmo nacionalista, de la tradición, de la abundancia de recursos, del miedo a la agresión externa, etc. Muchos pueden tomar el concepto de democracia en un sentido de orden, justicia y bienestar más que como un sistema de elecciones periódicas e instituciones asociadas al modelo democrático liberal de Occidente.

Vemos con frecuencia a sistemas dictatoriales que realizan elecciones. Si un régimen totalitario permite las elecciones ¿por qué no permitiría Twitter o blogs? Al fin y al cabo una tiranía con Internet y teléfonos móviles sigue siendo una tiranía. Los gobiernos buscan y producen información para sus ciudadanos como medio de supervivencia, con un tipo de censura y vigilancia más refinadas. Resulta que el denominado “dilema del dictador” es aparentemente una falacia. El mismo nos dice que, o el dictador censura la red y sufre las consecuencias, quedando fuera del sistema económico de la globalización, o no censura y se arriesga a la revolución. En ambos casos, el dictador está perdido. Sin embargo, salvo Corea del Norte, todos los Estados autoritarios del mundo han aceptado Internet y convivido bien con él.

La censura en la actualidad va más allá de bloquear una lista de recursos prohibidos. Se analiza el comportamiento del ciudadano del mismo modo que lo hacen los motores de búsqueda. Si no se utiliza más la censura es porque gran parte de la navegación en Internet es anónima, aunque existen dos fuerzas que apuntan en la dirección contraria: la comercial, con la integración de redes sociales y páginas web (por ejemplo, los famosos likes de Facebook); y la gubernamental, con una creciente preocupación por la delincuencia, derechos de propiedad, etc., que provoca que los gobiernos pretendan cada vez más una mayor identificación personal de los ciudadanos en la red.

Otro tipo de censura puede venir dado por la propia naturaleza de Internet -el código de Lawrence Lessig-. George Orwell comprendió muy bien que la primera norma del estado totalitario era el empobrecimiento del lenguaje -él lo denominó Nueva Lengua-. En su novela 1984, se nos dice por boca del filólogo Syme: “Estamos reduciendo el lenguaje al mínimo. Es una cosa hermosa; la destrucción de las palabras”. Pero en el mundo real no hace falta un Estado totalitario que se encargue de ello: tenemos los SMS y a Twitter y sus 140 caracteres.

La nueva generación de consumidores digitales se ha caracterizado como “omnívoros digitales”: ordenadores, teléfonos, tablets y todo tipo de dispositivos conectados continuamente a Internet, determinan no solo qué se consume, sino cómo se consume. El omnívoro digital devorará contenidos en cualquier lugar, en todo momento y mediante cualquier dispositivo. En los países avanzados se trata de una realidad

demográfica: una generación que nació entre la comercialización del VCR y la comercialización de Internet para los que la información estaba allí y venía dada en forma digital. Y ser omnívoro supone disponer de la información más nutritiva, pero también de las calorías más vacías. Azúcar, grasas, levaduras, o SMS, emails, RSS, feeds, actualizaciones de estado, tweets.

También nos encontramos con el fenómeno de los "ciudadanos periodistas accidentales", que llegó parejo con los blogs, timelines y tweets. El hecho de la inmediatez de la información hace que cualquier persona con un teléfono móvil pueda convertirse eventualmente en un periodista de guerra.

Las redes sociales son un medio perfecto para la difusión de la información, pero también de la desinformación. El flujo de información no verificada que circula por Internet cada día es inconmensurable. Se llega a fenómenos como Wikipedia que, con todas las ventajas indudables que tiene, termina siendo el altavoz de un murmullo y una cacofonía de millones de voces de Internet que el algoritmo de Google, Bing u otro buscador no puede discriminar. Con sus defectos y virtudes, Wikipedia será el primer o el segundo resultado de una búsqueda y por tanto, aparentemente, la última palabra en cualquier asunto.

La naturaleza viral de la cultura de las redes sociales también ayuda a resolver el problema de la "sobrecarga informativa". Desde la perspectiva del censor, quien no es popular no merece siquiera la censura: sin lectores, sus blogs dejarán de tener nuevas entradas con el simple transcurso del tiempo.

6. INTERNET Y PROPAGANDA

Todo este ruido puede ayudar a la propaganda y la censura gubernamentales. Cuando la censura no es práctica, ni políticamente posible o es prohibitivamente cara... se recurrirá a la propaganda y a la participación en el juego.

Para la Venezuela de Chávez, la opción nunca fue entre censura o libertad de expresión, sino entre estar fuera de las redes sociales o usarlas en beneficio del régimen. El presidente Chávez abrió su cuenta en Twitter en 2010 y su sucesor, Nicolás Maduro, hacía lo propio a los doce días del fallecimiento del primero[12].

Se ha comprobado que el sector más susceptible a la propaganda resulta ser la "clase media", es decir, personas con cierta educación y un nivel de vida adecuado: ni los pobres e ignorantes, ni los ricos y sofisticados son vulnerables a la misma (Geddes y Zaller, 1989) -los primeros no son capaces de entender su propósito y los segundos lo entienden demasiado bien como para hacerle caso-. Por tanto, simplemente haciendo que la población se conecte a Internet no se conseguirá provocar una revolución del pensamiento crítico. De hecho, puede que ocurra exactamente lo contrario (Carr, 2010).

La propaganda en la red recurre a métodos sutiles y menos intrusivos para minimizar el impacto de la información negativa o maximizar el efecto de una propaganda favorable. "Matar al mensajero" con acusaciones de inestabilidad psicológica, poniendo en duda sus fuentes de financiación o sus verdaderas intenciones... repetir el mensaje

12 Nicolás Maduro abre su cuenta en Twitter. CNN México. 17/03/2013.

en tweets y blogs, sembrar la desconfianza, etc. son sistemas de respuesta flexibles y ágiles que en el mundo de Internet equivalen a luchar con fuego contra el fuego.

El profesor de derecho norteamericano, Cass Robert Sunstein, recomendaba en 2008 al gobierno estadounidense la "infiltración cognitiva" en las redes sociales y grupos de Internet para influir en la opinión pública. Esto es una práctica habitual en muchos gobiernos en la actualidad: Rusia con figuras prominentes como Eugene Kaspersky, Maria Sergeyeva y la Escuela de Bloggers del Kremlin; China con una red de comentadores gubernamentales denominada el Partido de los 50 Centavos, que cuenta supuestamente con 300.000 miembros y debe su nombre a lo que presuntamente se cobra por cada comentario favorable; Nigeria con el personal del llamado Anti-Bloggers Fund, el gobierno cubano con su llamada a las cibertrincheras, Azerbaiyán y su Azerí Spinternet; la Guerrilla Comunicacional venezolana; Irán y su red social valayatmadaran, cuyo objetivo es combatir el "mal", etc. Esto no es más que una adaptación de la práctica, realizada desde hace tiempo por las empresas privadas, conocida como **astroturfing**[13].

Es precisamente la descentralización de Internet la que crea numerosos focos informativos que pueden hacer que la propaganda en la red resulte más fácil y económica que la convencional.

7. WIKILEAKS Y ANONYMOUS

Anonymous y WikiLeaks han sido dos fenómenos que han caracterizado el activismo en Internet en los últimos cinco o seis años.

El primero es un pseudónimo utilizado mundialmente por diferentes grupos e individuos para realizar acciones o publicaciones, individuales o concertadas. No se puede trazar un origen específico de algo tan difuso como un grupo de hacktivistas, pero podemos establecer una fecha arbitraria, como otras muchas, del origen de este tipo de activismo por Internet. Esta sería cuando en 2001 se utilizaron ataques DDoS contra la empresa aérea alemana Lufthansa en protesta por los vuelos de deportación de inmigrantes desde Alemania[14]. Los tribunales dictaminaron finalmente que se trataba de una forma legítima de protesta.

Para los denominados hacktivistas, la intrusión gubernamental y corporativa siempre será mal utilizada por quienes pueden utilizarla mal, pero la tecnología ofrece a la gente la posibilidad de equilibrar la balanza otorgando el poder a los ciudadanos. Y el poder fue utilizado: Anonymous fue un personaje activo en las protestas contra la censura de la iglesia de la Cienciología, operación TitStorm, Túnez, Primavera Árabe, Sony, PayPal, etc.

Su lema es: "**We are Anonymous. We are Legion. We do not forgive. We do not forget. Expect us**." Si lo hacéis mal, tarde o temprano lo pagaréis. Si la justicia no la hace el Estado… la justicia la hará la gente. Todos, algunos o ninguno… al final, será alguien que se llamará anonymous.

13 De AstroTurf, marca de césped artificial. Campañas de relaciones públicas y anuncios comerciales que pretenden dar una impresión de espontaneidad y autenticidad con amplio apoyo social. Se trataría figuradamente de simular el césped natural. Véase http://en.wikipedia.org/wiki/Astroturfing

14 Protest closes Frankfurt airport. CNN World. 29/07/2001.

La organización WikiLeaks se encarga desde 2007 de publicar informes anónimos y documentos filtrados con contenido sensible en materia de interés público, preservando el anonimato de sus fuentes. Entre sus múltiples filtraciones pueden destacarse:

- Diarios de la Guerra de Afganistán.
- Registros de la Guerra de Irak.
- Cablegate. Documentación diplomática y confidencial del Departamento de Estado de Estados Unidos.
- Stratfor. Global Intelligence Files.

El hecho de que WikiLeaks tenga más documentos clasificados en su poder que el resto de la prensa mundial combinada es un indicador importante. La gente que tiene el poder no lo cede gratuitamente… El mensaje que han lanzado este tipo de filtraciones en Internet es poderoso: “si realizas acciones inapropiadas o ilegales, tarde o temprano se sabrá y sufrirás las consecuencias”.

El mensaje de WikiLeaks es, por tanto, que los comportamientos inmorales o ilegales serán más difíciles de realizar. Recordemos que la organización tuvo su papel en la revolución tunecina y su extensión en Egipto. Y lo que es más importante, ha creado un debate ciudadano sobre el secretismo gubernamental.

8. LA RED Y LA VIGILANCIA

"Si hay algo que no quieres que sepa la gente, en primer lugar tal vez no deberías estar haciéndolo… pero si necesitas esa clase de privacidad, la realidad es que los motores de búsqueda retienen información durante algún tiempo y es importante, por ejemplo, que estamos sujetos a la Ley Patriótica en los Estados Unidos. Es por tanto posible que toda esa información esté disponible para las autoridades."

Eric Schmidt. CEO Google. 2009.

Un gobierno autoritario no elegirá entre inundar a la población con entretenimiento barato, censurar los contenidos o leer los correos de sus ciudadanos. Un régimen inteligente hará las tres cosas. La trinidad del autoritarismo es la propaganda, la censura y la vigilancia. Internet provoca cambios en cómo se realizan estas actividades. Si se hace más difícil la censura también se facilita la propaganda, si se facilita la encriptación también aumentan los objetivos blandos para vigilar -millares de amateurs movilizados por las redes sociales-, si se debilita la propaganda se puede reforzar la vigilancia. Como vemos, los tres pilares están interconectados.

El efecto de las campañas de vigilancia va más allá de lo obvio. Saberse observado sin saber cómo ni cuándo, puede llevar a la autocensura e incluso a la evitación de la crítica y a la limitación autoimpuesta de la libertad de expresión. Como bien sabía Jeremy Bentham, el mero hecho de la existencia de un clima de incertidumbre, de ansiedad y de miedo, refuerza los efectos de la vigilancia. Simplemente el desconocimiento del alcance de la vigilancia gubernamental inhibe la acción subversiva.

Pero la realidad es que, aleatoria o sistemáticamente, la vigilancia siempre se hizo. Como tantas otras cosas, se hace, pero nadie cuenta que se hace. No es necesaria una enumeración exhaustiva. Al igual que en otros aspectos de nuestra vida las

tecnologías van varios pasos por delante del marco legal necesario que garantice los derechos y libertades. Un desafio de gran magnitud para los próximos años.

Ya que hablamos de Internet, remitimos al lector a una lista pública comprensiva de los programas de vigilancia secretos de los gobiernos sobre sus ciudadanos en: http://en.wikipedia.org/wiki/List_of_government_surveillance_projects

8.1. TOTAL INFORMATION AWARENESS

En abril de 2002, el entonces director de D.A.R.P.A. (Defense Advanced Research Projects Agency) informó por primera vez al pueblo norteamericano sobre la creación de la Oficina de Reconocimiento de Información (I.A.O.), cuyo objetivo era el "desarrollo de los sistemas de información necesarios para encontrar, identificar, rastrear y comprender las redes terroristas e incrementar sustancialmente nuestro conocimiento sobre nuestros adversarios". En sus declaraciones de marzo de 2003, ante el Congreso de los Estados Unidos, confirmaba que el proyecto T.I.A. (Total Information Awareness) "no desarrollaba tecnologías ni mantenía expedientes sobre ciudadanos norteamericanos".

La T.I.A. era un "prototipo multiagencia experimental" que permitía a las oficinas gubernamentales la colaboración -"conectar los puntos"- y la prevención de los ataques terroristas. Lamentablemente el Congreso eliminó la financiación del programa y eliminó la Oficina para el Descubrimiento de la Información en 2003.

Pero en marzo de 2008, el diario The Wall Street Journal informaba que la National Security Agency (N.S.A.) había estado construyendo esencialmente el mismo sistema proyectado por la T.I.A… "monitorizando grandes cantidades de datos de los ciudadanos".

Pero no fue al final una institución gubernamental sino el surgimiento de las redes sociales -un concepto vago formado por un grupo de empresas oligopolísticas como Facebook, Twitter, Google+, Youtube, etc.- lo que facilitó el Control Total de la Información (la realización práctica de la T.I.A.).

El hecho es que no ha debido ser una propuesta gubernamental, sino la paulatina construcción de una tecnología y una infraestructura desde la iniciativa privada, lo que ha creado la realidad de un problema con la privacidad y la seguridad de los datos de los ciudadanos. El reconocimiento facial, el rastreo posicional, las aplicaciones sociales basadas en GPS, Google Street View, huellas digitales en fotografías, minería de datos… todas estas ventajas tecnológicas posibilitan y facilitan las labores de vigilancia de los gobiernos.

La propia D.A.R.P.A. tiene su círculo social de seguidores en Twitter, Facebook, Google+, Youtube… Y, en un movimiento muy orwelliano, la Oficina de Reconocimiento de Información fue renombrada como Oficina de Innovación de la Información con un presupuesto de 200 millones de dólares, mientras mantenía las mismas funciones en lo que era una reactivación práctica del T.I.A., a través de programas como ADAMS[15] (Anomaly Detection and Multiple Scales), diseñado para detectar regularidades y anomalías estadísticas en grandes conjuntos de datos.

15 Georgia Tech Helps to Develop System That Will Detect Insider Threats from Massive Data Sets. Abby Robinson. Georgia Tech. 10/11/2011.

Pero el problema que en el fondo siempre tuvo la T.I.A. fue que requería un sistema de minería de datos eficiente y efectivo. Esto se hizo realidad con las redes sociales.

La seguridad es un compromiso. Los costes pecuniarios, la intrusión en la privacidad de los usuarios y los efectos sobre el bienestar de los ciudadanos están implícitos en toda decisión y toda implementación de un sistema de seguridad. Esto es evidente también en el mundo digital. La gente toma decisiones continuamente asumiendo estos compromisos en su vida cotidiana.

Nadie debería extrañarse de que si cedes voluntariamente tus datos en aras de la provisión de ciertos servicios a empresas privadas cuyo leitmotiv es la obtención de beneficios, inevitablemente se producirán violaciones en la privacidad de los mismos.

9. PRIVACIDAD

"Puedes tener datos sin información, pero no puedes tener información sin datos."

Facebook Data Team. 2008.

No importa cómo protejamos nuestros datos o nuestros móviles. Da igual que evitemos el uso de aplicaciones de terceros en nuestros coches o nuestros hogares. No importa si desactivamos nuestras cuentas de Facebook o Twitter y también es poco importante que evitemos buscar en los motores de Google o Bing. Pese a todo ello, existen bases de datos sobre cada persona para quien esté dispuesto a pagar por ellas. Se trata de todo un mercado de empresas que venden registros públicos, nombres, fechas de nacimiento, teléfonos, historial de lugares de residencia, de matrimonios o de divorcios, propiedades, querellas judiciales, antecedentes penales o policiales, todo por una simple tarifa.

Existen determinados servicios -Google Street View es un ejemplo patente- que hacen impracticables avisos de privacidad del estilo: “con su presencia en esta calle usted reconoce que ha sido informado de que puede ser grabado y fotografiado como parte del servicio”. Por mucho que la empresa tome medidas para salvaguardar la privacidad de los ciudadanos, se trata del ejemplo de un caso en el que la utilidad de la información para millones de personas supera a la necesidad de privacidad de unos pocos. Pero tampoco es tan sencillo. En mayo de 2010 Google admitió que sus coches habían almacenado los datos de las redes inalámbricas desencriptadas16, al tiempo que realizaba su reconocimiento de ciudades en más de 30 países.

Otro ejemplo salió a la luz en 2011, cuando se reveló que la aplicación de seguimiento de ubicación del iPhone de Apple almacenaba de modo secreto la localización histórica del móvil del usuario durante un año, incluso aunque éste hubiera desactivado dicho servicio de localización.

El experto Andrew Lewis lo expresó claramente en agosto de 2010: “Si no estás pagando por algo no eres el consumidor, eres el producto que se vende”. Es desde esta óptica desde la que se debe ver la creación de una cuenta en Facebook o en Gmail[17].

16 Direcciones de correo, páginas web, claves, SSIDs, direcciones MAC…

17 Donde ya se expresa como mínimo el género, fecha de nacimiento, nivel formativo, lugar de trabajo, de residencia, intereses, aficiones, fotos y otros tipos de información privada como las relaciones sentimentales, etc.

Pete Cashmore, fundador y directivo de Mashable, uno de los portales de noticias en Internet más influyentes en la actualidad, decía en 2012 que “el mundo online está permitiendo ciertamente que cada uno de nuestros movimientos sea rastreado, mientras proporciona un contrapeso al concepto orwelliano del Gran Hermano. A diferencia del mundo distópico de Orwell, la gente hoy en día hace una elección consciente: mientras la Policía del Pensamiento de Orwell te rastreaba sin permiso, en la actualidad algunos consumidores se sienten cómodos compartiendo sus actividades online”.

Pero Cashmore no ha apreciado que este es el peor de los casos; cuando voluntariamente se cede la privacidad a cambio de cupones, prestigio, ser cool o lo que sea. Esto es aún más distópico que el Gran Hermano orwelliano, no hace falta que el Gran Hermano te vea porque probablemente tú estás viendo Gran Hermano, porque la población voluntariamente se conecta a él. Además, Facebook no es el Gran Hermano, sino tu Gran Amigo.

Empresas como Facebook[18] o como Google están tratando de predecir qué queremos buscar, qué queremos ver o qué es lo que nos gusta. Esto es algo que puede resultar muy útil de cara al usuario pero, por otro lado, puede convertirse en la herramienta definitiva para limitar las posibilidades de descubrimiento del ciudadano; la búsqueda de nuevos intereses o de ideas nuevas en la red. Cuando el Internet global se convierte en el Internet personal, es cuando la información deja de ser información en absoluto. En los servidores de Google se juega a un juego en el que se puede conseguir una era de un increíble enriquecimiento intelectual o una distopía sin precedentes de control social y vigilancia.

En 2012 más de dos mil millones de personas estaban conectadas online (más de un 28% de la población mundial). Muy pocos de ellos están dispuestos a luchar por la salvaguardia de su privacidad y un número muy elevado se muestra dispuesto a ceder una parte de la misma por “estar conectados”. Los riesgos son sobrepasados por la necesidad básica del consumidor de comunicarse. Para satisfacer su deseo insaciable de interactuar con alguien dispuesto a escuchar, el usuario ha estado y está dispuesto a sacrificar gran parte de su privacidad personal.

Facebook estuvo disponible para el mundo en febrero de 2004; en diciembre tenía un millón de usuarios activos. En septiembre de 2011, estos superaban los 800 millones. En mayo de 2012 la empresa cotizaba en bolsa y en verano del mismo año sus usuarios ascendían a 955 millones. La mitad de los ciudadanos estadounidenses tenían una cuenta de Facebook para entonces. Pero sus usuarios no eran especialmente vigilantes a la hora de salvaguardar su privacidad -dos terceras partes jamás habían cambiado su configuración o habían limitado lo que los demás podían ver de ellos online- y cada uno de ellos tenía en promedio 130 amigos.

En Internet lo publicado es accesible a todos y permanece en el tiempo. En principio, cualquiera podrá guardar la foto publicada e incluso los comentarios realizados en una página web cerrada permanecerán visibles por tiempo indefinido en lugares como “The Internet Archive”.

18 A imitación de Google y su PageRank, Facebook utiliza su propio algoritmo, EdgeRank, que determina quien ve qué y qué debe haber en un newsfeed de determinada cuenta de Facebook.

Los sitios “sociales” extienden la llamada presión entre iguales (peer presure) del mundo físico a un mundo virtual prácticamente infinito que existe online. Los niños y los adolescentes son los más vulnerables y susceptibles a verse influenciados por los mensajes e imágenes que obtienen de sus “amigos” en las redes sociales. Fenómenos mediáticos, como la serie televisiva “Gran Hermano”, muestran la aparentemente irrefrenable tendencia psicológica de millones de personas a acceder a la información privada de otras personas que no es en absoluto de su incumbencia. Muestra también el hecho de que hay mucha gente dispuesta a exponer su vida privada ante extraños sin prácticamente consideración alguna de las consecuencias.

El lanzamiento de YouTube, en febrero de 2005, democratizó y trasladó este fenómeno a la red -en la actualidad se sube en un mes más contenido en vídeo que el generado por las tres mayores cadenas televisivas norteamericanas en tres años-. Además, no todo el mundo puede salir por televisión, pero sí puede hacerlo en vídeos online; al fin y al cabo, el lema de YouTube es “Broadcast Yourself”. Una tendencia en boga más en la actualidad es la de las llamadas “historias patrocinadas” que sustituyen a los anuncios o banners tradicionales.

Aunque estas relaciones de identidad, de amistad, de carácter romántico o sexual, se han dado siempre entre los seres humanos, las redes sociales nos han conferido el poder de configurarlas en forma extrema en el sentido de que la gente se adorna, se falsifica, se hace individualista y narcisista y, en cierto modo, se inventa a sí misma.

Se da el resultado anecdótico de que el lenguaje de la comunicación por Internet y los dispositivos móviles, con su gramática, sintaxis, puntuación y semántica propios y uso de símbolos (emoticonos) consiguen en la práctica promover cierto analfabetismo por el efecto perverso de que éste se convierte en algo aceptable socialmente.

10. ESPIONAJE

"Facebook en particular es la máquina de espionaje más espantosa que jamás se ha inventado. Aquí nos encontramos con la base de datos más completa y eficiente acerca de las personas, sus relaciones, sus nombres, sus direcciones, su ubicación y sus comunicaciones entre sí y sus familiares, todo codo con codo con el gobierno y todo accesible para la inteligencia estadounidense."

Julian Assange. Fundador de WikiLeaks. Mayo 2011.

Sabemos que hoy en la red nuestros amigos digitales son nuestros peores enemigos. Los encontramos en Facebook o en otra red y si una entidad legítima puede recabar información de ellos... ¿Quién no querría que se prevenga un horrible crimen, el secuestro de un niño o una matanza en una escuela de bachillerato? Si pudiéramos suponer que todo podría hacerse simplemente analizando un gran volumen de datos. ¿Y si fuera tan fácil como detectar un “precrimen” y detener a los “preculpables”?

En julio de 2010 éramos conocedores de que algunas taquillas del metro de Tokio utilizaban webcams con software de reconocimiento facial para determinar el género y la edad de los pasajeros. El objetivo era determinar el tipo de persona que miraba cierto tipo de anuncios y a qué horas del día lo hacían. En principio no se trataba de un problema de privacidad; simplemente se trataba de la denominada “inteligencia comercial”, en recolección de datos, atracción de audiencias y venta innovadora de productos.

Pero extrapolemos esto a las redes sociales. Una empresa como Facebook se basa en la entrega de “anuncios sociales” a los consumidores. Los anuncios sociales son aquellos dirigidos a los usuarios que tienen “amigos”, que son “seguidores” o han interactuado con la marca anunciada y publicitan esta relación de forma conspicua en las redes sociales. Se trata simplemente de una aplicación de pulsar el botón “me gusta” –like- de Facebook. Este tipo de publicidad es un fenómeno muy interesante en cuanto a fenómeno psicológico, en tanto se refuerza a sí mismo por la aprobación o la necesidad de aprobación social y genera información muy valiosa sin coste alguno y muy centrada en las audiencias objetivo.

Un diario norteamericano[19] mostraba al público en 2002 el mencionado programa Reconocimiento Total de Información -Total Information Awareness-, que pretendía suministrar a los agentes de la ley y analistas de inteligencia acceso instantáneo a la información que proporcionaban los correos electrónicos personales, las llamadas por teléfono móvil, registros de tarjetas de crédito, historiales médicos, transacciones bancarias, documentos de viaje y otros datos de los ciudadanos estadounidenses, sin necesidad de ninguna orden judicial que autorizara tal registro.

Se está convirtiendo en práctica común, en las admisiones en determinadas escuelas universitarias o en solicitudes de empleo, la comprobación de perfiles en las redes sociales; especialmente para rechazar aspirantes por algún que otro rasgo indeseable -considérese el caso real en EE.UU. de un usuario de Facebook miembro de un grupo de apoyo de un determinada enfermedad y rechazado de un empleo subrepticiamente por razones médicas-.

La vigilancia digital es mucho más barata que la vigilancia tradicional al estilo del KGB. Hace poco tiempo, la Stasi alemana debía recurrir a la tortura para conocer los contactos de un activista; hoy basta con unirse a Facebook o mirar a los seguidores en Twitter. Una simple minería de datos en Amazon.com permite conocer las preferencias y las lecturas de los usuarios, que son compartidas abiertamente. Internet ha aumentado la productividad de la vigilancia.

Además, quedarse fuera de las redes sociales no es una opción realista para un disidente político. Necesitan hacerse visibles para dar su opinión, contrarrestar la propaganda oficial, movilizar apoyos, etc. Quedarse fuera significa sencillamente renunciar a la disidencia y mantenerse en el anonimato le quita su sentido. Y las ventajas de las redes sociales son también su vulnerabilidad: el hecho de poder buscar “amigos” en Facebook permite también buscar enemigos. La participación en grupos o en varias redes simultáneamente permite delimitar perfiles por “intersección de conjuntos”.

Una de las defensas contra la vigilancia es la denominada “seguridad por oscuridad” o el hecho de que nuestra información sencillamente se difumina en el vasto océano de datos digitales producidos por los demás usuarios. Pero la minería de datos y el procesamiento de los mismos han puesto esta protección en cuestión.

Técnicamente, un motor de búsqueda en Internet conoce las peticiones que recibe de palabras como “democracia” o “manifestación” en un país totalitario. Conoce su frecuencia, su distribución geográfica y las demás búsquedas realizadas por los “albo-

19 Pentagon Plans a Computer System That Would Peek at Personal Data of Americans. John Markoff. The New York Times. 09/11/2002.

rotadores" del régimen. Y un gobierno autoritario siempre será derrocado por sorpresa -como el régimen de Hosni Mubarak-, pues de no ser así lo que ocurre es que está cometiendo suicidio -como la URSS y el Bloque del Este-. Es preciso asumir que los gobiernos autoritarios harán uso de técnicas como la vigilancia y minería de datos en Internet para hacer que las sorpresas sean menos frecuentes.

Aunque pocas cosas pueden sorprender ya. Edward Joseph Snowden es un exconsultor privado estadounidense de la Agencia Central de Inteligencia (CIA) y de la Agencia de Seguridad Nacional (NSA) que ha revelado documentos clasificados sobre varios programas de la NSA, incluyendo el programa de vigilancia PRISM. Snowden sigue haciendo revelaciones desde Rusia, donde se encuentra asilado por razones políticas.

PRISM es el enésimo programa secreto de minería de datos y vigilancia electrónica llevado a cabo por la NSA norteamericana. El espionaje del sistema es masivo e incluye la colaboración de varios organismos gubernamentales estadounidenses, distintos países y numerosas compañías privadas. Estos "colaboradores" son también objeto de vigilancia, pues como el aclamado Carnivore (DCS1000) del FBI, estos sistemas adoran las cantidades ingentes de datos.

No comentaremos más esta última revelación o este último sistema. Recomendamos al lector una búsqueda en los diarios nacionales o en los internacionales si domina más idiomas. También puede elegir Wikipedia o Google, pero siempre con precaución[20].

11. SMARTPHONES

En la actualidad, los "teléfonos inteligentes" son los dispositivos portátiles más prevalentes en la interacción con las redes sociales. Hoy en día son más de 1.200 millones los artefactos de esta clase activos en el mundo[21]. De hecho, se ha creado un nuevo término: nomophobia, que define la patología psicológica caracterizada por el miedo a estar sin teléfono móvil.

Desde 2011 es un hecho acreditado[22] que este tipo de dispositivos graban regularmente su localización y el historial de la misma. Y "una persona que conoce los movimientos de otra puede deducir si es un visitante regular de una iglesia o de un prostíbulo, si es un alcohólico o un habitual de los gimnasios, un marido infiel, un enfermo recibiendo tratamiento o un simpatizante de determinados individuos o grupos políticos… o todo ello combinado"[23].

Las aplicaciones para dispositivos móviles son pequeños programas informáticos que proporcionan utilidades concretas a sus usuarios. No es, en absoluto, extraño que las empresas que los producen se vean envueltas en casos que muestran poco respeto por la privacidad de sus usuarios y es razonable pensar que muchas aplicaciones están reteniendo subrepticiamente información de sus usuarios sin el conocimiento de estos. Y todo es por la propia estructura del mercado: los usuarios ignoran que sus datos están siendo almacenados. En un mercado como el del sistema operativo Android, con más de 200.000 aplicaciones, 190 millones de usuarios y 10.000 nuevas

20 See Who's Editing Wikipedia - Diebold, the CIA, a Campaign. John Borland. Wired. 14/08/2007.
21 ITU Telecommunications World. Facts and Figures. 2011.
22 This Tech Bubble Is Different. Ashlee Vance. Bloomberg Businessweek. 14/04/2011.
23 Cell Phone Location Tracking Public Records Request. American Civil Liberties Union. 06/04/2012

aplicaciones descargadas cada día; o el de Apple Store con 650.000 aplicaciones, 100 millones de usuarios y 30.000 descargas diarias, es de esperar el surgimiento de las llamadas “rogue apps” -no literalmente aplicaciones fraudulentas, pero muy laxas en determinadas políticas con sus usuarios-.

Mucha gente afirma que los teléfonos móviles inteligentes son una tecnología liberadora, conveniente y disponible en cualquier momento y cualquier lugar, pero algunos otros no están de acuerdo cuando “en cualquier momento y cualquier lugar” se convierte en “en todo momento y en todo lugar”.

Se trata de un hardware que se vende en términos de enriquecimiento personal, de asunción de poder y de cada vez más autonomía. Pero la verdad es que lo que nos encontramos detrás de estos dispositivos inteligentes es, cada vez más, pérdida de control sobre nuestras propias vidas, más delegación y mayor dependencia. Lo que puede llegar a ocurrir es que nuestra tecnología sea lo que nos defina.

Pero el gran objetivo de la publicidad es dirigirse a la gente en la situación en que se encuentran y en el momento y el lugar más cercanos y apropiados para realizar la compra. De hecho los teléfonos inteligentes son tan relevantes que Facebook ha mostrado recientemente su interés en lanzar uno propio por el miedo a convertirse en una simple aplicación de otras plataformas móviles en caso de no hacerlo.

Poco después de la burbuja de las “.com” y coincidiendo con la incorporación de los dispositivos de telefonía móvil a la red, Internet entró en una Era Comercial. El ejemplo de Facebook es paradigmático de los tiempos: la empresa se creó bajo una fórmula habitual en la industria tecnológica del sector. Primero se ofrece al público un servicio, se recopila información respecto a cómo usa la gente dicho servicio y esta información es utilizada para vender publicidad a los usuarios. Por otro lado, los usuarios no tienen muchas más opciones: deben confiar en Internet para crear o gestionar sus negocios o para realizar transacciones online.

11.1. APLICACIONES SOCIALES DE CONTEXTO

Por este nombre se conocen las aplicaciones para dispositivos móviles que comparten automáticamente información de la ubicación o actividades del usuario en relación con gente cercana integrante de su red social o personas con intereses afines -Badoo, denominado el Facebook del sexo, sería un buen ejemplo-. Más y más gente pone a disposición de un amplio colectivo su información personal y su localización geográfica en tiempo real; la privacidad y la seguridad de los datos personales se convierten en este punto en un serio problema. Algunos avances, como el software de reconocimiento facial, que es capaz de reconocer a tu “amigo” entre una multitud e informarte de que está cerca de ti, muestran que el problema de la privacidad puede convertirse en algo serio.

12. CONCLUSIÓN

Lo que está caracterizando a Internet en los últimos tiempos es una pulsión por compartir los pensamientos y las experiencias con el resto del mundo. Las redes sociales han provocado que los usuarios se sientan cómodos con esta idea de compartirlo todo,

lo que ha facilitado la posibilidad de un “ajuste fino” de la vigilancia. Como decíamos al principio, llegamos a construir de forma voluntaria nuestro Panopticon digital. El entretenimiento compulsivo y la cesión voluntaria de datos también facilitan el control de la población por los regímenes autoritarios. Es un giro inesperado de la tecnología liberadora que se suponía que nos proporcionaría Internet.

El problema de esta tendencia de la red, por la que se ceden los datos voluntariamente, es que al final se convierte en idiosincrasia. Está en el carácter del usuario que quiere mirar y que le miren y desea escuchar y que le escuchen. Es un concepto que implica que todo ha de ser público. Es Facebook como exhibicionismo. Algo que está más allá de un sistema de vigilancia, más allá de un régimen autoritario o de un sistema fascista. El Gran Hermano de Orwell jamás pudo soñar algo así. Según ilustra magníficamente McMillan[24], basado en Neil Postman (Postman, 1985):

Orwell temía a los que prohibirían los libros, pero Huxley, autor del aclamado "Un mundo feliz”, temía que no hubiera razón para prohibir un libro porque no habría nadie que quisiera leer uno.

Orwell temía a los que nos ocultarían la información, pero Huxley temía a los que nos darían tanta que la harían irrelevante.

Orwell temía que la verdad sería ocultada al ciudadano, pero Huxley pensaba que la verdad se ahogaría en un mar de intrascendencia.

Orwell temía que la cultura sería negada, pero Huxley sospechaba que la cultura sería algo trivial, centrada en sensaciones, sensualidad y diversiones inocuas.

Orwell pensaba en el control mediante la imposición del castigo y el dolor, pero Huxley consideraba más bien el control por la imposición del placer.

En 1984 lo que temíamos nos podía destruir. En 2013, en un mundo feliz, es nuestro deseo, lo que nos gusta, el origen de nuestra ruina.

Los que se oponen a la tiranía siempre han infravalorado la necesidad del hombre por ser aceptado, valorado y por darse a conocer, así como el apetito casi infinito del ser humano por la distracción, el placer y el entretenimiento.

BIBLIOGRAFÍA

Amnesty International. (2010). From protest to prison: Iran one year after the election. Amnesty International Publications.

Assange, J. (2013). Cypherpunks: La libertad y el futuro de Internet. Deusto.

Brousseau, E., Marzouki, M., y Méadel, C. (2012). Governance, Regulations and Powers on the Internet. Cambridge University Press.

Carr, N. (2010). The Shallows: What the Internet Is Doing to Our Brains. W. W. Norton & Company.

Froomkin, M. (2000). Wrong Turn in Cyberspace: Using ICANN to Route Around the APA and the Constitution. University of Miami School of Law.

24 http://www.highexistence.com/amusing-ourselves-to-death-huxley-vs-orwell/

Geddes, B., y Zaller, J. (1989). Sources of Popular Support for Authoritarian Regimes. American Journal of Political Science, 33(2), 319-347.

Goldsmith, J., y Wu, T. (2006). Who controls the Internet? Illusions of a Borderless World. Oxford University Press.

International Telecommunication Union. (2011). The World in 2011: ICT Facts and Figures.

Lee, N. (2012). Facebook Nation: Total Information Awareness. Springer Science & Business Media.

Liang, B., y Lu, H. (2010). Internet Development, Censorship, and Cyber Crimes in China. Journal of Contemporary Criminal Justice, 26(1), 103-120.

Morozov, E. (2012). The Net Delusion: The Dark Side of Internet Freedom. PublicAffairs.

Postman, N. (1985). Amusing Ourselves to Death: Public Discourse in the Age of Show Business. Penguin Books.

Fecha de recepción: 21/05/2014. Fecha de aceptación: 24/06/2014

LA GESTIÓN DE LA I+D+i EN LA GUARDIA CIVIL

MIGUEL CAÑELLAS VICENS

RESUMEN

Desde el año 2008 la Guardia Civil está participando en calidad de coordinador/socio/observador en varios proyectos de Investigación, Desarrollo e Innovación (I+D+i) financiados por el Séptimo Programa Marco (7º PM) de la Comisión Europea (CE). La financiación de estos proyectos, dentro del área de seguridad, está orientada a proporcionar soluciones civiles a las agencias encargadas de la seguridad interior, en el caso español Fuerzas y Cuerpos de Seguridad del Estado (FCSE) y, más concretamente, la Guardia Civil. En este sentido la CE ha transmitido su visión actual sobre la trascendencia que representa para la industria actual del sector I+D+i europeo el hecho de que la aceptación de las soluciones tecnológicas y productos pase por la implicación del usuario final en los desarrollos industriales, desde el diseño inicial hasta su implementación. Y en el caso concreto de la industria de seguridad dicha tecnología debe tener un final público, esto es, resultar un beneficio que conlleve una mejora de la seguridad pública. Consciente de la importancia que tiene para España el impulso de su actividad empresarial, la Guardia Civil viene participando activamente en calidad de usuario final desde hace años y, continuando con este impulso transformador, colabora en la actualidad en la preparación, negociación y ejecución de numerosos proyectos tecnológicos dentro del escenario del 7º PM y Horizonte 2020.

Palabras clave: Guardia Civil, innovación, FP7, Horizonte 2020, industria de seguridad, gestión de proyectos.

ABSTRACT

Since the year 2008, the Spanish Guardia Civil is participating as coordinator/partner/observer in several projects of research and development and innovation (R&D and innovation) funded by the Seventh Framework Programme for Research (FP7) of the European Commission (EC). The funding of these projects, within the security area, focuses on providing the agencies responsible for internal security civilian solutions, in the Spanish case, State Security Forces and Corps, in particular, the Spanish Guardia Civil. In this regard, the EC has transmitted its current vision regarding the transcendence that represents for today's industry, in the European R&D and innovation sector, the fact that the acceptance of technological solutions and products are attached to the end-user involvement in the industrial developments, from the initial design to its implementation. In the case of the security industry such technology must have a public purpose, in other words, a benefit turn out entailing an improvement of public security. The Spanish Guardia Civil, aware of the importance for Spain of promoting its business activity, has participated actively for years as end-user and, continuing this momentum of change, currently collaborates in the preparation, negotiation and execution of many technological projects within FP7 and Horizon 2020.

Key words: Guardia Civil, innovation, FP7, Horizon 2020, secutity industry, project management.

1. INTRODUCCIÓN

El concepto de seguridad debe ser entendido como un todo integral, donde no existen espacios intermitentes entre la seguridad interior y la seguridad exterior, tanto en nuestro país como en la Unión Europea (UE). Por ello nuestra fortaleza debe residir en tener consciencia de la existencia de los vasos comunicantes que el fenómeno de la criminalidad pone de manifiesto. En este sentido el autor quiere destacar una serie de razones ya esgrimidas por el profesor Arteaga[1] para la implantación de la Estrategia Española de Seguridad (EES)[2], como fueron los siguientes aspectos de la estrategia que se encuentran relacionados con esta idea inicial planteada, como son: la novedad de los riesgos (escaso conocimiento, complejidad, transnacionalidad, mutabilidad…); continuidad entre lo externo y lo interno, lo local y lo global; multiplicación de las dimensiones de seguridad (tradicionales y no tradicionales) y de los niveles donde se decide (privado, público, subestatal, estatal, regional e internacional) y la necesidad de integrar la gestión frente a la coordinación tradicional (enfoque integral, interagencias, plataformas de intercambio, etc.). En este sentido, la nueva Estrategia de Seguridad Nacional (ESN)[3] destaca por su espíritu continuista respecto a la anterior y ambas son coincidentes en identificar los riesgos que afectan a la seguridad de España[4] en cada momento, así como el ofrecer una visión compartida del contexto estratégico que se prolonga en las líneas estratégicas para afrontar dichos riesgos[5].

Las Agencias y las Fuerzas policiales responsables de la seguridad interior de la UE son conscientes de que se enfrentan de forma constante a nuevos retos y amenazas para la seguridad, de carácter complejo y diverso, así como el hecho que la línea existente entre la amenaza externa e interna para el Espacio europeo de Libertad, Seguridad y Justicia (ELSJ)[6] es muy difusa, por lo que dicha amenaza se encuentra íntimamente relacionada y entrelazada.

1 ARTEAGA, Félix. Propuesta para la implantación de una Estrategia de Seguridad Nacional en España. Documento de Trabajo 19/2011 del Real Instituto Elcano. 16/12/2011. p.9

2 "La Estrategia Española de Seguridad, una responsabilidad de todos", documento aprobado por el gobierno español en junio de 2011, en el que se introducen modificaciones en cuanto al centro de gravedad del concepto de la Defensa, de modo que se evoluciona desde dicho concepto compacto hacia una inmersión en el amplio concepto de la Seguridad y sus dimensiones.

3 "La Estrategia de Seguridad Nacional, un proyecto compartido", documento aprobado por el gobierno español el 31 de mayo de 2013, y que actualiza la anterior versión fechada de 2011. La principal novedad sería la articulación de la Seguridad Nacional como Política de Estado, conteniendo las directrices que permitirían la reasignación de todos los recursos disponibles del Estado de manera eficiente para la preservación de la Seguridad Nacional.

4 "La Estrategia de Seguridad Nacional, un proyecto compartido" (2013). p.21-37

5 Ibídem. p. 38-52

6 Artículo 3.2 del Tratado de la Unión; El espacio de libertad, seguridad y justicia (ELSJ) es el nombre con que se designa un conjunto de políticas y actuaciones que la Unión Europea despliega, esencialmente dentro pero también fuera de sus fronteras, para lograr el objetivo de crear un área compartida entre sus Estados miembros, donde se alcance un alto grado de cooperación y coordinación política, policial y judicial a nivel comunitario que facilite la seguridad interior, una justicia eficaz y una fuerte protección de las libertades públicas para sus ciudadanos.

A este respecto debemos recordar que la Estrategia de Seguridad Interior de la UE[7] apuesta por la innovación como una de las líneas estratégicas de acción y destaca la necesidad de trabajar juntos para fomentar el desarrollo conjunto de nuevas tecnologías desde un enfoque común, así como para ahorrar costes y aumentar la eficiencia.

El conocimiento y el adecuado uso de las nuevas tecnologías, pueden formar parte de la respuesta a estas amenazas, de manera que, sin duda, una mayor competencia policial basada en la implementación de nuevas soluciones tecnológicas que refuercen sus capacidades policiales contribuirán a mejorar la seguridad interior de la UE. Sin embargo, debemos ser conscientes del ciclo de vida de las nuevas tecnologías[8], ya que a menudo pueden desaparecer tan rápido como emergen: el 80% de los servicios que se ofrecen hoy en día en el ámbito de las Tecnologías de la Información y las Comunicaciones (TIC) no existían hace 15 años y, por otro lado, los servicios relacionados con las TIC, que se ofrecían a modo de nueva tecnología hace 15 años, hoy ya no existen.

Las nuevas tecnologías cambian la forma en que operan las diversas formas de la criminalidad y, por lo tanto, modifican en el sentido contrario los patrones de respuesta policial para hacer frente a dichas amenazas. Ello implica que, mientras las Agencias y las Fuerzas policiales responsables de la seguridad interior de la UE tratan de adecuar sus arsenales y repositorios tecnológicos frente al reto que plantea dicha criminalidad evolutiva, una parte de la actividad delictiva se encuentra impune y difícil de contrarrestar. Las oportunidades que ofrecen las nuevas tecnologías, y la necesidad de hacer uso de ellas, obligan a modificar los parámetros existentes en la metodología de investigación de delitos, además de poner en cuestión el marco legal en el que Agencias y las Fuerzas policiales responsables de la seguridad interior de la UE y la justicia tienen que operar. Por lo tanto, los organismos encargados de hacer cumplir la ley se ven obligados a analizar el impacto del cambio tecnológico en este ámbito.

El análisis de dicho impacto debería tener en cuenta las prioridades establecidas para el aseguramiento del ELSJ, especialmente los que figuran en el Programa de Estocolmo[9], con el fin de mejorar la seguridad de los ciudadanos; las Agencias y las Fuerzas policiales responsables de la seguridad interior de la UE deben aumentar o mejorar sus capacidades policiales nacionales, para hacer frente a la naturaleza cambiante de las nuevas amenazas. Para ello es necesario identificar claramente las necesidades de seguridad operativas y, en mayor medida, participar en la investigación

7 CONSEJO DE LA UNION EUROPEA. Estrategia de Seguridad Interior de la Unión Europea: “Hacia un modelo europeo de seguridad”. Doc. 7120/10 Bruselas, 25,26 de febrero de 2010. 2010. p.15.

8 CONSEJO DE LA UNION EUROPEA. Conclusiones alcanzadas en la reunión ENLETS celebrada en Oostende, Bélgica, 23-24 Septiembre 2010 Doc. 16250/10 ENFOPOL 329. Bruselas, 15 Noviembre 2010.p.4. La Red ENLETS fue creada en 2008 bajo la Presidencia francesa del Consejo con el fin de recabar los requisitos para el usuario, explorar e incrementar la sensibilización ante las nuevas tecnologías y las prácticas más adecuadas, establecer criterios de referencia y ofrecer asesoramiento, si bien aún no se había producido el cambio de paradigma para el usuario final en el proceso de la innovación tecnológica.

9 CONSEJO DE LA UNION EUROPEA. Programa de Estocolmo. Una Europa abierta y segura que sirva y proteja al ciudadano. Doc. 5731/10 CO EUR-PREP 2 JAI 81 POLGEN 8. Bruselas, 3 de marzo de 2010.

relacionada con la seguridad y ayudar, en calidad de usuario final de la tecnología, al desarrollo de procesos y productos innovadores.

Esta visión forma parte de la estrategia de investigación en el campo de la seguridad que la Comisión Europea (CE) ha ido implementando a lo largo del Séptimo Programa Marco[10] de Investigación y Desarrollo Tecnológico de la UE (VIIPM), durante el período 2007-2013, y cuyo objetivo fundamental fue contribuir a que la UE se convirtiera en el espacio de investigación más importante y competitivo del mundo. El desarrollo e implementación de esta visión, plasmada en la estrategia de la CE en el ámbito de la investigación tecnológica de manera eficaz, requiere la participación de todos los actores relevantes del sector público y privado, tanto a nivel nacional como europeo.

El mercado de la tecnología de seguridad para las Agencias y las Fuerzas policiales responsables de la seguridad interior de la UE es inferior, si lo comparamos con otros ámbitos en el desarrollo de tecnologías (en comparación con otros sectores como defensa, telecomunicaciones o multimedia), y además se ve perjudicado debido a la fragmentación del mismo. En consecuencia, y hasta la fecha, los nuevos desarrollos tecnológicos son a menudo establecidos por los proveedores de soluciones tecnológicas de seguridad, en lugar de que sean los usuarios finales quienes definan dichos desarrollos tecnológicos.

Por lo tanto la participación del usuario final desde el inicio del proceso de la innovación de soluciones tecnológicas de seguridad, además de ofrecer como principal ventaja el contribuir a aumentar mejores niveles de seguridad pública para el beneficio de la ciudadanía de la UE, también ofrece la posibilidad de innovar en la metodología de la adquisición de la nueva tecnología por parte de las administraciones públicas[11]. Sin duda alguna, la incorporación del usuario final al proceso de la investigación y desarrollo de soluciones tecnológicas en el ámbito de la seguridad pública debe ponerse en valor como nuevo principio de la innovación en la seguridad.

1.1. LA SITUACIÓN ECONÓMICA COMO PRINCIPIO DE OPORTUNIDAD

En la actualidad dentro del contexto de escasez de medios que nuestra economía sufre y refleja, la inversión en Investigación, Desarrollo e Innovación (I+D+i) es considerada como uno de los pilares para la recuperación económica de un país. Por ello, desde la óptica institucional, debemos contribuir a tal recuperación, entendiendo que nos encontramos además ante un momento de oportunidad para el cambio y mejora en las dinámicas de la gestión interna.

10 Los Programas Marco son los principales instrumentos de financiación de proyectos de Investigación, Desarrollo Tecnológico y Demostración de la UE. Pertenecen a la DG- ENTERPRISE and INDUSTRY, y tienen como objetivos estratégicos principales: reforzar la base científica y tecnológica de la industria europea y favorecer su competitividad internacional, promoviendo una investigación que respalde las políticas comunitarias.

11 El nuevo procedimiento de Validación Pre Operacional (POV) implementado por la CE en las últimas convocatorias del 7 PM, y consolidado en Horizonte 2020, es un claro ejemplo de esta metodología de implicar al usuario final en todas las fases del proyecto. En este sentido, la Guardia Civil es el primer representante de la Administración Pública a nivel UE en liderar un consorcio en cuanto al desarrollo de un proyecto (CLOSEYE) financiado por este instrumento financiero.

La crisis en la zona euro, así como su versión nacional junto con sus consecuencias, representan un reto para las Agencias y las Fuerzas policiales responsables de la seguridad interior de la UE, y una institución policial como la Guardia Civil no es una excepción. El escenario económico ante el que nos enfrentamos limita de manera clara la inversión pública en nuevos desarrollos tecnológicos en el campo de la seguridad y, por ello, la inversión privada se fundamentaría como el vector sobre el cual poder establecer las bases para la recuperación de la inversión en materia de nuevas tecnologías para la seguridad. Sin duda, una de las consecuencias de la situación económica actual implica la necesidad de adoptar medidas de orden proactivo y tendentes, al menos, al mantenimiento de nuestro nivel de ambición, así como al desarrollo de nuevas capacidades policiales que permitan seguir cumpliendo con la misión encomendada a la Institución en los años venideros.

Sin embargo, no toda la inversión económica para la I+D+i puede ser asumida por parte del sector privado por razones evidentes. También es necesario ampliar el esfuerzo a desarrollar por parte del sector público en lo que podríamos entender como una asociación público-privada en materia de innovación tecnológica[12]. Y precisamente, en ese marco de colaboración, es donde la Guardia Civil viene demostrando desde hace más de una década su capacidad de asumir retos dentro del campo de la innovación para el desarrollo de nuevas soluciones tecnológicas que garanticen las capacidades policiales existentes, así como permitir el desarrollo de otras nuevas[13].

1.2. LA GUARDIA CIVIL COMO ACTOR EN LA I+D+i

De acuerdo con lo anterior, la Guardia Civil se encuentra inmersa en un continuo proceso de modernización como Institución y, tal como se establecía tanto en el anterior planeamiento estratégico de la Guardia Civil (PEGC) como en el actual para el período 2013-2016, se han fijado una serie de objetivos que pretenden continuar con la modernización del sistema de seguridad. Así, y siendo conscientes de la importancia que tiene para España el impulso de su actividad empresarial, la Guardia Civil desde hace años viene participando activamente en calidad de usuario final en determinados proyectos, tanto a nivel nacional como europeo, cuya razón de ser es el impulso de la I+D+i en materia de seguridad pública[14]. La evolución experimentada por la Guardia Civil en el campo de la participación de proyectos I+D+i en el ámbito de la seguridad

12 Estrategia Española de Ciencia y de Tecnología y de Innovación. Aprobada por Acuerdo de Consejo de Ministros de 1 de febrero de 2013. La Estrategia Española de Ciencia y Tecnología y de Innovación es el instrumento marco en el que quedan establecidos los objetivos generales a alcanzar durante el período 2013-2020 ligados al fomento y desarrollo de las actividades de I+D+i en España. Estos objetivos se alinean con los que marca la Unión Europea dentro del nuevo programa marco para la financiación de las actividades de I+D+i «Horizonte 2020» para el período 2014-2020, contribuyendo a incentivar la participación activa de los agentes del Sistema Español de Ciencia, Tecnología e Innovación en el espacio europeo.p.27

13 Ejemplos de dicho esfuerzo tecnológico innovador del Cuerpo de la Guardia Civil han sido los Programas SIVE (Sistema Integrado de Vigilancia Exterior) potenciando nuestras capacidades en vigilancia marítima o el Plan de Sistemas de Información y Comunicación de la Guardia Civil en lo que supuso un serio avance en nuestras capacidades TIC.

14 Concepto institucional de I+D+i: Generación de nuevos conocimientos y desarrollo de nuevas soluciones tecnológicas, las cuáles puedan ser susceptibles de ser introducidas con éxito dentro de la Guardia Civil para la obtención de nuevas capacidades policiales o significativamente mejoradas. Todo ello bajo el principio de la eficiencia de costes.

pública ha propiciado que la Institución haya adquirido una considerable visibilidad y relevancia a nivel nacional e internacional (UE) en este campo, siendo una Institución pública altamente valorada y requerida por parte del mundo de la I+D+i en materia de seguridad. Muestra de todo esto es el hecho de que la estrecha vinculación que existe entre la Guardia Civil y el CDTI[15], ha supuesto el reconocimiento del trabajo y esfuerzo, realizado hasta la fecha, por el Servicio de Innovación Tecnológica y Seguridad de la Información (SiTSI) de la Jefatura de Servicios Técnicos (JST), por su contribución al retorno de fondos para España derivados de la participación de la Guardia Civil[16] en el 7º Programa Marco de Financiación de la I+D de la UE.

Mediante la participación de la Guardia Civil en los distintos programas de financiación de proyectos de la UE en materia de I+D+i (7 Programa Marco[17], Horizonte 2020[18], ISEC/CIPS[19], CIP[20], etc.) se pretenden alcanzar cuatro objetivos concretos. De un lado, fortalecer nuestra responsabilidad social corporativa, por otro el acceso a fuentes de financiación externa a la de los propios Presupuestos Generales de Estado. También apoyar a la industria nacional mediante el desarrollo de soluciones tecnológicas "exportables". Y, en último lugar, lograr la dotación de soluciones y medios de orden tecnológico necesarios para los fines de la Guardia Civil y más adaptados a las necesidades operativas concretas y donde la Institución a través de sus respectivas Jefaturas, Servicios y/o Unidades, haya podido definir y participar activamente en el diseño y características las nuevas tecnologías de seguridad.

En el ámbito más concreto del contexto europeo, debemos tener presente que los cambios normativos introducidos en el Tratado de Lisboa en el ámbito de la seguridad dotan de mayores competencias a la UE en este campo, lo que conllevará un aumento de fondos y un mayor índice de programas de financiación de los ya existentes en este ámbito[21]. Como ejemplo de lo anterior, el pasado 1 de enero de 2014, entró en vigor el

15 Centro para el Desarrollo Tecnológico e Industrial. Entidad Pública Empresarial, dependiente del Ministerio de Economía y Competitividad (MINECO), que promueve **la innovación y el desarrollo tecnológico** de las empresas españolas. **Es la entidad que canaliza** las solicitudes de **financiación y apoyo** a los **proyectos de** I+D+i **de empresas españolas** en los ámbitos estatal e internacional. Así pues el objetivo del CDTI es contribuir a la **mejora del nivel tecnológico** de las empresas españolas.

16 A modo de ejemplo de la participación institucional en el 7 PM, en las tres últimas llamadas del programa (4ª, 5ª y 6ª) se han llevado a cabo un total de 64 propuestas de proyectos a financiar, acudiendo a cada una de ellas de forma integrada en un consorcio de socios potenciales (Industria, PYMEs, Universidades, Centros de Investigación, otros actores de la seguridad interior de la UE, Organismos Privados y Públicos, etc.)

17 Debemos tener presente que, para el período 2007-2013, se asignó un presupuesto de 1.400 millones de euros al capítulo sobre seguridad del Séptimo Programa Marco. http://cordis.europa.eu/fp7/home_es.html.

18 Actual Programa Marco de Investigación e Innovación para el período 2014/2020 de la DG-ENTERPRISE & INDUSTRY.

19 Se trata de los dos instrumentos anteriores del Programa Marco “Seguridad y defensa de las libertades”, que abarcaba la ejecución de los programas “Prevención y lucha contra la delincuencia” (ISEC) y “Prevención, preparación y gestión de las consecuencias del terrorismo y otros riesgos en materia de seguridad” (CIPS), todo ello dentro del ámbito de la DG-HOME. A partir del 1 de enero de 2014 han sido sustituidos por el Fondo de Seguridad Interior-Policía (Cooperación Policial y Gestión de Crisis).

20 Programa CIP: http://ec.europa.eu/cip/index_es.htm

21 Artículo 185 del Tratado de Lisboa (antiguo artículo 169 del Tratado de la UE) referente a la participación de la CE en programas conjuntos de Investigación y Desarrollo tecnológico. La iniciativa de la CE conocida como EUROSTARS, de ayuda a las PYMES intensivas en I+D, a desarrollar

nuevo programa de financiación para proyectos I+D+i de la UE, Programa Marco de Investigación e Innovación "Horizonte 2020" (2014/2020)[22], que servirá como elemento aglutinador de anteriores programas europeos de innovación e investigación (CIP, EIT, VII Programa Marco, etc.) y donde la potenciación de la innovación tecnológica supone uno de sus pilares fundamentales.

Siguiendo con la perspectiva internacional y valorando el impacto de la participación de la Guardia Civil en programas de financiación en el ámbito de la I+D+i, debemos tener presente lo recogido en el RD 998/2012, de 28 de junio, por el que se crea el Alto Comisionado del Gobierno para la Marca España y se modifica el RD 1412/2000, de 21 de julio, de creación del Consejo de Política Exterior, donde se pretende mejorar la imagen exterior de España visibilizada bajo la denominación "Marca España", que toma como modelo las iniciativas adoptadas por otros estados en ejecución del concepto marca-país. De ello se deduce la necesidad de promover la actuación coordinada de cuantas instituciones y entidades resultan comprometidas con iniciativas que coadyuven a la mejora de los resultados y al logro de contribuciones medibles para los intereses de España en los ámbitos económico, cultural, social, científico y tecnológico. En esta línea argumental, y ciñéndonos al ámbito tecnológico, la Guardia Civil entiende que, mediante su grado de compromiso y participación activa en dichos programas de financiación, se colabora desde nuestra Institución a mejorar la imagen exterior de España visibilizada bajo la denominación Marca España.

1.3. LA GUARDIA CIVIL COMO USUARIO FINAL DE LA TECNOLOGÍA

Desde mediados de la década pasada, la Guardia Civil viene participando de distinta manera e implicación en proyectos de innovación tecnológica dentro del marco nacional e internacional. Los proyectos relacionados con la I+D+i, en los que la Guardia Civil participa, están orientados a proporcionar soluciones civiles que supongan un beneficio para la seguridad de nuestro país y, por ende, para la seguridad interior de la Unión Europea (UE).

Es de todos conocida la visión actual, tras un proceso de evolución que obedece a los principios de racionalidad y eficiencia que se tiene, tanto a nivel nacional como de la UE[23], acerca de la trascendencia que representa para la industria actual del sector I+D+i el hecho de que la aceptación de las soluciones tecnológicas y productos pasa por la implicación del usuario final en dichos desarrollos industriales, de manera que, desde el diseño inicial hasta su implementación en el mercado, la participación del usuario final de la tecnología se haya puesto de manifiesto. Si bien es cierto que la industria dedicada a la I+D+i tiene como primordial objetivo acceder

proyectos trasnacionales orientados al mercado. Esta iniciativa nace por codecisión del Parlamento y del Consejo Europeo.

22 Los programas de trabajo serán adoptados por la Comisión, asistida por un Comité del programa. En concreto la Guardia Civil formaba parte del Comité del Programa de Seguridad del Séptimo Programa Marco (7PM), actual H2020, en calidad de experto de la delegación española desde el año 2011, de modo que la Institución participa, en gran medida, en el nivel político-estratégico de la decisión sobre la innovación tecnológica en materia de seguridad de la UE.

23 Comunicación de la COMISIÓN EUROPEA. "Política industrial en materia de seguridad - Plan de acción para una industria de la seguridad innovadora y competitiva" Doc. 13050/12. Bruselas, 26 de julio de 2012.

al mercado nacional e internacional, en el caso concreto de la industria de seguridad dicha tecnología debe tener un final público, esto es, la obligación de resultar un beneficio que conlleve una mejora de la seguridad pública. En otras palabras, la industria de la seguridad tiene como finalidad proporcionar y mejorar el marco de la seguridad de los ciudadanos y, con ello, acceder al mercado de una manera eficaz y contrastada. En el campo de la tecnología también resulta una necesidad el hecho de que el sector público y privado trabaje juntos. Basándose en los resultados de programas de investigación y desarrollo realizados en el Programa Común de Investigación y Desarrollo, la UE debería desarrollar normas y plataformas tecnológicas adaptadas a sus necesidades de seguridad[24].

Es necesario especificar que el usuario final (Agencias y Cuerpos responsables de la Seguridad Interior de la UE) de las soluciones y productos tecnológicos del ámbito de la seguridad no es un actor interesado en la investigación y desarrollo al mismo nivel que la industria. Sin embargo, es consciente de su necesaria implicación en los proyectos tecnológicos, los cuales podrán materializarse en herramientas e instrumentos que colaborarán en ofrecer una mejor calidad en el servicio a la ciudadanía. Por consiguiente, el usuario final pretende alcanzar sus necesidades propias al participar con la industria en la investigación y desarrollo tecnológico y donde su “saber hacer” supone una garantía para el conjunto del proyecto. Esta participación Institucional de la Guardia Civil en el proceso del desarrollo tecnológico en el ámbito de la seguridad tiene por objeto los siguientes propósitos:

- Mantener una actitud proactiva en la búsqueda de programas y soluciones tecnológicas eficientes, que permitan consolidar los objetivos planteados en el Plan Estratégico de la Guardia Civil (2009-2012) en materia de modernización de la seguridad, ayudar a alcanzar los nuevos objetivos en el ámbito de I+D+i en el Plan Estratégico 2013-2016 y, con ello, garantizar la misión principal de la Guardia Civil.
- Apoyar al sector industrial que investiga en materia de seguridad para que, contando con un Cuerpo policial prestigioso y de referencia como la Guardia Civil, puedan acceder a las ayudas financieras europeas mencionadas.
- Acceder a los productos y soluciones tecnológicas de seguridad que puedan ser posteriormente aplicables con éxito en la labor de seguridad pública que presta la Guardia Civil u otros cuerpos de seguridad europeos.
- Participar de manera activa en proyectos tecnológicos a modo de inversión eficiente, al considerar la obtención indirecta y de retorno de fondos e instrumentos de financiación para la Guardia Civil.

1.4. LA HERRAMIENTA PARA LA GESTIÓN DE LA INNOVACIÓN TECNOLÓGICA EN LA GUARDIA CIVIL

Por todo lo anteriormente dicho, la Institución se encuentra inmersa de manera activa en la preparación, negociación y ejecución de numerosos proyectos de

24 CONSEJO DE LA UNION EUROPEA. Conclusiones Consejo de política de investigación e industrial relacionada con la seguridad. Doc. 8985/13 COSI 43 ENFOPOL 124. Bruselas, 15 abril 2013.p.3

innovación tecnológica dentro del escenario de la seguridad pública, en aras de lograr los programas de retorno citados, tanto en lo financiero como en lo material. En este contexto, se hace necesaria la estructuración de dicha participación institucional mediante un elemento que actúe como catalizador de cuantas acciones e iniciativas se lleven a cabo de manera sobrevenida en el ámbito de la I+D+i dentro de la Guardia Civil.

Como consecuencia de todo ello, surge la necesidad de crear una Oficina de Gestión de Proyectos en la Institución que gestione, controle, priorice y coordine la implementación de los proyectos I+D+i en el seno de la Guardia Civil.

2. PANORAMA DE LA I+D+i EN LA GUARDIA CIVIL

2.1. ANTECEDENTES

Desde mediados de la década pasada la Guardia Civil viene participando de distinta manera e implicación en proyectos de Investigación, Desarrollo e Innovación, dentro del marco nacional e internacional. Los proyectos relacionados con la I+D+i en los que la Guardia Civil contribuye están orientados a proporcionar soluciones civiles que supongan un beneficio para la seguridad interior, tanto de nuestro país como de la UE. A tenor del marco normativo interno de la Guardia Civil[25], la labor de coordinación y supervisión citada viene siendo desarrollada desde el SiTSI en su ámbito específico (Área de Innovación de Proyectos I+D+i).

2.2. MOMENTO ACTUAL

La actuación de la JST, a través del SiTSI, podría verse enmarcada dentro del cuarto objetivo nacional de la Estrategia Española de Ciencia y Tecnología de Innovación[26] elaborada por el Ministerio de Economía y Competitividad (MINECO), en cuanto al apoyo a la I+D+i orientada a los retos de la sociedad, concretamente en el apartado octavo de Seguridad, Protección y Defensa, mediante el fomento

25 BOE número 66 del 18 de marzo de 2013, se publica la Orden PRE/422/2013 de 15 de marzo por la que se desarrolla la estructura orgánica de los Servicios Centrales de la Dirección General de la Guardia Civil, creándose el Servicio de Innovación Tecnológica y Seguridad de la Información (SiTSI). El SiTSI, bajo la dependencia orgánica de la Jefatura de Servicios Técnicos (JST), es el órgano especializado de la Dirección General en materia de seguridad de los Sistemas de Información y Comunicaciones de la Guardia Civil, así como del estudio y análisis de las nuevas tecnologías susceptibles de ser utilizadas por el Cuerpo de la Guardia Civil, manteniendo un banco de datos sobre las características y valoración económica, técnica y operativa de las mismas y de sus aplicaciones y desarrollos.

26 Tanto la Estrategia Española de Ciencia y Tecnología y de Innovación (2013-2020) como el Plan Estatal de Investigación Científica y Técnica y de Innovación (2013-2016) son los pilares sobre los que se asienta el diseño de la política del Gobierno en I+D+i para los próximos años. Tienen como objetivo el reconocimiento y promoción del talento y su empleabilidad, el impulso del liderazgo empresarial en I+D+i, el fomento de la investigación científica y técnica de excelencia y el desarrollo de actividades orientadas a resolver los retos globales de la sociedad.

del desarrollo de tecnologías e innovaciones que hagan florecer una industria de seguridad y defensa competitiva a nivel internacional[27].

Al mismo tiempo que se cumple con lo establecido en la Estrategia del MINECO, la actuación de la Jefatura se encuentra alineada con el planeamiento estratégico de la Guardia Civil para el período 2013-2016, donde se han fijado una serie de objetivos que pretenden la modernización del sistema de seguridad.

Debemos entender la gestión de proyectos I+D+i como una sucesión cronológica de hitos administrativos y operativos donde, en un mismo horizonte temporal, se llevan a cabo una enorme diversidad de actividades y confluencia de actores que intervienen en las distintas fases de un proyecto hasta su finalización. Todo ello sin perjuicio de que, por parte de la JST, se genere la necesidad de ejercer la coordinación y supervisión de todos y cada uno de los proyectos iniciados, a fin de disponer de una visión estratégica que permita generar en cualquier momento el mapa estratégico de la participación de la Guardia Civil en proyectos I+D+i.

2.3. VISIÓN DE FUTURO

A tal fin la JST, a través del Servicio de Innovación Tecnológica y Seguridad de la Información (SiTSI), tiene previsto acometer una serie de actividades para el citado período tendentes a la consecución de dichos objetivos. Entre otros destaca el fomento de la participación institucional en Proyectos I+D+i, tanto a nivel nacional como de la UE. Todo ello con vistas al horizonte institucional de servir de apoyo en alcanzar la misión principal de la Guardia Civil[28], siendo ésta el contribuir a garantizar la seguridad pública y asistir a los ciudadanos de forma excelente y cercana.

Los objetivos generales de la Oficina de Gestión de Proyectos I+D+i son:

- Incrementar la participación de la Guardia Civil en los programas de financiación de proyectos I+D+i.
- Aumentar el liderazgo de la Guardia Civil en las propuestas de participación en proyectos I+D+i.
- Mejorar la tasa de aprobación de proyectos en los que participen las distintas Jefaturas /Servicios y/ o Unidades de la Guardia Civil.
- Contribuir a que la Institución, en calidad de usuario final de soluciones tecnológicas, desempeñe un papel estratégico en el proceso de la definición de necesidades, que permita un adecuado asesoramiento en el campo de las nuevas tecnologías para la seguridad a nivel nacional y de la UE.

Las razones principales que en la actualidad inducen a la creación de la Oficina de Gestión de Proyectos I+D+i son:

27 Estrategia Española de Ciencia y de Tecnología y de Innovación. Aprobada por Acuerdo de Consejo de Ministros de 1 de febrero de 2013 p.32

28 Artículo 104 de la Constitución Española.

- Lograr la anticipación adecuada por parte de la Guardia Civil ante la tendencia presente en el ámbito de la I+D+i a incrementar los programas de financiación de proyectos de este ámbito, tanto a nivel nacional como en la UE.
- Canalizar y favorecer la gestión de la I+D+i en la Guardia Civil ante los retos futuros.
- Necesidad de consolidar la función del SiTSI como interlocutor único a nivel Institucional idóneo, tanto a nivel nacional como en la UE en el ámbito I+D+i.
- Coordinación centralizada del número elevado de proyectos I+D+i en los que participa la Guardia Civil hasta el momento, así como ante las previsiones futuras. Todo ello motivado y coincidiendo con el inicio temporal de la dispersión organizativa en la ejecución de proyectos I+D+i, así como la confluencia temporal de diversidad de proyectos con diferentes plazos temporales de preparación, negociación, ejecución y cierre.
- Ganar visibilidad dentro del escenario de la I+D+i en el panorama nacional y europeo, tanto de las necesidades por parte de la Guardia Civil, como de las ofertas por parte del sector privado que aporten soluciones ante dichas necesidades.
- Homogeneización institucional de la metodología a aplicar en la gestión de proyectos I+D+i.
- Garantizar la continuidad en la prestación de un servicio de calidad por parte del SiTSI, a través del Área de Innovación de Proyectos I+D+i.

En conclusión, y debido al actual grado de participación de las distintas Jefaturas/ Servicios y/ o Unidades de la Guardia Civil en proyectos I+D+i[29], así como ante el futuro y previsible aumento de dicha participación en nuevos proyectos, se hace necesaria la creación de una Oficina para la gestión de proyectos de innovación que informe y conozca el estado puntual de cada uno de los proyectos en los que se ve implicada la Institución.

3. LA OFICINA DE PROYECTOS I+D+i EN LA GUARDIA CIVIL (OPi)

Desde el punto de vista institucional, los sucesivos Planes Estratégicos de la Guardia Civil han establecido idénticos objetivos a alcanzar en el ámbito de la modernización del sistema de seguridad, si bien en el PEGC 2013-2016 se introduce un nuevo objetivo referido a la participación institucional en proyectos I+D+i. Es por ello que la Jefatura de Servicios Técnicos (JST) de la Guardia Civil ha tomado la decisión de crear una herramienta estratégica para dar seguimiento este nuevo objetivo, considerando para ello la creación de la Oficina de Gestión de Proyectos I+D+i de la Guardia Civil.

La JST, viendo la necesidad de continuar con el impulso transformador y modernizador que establecen los sucesivos PEGC's, y sin dejar de tener presente la actual situación económica y financiera por la que atraviesa España, requiere de la creación de una estructura formal que permita la adaptación de manera eficaz al cambio experimentado

29 Hasta la fecha, y desde el año 2008, la Guardia Civil está participando de forma activa en un total de 12 proyectos del 7 PM y H2020.

en el escenario de dotación presupuestaria actual y venideros. Para ello, la creación de la Oficina de Proyectos de Innovación (en adelante OPi), incardinada en la actual arquitectura organizativa de la JST, permitiría disponer de una herramienta de gestión que actuaría bajo los principios de la eficiencia y la coordinación. Dotando al conjunto de la Institución de un mecanismo coherente que permitiera obtener una visión estratégica, a la vez que detallada, del nivel de ambición e implicación por parte de la Guardia Civil en proyectos nacionales y europeos en I+D+i.

La creación de la OPi tiene dos objetivos claves para la organización. Primero, a nivel de gestión administrativa, tratar de lograr la mejor coordinación de los proyectos en los que participa la Guardia Civil, estableciendo un interlocutor único en relación a los mismos. Segundo, desde la perspectiva estratégica, situar la I+D+i dentro la estrategia global de la Institución, anticipando los cambios que se avecinan desde la UE y otorgando con ello mayor visibilidad a la labor que el Cuerpo realiza en I+D+i.

3.1. DEFINICION Y MISIONES

La OPi debe pretender ser una oficina que mantenga estándares de procesos, básicamente relacionados con la gestión de proyectos de I+D+i, dentro de la Guardia Civil.

Como es sabido, la misión principal del SiTSI, a través de su Área de Proyectos de Innovación I+D+i, es **liderar el desarrollo tecnológico de la Guardia Civil, potenciando, fomentando y coordinando las diferentes acciones en el ámbito tecnológico (interior y exterior del Cuerpo), la investigación, el desarrollo y la innovación**; y entre sus funciones principales estarían la coordinación y supervisión de la elaboración de propuestas, negociación y ejecución de todos los proyectos de Investigación, Desarrollo e Innovación, derivados de los distintos programas de financiación, nacionales e internacionales, principalmente de la UE. Del mismo modo, es el Servicio encargado de proponer a la JST el impulso sobre el uso de nuevas tecnologías mediante la información, selección y asesoramiento de las que pueden ser de utilidad en la Guardia Civil. Entre sus cometidos está el de participar en la planificación, diseño y evaluación de aquellos proyectos que incorporen nuevas tecnologías en la Guardia Civil y que, en definitiva, forman la gestión estratégica de la innovación tecnológica en la Institución.

La creación de la OPi en el seno del SiTSI tiene como principal objetivo el análisis de la viabilidad de la participación institucional en proyectos I+D+i[30], así como el seguimiento de los proyectos I+D+i de las TIC aplicables en la Guardia Civil, que permitirá a la JST, junto con el asesoramiento e informe preceptivo en materia de seguridad por parte de la OSIC[31], obtener una visión estratégica de los proyectos de nuevas tecnologías en los que la Guardia Civil pueda estar implicada en los diversos grados de participación.

Asimismo, la OPi permitirá una adecuada gestión integral de los proyectos I+D+i en la Guardia Civil, de modo que garantice el seguimiento de los mismos bajo los principios de centralización y coordinación.

30 Para ello, dicho estudio de viabilidad se haría de forma coordinada con el Secretaría Técnica de la SUBAPO.

31 Oficina de Seguridad de la Información Corporativa.

Los objetivos globales perseguidos con la Oficina en lo referente a la gestión de proyectos I+D+i son los siguientes:

- Mantener una actitud proactiva en la búsqueda de programas y soluciones tecnológicas eficientes que permitan consolidar los objetivos planteados en el Plan Estratégico de la Guardia Civil (2009-2012) en materia de modernización de la seguridad. Con ello permitirá ayudar a alcanzar los nuevos objetivos en el ámbito de I+D+i en el Plan Estratégico 2013-2016 y, con ello, garantizar la misión principal de la Guardia Civil.
- Acceder a los productos y soluciones tecnológicas de seguridad que puedan ser posteriormente aplicables con éxito en la labor de seguridad pública que presta la Guardia Civil.
- Participar de manera activa en proyectos tecnológicos a modo de inversión eficiente, al considerar la obtención indirecta y de retorno de fondos e instrumentos de financiación para la Guardia Civil, de modo que se obtenga cierto grado de oxígeno financiero específico para la innovación tecnológica en la Institución.
- Servir de apoyo al sector industrial nacional[32] que investiga en materia de seguridad para que, contando con la experiencia y saber hacer (know-how) de la Guardia Civil como usuario final, colabore en el logro de acceder a las diferentes ayudas financieras provenientes de programas de financiación para proyectos I+D+i.
- Proporcionar apoyo a las Unidades que hayan creado o no estructuras de gestión de proyectos y que quieran participar en propuestas de I+D+i o terminen formando parte de los consorcios ganadores del proyecto, para servir como punto de contacto entre ellas y el resto de socios, apoyándoles en cuestiones administrativas, legales y financieras.
- Incrementar la participación de las Unidades que ya participan en proyectos de I+D+i y potenciar la participación de las Unidades que aún no lo hacen.

La OPi permitirá a la JST disponer de un mecanismo idóneo que facilite la gestión y el control de los proyectos I+D+i, dentro del ámbito de su competencia. Consecuentemente, ayudará a disponer de una herramienta que sirva para el asesoramiento estratégico en caso de ser requerido por parte del Subdirector General de Apoyo de la Dirección General de la Guardia Civil u otras instancias de la Institución.

La OPi estará en consonancia al tipo de tareas a realizar, así como en las funciones de coordinación transversal que llevará en el seno de la Guardia Civil (DAO, MOPS, SUBAPO, SUBPER y Gabinete Técnico), para la necesaria agilidad requerida en la

32 En este sentido, la ESN 2013 estaría en su apartado de riesgos y amenazas; se definen 12 ámbitos prioritarios de actuación, delimitando para cada uno el objetivo principal y varias líneas de acción estratégicas. En el primer objetivo, de la Defensa Nacional, se hace mención expresa al ámbito propio de la misma, si bien podemos entenderlo de plena aplicación al ámbito de la Seguridad Nacional, en la línea de acción estratégica a seguir en cuanto al fortalecimiento del tejido industrial español de Defensa/Seguridad, mediante las acciones de fomento, proyección y colaboración con las capacidades nacionales que se estimen necesarias. Se potenciarán los vínculos entre los actores que conforman la arquitectura óptima en esta materia (Industria, Universidad y Defensa/Seguridad). p.40

coordinación y gestión de proyectos. Consecuentemente a la creación de una estructura de coordinación central en el SiTSI de la JST como sería la OPi, ésta iría secundada de la creación o diseño ad hoc de Oficinas Técnicas de Proyectos periféricas (en adelante OTP's) para la gestión y ejecución técnica de los mismos por parte de las Unidades, Servicios y/o Jefaturas directamente involucrados en el proyecto.

En cuanto a las funciones de coordinación transversal citadas, la OPi auxiliará a las OTP's en la planificación y gestión de los proyectos específicos. En este sentido diferenciaremos el modo de colaboración prestado por la OPi en función del grado de participación/implicación de la Unidad, Servicio y/o Jefatura en el proyecto (coordinador, socio de pleno derecho, observador, etc.). De forma que la OPi organizará y canalizará los procedimientos y esfuerzos, tanto de la propia OPi como de las OTP's, en aras a una adecuada gestión de los proyectos en los que se implique la Guardia Civil.

En este sentido debemos tener presente el grado de control e implicación sobre los proyectos ejercido por parte de la Opi, que irá en función del grado de avance en las fases de la "vida útil" de un proyecto. A medida que un proyecto vaya adquiriendo forma a través de las fases de preparación de propuestas, fase de negociación, fase de ejecución y fase de cierre, mayor irá siendo la presencia e implicación de las OTP's en dicho proyecto. Con ello se pretende alcanzar un balance idóneo entre las funciones de la OPi y las desarrolladas por parte de las distintas OTP's., donde el liderazgo integral (fase de propuesta, fase de negociación, fase de ejecución y fase de cierre) corresponderá a la OPi, mientras que el liderazgo del proyecto será asumido en la fase de ejecución por parte de las OTP's, debido a su carácter eminentemente técnico/ operativo.

En conclusión, la OPi ejercerá a modo de elemento de coordinación transversal de gestión con respecto a las OTP's existentes y creadas al efecto para la ejecución de cada proyecto.

En definitiva, la OPi deberá ser una herramienta que permita:

- Disponer de una visión global y estratégica compartida, integrada y unificada del conjunto de proyectos I+D+i.
- Ayudar a valorar los costes/beneficios de los proyectos y el uso de nuevas soluciones tecnológicas para la Guardia Civil.
- Potenciar el uso de una metodología, procedimientos y herramientas comunes de seguimiento de los proyectos, velando por el cumplimiento de hitos administrativos de los mismos.
- Apoyar y fomentar las labores de coordinación, comunicación y concienciación de la RED FUNCIONAL VERDE[33] de innovación tecnológica de la Guardia Civil en la gestión de proyectos y el mundo de la I+D+i.

33 Grupo funcional creado en el seno de la Guardia Civil con la finalidad de servir de foro de comunicación interno en el ámbito de las nuevas tecnologías aplicables en la Institución a través de la participación activa de las distintas Jefaturas/Servicios y/o Unidades que forman el colectivo de usuarios finales de las tecnologías de la seguridad.

3.2. PROYECTOS ACTUALES

En la actualidad, la OPi se encuentra gestionando los siguientes proyectos del FP7, así como preparando otros nuevos del H2020.

PROYECTO	PROGRAMA	Fecha Inicio	Objeto del proyecto	Servicio GC lider del proyecto
CLOSEYE	FP7	01/04/2013	Validación Pre-Operacional de nuevas herramientas y soluciones de vigilancia de fronteras	JEFATURA FISCAL Y FRONTERAS
PERSEUS	FP7	01/01/2011	Protección de las fronteras y los mares europeos mediante el uso inteligente de la vigilancia	JEFATURA FISCAL Y FRONTERAS
MISAFE	FP7	01/06/2013	Desarrollo y validación de análisis forense de suelo (genética forense medioambiental)	SERVICIO DE CRIMINALISTICA
MEPROCS	FP7	01/02/2012	Desarrollo de nuevos métodos y protocolos forenses para la identificación mediante técnicas de superposición	SERVICIO DE CRIMINALISTICA
AEROCEPTOR	FP7	01/01/2013	Desarrollo de un UAV para interceptar barcos y coches	JEFATURA FISCAL Y FRONTERAS
NEREIDS	FP7	01/06/2011	Uso de las tecnologías basadas en satélites donde las señales recogidas puedan ser integradas y tratadas en las plataformas actuales	SERVICIO DE TELECOMUNICACIONES
HOMER	FP7	01/11/2013	Proyecto para caracterizar explosivos y mezclas disponibles públicamente	ESTADO MAYOR
SAGRES	FP7	01/01/2013	Validación de los servicios propuestos en el documento CONOPS (Concepto fo Operations) para su implementación en EUROSUR	SERVICIO DE TELECOMUNICACIONES
EU-CISE	FP7	01/06/2014	Banco de Pruebas Europeo para compartir información en el ámbito marítimo	JEFATURA FISCAL Y FRONTERAS
EWISA	FP7	01/01/2015	Tecnología de Mejora de Vigilancia Terrestre	JEFATURA FISCAL Y FRONTERAS
EPOOLICE	FP7	01/01/2013	desarrollos para alerta temprana mediante la detección de indicios de crimen organizado	CENTRO DE ANALISIS Y PROSPECTIVA
CAPER	FP7	01/07/2011	Implantar plataforma de colaboración común y de intercambio de información para la detección y prevención de la delincuencia organizada que utiliza	SERVICIO DE INFORMACIÓN

- CLOSEYE (Collaborative Evaluation of Border Surveillance technologies in maritime environment by pre-operational validation of innovative solutions) – La Guardia Civil participa como Coordinadora del Proyecto.

  Se trata del primer proyecto europeo de innovación conducido y liderado por Guardia Civil, cuyo objetivo es mejorar las comunicaciones tácticas, así como incorporar a los sistemas de vigilancia marítima nuevas herramientas como aviones no tripulados, satélites o aerostatos, entre otros dispositivos, para la mejora de la seguridad fronteriza marítima.

  Algunos de los miembros del Consorcio son ISDEFE y el European Union Satellite Centre.

- PERSEUS (Protection of European seas and borders through the intelligent use of surveillance): tiene como objetivo la protección de los mares europeos y sus fronteras mediante el uso inteligente de la tecnología, integrando los sistemas

nacionales y europeos existentes y su actualización y mejora con innovaciones tecnológicas.

Algunos de los miembros del Consorcio son Indra Systems, ISDEFE (Ingeniería de Sistemas para la Defensa de España) y EADS (actualmente Airbus).

- MISAFE (The Development and Validation of Microbial Soil Community Analyses for Forensic Purposes): tiene como objetivo la investigación del suelo para la extracción de datos relevantes relacionados con la comisión de actos criminales, así como la operacionalización y armonización de métodos y protocolos de análisis.

  Algunos de los miembros del Consorcio son Libragen (Francia) y CLC BIO A/S (Dinamarca).

- MEPROCS (New methodologies and protocols of forensic identification by craniofacial superimposition): el objetivo de este proyecto es proponer un marco común en la Unión Europea que permita la aplicación, de forma extensiva, de la superposición craneofacial en la resolución de casos de identificación forense que abarquen desde los desastres naturales hasta el terrorismo.

  Algunos de los miembros del Consorcio son la Fundación para el Progreso del Soft Computing y la Universidad de Granada.

- AEROCEPTOR (Unmanned Aerial Vehicle based innovative means for land and sea non-cooperative vehicules stop): tiene como objetivo el control y la detección de vehículos marítimos y terrestres mediante el uso de la tecnología UAV.

  Algunos de los miembros del Consorcio son el INTA (Instituto Nacional de Técnica Aeroespacial), ISDEFE y GMV.

- NEREIDS (New Service Capabilities for Integrated and Advanced Maritime Surveillance): tiene como objetivo mejorar la fiabilidad en la detección de pequeñas embarcaciones, así como el cálculo de su posición y rumbo en tiempo casi real para mejorar el proceso de toma de decisiones.

  Algunos de los miembros del Consorcio son GMV Aerospace and Defence y la Universidad Politécnica de Cataluña.

- HOMER (Home made explosives (HMEs) and recipes characterization): su objetivo es implementar un estudio para mitigar la amenaza de los HMEs de origen terrorista, poniéndolo a disposición de las Fuerzas y Cuerpos de Seguridad para mejorar la seguridad de los ciudadanos europeos.

  Algunos de los miembros del Consorcio son el Centre For Research And Technology Hellas (Grecia) y The Queen's University Of Belfast.

- SAGRES (Services Activations for Growing Eurosur´s Success): tiene como objetivo poner a prueba y validar el flujo de trabajo y la tecnología para el seguimiento de los buques más grandes procedentes de puertos de un tercer país. También vigila las costas de los países que han sido identificados como puntos de partida para la inmigración irregular y la delincuencia transfronteriza.

  Algunos de los miembros del Consorcio son GMV y el European Union Satellite Centre.

- EU-CISE (European Test-bed for the Maritime Common Information Sharing Environment in the 2020 perspective): tiene como objetivo integrar los sistemas de vigilancia marítima para generar un intercambio de información que permita conocer la situación de las actividades llevadas a cabo en el ámbito marítimo.

  Algunos de los miembros del Consorcio son el National Center For Scientific Research "Demokritos" (Grecia), La University Of Cyprus (Chipre) y el Ministerio de Defensa.

- EWISA (Early Warning for Increased Situational Awareness): su objetivo es promover la cooperación entre las autoridades públicas y los usuarios finales, desarrollando nuevas soluciones que mejoren la calidad y la eficiencia de los servicios públicos encargados de la seguridad a través de la obtención de información mediante la videovigilancia e implementando la actual estrategia de Frontex contenida en Eurosur.

  Algunos de los miembros del Consorcio son la Policía de Fronteras de Rumanía y el Ministerio del Interior de Finlandia.

- EPOOLICE (Early Pursuit against Organized crime using environmental scanning, the Law and IntelligenCE systems): tiene como objetivo el preanálisis de un entorno que permita avanzar hacia un sistema de alerta temprana (avisos sobre cambios en patrones, tendencias, etc.) mediante un sistema de indicadores, con crawling de información, y análisis de cambios.

  Algunos de los miembros del Consorcio son Thales, ISDEFE y el Instituto Fraunhofer.

- CAPER (Collaborative Information, Acquisition, Processing, Exploitation and Reporting for the prevention of organized crime): tiene como objetivo la creación de una plataforma común para la prevención de la delincuencia organizada, a través del intercambio y análisis de fuentes de información entre agencias de seguridad.

  Algunos de los miembros del Consorcio son la Asociación Centro de Tecnologías de Interacción Visual y Comunicaciones-Vicomtech Y la S21SEC Information Security Labs S.L.

3.3. BENEFICIOS INSTITUCIONALES

Como ya se ha expuesto, la creación de una OPi supondrá un importante elemento potenciador y fortalecedor en cuanto a la gestión de la I+D+i dentro del Cuerpo.

Con ello, los principales beneficios esperados de la implantación de una OPi son:

- Disponer de una visión global, compartida, integrada y unificada del conjunto de proyectos en los que participa la Guardia Civil, que favorezca su análisis y una adecuada toma de decisiones en base a ella.

- Favorecer la correcta gestión de los proyectos I+D+i en cada una de las fases de los mismos (preparación, negociación, ejecución y cierre).

- Disponer de una herramienta enfocada a la gestión integral y unificada de los proyectos I+D+i en la Guardia Civil, donde la coordinación centralizada de las

fases de propuestas, negociación y cierre de proyecto desde la OPi coexistirá con una ejecución descentralizada desde las OTP's existentes en las Jefaturas/ Servicios/Unidades participantes.

- Materializar la labor actual de un equipo estructurado con experiencia, capaz de seguir y controlar las circunstancias particulares e inherentes a la gestión de los proyectos I+D+i.
- Disponer de un punto de comunicación definido que facilite el flujo de información entre los diferentes Servicios y Unidades implicadas en proyectos, asegurando el control y el orden en todo el proceso de gestión de los proyectos.
- Disponer de una unidad organizativa correctamente gestionada que garantice el seguimiento de los proyectos I+D+i dentro de la Guardia Civil, permitiendo una visualización de la participación institucional en programas de innovación tecnológica a nivel estratégico y operativo.
- Posibilidad de incrementar la eficacia institucional ante las distintas iniciativas a nivel nacional y UE, gracias a la completa visibilidad y conocimiento que de éstas alcanzarán los componentes de la OPi junto con los componentes de las OTP's.
- La creación de la OPi supondrá un ejercicio de anticipación por parte de la Guardia Civil ante los cambios que se avecinan desde la UE y, por lo tanto, la acertada gestión de proyectos en I+D+i deberá ser tenida en cuenta como un aspecto estratégico.

Como colofón a este punto, y a modo de dimensionar el posicionamiento de la Guardia Civil en la UE, la prolija participación en Grupos de Trabajo y foros nacionales y de la UE (desde el Comité de Expertos de Seguridad en el 7PM hasta el actual Comité de Expertos para el H2020), dedicados tanto al diseño de la política nacional y de la UE en el ámbito de la I+D+i como al estudio e investigación de soluciones tecnológicas en materia de seguridad[34], conlleva el disponer de una visión adecuada y lo más aproximada posible acerca de la I+D+i europea en su aspecto global, si bien centrado en el ámbito de seguridad.

4. CONCLUSIONES

La creación de una Oficina de Gestión de Proyectos I+D+i (OPi) debe ser entendida como el paso que ha sido necesario dar en el corto plazo, por parte de la Guardia Civil, para la gestión eficaz de los proyectos I+D+i en el seno de la Institución. La Oficina se presenta como el elemento fundamental en la actividad proactiva que debe asumir la

34 En la actualidad, la Guardia Civil dispone de presencia efectiva al más alto nivel estratégico en el ámbito de las políticas de innovación a nivel nacional y de la UE, a través de un representante de la Jefatura de Servicios Técnicos como experto nacional en el Comité del Programa, también se trabajó en colaboración con el Subgrupo nacional de expertos Horizonte 2020 para asistir, en el ámbito de seguridad, a los Consejeros permanentes de ciencia e innovación de la REPER de España ante la UE (Bruselas) en sus trabajos preparatorios, dentro del Grupo de Investigación que posteriormente asiste a su vez a los COREPER I, de cara a las reuniones del Consejo de Competitividad. Si bien, el hito más relevante sería el hecho que la Guardia Civil mantiene su participación en el Security Advisory Board for H2020.

Guardia Civil para la actual y futura gestión de proyectos I+D+i. A su vez organizará y canalizará los procedimientos y esfuerzos, tanto de la propia OPi como de las OTP's, en aras a una adecuada gestión de los proyectos en los que se implique la Guardia Civil.

La actual estrategia y visión de la Comisión Europea, así como del Consejo de la UE, con respecto a la necesidad de incorporar, desde el inicio del proceso de desarrollo de soluciones tecnológicas de seguridad, la presencia del usuario final de dicha futura tecnología supone un nuevo paradigma para el ámbito de la industria y pequeñas y medianas empresas de seguridad nacional y de la UE. Por ello la Guardia Civil, como una de las autoridades responsables de la seguridad interior de la UE, representa un actor de interés para dicho sector industrial, puesto que la ventana de oportunidad que se plantea desde el nivel político-estratégico de la decisión comunitaria sobre la necesaria participación del usuario final en la política de investigación e industrial relacionada con la seguridad, ubica a la Institución en el centro de gravedad nacional del proceso, no sólo del desarrollo tecnológico, sino en la participación de dicha política de investigación e industrial relacionada con la seguridad. En el mismo sentido, la vigente ESN, establece como línea de acción estratégica el fortalecimiento del tejido industrial español de Defensa, pudiendo ser éste extrapolado a la industria de la Seguridad.

La OPi representará un rol crucial como estructura administrativa de coordinación entre las Jefaturas, Servicios y Unidades participantes en las distintas fases de un proyecto, así como con las autoridades de la UE. Por lo tanto supondrá una trascendente herramienta de gestión durante toda la vida útil de un proyecto. El rol asumido por la Oficina dotará de la visión estratégica y operativa necesaria a la Guardia Civil, la cual servirá de apoyo a la función de mando, planeamiento y toma de decisiones en el ámbito de la participación de la Institución en proyectos I+D+i nacionales y de la UE.

Tanto la OPi como las OTP's permitirán adquirir un posicionamiento institucional adecuado para afrontar el reto que supone participar en el próximo programa marco H2020, de financiación para la Investigación e Innovación de la UE para el período 2014-2020. Si bien es cierto que no deberíamos limitar el campo de actuación y el valor añadido que representa esta nueva estructura para la gestión de proyectos al exclusivo ámbito de un único programa de financiación de proyectos de la UE. Y eso puesto que la innovación tecnológica en materia de seguridad que se lleve a cabo en la Institución lo será en la medida que se incorporen nuevas soluciones tecnológicas que vayan fortaleciendo nuestras capacidades policiales; siendo dichas nuevas tecnologías financiadas por distintos programas de financiación de proyectos (H2020, Fondo de Seguridad Interior, etc.).

Sin duda, la cultura de la gestión de proyectos en la Guardia Civil, así como lo que representa un proyecto en sí mismo, ha ido evolucionando notablemente desde los inicios de la participación institucional en cualquier tipo de proyecto hasta el momento actual. Con la creación de la OPi se pretende alcanzar una situación final deseada donde la cultura institucional en relación a la gestión de proyectos, en este caso, de innovación tecnológica, represente un valor añadido para los componentes de la Institución así como un modelo de gestión interna.

Fecha de recepción: 12/05/2014. Fecha de aceptación: 24/06/2014

LA ESTRUCTURA DE SEGURIDAD PÚBLICA DURANTE LA SEGUNDA REPÚBLICA (1931-1936)

JESÚS NARCISO NÚÑEZ CALVO

RESUMEN

Analizar, estudiar y debatir en profundidad el orden público y la estructura de seguridad pública del Estado español durante la Segunda República daría lugar a toda una tesis doctoral.

Sin embargo ese no es, evidentemente, el objetivo del autor del presente trabajo, sino exponer ante el lector una visión panorámica sobre la Guardia Civil y los demás cuerpos policiales que entonces constituían dicha estructura y eran responsables de garantizar el orden y la ley. Todo ello en uno de los periodos más convulsos de la Historia de España del siglo XX.

Palabras clave: orden público, estructura de seguridad pública, estado de excepción, coordinación, plantilla.

ABSTRACT

Analyse, study and discuss in depth the public order and the public security apparatus of the spanish State during the Second Republic would result in a whole doctoral thesis.

However, this is not, obviously, the objective of the author of this work, but to provide to the reader an overview of the Spanish Guardia Civil and the other police forces, which at that time, constituted this structure and were responsible of ensuring law and order. All of this during one of the most tumultuous periods of the 20th century in the history of Spain.

Key words: public order, public security apparatus, state of emergency, coordination and staff.

1. INTRODUCCIÓN

Este trabajo sobre la Segunda República comienza definiendo lo que se entiende por “orden público” y por “estructura de seguridad pública”, además de visionar el marco jurídico-legal, entonces vigente, de ambos conceptos tan relacionados entre sí.

El primero consiste, en todo su amplio sentido, en el mantenimiento del régimen de normalidad y buen funcionamiento de las instituciones, los servicios de interés para la comunidad y la pacífica convivencia ciudadana.

El segundo es el conjunto dirigido, organizado e interrelacionado de diferentes estamentos y organismos de la Administración del Estado a quienes compete legalmente la responsabilidad de velar por aquel mantenimiento y en su caso reaccionar oportuna y proporcionadamente para su más pronto restablecimiento.

Difíciles y arduas cuestiones que supusieron uno de los principales caballos de batalla –si no el que más- que padeció y desgastó irreversiblemente a la Segunda República Española.

El orden público fue durante dicho periodo, violenta y constantemente socavado por unos y otros, en función de sus intereses y estrategias políticas, mientras que la estructura de seguridad pública se vió con frecuencia desbordada y avocada a afrontar y reprimir, con los medios legales de un Estado democrático, la acción reaccionaria y, sobre todo, la revolucionaria.

Prueba de todo ello es el hecho de que los sucesivos gobiernos de la Segunda República tuvieron que acudir casi permanentemente, en los dos últimos años de su vigencia, a la declaración de unos estados de excepcionalidad de las garantías ciudadanas, previstas en la legislación vigente.

Mención especial merecen los violentos y sangrientos sucesos revolucionarios de octubre de 1934 y su contundente represión, que marcaron un antes y un después en la percepción del orden público republicano. De hecho, desde la proclamación del nuevo régimen en 1931 hasta el inicio de la sublevación militar de 1936, no se produjeron unos incidentes de tanta virulencia ni que produjeran tantas víctimas, conmocionando profundamente a toda la estructura de seguridad pública del Estado.

Por otra parte hay que significar que, si bien definir la composición de dicha estructura no es difícil, no se puede decir lo mismo respecto a la cuestión de plantillas orgánicas y despliegues que conformaban la misma, y que bien daría lugar a la elaboración de otro trabajo diferente.

La estructura de seguridad pública puede decirse que estaba integrada principalmente por un componente político e institucional y por un componente policial y operativo.

El primero lo conformaban el ministro de la Gobernación y su aparato ministerial así como, por delegación, los gobernadores civiles y los alcaldes.

El segundo estaba compuesto por las Fuerzas de Seguridad del Estado, es decir, el Instituto de la Guardia Civil, que era el de mayor número de efectivos y despliegue territorial; así como por la Policía Gubernativa, integrada a su vez por dos cuerpos: el de Investigación y Vigilancia y, el de Seguridad (y Asalto), ambos antecesores históricos del actual Cuerpo Nacional de Policía.

También, en un segundo nivel y conforme a las competencias establecidas en la legislación de la época, se encontraban el Instituto de Carabineros (posteriormente absorbido por la Guardia Civil mediante la Ley de 15 de marzo de 1940) y los demás cuerpos auxiliares, regionales y locales.

Respecto a la entidad y número de efectivos que tenían las diferentes fuerzas y cuerpos de seguridad pública, cada autor que ha estudiado la cuestión suele aportar sus propios datos, si bien las variaciones entre unos y otros no son excesivamente significativas.

Como cifras orientativas, que no definitivas, podría decirse que la Guardia Civil, que estaba organizada en una Inspección General, cinco Zonas, 24 Tercios y 59 Comandancias, tenía un total de 34.391 hombres; el Cuerpo de Investigación y Vigilancia disponía de unos 3.800 efectivos que estaban distribuidos principalmente en comisarías ubicadas en las principales poblaciones; el Cuerpo de Seguridad (y Asalto) estaba

distribuido en 18 Grupos y 100 Compañías, además de dos Grupos de Escuadrones a caballo, e integrado por 17.660 hombres; y el Instituto de Carabineros contaba con una Inspección General, 10 Zonas y 20 Comandancias, sumando un total de 15.251 hombres. Respecto a las fuerzas locales de los Cuerpos de Miqueletes de Guipúzcoa, Miñones de Alava y Vizcaya, así como los Mozos de Escuadra de Cataluña, no pasaban de 1.500 hombres en conjunto[1].

2. EL MARCO LEGAL

La Segunda República, desde el primer momento de su implantación, fue consciente de que sería objeto de las más variadas agresiones con el principal objetivo de malograr el nuevo régimen que acababa de surgir.

Aunque inicialmente quienes lideraron aquel proceso creyeron que el peligro acecharía principalmente desde las filas del conservadurismo monárquico más reaccionario, que intentaría recuperar por el medio que fuera el poder perdido, pronto comprobarían que tendrían abierto otro frente más combativo: el revolucionario.

De inmediato comenzó a dotarse al nuevo Estado de instrumentos legales que le protegieran frente a sus enemigos. La primera medida fue el Estatuto Jurídico del Gobierno, aprobado el mismo 14 de abril de 1931, por el primer Consejo de Ministros del Gobierno Provisional[2].

Tal y como expuso el profesor Gil Pecharromán, dicha norma vino a dar seguridades sobre el respeto a los derechos ciudadanos, pero también manifestaba la restricción a las actividades públicas de aquellos adversarios del nuevo régimen que, "desde fuertes posiciones seculares, y prevalidos de sus medios, puedan dificultar su consolidación"[3].

Amén de someter "inmediatamente en defensa del interés público, a juicio de responsabilidad", a quienes habían sido directos colaboradores de la Dictadura de Primo de Rivera, se contemplaba en su artículo 6 que el Gobierno se reservaba la facultad de fiscalizar los derechos ciudadanos, dotándose de "plenos poderes" para gobernar por decreto con carácter transitorio, de cuyo uso daría cuenta a las Cortes Constituyentes, previstas para el mes de junio.

Esto último equivalía en la práctica al establecimiento de un estado de excepción temporal en los dos primeros meses para acometer las reformas más urgentes a través de decretos ministeriales que luego ratificaría como leyes el Parlamento[4].

En aquellos primeros momentos se apuntaba más a la prevención y represión de los desórdenes potenciales de tipo ideológico y conspirativo que a los reales de desorden

1 SALAS LARRAZABAL, Ramón. "La organización militar, el Alzamiento y la Guerra Civil" en Aproximación histórica a la Guerra Española (1936-1939). Madrid: Universidad de Madrid, 1970. p. 99; Anuario Militar de España, año 1936, pp. 112-114 y 129; MIGUELEZ RUEDA, José María. Los Cuerpos de Policía durante la Guerra Civil. Tesis doctoral inédita, UNED, 2008, p. 608.

2 Gaceta de Madrid, núm. 105, 15/04/1931, pp. 194-195.

3 GIL PECHARROMAN, Julio. Conservadores subversivos. La derecha autoritaria alfonsina (1913-1936). Madrid: Eudema: 1994, pp. 91-92.

4 GIL PECHARROMAN, Julio. La Segunda República española (1931-1936). Madrid: U.N.E.D., 1995, p. 51.

público o callejero, si bien pronto comenzaron estos últimos, produciéndose graves alteraciones del orden público en diferentes ciudades y poblaciones de la nación.

En palabras del desaparecido profesor Tussell Gómez, la "luna de miel" entre el país y su nuevo régimen no duró mucho y el ambiente entusiástico de los primeros días fue sustituido por el hosco y violento[5].

El siguiente paso de creación de un instrumento legal de protección del nuevo régimen fue la aprobación, el 21 de octubre de 1931 -cuando todavía se estaba en periodo constituyente-, de la denominada Ley de Defensa de la República.

En ella se definían aquellos actos que se consideraban constitutivos de agresión al sistema republicano, recogiéndose los directamente relacionados con el orden público y fijándose las correspondientes sanciones gubernativas sin perjuicio de la acción penal, así como las pertinentes atribuciones del ministro de la Gobernación.

Mes y medio después -el 9 de diciembre- se aprobó tras amplio debate la Constitución de la República Española, norma fundamental donde se contemplaban también diversas cuestiones de interés relacionadas con la seguridad pública[6].

Así en su artículo 14 se establecía la exclusiva competencia del Estado español para legislar en materia de defensa de la seguridad pública en los conflictos de carácter suprarregional o extrarregional (punto 4); sobre policía de fronteras, emigración, inmigración y extranjería (punto 16) y fiscalización de la producción y comercio de armas (punto 18).

También había una parte de su articulado en el que se garantizaba el ejercicio de una serie de derechos constitucionales y que consiguientemente afectaban al orden público, tales como los contemplados en los artículos 27 (libertad de conciencia y de profesar y practicar libremente cualquier religión), 31 (libertad de circulación por el territorio español y elección de residencia en el mismo), 33 (libertad de elección de profesión), 34 (libertad de opinión y expresión), 35 (libertad de elevar peticiones individuales o colectivas a los poderes públicos y autoridades), 38 (libertad de reunión y manifestación sin armas) y 39 (libertad de asociación o sindicación).

Mención especial merece el último párrafo de la disposición transitoria segunda de la nueva Constitución mediante la cual la citada Ley de la Defensa de la República conservaba su vigencia constitucional mientras subsistieran las Cortes Constituyentes, si antes no la derogaban expresamente.

La entrada en vigor de la Constitución no derogó dicha Ley, pues como expone Garijo Ayestarán ésta había sido concebida con tal amplitud que lo mismo se comprendía en ella la incitación a resistir o desobedecer las leyes y a la indisciplina, la difusión de noticias que pudieran quebrantar el crédito o perturbar la paz o el orden público y la comisión de actos de violencia por motivos religiosos, políticos o sociales, como la suspensión de industrias sin justificación bastante, las huelgas no anunciadas con ocho días de anticipación, la alteración injustificada de precios y la falta de celo o negligencia de los funcionarios públicos[7].

5 TUSELL GOMEZ, Xavier. La España del siglo XX. Barcelona: DOPESA, 1975, p. 235.
6 Gaceta de Madrid, núm. 344, 10/12/1931, pp. 1.578-1.588.
7 GARIJO AYESTARAN, María Josefa. El Ministerio de la Gobernación. Materiales para un estudio de su evolución histórica hasta 1937. Madrid: Ministerio de la Gobernación, 1977, p. 135.

En ella se autorizaba al ministro de la Gobernación a suspender reuniones o manifestaciones públicas, clausurar centros o asociaciones, investigar los fondos de éstas y decretar la incautación de armas, incluso las tenidas lícitamente.

A juicio del profesor Gil Pecharromán aquella Ley era una durísima medida de excepción que permitió al Gobierno actuar contra sus enemigos manifiestos con rapidez y al margen del sistema judicial, anulando de hecho las garantías constitucionales, pero sin violar técnicamente la Constitución gracias a esa disposición transitoria.

Dicha Ley se convirtió, no obstante, en un instrumento eficaz para defender de sus adversarios un orden democrático y un sistema de libertades pocas veces tan logrados a lo largo de la historia de España[8].

Así por ejemplo, "Solidaridad Obrera" –órgano de expresión anarcosindicalista- se encargó expresamente de denunciarla como "el pretexto para intensificar la persecución contra la CNT e imposibilitar el regular funcionamiento de los sindicatos"[9].

Finalmente como consecuencia directa de ese carácter transitorio fijado en la misma Constitución y las fuertes críticas sobre su posible inconstitucionalidad, se terminó por elaborar y aprobar, el 28 de julio de 1933, una nueva norma protectora de la República, "dictando las disposiciones que deben observarse en el caso de suspensión de las garantías constitucionales", y que pasó a ser conocida como la Ley de Orden Público[10].

Ésta se encomendaba al ministro de la Gobernación y, bajo su subordinación, a los gobernadores civiles y a los alcaldes, distinguiéndose tres tipos de situaciones: de prevención, cuando se sospechase de un ataque al orden público; de alarma, cuando éste alcanzase efectividad; y de guerra, cuando las autoridades gubernativas se vieran desbordadas por la situación[11].

La Ley de Vagos y Maleantes o de "estados peligrosos y medidas de seguridad"[12], aprobada una semana después, el 4 de agosto de 1933, vino a completarla en alguno de sus aspectos. El reglamento para su aplicación se aprobó casi dos años más tarde[13], siendo de bastante utilización por el estamento policial y el gubernativo.

Los Cuerpos encargados de velar entonces por la conservación y defensa del orden público, bajo las órdenes del ministro de la Gobernación, eran los de la Guardia Civil, Investigación y Vigilancia, y Seguridad (y Asalto), todo ello sin perjuicio, caso necesario, del auxilio de otras instituciones, cuerpos y fuerzas de ámbito estatal, regional, provincial o municipal.

Sin embargo la experiencia adquirida en el agitado periodo republicano había demostrado la necesidad de someter ese amplio conjunto de servicios auxiliares del orden público a una ordenación general, a una misma disciplina y a un único mando, con lo cual recibirían nuevo impulso, multiplicarían su eficacia y alcanzarían nuevas zonas de autoridad, tanto para la represión de los trastornos que anormalmente

8 GIL PECHARROMAN: op. cit, pp. 191-192.
9 PADILLA BOLIVAR, Antonio. El movimiento anarquista español. Barcelona: Editorial Planeta, 1976, p. 273.
10 Gaceta de Madrid, núm. 211, 30/07/1933, pp. 682-690.
11 GARIJO AYESTARAN: op. cit, p. 135.
12 Gaceta de Madrid, núm. 217, 05/08/1933, pp. 874-877.
13 Gaceta de Madrid, núm. 125, 05/05/1935, pp. 1.044-1.053.

pudieran producirse, como en las cotidianas atenciones de vigilancia y de protección a personas y haciendas.

La gravedad de los sucesos revolucionarios de octubre de 1934 motivaron la declaración del estado de guerra previsto en el artículo 48 de la citada Ley de Orden Público y su estricta aplicación durante varios meses hasta que comenzó a ser progresivamente levantado.

Pero no sólo se adoptaron medidas gubernativas excepcionales durante ese periodo, sino que también se tomaron en el orden penal, al decretarse y sancionarse la Ley de 11 de octubre de dicho año, en cuyo artículo final se hacía constar expresamente que estaría en vigor durante un año a contar de dicha fecha.

En su artículo 1º, de los seis que comprendía, se establecieron duras penas, incluida en su caso la de muerte, para quienes con el propósito de perturbar el orden público aterrorizaran a los habitantes de una población o realizaran alguna venganza de carácter social, utilizaran sustancias explosivas o inflamables o emplearan cualquier otro medio o artificio proporcionado y suficiente para producir graves daños, originar accidentes ferroviarios o en otros medios de locomoción terrestre o aérea[14].

Por otra parte, fruto de ese convencimiento y de esa necesidad de implicar y coordinar a todas las autoridades, cuerpos y organismos de cualquier tipo y nivel de la Administración, en el mantenimiento del orden público, se dictó el Decreto de 16 de septiembre de 1935,[15] donde se disponía que las autoridades, cuerpos y organismos que se citaban estaban obligados a cooperar a la defensa del orden y seguridad públicos en los términos que se indicaban; dictándose asimismo normas para la concesión de licencias o autorizaciones gratuitas para uso de armas y determinando las pensiones que disfrutarían las familias de los funcionarios que fallecieran en defensa del orden público.

Realmente dicho decreto, emanado de la mentada Ley de Orden Público de 28 de julio de 1933, venía a terminar de conformar la estructura de seguridad republicana a la vez que definía conceptos y preceptos con una claridad meridiana que hasta entonces no se había visto:

"El orden público no consiste solo en impedir el material disturbio o reprimirlo. Al Gobierno alcanza, además, el fundamental deber de mirar al ambiente moral, a los estados de opinión, para prevenir y atajar, cuanto las leyes lo consientan, la preparación de las perturbaciones y las provocaciones al desorden. Las prevenciones o acuerdos de carácter revolucionario o para la comisión de delitos y las noticias notoriamente falsas, con propósito de alarma, no sería tolerable que circulasen y se extendiesen merced aquellos medios de comunicación oficial".

En dicho decreto se establecía que las autoridades, cuerpos y organismos del poder central, regiones, provincias o municipios, cuyos componentes ostentasen el carácter de agentes de la autoridad o desempeñasen servicios relacionados con el orden público o quienes se concediera el uso gratuito de armas, estaban obligados a cooperar a la defensa del orden y de la seguridad general, bajo la dependencia del ministro de la Gobernación, a quien competía, especial y directamente, aquella función en todo el territorio nacional (art. 1).

14 Gaceta de Madrid, núm. 290, 17/10/1934, p. 379.

15 Gaceta de Madrid, núm. 261, 18/09/1935, pp. 2.173-2.178. El día anterior se había publicado dicho decreto pero, al haberse detectado errores materiales de copia en su inserción, se volvió a reproducir, debidamente rectificado.

Asimismo se decidía que la facultad de disponer y coordinar esos servicios en los cuerpos, organismos e individuos mencionados la ejercería el ministro de la Gobernación por sí o por medio del director general de Seguridad, en Madrid; del delegado del poder central, para el orden público, en las regiones autónomas y de los gobernadores civiles o alcaldes en las respectivas jurisdicciones (art. 2).

Al objeto de alcanzar el fin perseguido en dicho decreto, se encargó a la Guardia Civil la inspección y vigilancia sobre su disciplina de los Cuerpos, de Miqueletes de Guipúzcoa, de Miñones de Vizcaya y Alava, de los Mozos de Escuadra de Barcelona, del Cuerpo de Vigilantes de Caminos y de guardas jurados, peones camineros y agentes del Resguardo de la Compañía Arrendataria de Tabacos.

A su vez, dichas funciones serían desempeñadas por la Dirección General de Seguridad sobre los Guardias Municipales y otros empleados municipales, como los encargados de la vigilancia de las alcantarillas, los serenos, servicios de telégrafos, teléfonos y telecomunicación en general (art. 3). En ambos casos se crearon las correspondientes juntas de coordinación de los servicios de orden público[16].

Los cuerpos y agentes auxiliares del orden público debían dar conocimiento inmediato de cuantas intervenciones hubieran efectuado en relación con los deberes que dicho decreto les imponía, a su jefe inmediato y al de la Guardia Civil o al de la Policía de su demarcación, según procediera (art. 7).

Sin embargo, al desarrollar los preceptos del citado Decreto de 16 de septiembre de 1935, en la parte que afectaba a los servicios que como auxiliares del orden público debían de prestar los guardias y empleados municipales, cuya inspección y disciplina, conforme al citado artículo 3º, quedaba a cargo de la Dirección General de Seguridad, surgieron las primeras dificultades.

Éstas habrían de presentarse en la práctica al intentar ser ejercidas las mentadas funciones de inspección por los funcionarios del Cuerpo de Investigación y Vigilancia en aquellas poblaciones donde no existiese plantilla del mismo, ya que según los artículos 41 al 46 del decreto de referencia, era de su competencia coordinar esos servicios de los guardias y empleados municipales con los demás del orden público.

Para evitar cualquier problema al respecto, y considerándose que eran de gran interés los servicios que pudieran prestar los citados funcionarios municipales en auxilio de las fuerzas encargadas del mantenimiento del orden público, se acordó mediante Orden Ministerial de Gobernación, de 15 de enero de 1936, que la reiterada función de inspección y disciplina sobre dicho personal fuera encomendada al Instituto de la Guardia Civil en las localidades que no existiera plantilla del Cuerpo de Investigación y Vigilancia.

Así, tales funciones pasarían a ser ejercidas, según se disponía en el citado decreto, por los primeros jefes de las Comandancias de la Guardia Civil, bien por sí o delegando en sus oficiales. De igual forma, los deberes y obligaciones que a las autoridades, guardas y dependientes municipales se imponían en los mentados artículos 41 al 46 inclusive del referido decreto, relativos a la coordinación de sus servicios con los de los Cuerpos de Seguridad y Vigilancia, debían cumplirlos con respecto a los

16 TURRADO VIDAL, Martín. La Policía en la historia contemporánea de España (1766-1986). Madrid: Ministerio de Justicia e Interior, 1995, p. 204.

Puestos de la Guardia Civil enclavados en sus demarcaciones cuando en ellas no existiera personal de plantilla de aquellos cuerpos[17].

Otra de las cuestiones de gran interés que contenía el tan reiterado decreto de 16 de septiembre de 1935 era el conjunto de normas de coordinación entre los Cuerpos de la Guardia Civil y de Carabineros en materia de orden público.

La coordinación entre los diferentes cuerpos policiales con competencia en seguridad y orden público siempre fue una de las mayores preocupaciones y responsabilidades de los dirigentes políticos del Ministerio de Gobernación, si bien, nunca se alcanzaba ni el necesario consenso ni el eficaz equilibrio que la realidad exigía.

De hecho, ya se había intentado coordinar infructuosamente poco antes a los propios Cuerpos de la Guardia Civil, de Investigación y Vigilancia y de Seguridad (y Asalto).

Concretamente, mediante el Decreto de 28 de marzo de 1933 se llegó a crear en el propio Ministerio de la Gobernación y, más detalladamente, en su sección de Orden Público, una Secretaría Técnica encargada de estudiar y proponer la coordinación de los servicios de dichos cuerpos, siendo presidida por un teniente coronel de la Guardia Civil[18].

A su vez, en el mismo texto se disponía la constitución de una junta compuesta por el subsecretario de Gobernación, el director general de Seguridad y el inspector general de la Guardia Civil para conocer las propuestas que se formulasen y elevarlas al ministro. Sin embargo dicho intento fracasó y su vigencia fue muy efímera ya que, casi un año después, el 10 de marzo de 1934, “no considerando ya necesaria la Secretaría y Junta” fueron suprimidas[19].

Bien es cierto que los gobiernos responsables de ambos decretos, así como sus respectivos ministros de Gobernación –Santiago Casares Quiroga y Rafael Salazar Alonso- eran bien diferentes, pero dicha asignatura quedó pendiente para todos.

3. GOBERNADOR CIVIL Y ALCALDES

El mantenimiento de la seguridad pública ha sido tradicionalmente una de las principales preocupaciones y tareas de los gobiernos a través de los tiempos, intentando dotar a su administración de los instrumentos más eficaces para ello y constituyendo el gobernador civil una figura clave.

Ejemplo de ello, y sobre la tradicional relevancia que ya tenía dicha figura en la Guardia Civil desde sus tiempos fundacionales, se encuentra en su reglamento para el servicio, aprobado por RD de 9 de octubre de 1844. En su artículo 11 se precisaba que aquél –denominado entonces Jefe Político[20]- disponía el servicio de la parte del Instituto destinado a su provincia respectiva, manteniendo diversas

17 Boletín Oficial de la Guardia Civil, núm. 3, 23/01/1936 (correspondiente al día 20), pp. 86-87.
18 Gaceta de Madrid, núm. 89, 30/03/1933, p. 2.340.
19 GARIJO AYESTARAN: op. cit, p. 138.
20 El nombre de jefe político, con el que se designó, no puede inducir a engaño. Político como adjetivo, no tenía el significado que tiene en la actualidad. Político se contraponía a militar: su equivalente actual sería el de civil. De hecho, terminaría sustituyéndose por la denominación de gobernador civil. TURRADO VIDAL, Martín. Estudios sobre Historia de la Policía. Vol.2. Madrid: Ministerio del Interior, 1991, p. 123.

potestades sobre las unidades y miembros que las integraban y que se detallaban en los artículos siguientes[21].

Los orígenes de dicha figura, cuyo titular era designado expresamente por el gobierno de la nación, se remontan a las Cortes de Cádiz, donde fue objeto, junto a la articulación del orden público, de largos debates, dada la gran importancia que tenía la cuestión. De hecho, tal y como afirma Turrado Vidal, el jefe superior político –primera denominación de la época- centró su actuación en dos materias muy concretas: las elecciones y el orden público.

También, a principios del siglo XX, se reforzó dicha figura –según Morales Villanueva-[22] como jefe de los Cuerpos de Vigilancia y Seguridad, en detrimento de la dependencia del primero de las autoridades judiciales, estando ello motivado por las frecuentes alteraciones de orden público que exigían una dedicación preferente y una actuación rápida para sofocarlas desde el primer momento e incluso abortarlas en su preparación.

Buen ejemplo de lo anteriormente citado se encuentra en el artículo 1º de la Ley de 27 de febrero de 1908, mediante la que se establecía que la Policía gubernativa en toda España estaría constituida por los Cuerpos de Vigilancia y Seguridad a las órdenes del gobernador civil de la provincia[23].

Ya en plena etapa republicana la entrada en vigor de la Ley de Orden Público de 28 de julio de 1933, donde se regulaban los estados de prevención, alarma y guerra, supuso dar fuertes poderes –tal y como expone Carmona Obrero[24]- a los gobernadores civiles en su actuación con respecto al orden público, así como a los alcaldes, a quienes la citada ley les confirió también significativas responsabilidades en dicha materia.

Concretamente, en el caso de los gobernadores civiles, conforme a lo dispuesto en el artículo 7 de dicha ley y a los efectos de la misma, debían asumir el ejercicio de la autoridad gubernativa en todo el territorio de sus respectivas provincias, correspondiéndoles la distribución y dirección de los agentes y fuerzas pertenecientes a los Institutos destinados a guardar el orden y seguridad pública, todo ello dentro de lo preceptuado en los Reglamentos de dichos Institutos y sin perjuicio de su disciplina.

Asimismo los gobernadores civiles podían nombrar, para zonas y casos determinados, dentro del territorio de sus respectivas jurisdicciones, delegados de su autoridad que la representasen en el mantenimiento del orden público. Este recurso fue empleado en numerosas ocasiones.

Respecto a los alcaldes, la mentada ley disponía en su artículo 6 que, en el ejercicio de sus funciones delegadas por el Gobierno, a los exclusivos efectos del mantenimiento del orden público, quedaban subordinados al ministro de la Gobernación y de sus respectivos gobernadores civiles, así como que dispondrían de la fuerza pública dentro del término municipal que presidiesen.

21 “Cartilla del Guardia Civil”. Madrid: Inspección General de la Guardia Civil, 1845, pp. 125-127.

22 MORALES VILLANUEVA, Antonio. Administración Policial Española. Madrid: San Martín, 1988, p. 187.

23 CAAMAÑO BOURNACELL, José. La Policía a través del tiempo (1908-1958). Madrid: Secretaría de Estado de Seguridad, 1999, p. 37.

24 CARMONA OBRERO, Francisco José. Violencia y Orden Público en Andalucía Occidental (1933-1934). Ministerio del Interior. Madrid, 2002, p. 20.

También se les encomendaba en el artículo 8 que, bajo la autoridad y dirección del gobernador civil correspondiente, coadyuvarían a la conservación del orden público dentro de sus respectivos términos municipales.

En caso de que tuvieran que ejercer dicha autoridad gubernativa en circunstancias que impidiesen pedir o recibir instrucciones, debían obrar entonces por propia iniciativa y responsabilidad, dando cuenta lo más rápido posible de sus actos al gobernador civil.

4. EL CUERPO DE LA GUARDIA CIVIL

La evolución de la historia del Cuerpo de la Guardia Civil desde sus orígenes hasta la proclamación de la Segunda República no estuvo exenta de graves complicaciones y tensiones que de una u otra forma fue superando sin que llegara a desaparecer, tal y como había sucedido a otros cuerpos e instituciones encargados de velar por la seguridad pública que le habían precedido.

Morales Villanueva afirma que al tratarse de un cuerpo militar, integrado en la administración castrense pero prestando su servicio a las autoridades civiles, se plantearon graves problemas, motivando que las futuras reformas de las que fue objeto el Instituto oscilaran entre ambas administraciones, con predominio de una sobre la otra, según fuese el régimen político y las necesidades de la paz pública[25].

La implantación del nuevo régimen republicano supuso para la Guardia Civil una serie de importantes reorganizaciones que en su conjunto originaron gran controversia interna, si bien se alcanzaron logros y mejoras muy significativas en materia de personal y retribuciones.

Aunque inicialmente sus plantillas se redujeron, se tuvo que rectificar y ser ampliadas como consecuencia de la imperiosa necesidad de contar con los efectivos suficientes para afrontar los constantes problemas de seguridad pública que padecía la Segunda República, especialmente en las zonas urbanas. De hecho durante ese periodo la Guardia Civil experimentó en su conjunto un significativo aumento en su plantilla que llegó al 25 %[26].

Tal y como expone Morales Villanueva, ese aumento de personal fue destinado principalmente a las zonas de mayores problemas de orden público y conflictividad social (Barcelona, Madrid, Sevilla y Valencia) no existiendo, respecto al Cuerpo de Seguridad (y Asalto) que también actuaba con la misma misión específica, prioridad en las actuaciones ni compartimentación territorial, potenciándose las unidades móviles que acudían rápidamente a los sitios donde sus servicios se hacían necesarios[27].

También reconoce Carmona Obrero, en su trabajo de investigación, que la Guardia Civil estuvo muy presente en el ámbito urbano durante la Segunda República, debiendo

25 MORALES VILLANUEVA, Antonio. Las Fuerzas de Orden Público. Madrid: San Martín, 1980, pp. 115-116.

26 La plantilla del Instituto pasó de tener en 1930 un total de 27.482 efectivos a 34.391 en 1936, es decir 6.909 más, lo cual significaba un 25 % de aumento en ese periodo. Anuario Militar de España, años 1930 y 1936.

27 MORALES VILLANUEVA (1980): op. cit, pp. 119-124.

abandonarse durante dicho periodo la concepción dominante en la historiografía española de que fuera un cuerpo exclusivamente rural[28].

La Guardia Civil, conforme a las directrices gubernamentales recibidas -tanto a través del Ministerio de la Gobernación como de los gobernadores civiles-, hizo del orden público durante la Segunda República su máxima prioridad, estando la mayor parte de sus servicios encaminados a ello, lo cual le obligaría a ocupar el primer puesto de la seguridad pública, habida cuenta de ser tanto el de mayor efectivos como el único cuerpo de carácter policial cuyo despliegue abarcaba permanentemente todo el territorio nacional.

Ello evidentemente implicó ser no solo la principal fuerza de intervención en las zonas urbanas y rurales para el mantenimiento de la seguridad pública, como en su caso la represión de quienes pretendieran alterarla, sino también el principal objetivo de los ataques ideológicos y físicos.

El número de ataques sufridos por la Guardia Civil, las numerosas bajas propias producidas y el desamparo económico en que quedaban los interesados o sus familias motivó que el gobierno de la República dictara la Orden Circular de 29 de marzo de 1932, mediante la cual pasaban a considerarse como hechos de guerra, a todos los efectos, para los miembros del instituto que hubieran resultado muertos o heridos en el cumplimiento de su deber en cualquier alteración del orden público que hubiese tenido lugar desde el 14 de abril de 1931[29].

La situación realmente se tornó con frecuencia, y a medida que fue transcurriendo el tiempo, especialmente difícil para las pequeñas unidades de la Guardia Civil. Es decir, los Puestos, diseminados por toda la geografía nacional, dotados de una reducida fuerza y a los que los sectores revolucionarios acusaban de ser instrumento de represión del capitalismo, la oligarquía y el caciquismo. Aguado Sánchez, al estudiar aquel periodo, definió la paradoja que sufrió el Cuerpo.

"Nunca el Cuerpo habrá gozado de tanta largueza presupuestaria como en tiempos de la Segunda República, pero tampoco nunca morían en las calles tantos guardias civiles, ni nunca la Guardia Civil había soportado tanto desmán, ofensa, crimen, atentado o ataque. El asalto a cuarteles, durante la Segunda República, era cosa diaria o, cuando menos, semanal. … /…Ninguna institución se había sacrificado tanto ni ofrendado tantas vidas al servicio de la República como la Guardia Civil, no por especial afecto al régimen, sino por tradicional e indiscutido sentido del deber"[30].

Por otra parte, la frustrada sublevación del 10 de agosto de 1932, encabezada por quien había sido su anterior director general, el teniente general José Sanjurjo Sacanell, y el hecho de que fuera secundado por fuerzas de la Guardia Civil destacadas en Sevilla y la localidad gaditana de Jerez de la Frontera, tuvo drásticas consecuencias para el Instituto.

La primera de todas se produjo tan sólo tres días después. El 13 de agosto se decretó la disolución del 4º Tercio de la Guardia Civil cuya cabecera estaba ubicada en Sevilla, resultando disueltas también la Comandancia de Sevilla y la Comandancia de Caballería, quedando en situación de disponible todos sus jefes y oficiales[31].

28 CARMONA OBRERO: op. cit, p. 39.
29 Colección Legislativa del Ejército, año 1932, núm. 171, p. 489.
30 AGUADO SANCHEZ, Francisco. Historia de la Guardia Civil. Planeta. Madrid, 1985, vol. 5, pp. IX-X.
31 Colección Legislativa del Ejército, año 1932, núm. 439, p. 555.

Asimismo se dispuso por Orden de 15 de agosto, dimanante ya del Ministerio de la Gobernación, el traslado a la capital hispalense de la plana mayor del 28º Tercio Móvil que tenía su residencia en la localidad gaditana de Jerez de la Frontera, al objeto de hacerse cargo de las citadas unidades disueltas[32].

El general de división Miguel Cabanellas Ferrer, director general del Instituto, fue cesado, despidiéndose de los guardias civiles mediante una emotiva orden general de 16 de agosto publicada en el boletín oficial:

"Ceso en el Mando del Instituto en días de emoción para todo el personal que lo integra. La conducta desleal de un número muy reducido que en Sevilla acataron las órdenes de un mando faccioso han motivado justas medidas de gobierno que, por su rigor y ejemplaridad, han surtido saludables efectos en los responsables, aunque al resto de la Institución y al que hasta ahora ha sido vuestro director nos hayan proporcionado hondo dolor y amargura, …"[33].

El 16 de agosto también se dictó un decreto suprimiendo la Dirección General del Instituto en el Ministerio de la Guerra, creando la Inspección General en el Ministerio de la Gobernación. A la vez también se establecía en éste una Sección especialmente afecta al despacho de los asuntos de personal y servicios de la Guardia Civil. El inspector general sería un miembro del Estado Mayor General del Ejército que estaría a las inmediatas órdenes del ministro de la Gobernación, teniendo atribuciones plenas en materia de disciplina y mando sobre las fuerzas de dicho Instituto[34].

Con esta medida, también adoptada respecto al Instituto de Carabineros, el gobierno de la República quería alejar de la jerarquía y subordinación directa castrense a los dos institutos militares que contaban con mayor número de efectivos, todos ellos profesionales, pasando a depender en lo sucesivo solo de autoridades civiles como eran los ministros de Gobernación y Hacienda respectivamente.

Por otra Orden de 31 de agosto se dispuso que la Comandancia de Huelva pasara a formar parte del 28º Tercio Móvil, para todos los efectos, quedando constituida por la misma fuerza y situación que tenía anteriormente, encargándose éste de las también disueltas Comandancias de Sevilla y Caballería[35].

Por Ley de 8 de septiembre siguiente, se dio fuerza de ley al decreto de disolución de la Dirección General de la Guardia Civil, disponiéndose también la supresión del cargo y jerarquía de general subdirector del Instituto[36], cuyo titular, el general de división Benito Pardo González, quedó disponible, situación en la que permaneció hasta su pase a la de reserva por edad.

Otra orden ministerial de 28 de septiembre de 1932 dispuso que la plana mayor del 28º Tercio Móvil se convirtiera en el nuevo 28º Tercio, pero ya con residencia definitiva en la capital hispalense, pasando a ser integrado por las unidades disueltas de la Comandancia de Sevilla y la Comandancia de Caballería del antiguo 4º Tercio, además de la Comandancia de Huelva[37].

32 Colección Legislativa del Ejército, año 1932, núm. 473, pp. 577-578.
33 Boletín Oficial de la Guardia Civil, núm. 24, 20/08/1932, p. 210.
34 Colección Legislativa del Ejército, año 1932, núm. 445, pp. 559-560.
35 Colección Legislativa del Ejército, año 1932, núm. 477, p. 579.
36 Colección Legislativa del Ejército, año 1932, núm. 497, p. 588.
37 Colección Legislativa del Ejército, año 1932, núm. 534, pp. 631-632.

En la Ley de Presupuestos de 28 de enero de 1933 se incluyeron las cuantías necesarias para proseguir con una profunda reorganización de la Guardia Civil prevista por el gobierno tras la supresión de la Dirección General del Instituto, pero al ser la cantidad consignada insuficiente fue necesario presentar otro proyecto de ley arbitrando nuevos recursos con que dotar los servicios reorganizados del Cuerpo, aprobándose finalmente el 26 de julio de 1933[38].

Dos días después -el 28- se dictó un decreto reorganizando al Cuerpo en cuanto a servicios, personal y acuartelamiento. Conforme a ello, entre otras cuestiones, se redujo muy sensiblemente la plantilla[39] y el número de Tercios, que pasaron de 29 a 19, se suprimieron los dos Tercios Móviles que quedaban, creándose en cambio el de Ferrocarriles, desapareciendo también las unidades específicas de Caballería, convirtiéndose todas las del Cuerpo en mixtas, si bien mejoraron las condiciones económicas y de alojamiento[40].

En el caso de la Comandancia de Cádiz, quedó integrada junto a las Comandancias de Málaga, Las Palmas de Gran Canaria y Santa Cruz de Tenerife en el 16º Tercio, cuya cabecera se establecía en la capital malagueña, dependiendo éste a su vez de la 2ª Zona, cuya jefatura se ubicaba en la capital cordobesa.

En general supuso una drástica reorganización para la Guardia Civil que pronto se comprobó ineficaz, siendo necesario efectuar nuevas reorganizaciones y, sobre todo, aumentar y potenciar progresivamente unas plantillas que cuando menos hacía falta habían sido mermadas.

El 15 de agosto de 1933 la Inspección General del Instituto publicó el cuadro orgánico con las nuevas plantillas que deberían quedar tras la reorganización, quedándose en un total de cinco generales, 882 jefes y oficiales, 1.231 suboficiales, 20.153 de tropa de infantería y 4.907 de tropa de caballería[41].

38 Colección Legislativa del Ejército, año 1933, núm. 367, pp. 452-453.

39 "Art. 3º. En virtud de la nueva organización que se implanta en el Instituto, se suprimen nueve plazas de coroneles, 15 de tenientes coroneles, 54 de comandantes, 76 de capitanes, tres médicos, un veterinario, dos maestros armeros y 1.200 plazas de guardia 2º. Se suprime también el empleo de alférez en la Guardia Civil, siendo sustituidos en las vacantes que reglamentariamente vayan sucediéndose, hasta su extinción, por los subtenientes del Cuerpo de Suboficiales que se crea en el Instituto por este decreto". Colección Legislativa del Ejército, año 1933, núm. 374, p. 466. La plantilla de la Guardia Civil en 1933 era de 29.058 efectivos: cinco generales; 1.236 jefes, oficiales y asimilados, 22.499 suboficiales y personal de tropa de infantería; y 5.318 suboficiales y personal de tropa de caballería. Anuario Militar de España, año 1933, p. 135. La plantilla de la Guardia Civil en 1934 era de 28.269 efectivos: seis generales; 906 jefes, oficiales y asimilados, 21.201 suboficiales y personal de tropa de infantería; y 6.156 suboficiales y personal de tropa de caballería. Anuario Militar de España, año 1934, p. 135.

40 Colección Legislativa del Ejército, año 1933, núm. 374, pp. 466-470.

41 Cinco generales de brigada, 24 coroneles, 56 tenientes coroneles, 68 comandantes, 262 capitanes, 472 tenientes, 229 subtenientes, 157 subayudantes de infantería, 33 subayudantes de caballería, 281 brigadas de infantería, 63 brigadas de caballería, 381 sargentos primeros de infantería, 87 sargentos primeros de caballería, 1.019 sargentos de infantería, 193 sargentos de caballería, 2.064 cabos de infantería, 435 cabos de caballería, 529 cornetas, 167 trompetas, 1.078 guardias 1º de infantería, 238 guardias 1º de caballería, 14.833 guardias 2º de infantería y 3.874 guardias 2º de caballería. Colección Legislativa del Ejército, año 1933, núm. 374, p. 12. Dicha plantilla nunca llegó a cumplirse ya que, antes de que pudiera completarse la amortización de las vacantes necesarias para ello, comenzó a decretarse nuevos e importantes aumentos de plantilla. N. del A.

El 31 de agosto de 1933 se dictó otra orden ministerial sobre reglas para la aplicación de los preceptos del decreto citado de 28 de julio, con el objeto de poner en práctica la organización de las Zonas, Tercios, Comandancias, Compañías y Líneas, así como de los servicios de dicho Instituto.

Entre lo dispuesto destacaba que cada una de las cuatro Zonas sería mandada por un general de brigada y que las Comandancias se clasificaban en tres categorías en función del número de compañías que la integrasen.

Asimismo se disponía que los jefes de Comandancia dejaban de ser plazas montadas, dado el poco eficaz uso del caballo ante las continuas servidumbres del ejercicio del mando, debiéndose dotarles de vehículos para facilitar su rápido desplazamiento a aquellos lugares que las necesidades del servicio requirieran[42].

Casi al finalizar el año y como consecuencia del traspaso de los servicios de la Guardia Civil a la Generalidad, acordado por la Junta de Seguridad de Cataluña y sancionado por decreto de 8 de diciembre[43], se hizo necesario modificar una vez más la organización de las unidades y del servicio del Instituto, especialmente en lo que afectaba a la estructuración de las Zonas, ya que por su carácter administrativo precisaba armonizar las demarcaciones de las mismas con el número de unidades orgánicas a que cada una había de atender.

Las Zonas que se establecieron fueron la 1ª de Valencia, la 2ª de Córdoba, la 3ª de Valladolid, la 4ª de Madrid y la 5ª de Barcelona. Para dotar a esta última de nueva creación con personal para su plana mayor se amplió la plantilla del Cuerpo en un general de brigada, un teniente coronel, cuatro comandantes y tres capitanes[44].

Al año siguiente comenzaron a aprobarse los primeros aumentos de plantilla, comenzando con la recuperación de las 1.200 plazas de guardia 2º de infantería que se habían disminuido de la plantilla del Instituto en la pasada Ley de 26 de julio de 1933, aprobándose a tal efecto la Ley de 20 de marzo de 1934, mediante la que se creaban también 10 plazas de teniente y 1.000 de guardia para las Secciones de Vanguardia (Asalto) del Cuerpo de Seguridad[45].

Por Decreto de 3 de julio siguiente, y como consecuencia de la ley de presupuestos generales del Estado para el ejercicio económico correspondiente al segundo semestre de ese año[46], se volvió a reorganizar una vez más la Guardia Civil, que pasó a estar integrada por 23 Tercios, creándose el 4º Tercio Móvil de Madrid.

Se mantuvo la Comandancia de Cádiz en el 16º Tercio de Málaga en unión de la Comandancia de dicha provincia, pero dejando de estar encuadradas en el mismo las de Las Palmas de Gran Canaria y Santa Cruz de Tenerife que, al igual que la de Baleares, pasaban a quedar exentas de la dependencia de Tercio y Zona, empezando a partir de entonces a hacerlo directamente de la Inspección General.

42 Recopilación de Leyes, Decretos, Órdenes, Circulares y Disposiciones de interés para la Guardia Civil, año 1933, pp. 79-85.
43 Colección Legislativa del Ejército, año 1933, núm. 576, pp. 684-689.
44 Colección Legislativa del Ejército, año 1933, núm. 583, pp. 692-693.
45 Gaceta de Madrid, núm. 81, 22/03/1934, pp. 2.187-2.188.
46 Gaceta de Madrid, núm. 183, 02/07/1934, pp. 34-65.

Asimismo todas las Comandancias pasaban a ser de la misma categoría y con el personal de Caballería de los Tercios 14º de Madrid y 19º de Barcelona se organizaron los tan necesarios escuadrones para el control del orden público, quedando afectos a las Comandancias que integraban dichas unidades, debiendo hacerse lo mismo en aquellas capitales y poblaciones que estuvieran guarnecidas por fuerzas de dicha Arma suficiente en número para organizarse tácticamente en uno o más escuadrones[47].

Al día siguiente se dictó una orden ministerial de Gobernación, determinando las demarcaciones provinciales que habían de comprender las cinco Zonas en que se agrupaban orgánicamente los Tercios y organizando las jefaturas de aquellas[48].

Respecto al 4º Tercio Móvil de Madrid, se dictó el 19 de julio siguiente un decreto mediante el que se fijaba las residencias de sus compañías. El objeto principal de ello era precisamente hacerlo con carácter permanente, armonizando las exigencias del servicio que las realidades sociales y de orden público imponían en las distintas provincias con las conveniencias de no gravar el Erario público con el constante devengo de dietas y pluses que el desplazamiento de dichas fuerzas traía consigo.

El citado Tercio Móvil tenía dos Comandancias y las cuatro compañías de la misma quedaban fijadas en Madrid, Jerez de la Frontera, Sevilla y Málaga, respectivamente, mientras que las otras cuatro de la segunda quedaban ubicadas en Madrid, Badajoz, Zaragoza y Valencia[49].

Dos días después, el 21 de julio, se dictó una Orden Circular mediante la que se determinó la residencia permanente de las cabeceras de las secciones que integraban las ocho compañías del 4º Tercio Móvil. Los efectivos de las 24 secciones del Tercio serían distribuidos y situados, dentro de cada provincia, en los destacamentos que los gobernadores civiles considerasen necesarios establecer, con el objeto de atender con urgencia las necesidades de carácter social y orden público que se produjeran, evitándose con ello el que quedase desatendida la vigilancia de las demarcaciones de los puestos rurales por tener que concentrarse en otros puntos la fuerza que los constituye[50].

El 6 de octubre de 1934 se declaraba en España el estado de guerra como consecuencia de los sucesos revolucionarios encabezados principalmente por socialistas y anarquistas en diversos puntos del país[51], alcanzando la mayor violencia en la zona de Asturias. Las casas-cuartel de la Guardia Civil se convirtieron en el principal objetivo de los extremistas, produciéndose numerosas bajas en las filas del Instituto, que una vez más, fue el colectivo policial que más afectado resultó.

La Revista Técnica de la Guardia Civil, un periódico mensual de carácter no oficial y que desde el año 1910 se editaba particularmente por guardias civiles y para guardias civiles, convirtiéndose en una fuente de obligada referencia para tomar el pulso interno al Instituto, publicó la relación nominal de los primeros 96 guardias civiles muertos (un teniente coronel, un comandante, un capitán, tres tenientes, un subteniente, tres brigadas, dos sargentos 1º, siete sargentos, seis cabos y 71 guardias) y de los primeros 147 heridos (un comandante, dos capitanes, cinco

47 Colección Legislativa del Ejército, año 1934, núm. 365, pp. 399-401.
48 Colección Legislativa del Ejército, año 1934, núm. 371, pp. 404-405.
49 Colección Legislativa del Ejército, año 1934, núm. 419, pp. 431-432.
50 Colección Legislativa del Ejército, año 1934, núm. 428, pp. 435-436.
51 Gaceta de Madrid, núm. 280, 07/10/1934, p. 194.

tenientes, dos subtenientes, un brigada, cuatro sargentos 1º, cinco sargentos, 12 cabos, un corneta y 114 guardias) de los que se tuvo conocimiento, haciendo constar respecto a los fallecidos que "han muerto a consecuencia de heridas recibidas y algunos más, cuyos nombres no hemos podido todavía averiguar". Aunque la mayor parte de las bajas correspondían a Asturias, también se hallaban en las provincias de Albacete, Alicante, Barcelona, Burgos, Ciudad Real, Córdoba, Guipúzcoa, Jaén, León, Lérida, Madrid, Málaga, Murcia, Navarra, Palencia, Tarragona, Valladolid, Vizcaya y Zaragoza[52].

El número final de bajas entre las filas del Instituto -según Aguado Sánchez- fue de 111 muertos y 182 heridos[53]. La citada Revista Técnica dedicó numerosas páginas a lo sucedido desde el sentir interno de la propia Guardia Civil:

"Emocionados ante las extensas listas de los que heroicamente sucumbieron o derramaron su sangre durante las cruentas jornadas de octubre, rendimos a todos el tributo de nuestra admiración, elevando al Cielo una plegaria por los muertos y testimoniando a los que sobreviven el fervoroso deseo de que curen para que puedan seguir dándonos ejemplo de su envidiable bizarría y patriotismo"[54].

En el Cuerpo aquellos sucesos marcarían profundamente a sus integrantes y el recuerdo de aquello fue una de las cuestiones que también estuvieron presentes en el ánimo de buena parte de ellos al iniciarse la sublevación militar de julio de 1936. Para los guardias civiles sus compañeros caídos eran héroes:

"En este inolvidable mes de octubre de 1934 y de los días 5 al 12, la Guardia Civil, en una verdadera semana de pasión, ha dado a la posteridad episodios de lucha, de heroicidades, de bravura netamente española, entremezcladas con escenas de sufrimiento que espantan al más valeroso, …"[55].

También se produjeron bajas entre las filas del Ejército, Cuerpo de Seguridad (y Asalto), Investigación y Vigilancia, Carabineros, así como entre población civil como consecuencia de las acciones de los revolucionarios que finalmente fueron sofocados por la intervención de fuerzas del Ejército, entre las que destacaron las del Tercio de Extranjeros y Regulares Indígenas.

La represión posterior fue muy dura, encarcelándose a numerosos dirigentes, militantes y sindicalistas de izquierda, clausurándose sus locales y periódicos y cesando gubernativamente a sus alcaldes y concejales en todo el país.

Respecto a los muertos y heridos, por uno y otro lado, nuevamente la cuestión de las cifras entra en liza según los autores que se consulten, echándose de menos la elaboración de un estudio riguroso al respecto.

Arrarás Iribarren dio la de 1.198 bajas entre las filas del Ejército y las Fuerzas de Seguridad y más de 3.000 entre los paisanos, sin distinguir entre estos últimos cuales fueron los causados por la acción revolucionaria y cuántos en la represión posterior[56],

52 Revista Técnica de la Guardia Civil, núm. 297, noviembre de 1934, pp. 426-428.
53 AGUADO SANCHEZ: op. cit, vol 5, p. 121.
54 Revista Técnica de la Guardia Civil, núm. 297, noviembre de 1934, p. 428.
55 Ibidem, p. 429.
56 Ejército: 129 muertos, 550 heridos y cinco desaparecidos; Guardia Civil: 111 muertos y 168 heridos; Fuerzas de Seguridad (Investigación y Vigilancia/Seguridad y Asalto: 70 muertos, 136 heridos y dos desaparecidos; Carabineros: 11 muertos y 16 heridos. Paisanos: 1.051 muertos y más de 2.000 heridos. ARRARAS IRIBARREN, Joaquín. Historia de la Cruzada Española. Ediciones Españolas, S.A. Madrid, 1940, vol. 2, p. 266.

mientras que Hugh Thomas, tras calcular que en total murieron de 1.500 a 2.000 personas, de las que unas 320 eran guardias civiles, soldados, guardias de asalto y carabineros y casi 3.000 resultaron heridas, se remite a un informe del Ministerio de la Gobernación de 3 de enero de 1935 que dio una lista global de bajas, relativa a toda España, de 1.335 muertos y 2.951 heridos[57].

Lo acontecido en octubre de 1934 provocó una inmediata reacción del Gobierno que puso en marcha una serie de medidas para ampliar la plantilla de la Guardia Civil y comenzar la adquisición de determinados tipos de armamento y vehículos más modernos y eficaces que los que hasta entonces se tenían de dotación. De hecho, el propio ministro de la Gobernación, Eloy Vaquero Cantillo, facilitó el 15 de octubre una nota oficiosa a la prensa en la que se podía leer:

"Los elementos coactivos del Estado, en su aspecto material deficiente, fueron suplidos ahora con el corazón y el esfuerzo heroico de la fuerza pública. Es necesario llevar a ésta la interior satisfacción mediante las dotaciones perfectas de armas e instrumentos modernos de combate y de transporte, aumentar los efectivos y estudiar la geografía política y social del país para ordenar una útil y eficaz distribución, …"[58].

Así, dos días antes, se había sancionado la Ley de 13 de octubre de 1934[59], aprobada tras los sangrientos sucesos revolucionarios de la semana anterior, en la que se concedieron los créditos necesarios para aumentar la plantilla general del Instituto en siete tenientes coroneles, 26 tenientes, 39 subtenientes, nueve brigadas, 3.582 guardias 2º de infantería y 222 de caballería.

Se procedió a dictar, el día 27 de dicho mes, la orden ministerial de Gobernación mediante la cual se volvían a reorganizar sus fuerzas y servicios, desdoblándose las Comandancias de Sevilla y Valencia, potenciándose las plantillas de las Comandancias de Las Palmas y Santa Cruz de Tenerife, así como otros servicios centrales[60]. En otra orden de 31 siguiente se dictaron instrucciones para organizar las unidades citadas en la norma anterior[61].

También el 13 de octubre el coronel José Aranguren Roldán –presidente de la Comisión de Armamentos de la Guardia Civil- convocó para la elección de un modelo de pistola ametralladora y de subfusil, a las "casas productoras", para que remitieran en el plazo de 15 días "un ejemplar de cada uno de los modelos de pistola automática y de fuego ametrallador", al objeto de ser sometidos a diversas pruebas de evaluación. El 29 de noviembre se dictó un decreto autorizando la contratación, por gestión directa, del armamento y municiones necesarios, cuya urgencia en dicho trámite "así lo exige la intensidad extraordinaria que en el cometido de la Guardia Civil imponen las presentes circunstancias"[62].

Por Decreto de 21 de noviembre de 1934 volvió a constituirse la Comandancia de Marruecos. Su cabecera se fijaba en Ceuta, cesando la dependencia de la Comandancia

57 THOMAS, Hugh. La Guerra Civil Española. Urbión. Madrid, 1979, vol. 1, p. 261.
58 Revista Técnica de la Guardia Civil, núm. 297, noviembre de 1934, p. 428.
59 Gaceta de Madrid, núm. 290, 17/10/1934, pp. 379-383.
60 Colección Legislativa del Ejército, año 1934, núm. 578, pp. 653-655.
61 Colección Legislativa del Ejército, año 1934, núm. 585, pp. 657-658.
62 NUÑEZ CALVO, Jesús Narciso. El armamento de la Guardia Civil (1844-2002). Madrid: Paul Parey España, 2002, pp. 63 y 104.

de Cádiz[63], así como potenciando su plantilla. La nueva Comandancia debía atender el servicio propio del Instituto en las plazas de soberanía, Protectorado de España en Marruecos y Territorio de Ifni, bajo las órdenes del Alto Comisario, con cabecera en Ceuta, que podía utilizarla también en conjunción de las Mehaznías armadas que precisamente estaban instruyendo miembros de la Guardia Civil[64], siendo todo ello confirmado por la Ley de 31 de mayo siguiente[65].

El 7 de enero de 1935 se dictó un decreto reorganizando las fuerzas del Cuerpo que con carácter fijo estaban destacadas en Cataluña[66], lo cual motivó que dos días después se firmara una orden ministerial de Gobernación modificando el cuadro orgánico de la plantilla general de la Guardia Civil[67].

Por otra parte, el gobierno de la República decidió recompensar y reconocer públicamente la labor realizada por la Guardia Civil durante todo el periodo republicano y muy especialmente, el sacrificio realizado con motivo de los sucesos revolucionarios de octubre, dictando el Decreto de 11 de febrero de 1935:

"Vengo en conceder la corbata de la Orden de la República[68] al Instituto de la Guardia Civil, para premiar como recompensa colectiva los innumerables actos heroicos llevados a cabo por el personal del mismo y los relevantes servicios de carácter cívico y humanitario que ha rendido a España y a la República en el cumplimiento de sus deberes"[69].

Siguiendo con la política de disoluciones y creaciones de nuevas unidades, con las consiguientes reorganizaciones, un decreto de 19 de junio de 1935 suprimió el 4º Tercio Móvil. La idea inicial para la que había sido creado no había dado los resultados esperados, decidiéndose con las fuerzas de aquel la creación del 4º Tercio de Madrid y la reorganización del 14º Tercio, también de Madrid[70].

El nuevo 4º Tercio reforzaría el núcleo de fuerzas del Instituto residentes en la capital de la República, ya que todas sus unidades subordinadas quedaban ubicadas en Madrid y no desplegadas en otras provincias como sucedía con el disuelto 4º Tercio Móvil.

También pasaría a constituir una reserva a emplear en aquellos puntos del territorio nacional donde se hiciera precisa su intervención, mediante un desplazamiento rápido desde Madrid utilizando los elementos de motorización convenientes para el transporte de sus efectivos.

63 La Comandancia de Málaga tenía por aquel entonces destacada una compañía en la zona de Melilla, disponiéndose por orden ministerial de Gobernación, de 08/03/1935, que pasase a integrarse en la nueva Comandancia de Marruecos, a la cual pertenecería para todos los efectos, excepto para los administrativos, en los que continuaría dependiendo de aquella. Colección Legislativa del Ejército, año 1935, núm. 143, pp. 150.

64 Colección Legislativa del Ejército, año 1934, núm. 613, pp. 684-685.

65 Colección Legislativa del Ejército, año 1935, núm. 309, pp. 348-349.

66 Colección Legislativa del Ejército, año 1935, núm. 70, p. 53.

67 Colección Legislativa del Ejército, año 1935, núm. 77, pp. 57.

68 Por Decreto de 30/10/1934 del Ministerio de Estado, se creó la Corbata de la Orden de la República para premiar, como recompensa colectiva, actos heroicos de Institutos armados o de colectividades civiles en el cumplimiento de su deber o que se hubieran prestado excepcionales y especialísimos servicios de carácter cívico, humanitario, etc. Colección Legislativa del Ejército, año 1934, núm. 583, p. 656.

69 Gaceta de Madrid, núm. 43, 12/02/1935, p. 1.266.

70 Colección Legislativa del Ejército, año 1935, núm. 373, pp. 405.

Con ello se quería llevar a realidades prácticas los fines para los que fue creado en 1934 el suprimido Tercio Móvil, ya que sus componentes habían terminado siendo absorbidos en el servicio habitual de los puestos y destacamentos –siempre necesitados de personal- de las provincias en las que se habían fijado su residencia, desvirtuándose el cometido especial que se les había asignado como núcleos de fuerzas concentradas dispuestos a desplazarse a otros puntos donde su acción se hiciera necesaria[71].

5. EL CUERPO DE INVESTIGACIÓN Y VIGILANCIA

La Ley de 27 de febrero de 1908 disponía en su artículo 1º que la Policía gubernativa en toda España estaba constituida por los Cuerpos de Vigilancia y de Seguridad, a las órdenes del gobernador civil de cada provincial[72].

Veinticinco años después, con la Segunda República ya proclamada y tras la Ley de Presupuestos de 1932, el Cuerpo de Vigilancia pasó a denominarse Cuerpo de Investigación y Vigilancia[73], estructurándose su nueva plantilla, que pasaba a estar integrada por 3.447 funcionarios: siete comisarios generales, 10 comisarios jefes, 70 comisarios de 1ª clase, 50 comisarios de 2ª, 70 comisarios de 3ª, 170 inspectores de 1ª clase, 250 inspectores de 2ª, 820 agentes de 1ª clase, 1.090 agentes de 2ª y 959 agentes de 3ª[74].

Dicha plantilla suponía una disminución de 147 funcionarios respecto a la última aprobada por el régimen anterior, contemplada en la Ley de Presupuestos de 1931, cuyos efectivos ascendían a 3.594 hombres[75]. Recuérdese que también la Guardia Civil vio reducida durante el bienio azañista su plantilla.

Una mención singular merece el también llamado Cuerpo de Policía Local que, si bien fue una institución policial con entidad y personalidad propia, es abordada dentro de este apartado dedicado al Cuerpo de Investigación y Vigilancia, ya que se nutrió de él y al que terminaron por regresar sus miembros, amén de desarrollar el mismo tipo de funciones, si bien circunscritas a su reducido ámbito local. Su denominación más común fue la de Policía Local Gubernativa y funcionalmente estaba bajo mando directo de los alcaldes[76].

En decreto del Ministerio de la Gobernación, fechado el 11 de julio de 1931, se dispuso la creación, dependiente de la Dirección General de Seguridad, de dicho Cuerpo, y que no debe confundirse con el de la Policía Municipal que actuó en otras competencias administrativas y en delitos menores, determinándose sus funciones y jurisdicción así como que el mismo se constituyera con el personal de vigilantes

71 Boletín Oficial de la Guardia Civil, núm. 18, 24/06/1935 (correspondiente al día 20), pp. 677-678.
72 CAAMAÑO BOURNACELL: op. cit., p. 37.
73 Ibídem, pp. 195-196.
74 CAAMAÑO BOURNACELL: op. cit., p. 177.
75 Dos comisarios generales, dos secretarios generales, 10 comisarios jefes, 25 comisarios jefes de 1ª clase, 45 comisarios jefes de 2ª, 65 comisarios jefes de 3ª, 155 inspectores de 1ª clase, 220 inspectores de 2ª, 820 agentes de 1ª clase, 820 agentes de 2ª, 820 agentes de 3ª, 224 vigilantes de 1ª, 358 vigilantes de 2ª y 28 agentes escribientes. VIQUEIRA HINOJOSA, Antonio. Historia y anecdotario de la Policía Española, 1833-1931. Madrid: San Martín 1989, pp. 307-308.
76 CARMONA OBRERO: op. cit, p. 27.

de 2ª clase del Cuerpo de Vigilancia de la Policía gubernativa que voluntariamente solicitase su ingreso[77].

Las vacantes se hicieron por concurso de méritos entre las clases de Ejército, Marina, Guardia Civil y Carabineros, que debían renunciar a su fuero militar en caso de ingreso. Entre los beneficiados se encontraban buena parte de los sargentos del Ejército que en su día habían ingresado en el Cuerpo de Vigilancia como vigilantes de 2ª en virtud del RD de 8 de mayo de 1926 como consecuencia de las facilidades dadas durante la Dictadura de Primo de Rivera, pero que con la llegada de la República habían sido suspendidos al entrar en vigor la Orden de 1º de mayo de 1931 dimanante del Ministerio de la Guerra.

La función de esta nueva fuerza policial, tal y como determinaba el artículo 2º del citado decreto, era la de investigación y vigilancia y, en general, la misma que estaba atribuida entonces al Cuerpo de Vigilancia en las capitales de provincia.

El artículo 13 del mentado decreto preveía que, si fuera menester, por no cubrirse las plantillas que se aprobaran con los citados vigilantes de 2ª clase, hacer nuevos nombramientos, que se harían por concurso de méritos entre las clases del Ejército, Marina, Guardia Civil y Carabineros.

Finalmente todos los efectivos de dicho Cuerpo se integraron en el de Investigación y Vigilancia, en calidad de agentes auxiliares de 3ª clase, al haber sido suprimido el 6 de agosto de 1935. La creación de dicha escala auxiliar, con el objeto de que se integraran en ella los componentes de la Policía Local, había sido recogida en el artículo 15 de la Ley de Presupuestos del año 1933[78].

6. EL CUERPO DE SEGURIDAD (Y ASALTO)

La llegada de la República supuso un gran impulso del Cuerpo de Seguridad como consecuencia de la creación de una nueva especialidad en su seno: las Secciones de Vanguardia o Asalto.

Con el nuevo régimen los cambios en esta institución policial no solo consistieron en el de su emblema por otro nuevo sin la coronal real y su tradicional casco por una gorra de plato, sino que fue mucho más allá al introducir un novedoso y eficaz modelo de unidades especializadas en la prevención y represión de los desórdenes públicos.

Su prestigio y proyección en la época fueron tales que, aunque en todo el periodo republicano continuó existiendo el Cuerpo de Seguridad, lo que ha terminado trascendiendo tanto popularmente como en la historiografía ha sido la llamada Guardia de Asalto, cuando realmente esta denominación como tal nunca existió oficialmente para referirse a la institución y sí para definir al guardia de 1ª o 2ª clase, constando en la documentación otras como las de Secciones de Vanguardia, Sección de Asalto o posteriormente la más genérica de Compañías de Asalto, pero formando siempre parte del mentado Cuerpo de Seguridad.

77 Gaceta de Madrid, núm. 193, 12/07/1931, pp. 345-346.
78 Gaceta de Madrid, núm. 364, 28/12/1932, p. 2.195.

Curiosamente, en los meses anteriores a la sublevación militar, comenzó a verse publicada en las disposiciones oficiales relacionadas con las vicisitudes de sus miembros la expresión de "Cuerpo de Seguridad y Asalto", manteniéndose en otras la de "Cuerpo de Seguridad", si bien no se ha podido localizar la norma concreta mediante la cual se había modificado la denominación original.

Por su parte, la Ley de 30 de enero de 1932, que daba carta de naturaleza a dicho Cuerpo, disponía en la parte que más interesa[79]:

"Artículo 1º. Se aumenta el número de Guardias de Seguridad de 1ª clase consignado en el presupuesto vigente en 2.500 para la ampliación de las Secciones de Vanguardia (Asalto) con el número de Jefes, Oficiales y clases necesarias, y en 100 de vigilantes conductores de vehículos de la Dirección General de Seguridad.

Artículo 2º. Se autoriza la adquisición de 60 camiones automóviles, de 40 automóviles de tipo fuetón para el transporte de fuerzas, de tanques de agua a presión, (…)".

Los cuadros de mando que se citaban como necesarios eran dos comandantes, 30 capitanes, 40 tenientes, 30 suboficiales, 50 sargentos y 70 cabos, además de 30 profesores de gimnasia y otros tantos médicos[80].

En la Orden Circular de 8 de febrero siguiente se publicaron diversas instrucciones relacionadas con la creación de las Secciones de Vanguardia y que supondrán el inicio de su despliegue por las principales capitales y ciudades del país:

"Artículo 18. El orden de calificación dará derecho a los aspirantes aprobados a la elección del lugar en que deban prestar servicio entre aquellos que hayan de establecerse las Secciones de Vanguardia que se creen"[81].

Desde entonces las plantillas de Asalto continuaron aumentando, creándose el 8 de septiembre siguiente otras 2.500 plazas más de guardias 1º del Cuerpo de Seguridad y así sucesivamente, significándose que tanto jefes como oficiales procedían del Ejército y la Guardia Civil[82].

La fuerza de Asalto se fue estructurando en 13 Grupos, cada uno de ellos mandado por comandantes y formado por tres compañías de fusileros-granaderos y una de especialidades –ametralladoras, morteros y gases- sobre automóviles, mandadas a su vez por capitanes. Las compañías estaban constituidas cada una de ellas por tres secciones mandadas por tenientes, estas a su vez por tres pelotones cada una, mandados por sargentos y estos a su vez por tres escuadras cada una, mandadas por cabos[83].

El Cuerpo de Seguridad se organizó en tres secciones: Servicios locales, dedicados a la vigilancia de las capitales y ciudades en las que estaba desplegado; Caballería, tratándose de fuerzas montadas que efectuaban su servicio de vigilancia en largos recorridos por el interior del casco de las poblaciones; y de Asalto, que

79 Gaceta de Madrid, núm. 36, 05/02/1932, pp. 914-916.

80 Dichas cifras y empleos fueron modificados por la orden ministerial de 26/04/1932, consignándose finalmente 1 coronel, 2 tenientes coroneles, 12 comandantes, 57 capitanes, 176 tenientes, 67 suboficiales, 235 sargentos, 666 cabos y 2.230 guardias. Gaceta de Madrid, núm. 124, 03/05/1932, pp. 843-844.

81 Gaceta de Madrid, núm. 40, 09/02/1932, pp. 1.012-1.013.

82 Gaceta de Madrid, núm. 261, 17/09/1932, pp. 2.013-2.014.

83 MUÑOZ BOLAÑOS, Roberto. Las Fuerzas y Cuerpos de Seguridad en España (1900-1945). Almena Ediciones, Serga, Especial nº 2. Madrid, 2000, p. 58.

estaban motorizados y dotados de armas de combate y artificios de guerra, además de material antidisturbios[84].

En la Ley de Presupuestos para el año 1933, de 28 de diciembre de 1932[85], se fijó la primera plantilla del Cuerpo de Seguridad en la etapa republicana, incluido el personal de Asalto, y gracias a los aumentos pasaba a estar compuesta por 12.028 hombres: un coronel, tres tenientes coroneles, 14 comandantes, 81 capitanes, 231 tenientes, 91 suboficiales, 310 sargentos, 874 cabos y 10.423 guardias[86].

Por orden ministerial de 20 de marzo de 1934 el Cuerpo de Seguridad aumentó en 10 plazas de tenientes y 1.000 guardias más para las Secciones de Vanguardia (Asalto), a la vez que en la misma disposición se aumentaba la plantilla de la Guardia Civil en 1.200 hombres más[87].

Aunque el Cuerpo de Seguridad era desde su creación de naturaleza civil, sus componentes estaban imbuidos de un elevado sentido de la disciplina, estando sometidos al fuero castrense solo en cuestiones de subordinación con sus superiores, tal y como se manifiesta en la siguiente instrucción dirigida a quienes quisieran optar al ingreso en el mismo:

"Los concursantes deberán tener en cuenta que la característica principal del Cuerpo de Seguridad es su férrea disciplina, por lo cual todos sus componentes están sometidos en todo momento y ocasión, por lo que respecto a la misma, subordinación, obediencia y fidelidad y respeto a todas las jerarquías y órdenes que de ellos emanan, a los preceptos de las Ordenanzas militares y Código de Justicia Militar, para lo cual firmarán su compromiso antes de tomar posesión"[88].

El prestigio y alto grado de eficacia que fue alcanzando el Cuerpo de Seguridad, que además había sufrido 70 muertos, 67 heridos graves y 98 heridos leves en los sucesos revolucionarios del mes de octubre de 1934 en Asturias[89], terminó por serle reconocido por el gobierno de la República mediante la concesión el 11 de junio de 1935, del uso de la bandera nacional:

"El Cuerpo de Seguridad, creado con la noble y alta misión de velar por el orden público, ha puesto siempre abnegación y sacrificio en el cumplimiento del deber; pero sus virtudes como cuerpo civil o Institución armada, han culminado en los días de la pasada agitación revolucionaria, en que sus secciones de Vanguardia y Asalto, cooperó heroicamente al restablecimiento de la paz pública. El gobierno recogiendo el sentimiento de gratitud del pueblo español, quiere premiar la ejemplar conducta del Cuerpo de Seguridad, cuya disciplina y subordinación descansan sobre principios de organización militar, concediéndole el derecho al uso de la bandera republicana que es el supremo símbolo de la patria"[90].

Como consecuencia de los sucesos revolucionarios del mes de octubre de 1934, el día 13 de dicho mes se aprobó una ley mediante la cual se concedieron los créditos necesarios para aumentar, además de 38 vigilantes-conductores de 3ª clase del Cuerpo de Investigación y Vigilancia, la plantilla general del Cuerpo de Seguridad (Asalto) en cuatro comandantes, 28 capitanes, 70 tenientes, 32 suboficiales, 100 sargentos,

84 CABO MESEGUER, Vicente; CORREA GAMERO, Manuel; CAMINO DEL OLMO, Miguel Ángel. Policía Española. Notas e imágenes. Lunwerg editores y Fundación Policía Española. Barcelona, 1999, p. 74.
85 Gaceta de Madrid, núm. 364, 29/12/1932, pp. 2.194-2.243.
86 CAAMAÑO BOURNACELL: op. cit., p. 177.
87 Gaceta de Madrid, núm. 81, 22/03/1934, pp. 2.187-2.188.
88 Gaceta de Madrid, núm. 338, 04/12/1934, pp. 1.855-1.866.
89 CAAMAÑO BOURNACELL: op. cit., pp. 256-259.
90 Gaceta de Madrid, núm. 163, 12/06/1935, pp. 2.111-2.112.

140 cabos y 4.000 guardias, además de dos capitanes, seis tenientes, dos subtenientes, ocho sargentos, 24 cabos y 206 guardias de aumento en las plantillas de los escuadrones de caballería de dicho Cuerpo[91].

En 1936 el número de integrantes del denominado Cuerpo de Seguridad (y Asalto) era de 17.660 -450 jefes y oficiales, 543 suboficiales y 16.667 guardias- de los que poco más de la mitad correspondían a Asalto[92].

7. EL CUERPO DE CARABINEROS

Dos semanas antes de la proclamación de la Segunda República, por Real Orden Circular del Ministerio del Ejército de 31 de marzo de 1931, "el Rey (q. D. g.), de conformidad con la organización de servicios realizada por el Ministerio de Hacienda, se ha servido aprobar el adjunto cuadro orgánico del Instituto de Carabineros"[93], constituido por mando y plana mayor de la Dirección General, 15 Subinspecciones, 33 Comandancias, una compañía exenta de Africa además como otros órganos y destinos varios para una plantilla total de 16.101 hombres y 64 mujeres[94].

Hasta esa fecha habían estado encuadrados, además de mando y plana mayor de su Dirección General, en 14 subinspecciones, 32 comandancias, 110 compañías, 12 secciones de caballería y 1.682 puestos[95].

La implantación del nuevo régimen republicano no pareció que conmocionara mucho a nivel interno al Cuerpo de Carabineros ni fue objeto inicial de especial protagonismo o referencia para líderes republicanos y responsables monárquicos de aquellas históricas jornadas, al contrario que otras fuerzas de seguridad del Estado.

De hecho fue el Cuerpo que parece ser que mejor y más rápidamente asimiló la nueva situación, tal vez por estar sus misiones principalmente más orientadas a actuar como resguardo fiscal del Estado que a las del orden público, donde realmente solo se veía hipotecado en circunstancias muy extremas.

Diversos historiadores han defendido que fue la fuerza de seguridad más favorecida y potenciada por el nuevo régimen, si bien nadie ha razonado ni expuesto de forma detallada y rigurosa las razones que inducen a tal afirmación, no existiendo siquiera en toda la historiografía un estudio académico sobre el Cuerpo de Carabineros, al contrario que si los hay sobre la Guardia Civil y la Policía.

91 Gaceta de Madrid, núm. 290, 17/10/1934, pp. 379-383.
92 MUÑOZ BOLAÑOS: op. cit, p. 59.
93 Colección Legislativa del Ejército, año 1931, núm. 123, pp. 189-191.
94 Tres oficiales generales (un teniente general, un general de división y un general de brigada), 142 jefes (19 coroneles, 41 tenientes coroneles y 82 comandantes), 600 oficiales (173 capitanes, 299 tenientes y 128 alféreces), 14.512 hombres de Infantería (130 suboficiales, 894 sargentos, 878 cabos, 11 cabos de cornetas, 400 cornetas, 889 carabineros de 1ª clase y 11.310 carabineros de 2ª clase), 350 de Caballería (dos suboficiales, 23 sargentos, 26 cabos, 10 trompetas, 25 carabineros de 1ª clase y 264 carabineros de 2ª clase), 460 de Mar (seis suboficiales, 23 sargentos, 42 cabos, 34 carabineros de 1ª clase y 355 carabineros de 2ª clase), 34 armeros y 64 matronas (seis de 1ª clase y 58 de 2ª clase).
95 Anuario Militar de España, año 1930, pp. 188-190.

Así por ejemplo, Aguado Sánchez, quien ha abordado la historia genérica de dicho Instituto, ofrece su propia visión no exenta de cierta distorsión ideológica, afirmando que:

"Durante la Segunda República, la recuperada consistencia moral de la institución, la eficacia de sus servicios y la autoridad y respeto que se habían logrado descendieron visiblemente. Su tropa, principalmente, fue objeto de manipulación y politización, y perdió bastante cohesión y disciplina. Por cuestiones que sería largo comentar, en primer lugar las de herencia histórica, el Cuerpo de Carabineros estuvo marcado por influencias del liberalismo progresista, derivadas luego hacia una exaltada y equivocada ideología de extrema izquierda, lo que justificaría conductas posteriores"[96].

El cambio más importante en su organización se produjo a raíz de la frustrada sublevación del 10 de agosto de 1932, que había encabezado precisamente su director general el teniente general Sanjurjo -que fue detenido, encarcelado, procesado y condenado-, si bien no conllevó el apoyo del personal de su propio Cuerpo.

Consecuencia de aquello fue que, al igual que había pasado con la Guardia Civil respecto al Ministerio de la Gobernación, tres días después, el 13 de agosto, se decretó por el gobierno de la República la supresión de la Dirección General de Carabineros, quedando reorganizada inicialmente en dos inspecciones, una en el Ministerio de la Guerra y otra en el de Hacienda[97].

Para facilitar su cumplimiento se dictó dos días más tarde, por el Ministerio de la Guerra, otro decreto con las instrucciones necesarias para ello, entre las que además se aprovechó para reorganizar la orgánica del propio Instituto.

Las Subinspecciones tomaron el nombre de Zonas que a su vez quedaron agrupadas en dos Circunscripciones, que serían mandadas por generales. La primera de ellas establecía su cabecera en Sevilla y se componía de las Zonas 2ª de Valencia, 3ª de Alicante, 4ª de Almería, 5ª de Málaga, 6ª de Cádiz (comprendía las Comandancias de Cádiz y Algeciras), 7ª de Sevilla y 14ª de Madrid, mientras que la segunda, con cabecera en Barcelona, se formaba con la 1ª de Barcelona, 8ª de Salamanca, 9ª de Coruña, 10ª de Asturias, 11ª de Guipúzcoa, 12ª de Navarra, 13ª de Figueras y 15ª de Tarragona[98]. La Ley de 27 de agosto elevó de rango el citado decreto de 13 de agosto[99].

Sin embargo dicha dualidad de inspecciones y la todavía excesiva dependencia militar provocó importantes disfunciones en su actividad diaria, siendo además deseo del gobierno que la dependencia fuera exclusiva de una autoridad civil.

Por lo tanto fue necesario dictar, el 19 de noviembre siguiente, un nuevo decreto reorganizando el Instituto de Carabineros, disponiéndose que todos sus organismos y servicios pasaran a depender únicamente del Ministerio de Hacienda, de quien también dependería directa e inmediatamente su inspector general, que a su vez estaría auxiliado por una secretaría en la nueva Inspección General.

En dicho Ministerio se organizó, bajo la dependencia inmediata de la Subsecretaría, una Sección de Carabineros, al objeto de hacerse cargo de aquellas competencias y responsabilidades que anteriormente se detentaban en el Ministerio de la Guerra[100].

96 AGUADO SANCHEZ: op. cit., vol. 6, p. 154.
97 Colección Legislativa del Ejército, año 1932, núm. 440, p. 555.
98 Colección Legislativa del Ejército, año 1932, núm. 444, p. 559.
99 Colección Legislativa del Ejército, año 1932, núm. 474, p. 578.
100 Colección Legislativa del Ejército, año 1932, núm. 613, pp. 697-698.

Tanto la Inspección General como la Sección de Carabineros citadas fueron organizadas mediante decreto de 17 de diciembre siguiente, en relación con otros departamentos ministeriales y autoridades[101].

Una orden ministerial de Hacienda, de 3 de diciembre de 1932, modificó la residencia de los dos generales jefes de ambas circunscripciones para fijarla en Madrid, volviendo a variarse la misma por otra orden de 21 de febrero de 1935 y pasarlas a Córdoba la 1ª y a Valladolid la 2ª[102].

El reiterado Decreto de 16 de septiembre de 1935 dedicaba una serie de artículos –del 17 al 21- a la coordinación entre las fuerzas de la Guardia Civil y Carabineros, que revistió gran interés ya que existían comandancias donde ambas fuerzas prestaban servicio en las mismas zonas y localidades.

En primer lugar se establecía la obligación que tenían los miembros del Instituto de Carabineros, aparte de denunciar los delitos y detener a los delincuentes, de cooperar al mantenimiento del orden con arreglo a su Reglamento y a las normas que se citaban expresamente para ellos (art. 17).

Las instrucciones que se impartieran al respecto serían siempre por conducto de los gobernadores civiles que se dirigirían a los respectivos jefes de Comandancia (art. 18).

Asimismo las informaciones que adquiriera el personal de Carabineros y las intervenciones que realizasen en relación con el orden público las debían poner en conocimiento de los jefes de las fuerzas de la Guardia Civil más próximas, quienes, sin perjuicio de adoptar las medidas procedentes, las debían transmitir al gobernador civil de la provincia (art. 19).

Cuando el orden público fuera alterado en las localidades donde coincidiesen fuerzas de la Guardia Civil y de Carabineros, ambas deberían coordinar sus servicios y prestarlos con sujeción a sus reglamentos y bajo los respectivos mandos, salvo que las circunstancias requirieran una acción militar conjunta, en cuyo momento tomaría el mando de toda la fuerza el de mayor empleo de ambos Cuerpos, actuando con arreglo a los preceptos de la legislación militar entonces vigente (art. 20).

En las localidades en que sólo existieran fuerzas de Carabineros, éstas comunicarían, directamente al gobernador civil de la provincia y al comandante del puesto de la Guardia Civil en cuya demarcación estuvieran enclavados, los partes y noticias relacionadas con el orden público, adoptando a la vez aquellas medidas de carácter preventivo que considerasen convenientes y, si aquél se alterase, debían restablecerlo, cumpliendo sus deberes reglamentarios y dando cuenta también al gobernador civil de la provincia (art. 21).

Si bien la historiografía ha situado habitualmente al Cuerpo de Carabineros como una de las instituciones más cuidadas y mejor tratadas por el régimen republicano, se produjo una significativa -pero poco conocida y menos citada- reducción de sus

101 Colección Legislativa del Ejército, año 1932, núm. 672, p. 754.
102 Colección Legislativa del Ejército, año 1935, núm. 109, pp. 126-127.

unidades y efectivos, con motivo de una importante reestructuración que experimentó toda la orgánica del Ministerio de Hacienda.

Así, por decreto de 28 de septiembre de 1935, dimanante del propio Ministerio de Hacienda, se procedió a reorganizar sus dependencias administrativas y los servicios afectos al Cuerpo de Carabineros, todo ello en uso de la autorización concedida por el Gobierno en la Ley de 1 de agosto anterior y que supuso una reducción de plantillas y unidades que implicó la disminución global de 785 plazas de las 16.154 de que se componía[103], es decir, casi el 5 %[104].

Se suprimieron las dos Circunscripciones con sus respectivos cuadros de mando, así como cinco de las Zonas y 13 de las Comandancias, entre ellas la de Algeciras –aunque ésta por error- con sus correspondientes cuadros de mando, quedando por lo tanto 10 Zonas y 20 Comandancias. La Comandancia de Cádiz, con el número de décima, quedó integrada en la 5ª Zona, junto a la Comandancia de Málaga. También se suprimieron la fuerza de Caballería y los ordenanzas, creándose por el contrario solo la plaza de general subinspector[105].

Sin embargo enseguida se constató que había habido varios errores en su publicación que tuvieron que ser subsanados en sucesivas disposiciones hasta que por fin la orden ministerial de 22 de octubre siguiente publicó el cuadro orgánico definitivo, conforme a la cual ya no figuraba la Comandancia de Algeciras –de gran importancia en materia de represión del contrabando- entre las desaparecidas, integrando con el número de décima y junto a la de Málaga-Estepona la 5ª Zona. La de Cádiz quedaba encuadrada en la 6ª Zona con el numeral onceavo y formando parte de aquella con la Comandancia de Sevilla-Huelva[106].

El 18 de julio de 1936 el Cuerpo de Carabineros contaba con una plantilla total de 15.321 plazas[107].

103 Tres generales, 18 coroneles, 38 tenientes coroneles, 80 comandantes, 164 capitanes, 301 tenientes, 128 alféreces, 52 suboficiales de Infantería, dos suboficiales de Mar, 1.086 brigadas y sargentos de Infantería, 29 brigadas y sargentos de Mar, 13.444 hombres de tropa de Infantería (823 cabos, 400 cornetas, 889 carabineros de 1ª clase y 11.332 carabineros de 2ª clase), 285 hombres de tropa de Caballería (nueve trompetas, 24 carabineros de 1ª clase y 252 carabineros de 2ª clase) y 425 hombres de tropa de Mar (40 cabos, 34 carabineros de 1ª clase y 351 carabineros de 2ª clase); 34 armeros; y 65 matronas (seis de 1ª clase y 59 de 2ª clase). Escalafón de jefes y oficiales de Carabineros, año, 1935.

104 Se suprimieron 852 efectivos pertenecientes a los siguientes empleos: un general de brigada, seis coroneles, 13 tenientes coroneles, 50 comandantes, 19 capitanes, cinco tenientes, 441 carabineros de 2ª clase de Infantería, 285 hombres de tropa de Caballería (nueve trompetas, 24 carabineros de 1ª clase y 252 carabineros de 2ª clase) y 32 maestros armeros. Se aumentaron 67 efectivos pertenecientes a los siguientes empleos: 34 alféreces, cinco cabos de Infantería, 24 carabineros de 1ª clase de Infantería y cuatro carabineros de 2ª clase de Mar. Elaboración propia tras comparar las plantillas de 1935 y 1936, antes y después de la entrada en vigor del mencionado decreto.

105 Colección Legislativa del Ejército, año 1935, núm. 633, pp. 746-750.

106 Gaceta de Madrid, núm. 297, 4-10-1935, p. 663.

107 Dos generales, 12 coroneles, 25 tenientes coroneles, 30 comandantes, 145 capitanes, 296 tenientes, 162 alféreces, 486 brigadas y 600 sargentos de Infantería, seis brigadas y 23 sargentos de Mar, 13.032 hombres de tropa de Infantería (828 cabos, 400 cornetas, 913 carabineros de 1ª clase y 10.891 carabineros de 2ª clase), 429 hombres de tropa de Mar (40 cabos, 34 carabineros de 1ª clase y 355 carabineros de 2ª clase), cuatro médicos, un director de música, un profesor de esgrima, dos maestros armeros y 65 matronas. Anuario Militar de España, año 1936, p. 134.

8. EPÍLOGO

Tras la Guerra Civil, nada sería igual para ninguno de los Cuerpos que habían conformado la estructura de seguridad pública del Estado durante la Segunda República.

La Guardia Civil, tras haber sido disuelta en la zona gubernamental, previa una efímera reconversión en Guardia Nacional Republicana y una incompleta integración en el nuevo Cuerpo de Seguridad, sufrió al inicio de la posguerra una importante metamorfosis interna, enriquecida y robustecida por la absorción de Carabineros que desapareció como tal, pasando a integrar su personal y asumir sus competencias.

La Policía Gubernativa, constituida por el Cuerpo de Investigación y Vigilancia así como el de Seguridad (y Asalto), que fueron integrados durante la contienda en la zona republicana en el nuevo Cuerpo de Seguridad, pasaría a estar formada en la posguerra por el Cuerpo General de Policía y la Policía Armada y de Tráfico, respectivamente.

Comenzaba un nuevo periodo de la Seguridad Pública española, pero esa ya es otra historia.

Fecha de recepción: 02/05/2014. Fecha de aceptación: 24/06/2014

A VECES LA VOZ DICE MÁS QUE LAS PALABRAS

JOSÉ MANUEL PETISCO RODRÍGUEZ Y RAFAEL MANUEL LÓPEZ PÉREZ

RESUMEN

Todos sabemos la importancia que tiene la voz en cualquier acto comunicativo. A través de ella transmitimos información verbal y no verbal pero, cuando tratamos de descifrar el mensaje que nos transmite otra persona, el componente no verbal paralingüístico pasa desapercibido en la mayoría de los casos, ya que nos fijamos más en otros aspectos como las palabras, la expresión facial o los gestos. Pero, si nos centramos en el canal vocal, sería de interés conocer si sabemos descifrar la información no verbal que nos llega, si podemos identificar con certeza el estado emotivo de una persona a través de su voz, si podemos identificar algún rasgo de su personalidad o qué nos pueden indicar diferentes parámetros del habla como el tono, volumen, velocidad o la latencia de respuesta. Otros tantos interrogantes se nos plantean ante la aparición de tartamudeos, balbuceos, errores en el habla, repeticiones y omisiones. En este artículo se intenta dar respuesta a todos estos interrogantes, partiendo de una breve descripción de la fisiología de la fonación para luego pasar a tratar cada uno de esos apartados.

Palabras clave: detección de mentiras, paralenguaje, comunicación no verbal, prosodia.

ABSTRACT

We all know the importance of the voice in any communicative act. Through it we can transmit verbal and nonverbal information but, when we try to decipher the message transmitted by another person, nonverbal paralinguistic component is unnoticed in most cases, and we look further into other aspects such as words, facial expression or gestures. However, if we focus on the voice channel, it would be interesting to know if we can decode the nonverbal information we receive. It would also be interesting to see if we can accurately identify the emotional state of a person through his voice and if we can identify some of his personality traits, or which is the meaning of the different speech parameters such as pitch, volume, and speed or response latency. Other questions appear in relation with stuttering, stammering, speech errors, omissions and repetitions. This article attempts to answer these questions, beginning with a brief description of the physiology of phonation to continue dealing with each of those topics.

Keywords: deceit detection, paralanguage, nonverbal communication, prosody.

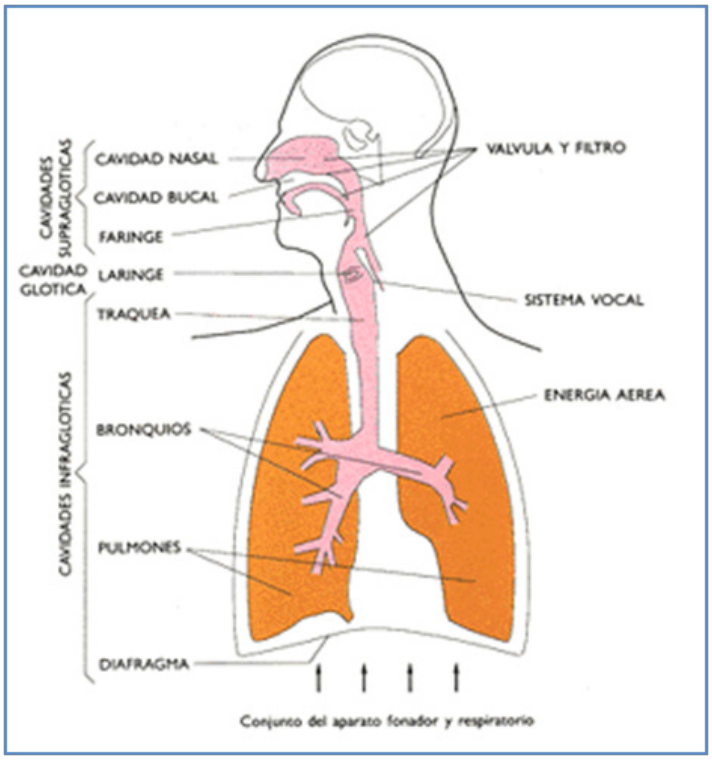
1. FISIOLOGÍA DE LA FONACIÓN

La voz es una herramienta fundamental en el desarrollo de nuestra vida personal y laboral. En la emisión de la voz intervienen estructuras cuyas misiones primitivas (respiración, masticación, deglución ,etc) se han ido adaptando a las necesidades

del habla humana. En la produción de la voz intervienen varios sistemas: respiratorio, fonador, resonador, sistema de articulación y sistema nervioso.

Para Quilis (1997) los órganos que intervienen en la fonación o producción del sonido articulado se pueden clasificar en tres grupos:

- Las cavidades infraglóticas, formadas por el sistema respiratorio o “fuelle” (musculatura respiratoria y torácica, pulmones, bronquios, tráquea, diafragma), que se encargarían de fabricar un soplo de aire controlado y controlable para poder producir el sonido.
- La cavidad laríngea o glótica, formada por la laringe o “pieza vibradora” (estructura compleja de cartílagos, ligamentos y músculos que constituyen las cuerdas vocales), que se encargaría de producir la vibración de parte de su estructura al recibir aire a presión procedente del soplo pulmonar produciéndose así ruido.



[Ilustración 1. Aparato fonador y respiratorio]

- Las cavidades supraglóticas o de resonancia (cavidad faríngea, cavidad bucal, cavidad nasal y cavidad labial), que se encargarían del redondeo y mejora del sonido laríngeo antes de salir al exterior.

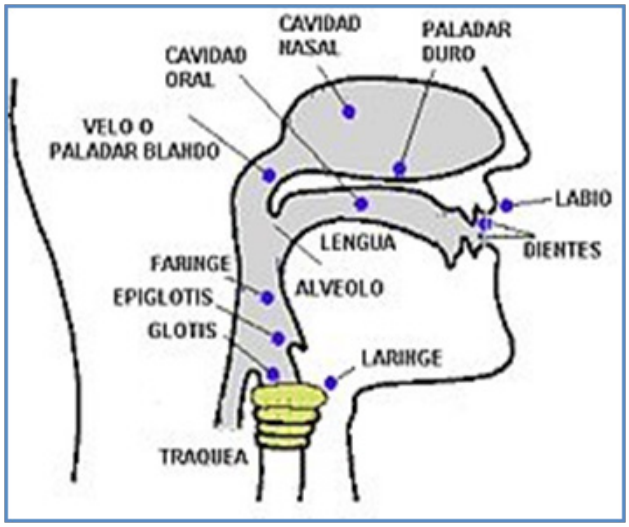
Todo ello sería controlado por el sistema auditivo y el sistema nervioso central. El sistema auditivo se encargaría de recoger el feedback sobre la intensidad, el tono y el timbre de nuestra voz, para ejercer el control el sistema nervioso central.

1.1. PRODUCCIÓN DEL SONIDO ARTICULADO

Los pulmones están constantemente realizando dos movimientos: inspiración (absorción de aire) y espiración (expulsión de aire). Durante este segundo movimiento es

cuando puede producirse el sonido articulado. Para ello el aire de los pulmones pasa a los bronquios y de allí a la tráquea, órgano formado por anillos cartilaginosos superpuestos, que desemboca en la laringe. En la laringe (compuesta por cuatro cartílagos: cricoides, tiroides y dos aritenoides) se encuentran dos membranas, las cuerdas vocales y la glotis (abertura que queda entre las cuerdas vocales).

Existen múltiples teorías sobre la mecánica vocal (Le Huche y Allali, 2004). Las más aceptadas son aquellas que establecen que para que se produzca la fonación se precisa el acercamiento entre sí de las cuerdas vocales. Quilis (1997), basándose en los estudios del fonetista danés Svend Smith, expone que cuando se va a iniciar la fonación la glotis se cierra. Entonces el aire presiona contra los lados de la tráquea y contra la glotis, separando sus bordes y dejando salir una determinada cantidad de aire entre las cuerdas vocales, las cuales se aproximan nuevamente por su parte inferior (debido a su elasticidad interior) y llegando a cerrar la glotis de nuevo. Esta oclusión se desplaza hacia lo alto, repitiéndose este mismo movimiento una y otra vez: pequeñas masas de aire pasan una detrás de otra a través de la glotis, desplazando su punto de oclusión de abajo hacia arriba, a medida que la presión del aire infraglótico tiende a separar las cuerdas vocales, que se cierran nuevamente después del paso de cada pequeña cantidad de aire.



[Ilustración 2. Aparato fonador]

Esta salida interrumpida, debida a los reiterados cierres y aberturas de la glotis y a la tensión de las cuerdas vocales, es lo que origina las vibraciones de aire de la misma frecuencia fundamental que los cierres y abertura de la glotis. Así la vibración de las cuerdas vocales (cierre y abertura sucesivos) es la que produce las vibraciones del aire, las cuales, a su vez, originan la frecuencia fundamental de la onda sonora (efecto conjuntado de la presión infraglótica y la tensión de las cuerdas vocales).

Según Quilis (1997) el comportamiento de las cuerdas vocales produce la primera clasificación de los sonidos articulados: si las cuerdas vocales vibran los sonidos son sonoros, como las vocales y algunas consonantes (b, d, g, m, etc.); si no vibran los sonidos son sordos (s, f, x, etc.). Al pasar la corriente de aire por la zona laríngea (vibrando o no, según haya sido la actuación de las cuerdas vocales) entra en la laringofaringe y luego en la faringe oral, donde se va a producir otra gran división de los sonidos, según la acción del velo del paladar, pudiéndose producir los sonidos

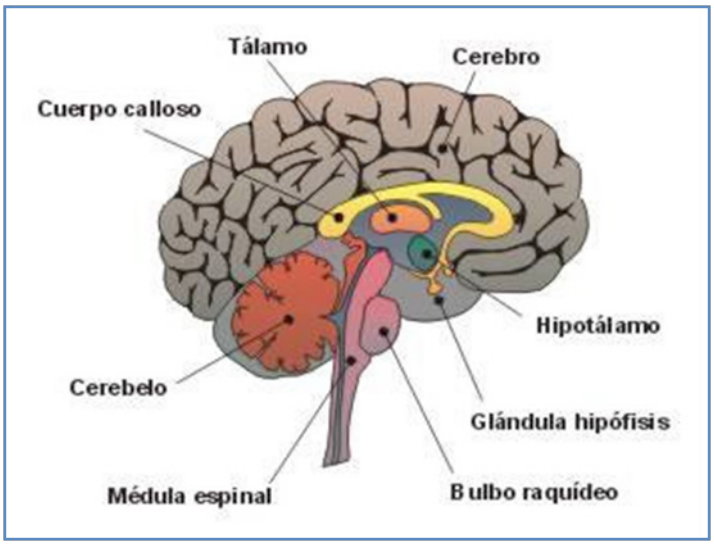
articulados orales (velo del paladar adherido a la pared faríngea) o los sonidos consonánticos nasales (velo del paladar desciende de la pared faríngea y cierre de la cavidad bucal).

En definitiva, el sonido al pasar por los resonadores acústicos de la cavidad supraglótica (cavidad oral, cavidad labial y cavidad nasal; correspondientes a la garganta, los labios y la nariz respectivamente) puede sufrir diferentes cambios de acuerdo a la forma que adopten el velo del paladar, la lengua y los labios.

1.2. CONTROL DE LA FONACIÓN POR EL SISTEMA NERVIOSO CENTRAL

Un primer control del aparato fonador se produce a nivel de la corteza cerebral, en las áreas motoras y premotoras de los actos volutivos. Como expone Blasco (2006) en su manual de técnica vocal, la corteza cerebral comprende la iniciativa motriz de la actividad muscular fonatoria y el control de las reacciones afectivas. Un segundo control se produce a nivel del diencéfalo (tálamo e hipotálamo), lo que da a la voz el carácter afectivo y las repercusiones que tienen sobre ella los diferentes estados de ánimo. En concreto el tálamo recibe las impresiones corporales, estableciendo la tonalidad afectiva, agradable o desagradable de las sensaciones. A nivel del bulbo raquídeo se asientan los núcleos de los pares craneales motores o sensitivos implicados en la fonación. Parece ser que el bulbo interviene en el mantenimiento del tono general y del tono laríngeo en particular.

Y por último, a nivel cerebelo se controlan los movimientos finos musculares y su coordinación en el espacio. El cerebelo desempeña una función importante en el mantenimiento del tono muscular y un influjo regulador sobre los movimientos de los músculos vocales (Blasco, 2006).



[Ilustración 3. Partes del Sistema Nervioso Central]

Los estudios sobre el control de la fonación se han basado principalmente en el seguimiento de pacientes con lesiones cerebrales. Así, diversos estudios muestran que una lesión en el hemisferio derecho (HD) en pacientes diestros puede provocar alteraciones de la comunicación verbal. Dichos déficit pueden interferir, de manera

diferencial, en la prosodia, el procesamiento semántico de las palabras y/o en las habilidades discursivas y pragmáticas (Joanette et al., 2008).

2. PROSODIA Y TIPOS DE PROSODIA

Partiendo de que cualquier enunciado verbal posee una figura tonal propia, la prosodia sería el componente del lenguaje referido al procesamiento cognitivo necesario para comprender o expresar intenciones comunicativas, usando diversos aspectos del habla como las variaciones en la entonación, las pausas o las modulaciones de la intensidad de la voz (Joanette et al., 2008).

El concepto de prosodia trata la manifestación concreta en la producción de las palabras observada desde un punto de vista fonético-acústico, considerando aspectos suprasegmentales que afectan a la entonación de la frase en su conjunto y aspectos o fenómenos locales de coarticulación y acentuación controlados por la melodía. La prosodia se genera mediante sistemas basados en reglas, obtenidas a partir de estudios lingüísticos que posteriormente evolucionan en base a la experiencia del individuo hasta conseguir un habla sintética aceptable, modificando variables personales como la entonación o evolución de la frecuencia fundamental, el ritmo o duración y localización de los diferentes signos de síntesis (Cantero, 2002; González y Romero, 2002).

El análisis de prosodia se basa por tanto en el estudio de la melodía del habla producida principalmente por las variaciones del ritmo, tono y énfasis que se producen cuando hablamos.

Algunos autores hablan de 4 tipos diferentes de prosodia (Monrad-Krohn, 1947):

- Prosodia intelectual.
- Prosodia intrínseca.
- Prosodia inarticulada.
- Prosodia emocional.

La prosodia intelectual se refiere al uso de sutilezas de la entonación para resaltar o enfatizar algunos aspectos del mensaje. Así ante la frase “él es hábil” yo puedo enfatizar la habilidad (“él ES hábil”), el atributo del individuo respecto a otros (“ÉL es hábil”) o darle cierto tono sarcástico (él es HÁBIL”).

La prosodia intrínseca consiste en ciertos patrones melódicos que determinan diversas connotaciones semánticas. Así empleando las mismas palabras podemos diferenciar una afirmación (“él es hábil”) de una pregunta (“¿él es hábil?”).

La prosodia inarticulada estaría referida a aquellos “sonidos” que aportan información adicional a la comunicación como chistar, gruñir, jadear, etc.

Por último, la prosodia emocional estaría directamente relacionada con la comunicación de emociones. Para autores como Fernández-Abascal, Jiménez y Martín (2003) la prosodia emocional es el fenómeno consistente en introducir contenidos emocionales en el mensaje, los cuales a su vez son interpretados por el oyente, fiándose como vehículo de expresión de las emociones y contribuyendo por tanto a las funciones adaptativa, social y motivacional de éstas.

3. LA EMOCIÓN EN EL HABLA

3.1. EL ESTADO DE ÁNIMO A TRAVÉS DEL TONO DE VOZ

Las emociones afectan a la voz y esta afirmación ya fue apuntada por Darwin (1872) en su obra “La expresión de las emociones en el hombre y en los animales”. En este escrito Darwin ya hacía una descripción de cómo afectan las emociones al comportamiento y al lenguaje de los animales. Hoy sabemos que el tono de voz de una persona nos habla de su estado de ánimo, de su estado psicológico y de su salud mental. Incluso diversos estudios ponen de manifiesto la importancia que los psicoterapeutas le asignan a los aspectos no verbales de sus propias voces y a las de sus pacientes (Tomicic, Bauer, Matínez, Reinoso, y Guzmán, 2009).

Gracias a las características vocales de una persona nos percatamos de las emociones que está sintiendo, aun cuando no entendamos su idioma. Numerosos estudios constatan esta afirmación al identificar los sujetos la emoción sentida basándose solo en la percepción de una voz, ya sea leyendo números (Pfaff, 1954), pronunciando las letras del alfabeto (Davitz y Davitz 1959; Dusenbury y Knower, 1938), aumentando la relación señal/ruido mientras el sujeto lee las frases (Pollack, Rubenstein, y Horowitz, 1960) o eliminando el efecto del tono de voz y susurrando las letras (Knower, 1941).

Si a cualquier persona se le pregunta cómo se encuentra, en la mayoría de los casos dirá que “bien”. Esta respuesta se ha convertido en una fórmula convencional para saludarnos, pero detrás de las mismas palabras podemos detectar estados de ánimo bien distintos, y es que nuestras emociones pueden detectarse por nuestro tono de voz. Scherer (1982) afirma que en las características vocales el emisor nos brinda inconscientemente información extra sobre sus emociones. Lillian Glass (2003) llegó a establecer que entre un 60 y un 65% de las veces podemos detectar con éxito el estado emocional en que se encuentra un individuo por su tono de voz.

Por otro lado, Hughes, Bradley y Rhodes (2010), en un estudio sobre los cambios vocales y fisiológicos en respuesta al atractivo físico, encontraron que ambos sexos utilizan un tono de voz más bajo y muestran un mayor nivel de activación fisiológica cuando hablan con individuos atractivos del sexo opuesto.

3.2. ATRIBUCIÓN DE RASGOS FÍSICOS POR LAS CARACTERÍSTICAS DE LA VOZ

Cuando tratamos intencionadamente de descodificar lo que nos trasmite a través de la voz una persona se debe distinguir claramente entre una alteración pasajera y la voz constante de esa persona. En el primer caso estaríamos detectando aspectos del estado emocional de alguien en un momento dado; en el segundo caso podríamos obtener información de aspectos de su personalidad e incluso claves físicas.

Cuando escuchamos a una persona por vía telefónica de forma automática le atribuimos ciertos rasgos físicos, atractivos si es una voz modulada y menos atractivos cuando no lo es. Al ver físicamente a la persona tratamos de unir las apreciaciones físicas con la voz, provocando en ocasiones, como resultado, cierta desilusión. Un ejemplo de esto ocurre cuando escuchamos un programa de radio. Puede suceder que recordemos el timbre de voz del locutor, atribuyéndole ciertos

rasgos de personalidad y no lo relacionemos con su rostro. Las personas cuyo atractivo físico y vocal no coinciden pueden obtener más impresiones negativas que aquellos que poseen tanto un rostro como una voz considerados atractivos (Zuckerman y Sinicropi, 2011). Por todos son conocidas, en este sentido, las primeras impresiones que produjo en el jurado la cantante Susan Boyle cuando se presentó al programa de televisión Britain´s Got Talent[1].

3.3. LAS EMOCIONES Y LA VELOCIDAD EN EL HABLA

En cuanto a los componentes más relevantes del habla para detectar emociones, Scherer (1979) destaca el "pitch" o frecuencia fundamental, la duración y la calidad de la voz. Según Blondet (2006) la frecuencia fundamental, la melodía, el ritmo y la intensidad de la voz cambian con el estado emocional, evidenciando de manera inequívoca lo que el sujeto siente en ese momento.

Otros estudios realizados en diferentes países, como el de Banse y Scherer (1996), han puesto de manifiesto como las emociones afectan a la velocidad del habla. Así podríamos afirmar que las emociones de ira, alegría y miedo provocarían un incremento en la tasa de velocidad del habla. Por su parte, el aburrimiento, la tristeza, el pesar y el disgusto estarían caracterizados por una desaceleración de la velocidad.

Pero cuidado, diversos estudios han demostrado que existe una variación de los patrones acústicos que caracterizan cada emoción dependiendo del idioma y de la cultura en la que nos encontremos (Muñoz y Jiménez, 1990).

En resumen, diversas investigaciones ponen de manifiesto que el estudio de los parámetros acústicos y de la velocidad del habla es útil para diferenciar y codificar emociones como la ira, la alegría y la tristeza. Pero más que existir una variable acústica que caracterice cada emoción, lo que realmente existe es un conjunto de variables que se coordinan de una forma determinada para caracterizar cada tipo de emoción. Una variable acústica a considerar es la duración de las sílabas (tanto promedio como interna), debido a que los distintos patrones de duración de las sílabas finales de un enunciado permiten distinguir algunas de las emociones.

3.4. EL PITCH

El pitch es la frecuencia fundamental (f0) a la cual vibran las cuerdas vocales. Esta frecuencia fundamental es uno de los principales componentes de la voz que nos da información sobre las emociones. El pitch presenta tres características interesantes de analizar (Ortego, 2009):

- Su valor medio, ya que refleja el nivel de excitación del locutor (un valor medio elevado indicaría un mayor grado de excitación).

1 A sus 47 años Susan Boyle sorprende al jurado con su actuación en la tercera temporada del programa británico de televisión Britain´s Got Talent, cantando I Dreamed a Dream (Soñe un sueño) de Los Miserables. Antes de que ella cantara, el público y los jueces, basándose en su apariencia, parecían expresar escepticismo sobre su capacidad para cantar. En cambio su voz fue tan destacada que recibió de inmediato la ovación de la audiencia, atrayendo para sí los votos de los jueces.

- Su rango o distancia entre su valor máximo y mínimo. El rango indica también el grado de exaltación del hablante (un rango más amplio que el normal reflejaría excitación emocional o psicológica).
- Sus fluctuaciones o velocidad de las fluctuaciones entre valores altos y bajos y si son abruptas o suaves (en general es abrupta para las emociones negativas como miedo e ira y suave para la emoción positiva de alegría).

3.5. LA DURACIÓN

La duración sería la componente prosódica definida por la velocidad del habla y por la situación de los acentos, cuyos efectos serían el ritmo y la velocidad del habla.

Para el reconocimiento de emociones, en base a la duración, se pueden distinguir una serie de parámetros:

- Velocidad de locución. Así generalmente un emisor excitado acortará la duración de las sílabas, por lo que la velocidad de locución (sílabas o palabras por segundo) se incrementará.
- Número de pausas y su duración. Un emisor eufórico tenderá a hablar rápidamente haciendo menos pausas y siendo estas más cortas; sin embargo un emisor deprimido hablará más lentamente e introducirá pausas más largas.
- Cociente entre el tiempo de locución y el de pausas. Esta medida relacionaría las dos variables anteriores.

3.6. LA CALIDAD DE LA VOZ

Algunas de las principales características que diferenciarían la calidad de la voz serían las siguientes:

- La intensidad, que estaría relacionada con el volumen y se reflejaría en la amplitud de la forma de la onda.
- Las irregularidades vocales, que abarcarían un gran rango de características vocales como la aparición del jitter vocal en la emoción de ira (refleja las fluctuaciones de un pulso de la glotis al siguiente) o la desaparición de voz en algunas emociones como la pena (el habla se convierte en un susurro).
- El cociente entre energía de alta y baja frecuencia, que mostraría como una alta concentración de energía en las frecuencias altas se asociaría con agitación (enfado, ira), mientras que una baja concentración de energía en las frecuencias altas se relacionaría con calma (depresión, pena).
- El breathiness y la langerización, que reflejarían las características del tracto vocal y estarían más relacionadas con la personalidad de cada voz. El breathiness describiría la generación de ruido respiratorio de forma que la componente fundamental tendería a ser más fuerte, mientras que las frecuencias altas serían reemplazadas por ruido aspiratorio. La langerización se definiría por una

vibración aperiódica de las cuerdas vocales, con un pulso de glotis estrecho y pitch bajo, lo que se traduciría en una voz chillona.

3.7. INFORMACIÓN VISUAL E INFORMACIÓN ACÚSTICA RECIBIDA

La percepción de una emoción por la voz se puede ver modificada por la información que se recibe por otros canales como el visual. En diversos experimentos, llevados a cabo en este sentido, se ha puesto de manifiesto como la disponibilidad de información visual modifica la percepción de la información acústica recibida, pudiendo concluir que el producto del proceso de percepción audiovisual es una correlación del procesamiento de las informaciónes visual y sonora (Martínez, Rojas, y Suárez, 2013).

En ese proceso de percepción audiovisual en ocasiones la información que fluye por ambos canales puede ser contradictoria. Así, mediante el tono de voz se puede fingir determinada emoción sin que exista correlación con la información visual que se genera. Valgan como ejemplo las declaraciones que en el año 2002 hizo Annamaría Franzoni tras el asesinato de su hijo de tres años, Samuele Lorenzi; caso que tuvo una importante cobertura de medios, principalmente debido a las muchas entrevistas de televisión concedidas por Franzoni inmediatamente después del crimen[2].

[Ilustración 4. Annamaría Franzoni en una de sus apariciones en TV]

En dichas declaraciones se apreciaba claramente un tono de voz muy triste, simulando el llanto, mientras que la expresión de su rostro no daba muestras de mucha tristeza. Pero su puesta en escena, unida a la ayuda de su familia que contrató a un reputado abogado y movilizó a la opinión pública, más la ayuda de periodistas, juristas y personajes de la vida pública italiana, consiguió que quedara en libertad. El caso se prolongó y no fue hasta mayo de 2008 cuando la Corte Suprema la reconoció como culpable del crimen de su propio hijo[3].

2 A este respecto puede consultarse en internet el vídeo “10 anni di cronaca. Annamaria Franzioni e il delitto di Cogne” en http://www.youtube.com/watch?v=hBHRMtiiVSU

3 Para una descripción detallada del caso y la inicial puesta en libertad de la madre de Samuele, véase el artículo de Lola Galán en el País, de fecha 2 de abril de 2002.

3.8. EL SIGNIFICADO DE LA VOZ GRAVE

Constantemente estamos oyendo malas noticias en todos los telediarios ¿alguna vez nos hemos fijado en como el tono de voz del presentador de turno se vuelve más grave en ese momento? Pensemos en noticias impactantes y de cierta repercusión, como un accidente de tren o de avión donde han fallecido muchas personas. Los presentadores de televisión no son ajenos al ámbito de las emociones y, sin quererlo, a través de sus tonos de voz más graves en ese momento nos transmiten su malestar por el suceso, nos transmiten que el tema les afecta. En definitiva, la voz de una persona se hace más grave cuando habla de un tema que le deprime, que le entristece o que trata de ocultar porque le afecta (disimulo).

También la voz grave se asocia a una voz más varonil y en la información radiofónica, por ejemplo, no se tolera bajo ningún concepto una voz aguda de hombre. Al menos esa es una de las conclusiones a las que se ha llegado en algunos estudios comparativos sobre las preferencias por una voz masculina o femenina en los informativos radiofónicos (Rodero, 2001). Según la autora, el tono de voz grave resulta una cualidad determinante para que la voz de un hombre nos agrade, pero no lo es para las voces femeninas que trabajan en los medios, donde los sujetos experimentales no se mostraron tan radicales respecto a dichas voces (no las tachaban de desagradables pero sí de inconvenientes para la información radiofónica). Además, la voz grave masculina se asociaba siempre con perfiles masculinos físicos y psicológicos positivos: mayor belleza, heroicidad, galantería, seguridad, etc. Sin embargo las voces masculinas más agudas no se toleraban en dicho estudio, de la misma manera que tampoco presentaban una imagen social favorable. Las voces agudas masculinas, al ser más propias de voces femeninas e infantiles, tendemos a juzgarlas como afeminadas o aniñadas, asociando dicha voz a perfiles masculinos poco favorables.

También la voz grave transmite más seguridad que una voz más aguda, quizás por ello Magaret Thatcher, en su primera etapa como primera dama, educó su voz para evitar tonos muy agudos y transmitir así mayor sensación de seguridad. “Su voz, según es conocido, era muy aguda y hubo que convencerla para rebajar su estridor con participación de un logopeda”, recuerda uno de los asesores políticos de la Dama de Hierro[4].

[Ilustración 5. Margaret Thatcher en una conferencia de prensa en su primera etapa como primera dama.]

4 **Ferdinand Mount**, escritor de la mejor progenie británica y asesor político de Thatcher.

Otros autores afirman que la voz grave es empleada en la seducción para simular y suscitar deseo. Cyr (2005) señala que cuando una persona está excitada sexualmente su voz se hace más grave y que los seductores utilizan deliberadamente una voz más grave para simular y suscitar deseo.

En otros estudios se sugiere que algunos rasgos vocales asociados a la testosterona influyen en la mejora de las posibilidades de los hombres de encontrar pareja. Una voz sana y cuidada mejoraría nuestras relaciones interpersonales y nos ayudaría a reforzar nuestro desempeño profesional (Puts, Jones, y DeBruine, 2012).

4. LA VOZ Y LA MENTIRA

4.1. VARIACIONES EN LA INTENSIDAD DE LA VOZ

Todos sabemos que subir el volumen de nuestra voz puede ser una estrategia para llamar la atención en un momento dado. El volumen de voz aumenta cuando un individuo siente miedo, excitación o rabia[5]. Un volumen de voz alto sería un buen indicador del nivel de energía de una persona en un momento dado. Para algunos autores las personas que hablan siempre con un volumen de voz muy alto se ajustarían a un tipo de personalidad colérica y hostil (Glass, 2003).

Si subir el volumen de voz puede servirnos para captar la atención, bajarlo puede ser una manera de minimizar la importancia que se quiere dar a un tema concreto, o de tratar un tema sobre el que no se quiere llamar la atención, ya que lo que interesa es que pase desapercibido. En este sentido Dimitrus y Mazzarella (1999) afirman que bajar el volumen de voz podría ser en algunos casos un indicio de mentira.

4.2. LA VELOCIDAD EN EL HABLA

Cada uno de nosotros hablamos siguiendo un patrón más o menos constante, siguiendo un determinado ritmo. Este ritmo al hablar es diferente de unas personas a otras. Hay personas capaces de generar multitud de ideas sobre un tema, como si su mente prodigiosa se llenara rápidamente de argumentos, frases e ideas y las intentara evacuar lo antes posible para no perder información. Estas personas tienen un ritmo de habla mayor que el de las personas normales. Sin embargo, indistintamente de nuestro ritmo habitual, cuando nos ponemos nerviosos ese ritmo puede volverse más lento y pueden producirse más errores en el habla. Ello sería debido principalmente al mayor esfuerzo mental que tenemos que realizar para controlar lo que se dice cuando estamos nerviosos. Según Cyr (2005) una disminución en el ritmo del habla podría estar asociada a estados de cansancio, confusión, tristeza y desinterés y, en algunas personas, ser un indicio de mentira (cuando alguien ralentiza de repente su discurso porque mide sus palabras o está buscando un pretexto para no decir la verdad).

5 En este sentido puede visionarse un vídeo del reciente caso Bretón, donde el acusado da claras muestras de excitación y rabia a través de su voz, en http://www.youtube.com/user/Analistanoverbal

Para otros autores como Martínez Selva (2005), el miedo a ser pillado en una flagrante mentira y el apresurarse a explicarse antes de que el otro se enfade puede incitar al mentiroso a hablar más deprisa. Así, cuando el individuo se pone nervioso puede que su ritmo de habla aumente, por ejemplo por la mayor afluencia de ideas que trata de manifestar intentando defenderse. También el aumento del ritmo del habla podría deberse a que el individuo siente ira, miedo, impaciencia, excitación o porque lo que dice es una repetición de lo dicho anteriormente (Cyr, 2005).

Por si fuera poco, respecto a la ralentización o aceleración del discurso, algunos autores como Vrij (2000) han constatado que la velocidad del habla no tendría relación con el engaño.

Concluyendo, el aumento o disminución en el ritmo del habla como indicio de mentira no ha recibido apoyo claro de las investigaciones puesto que se han hallado resultados contradictorios.

4.3. LATENCIA DE RESPUESTA

Siguiendo el mismo principio del mayor esfuerzo mental que tenemos que realizar para controlar lo que decimos, el tiempo que tardamos en comenzar a hablar, cuando nos plantean determinada pregunta comprometedora, también sería mayor que ante una pregunta neutra. Ello podría ser indicio de intento de engaño, ya que lo que se pretende es ganar tiempo para preparar una respuesta coherente con la línea a seguir y no entrar en contradicciones con lo dicho anteriormente. En este sentido Walters (2003) afirma que cuando una persona miente la demora en la respuesta es mayor que la demora media de una persona que no miente. Pero habría que tener muy en cuenta si esa persona es poco elocuente y habitualmente duda antes de pronunciarse sobre algo, es decir, comparar su latencia de respuesta con su latencia habitual, comparando la respuesta a una pregunta clave con la línea basal de comportamiento. Todo ello sin perjuicio de tener en cuenta situaciones anómalas, como el hecho de estar bajo los efectos de determinadas drogas o medicamentos, que puedan inducir o provocar que aumente la latencia de respuesta.

Vrij, Edward, Roberts y Bull (2000), en un estudio sobre la detección del engaño a través de la conducta verbal y no verbal, encontraron que los mentirosos presentaban más disturbios en el habla (ah) y esperaban más tiempo antes de dar una respuesta, en comparación con los que decían la verdad (además de realizar menos ilustradores y llevar a cabo menos movimientos con las manos y los dedos).

Esa latencia de respuesta dilatada, como intento de ganar tiempo, puede ser ocupada por interjecciones y expresiones del tipo “eeh”, “um”, “esto…”, “bueno…”, etc., o repitiendo la pregunta planteada antes de contestar (Vrij, 2008).

Por otra parte, si el individuo intuye o conoce de antemano la pregunta que le van a plantear y se ha preparado bien la respuesta, esta latencia será menor y el ritmo de habla se acelerará al contestarla.

Por tanto, cualquier variación sobre la latencia de respuesta que se produzca ante una pregunta comprometedora podría hacernos pensar en la hipótesis del engaño, basada bien en la aparición de carga cognitiva asociada a la mentira, que dilatará la latencia, bien por tener preparada la respuesta de antemano, que acortará la latencia.

Así, otros estudios indican que si ante una pregunta comprometedora la latencia es mayor o menor que ante preguntas neutras, podríamos plantear la hipótesis de que esa persona está a punto de mentirnos o que trata de eludir la respuesta (Sheridan y Flowers, 2010).

4.4. LAS PAUSAS

Anolli y Ciceri (1997), en un estudio sobre las estrategias vocales de mentirosos ingenuos y expertos, encontraron que el engaño provocó en los sujetos un incremento en F0, un mayor número de pausas y palabras y unos índices de locuacidad y fluidez superiores; también encontraron que cuando los mentirosos hacían esfuerzos por controlar su voz daban muestras de un tono sobrecontrolado o carente de control (fugas).

Pero también una persona exaltada tenderá a hablar rápidamente con menos pausas y más cortas, mientras que una persona deprimida hablará más lentamente, introduciendo pausas más largas.

4.5. LA VOZ AGUDA

Cuando alguien está viviendo una situación de estrés es probable que su cuerpo y su rostro den muestras de tensión o nerviosismo y que incluso su voz suene también tensa. Sabemos que en situaciones de emociones intensas el tono de voz de una persona se vuelve más agudo, ya que se eleva su frecuencia fundamental (f0). Ello es debido a que esa mayor intensidad emocional provoca un aumento en la tensión de las cuerdas vocales (los músculos de la laringe se contraen), por lo que los sonidos que emitimos serán más agudos. En este sentido, DePaulo, Lindsay, Malone, Muhlenbruck, Charlton y Cooper (2003), en su exhaustivo meta-análisis sobre indicadores verbales y no verbales del engaño, concluyeron que la voz del mentiroso suena más tensa y su frecuencia fundamental es más aguda que la del que dice la verdad.

En general la voz se agudiza cuando sentimos estrés, nerviosismo, excitación, frustración o ira. Como algunas de estas emociones aparecen cuando se miente, la voz aguda se asocia a menudo a la mentira (Cyr, 2005; Martínez Selva, 2005).

Este hecho es bastante conocido a nivel popular. Según Alderd Vrij (2008) la creencia popular de que al mentir se habla con un tono de voz más agudo es acertada (al igual que la de que las pausas al hablar son de mayor duración al mentir que al decir la verdad).

4.6. EL TARTAMUDEO

Cuando alguien, sin problemas de tartamudez, intenta hablar demasiado rápido porque al mismo tiempo quiere expresar todas las ideas que afloran en su mente en un momento puntual, puede que comience a tartamudear. Alguien que intenta engañar puede sufrir este fenómeno cuando le sorprendemos con preguntas inesperadas. Ante dichas preguntas la primera respuesta que tiende a salir es la verdad, si bien el mentiroso deberá controlar esa respuesta y elegir otra adecuada a su mentira y que no se contradiga con la información contextual, ni con la información enunciada por él en momentos anteriores. Esto supone el acceso no solo a la memoria de trabajo, sino también a la

memoria a largo plazo, unido a tener que elegir entre multitud de respuestas posibles. El comportamiento asociado a este proceso bien podría ser el tartamudeo o la duda en el inicio de la respuesta (Walczyk, Roper, Seemann, y Humphrey, 2003).

En este sentido todos recordamos las declaraciones de Bill Clinton ante el Senado por el caso de Mónica Lewinsky y sus tartamudeos antes de contestar a algunas preguntas, declaraciones que fueron también analizadas por la comunidad científica (Upchurch y O'Connell, 2000)[6].

4.7. EL BALBUCEO

El balbuceo consiste en hablar o leer con una pronunciación vacilante o entrecortada. Cuando tenemos dudas de lo que vamos a decir y comenzamos a hablar, antes de haber decidido qué decir, puede que balbuceemos. Por decirlo de alguna forma, sería como una especie de censura que trata de evitar que cometamos un error y retenemos lo que vamos a decir en el último momento. Este fenómeno puede aparecer en personas que mienten, cuando se les va a escapar algo que puede perjudicarles.

En este sentido, DePaulo y colaboradores (2003) llegaron a la conclusión de que el mentiroso se muestra más inseguro y vacilante en su voz y en sus palabras que el que dice la verdad.

Podríamos decir, por tanto, que el balbuceo es un comportamiento análogo al anteriormente descrito que aflora ante el mismo proceso psicológico asociado con el acto de mentir.

4.8. LOS ERRORES DEL HABLA

Todos podemos cometer errores al articular determinadas palabras cuando estamos cansados. También conocemos los efectos en este sentido de determinadas drogas como el alcohol o determinados medicamentos (ansiolíticos, tranquilizantes, etc.).

Pero cuando una persona se ve desbordada por múltiples ideas, que trata de expresar en un momento dado, es probable que cometa errores de articulación a la hora de exponerlas. En este tipo de situaciones nuestro cerebro demanda excesivo esfuerzo, al estar evaluando una situación, pensando en el comentario que nos acaban de hacer, en qué voy a responder y en cómo voy a decirlo. El mentiroso en algunas ocasiones, ante determinadas preguntas (por ejemplo ante una pregunta directa e inesperada), debe hacer un esfuerzo extra que puede provocarle errores a la hora de articular las palabras a emplear, lo que podría ser indicio de mentira; pero en muchas ocasiones tendrá preparado su relato y cometerá incluso menos errores que la persona que no miente.

Por tanto, debemos establecer claramente la diferencia entre errores en el habla de los errores contenidos en el relato. Los primeros pueden ser fruto del proceso psicológico expuesto anteriormente y ser indicadores de mentira. Los segundos serán fruto de la manera normal que tenemos de contar un relato. Cuando contamos un relato verídico es habitual que este vaya plagado de imperfecciones (olvidos, desestructuración, detalles raros, etc.),

6 Vídeo del testimonio completo de Bill Clinton ante el Gran Jurado en http://www.youtube.com/watch?v=fdChg4P1wWY

tal y como muestra el protocolo elaborado por Trankell (1982). Curiosamente el discurso del mentiroso estará exento de estos errores y será extrañamente perfecto.

Por todo ello sería una creencia errónea pensar que los mentirosos comenten más errores que los que dicen la verdad.

4.9. LAS REPETICIONES EN EL HABLA

Cuando un tema nos preocupa, y es tan importante para nosotros que ocupa constantemente nuestra mente, es probable que al hablar repitamos determinadas frases o palabras. En este sentido, el estrés y la ansiedad pueden hacer que en un momento dado no pensemos con claridad y aparezcan estas repeticiones.

Sin embargo no por ello debemos pensar que el individuo miente. En este sentido un aspecto a tener en cuenta es que una persona inocente también estará preocupada porque se esclarezca su inocencia.

4.10. FRASES SIN FINALIZAR Y OMISIÓN DE PALABRAS

En ocasiones, cuando una persona presenta determinados tabúes y no quiere pronunciar palabras que le avergüenzan (o valora que no es apropiado emplear determinada palabra en ese ámbito) suprime esa palabra y deja la frase sin finalizar (ej. “le pegó una…”).

Más interesante parece la omisión de palabras en una determinada frase que suele cometerse tras valorar el individuo que dicha elección no le beneficiaría, por lo que buscará una más suave o adecuada al contexto en el que se encuentra (“le exi… pedí que lo hiciera”). En este caso la persona no omite totalmente la palabra sino que comienza a pronunciarla, se para y continúa la frase con una palabra políticamente más correcta.

En el caso del mentiroso, la verdad tiende a salir y este debe inhibirla sustituyéndola por otra, pero en ocasiones este mecanismo no evita que verbalmente la verdad se abra paso pronunciando una parte de una palabra e incluso una o varias palabras completas. El mentiroso al darse cuenta rectificará y sustituirá el final de la palabra y/o frase. Esto vendría a corroborar los planteamientos de Walzick (2003).

Esta omisión podría ser fruto también de la necesidad que tiene el mentiroso de generar un distanciamiento con el hecho. En este sentido DePaulo et al. (2003) llegaron a la conclusión de que los mentirosos responden de manera menos directa y clara y hacen uso de más evasivas y respuestas impersonales que los que dicen la verdad.

4.11. CREENCIAS Y VERDADES SOBRE LA DETECCIÓN DEL ENGAÑO A TRAVÉS DE LA VOZ

¿En qué medida son acertadas las creencias que las personas tienen acerca de las señales de engaño relacionadas con la voz? Una buena respuesta a esta pregunta fue la recogida por Vrij (2000), el cual comparó las creencias que las personas tienen acerca de las señales de engaño con el comportamiento real de los mentirosos y el habla. En lo relativo al habla, un resumen de las conclusiones a las que llegó el autor

está reflejado en la siguiente tabla, en la cual se recogen los indicadores reales (aquellos que se presentan en situaciones de mentira y verdad) y los indicadores subjetivos (aquellos que la gente piensa que se presentan en situaciones de verdad y mentira).

Como se puede observar, en la primera columna, "tipo de indicador", se muestran los posibles indicadores vocales de engaño. En la segunda columna se exponen los «indicadores objetivos de engaño», etiquetados según sean mostrados por los mentirosos con una mayor frecuencia (>) que por los que dicen la verdad, por una menor frecuencia (<) o si no tienen relación con el engaño (-). En la tercera columna de la tabla se presentan los «indicadores subjetivos de engaño «, etiquetados con el correspondiente signo en función de si creían los observadores que los mentirosos muestran la señal con menos frecuencia que los que dicen la verdad (<), con más frecuencia (>) o si los observadores no asociaban ese indicador con el engaño (-).

Para Vrij sólo el tono de voz más agudo, la latencia y la duración de las pausas tendrían relación con el engaño.

Tipo de indicador (señales vocales)	Indicadores objetivos (reales)	Indicadores subjetivos (creencias)
Dudas	-	>
Errores del habla	-	>
Tono de voz agudo	>	>
Índice de velocidad	-	-
Periodo de latencia	>	-
Duración de las pausas	>	-
Frecuencia de las pausas	-	>

5. CONCLUSIONES

Los efectos de las emociones en la voz, y sus posibles aplicaciones, han sido motivo de estudio en los últimos años. Existen componentes del habla como la frecuencia fundamental, la duración y la calidad de la voz que son importantes para identificar emociones. La voz de una persona se hace más grave cuando habla de un tema que le deprime o que le entristece y se asocia a una voz más varonil, así como a perfiles masculinos positivos de belleza, heroicidad, seguridad o seducción. El volumen de voz aumenta cuando un individuo siente miedo, excitación o rabia.

Ahora bien, en lo relativo a la aplicación de estos indicadores en el ámbito de la detección del engaño, el avance ha sido mínimo. Algunos autores afirman que bajar el volumen de voz podría ser un indicio de mentira, o al menos de inseguridad en lo que se dice, si bien no existe investigación empírica suficiente para hacer esta afirmación con seguridad. Diversos estudios han puesto de manifiesto que la voz del mentiroso suena más tensa y su frecuencia fundamental es más aguda que la del que dice la verdad, pero tampoco se ofrecen resultados contundentes. Por otro lado, el aumento o disminución en el ritmo del habla como indicio de mentira no ha recibido apoyo claro de las investigaciones puesto que se han hallado resultados contradictorios. Las disfunciones verbales como balbuceos, tartamudeos, pausas prolongadas, omisión de palabras y errores en la articulación pueden denotar confusión mental y falta de claridad, pero solo la mayor duración de las pausas y la aparición de balbuceos

tendrían vinculación con el engaño. Respecto al resto de disfunciones verbales no existe investigación al respecto que las vincule a la mentira.

Quizá los datos más esperanzadores vengan de la mano de la latencia de respuesta. Si ésta, ante una pregunta comprometedora, es mayor o menor que ante preguntas neutras podríamos plantear la hipótesis de que esa persona está a punto de mentirnos o que trata de eludir la respuesta (Sheridan y Flowers, 2010).

La falta de resultados de investigación claros, en lo relativo a indicadores de mentira a través del habla, está en consonancia con los resultados obtenidos para el resto de indicadores no verbales. Esto va unido a los planteamientos de investigación dominantes hasta hace escasos años, en los cuales predominaba la búsqueda de indicadores patognomónicos de la mentira, es decir, la búsqueda de conductas espontáneas generadas por los mentirosos. Estos planteamientos obtuvieron indicadores con tasas de acierto que mínimamente superaban el azar.

Ha sido a partir del año 2008 cuando la investigación da un giro radical y comienzan a aparecer planteamientos que cuestionan la espontaneidad de los comportamientos.

Son planteamientos que no dudan de los indicadores, sino de su aparición espontanea. Se comienza, entonces, a establecer la necesidad de una participación activa del entrevistador que genere la aparición de los indicadores. Sabiendo qué preguntar, cómo preguntar, cuándo preguntar y utilizando diferentes técnicas, los índices de acierto se disparan llegando a cifras incluso cercanas al 100% de acierto en la detección de veracidad.

Aún está por verse el alcance que este giro, en el ámbito científico de la detección del engaño, producirá sobre la aparición de nuevos estudios en los cuales se analicen indicadores de mentira en el habla ante determinadas preguntas bien realizadas en contenido, forma y tiempo.

BIBLIOGRAFÍA

Anolli, L., y Ciceri, R. (1997). The voice of deception: Vocal strategies of naïve and able liars. Journal of Nonverbal Behavior, 21(4), 259-284.

Banse, R, y Scherer, K. R. (1996). Acoustic profiles in vocal emotion expression. Journal of Personality and Social Psychology, 70(3), 614-636.

Blasco, V. (2006). Manual de técnica vocal. Ejercicios prácticos. Ciudad Real: Ñaque.

Blondet, M. A. (2006). Variaciones de la velocidad de habla en español: Patrones fonéticos y estrategias fonológicas. Un estudio desde la producción. (Tesis doctoral). Mérida, Venezuela: Universidad de Los Andes.

Cantero, F. J. (2002). Teoría y análisis de la entonación. Barcelona: Universitat de Barcelona.

Cyr, M. F. (2005). ¿Verdad o mentira?: Los cuatro códigos para detectar el engaño. Barcelona: Paidós.

Darwin, C. (1872). The expression of the emotions in man and animals. New York: Appleton and Company.

Davitz, J. R., y Davitz, L. J. (1959). The communication of feelings by content-free speech. Journal of Communication, 9, 6-13.

DePaulo, B. M., Lindsay, J. J., Malone, B. E., Muhlenbruck, L., Charlton, K., y Cooper, H. (2003). Cues to deception. Psychological Bulletin, 129(1), 74-118.

Dimitrius, J. E., y Mazzarella, M. (1999). A primera vista: Un método para "leer" el comportamiento no verbal. Barcelona: Urano.

Dusenbury, D., y Knower, F. H. (1938). Experimental studies of the symbolism of action and voice. A study of the specificity of meaning in facial expression. Quaterly Journal of Speech, 24, 424-435.

Fernández, E., Jiménez, M. P., y Martín, M. D. (2003). Emoción y motivación: La adaptación humana. Madrid: Centro de Estudios Ramón Areces.

Glass, L. (2003). Sé lo que estás pensando: Utiliza los cuatro códigos del lenguaje corporal para mejorar tu vida. Barcelona: Paidós.

González, A., y Romero, C. (2002). Fonetica, entonacion y ortografia. Edelsa Grupo Didascalia, S.A.

Hughes, S., Farley, S., y Rhodes, B. (2010). Vocal and physiological changes in response to the physical attractiveness of conversational partners. Journal of Nonverbal Behavior, 34(3), 155-167.

Joanette, Y., Ansaldo, A. I., Kahlaoui, K., Côté, H., Abusamra, V., Ferreres, A., y Roch-Lecours, A. (2008). The impact of lesions in the right hemisphere on linguistic skills: Theoretical and clinical perspectives. Revista de Neurologia, 46(8), 481-488.

Knower, F. H. (1941). Analysis of some experimental variations of simulated vocal expressions of the emotions. Journal of Social Psychology, 14, 369-372.

Le Huche, F., y Allali, A. (2004). La voz. Anatomía y fisiología de la voz y del habla (Vol. 1). Barcelona: Masson.

Martínez, H., Rojas, D., y Suárez, F. (2012). Influencia de la información visual durante la percepción de la prosodia de las emociones actuadas. Estudios de Fonética Experimental, 163-193. Barcelona: Universitat de Barcelona.

Martínez, J. M. (2005). La psicología de la mentira. Barcelona: Paidós.

Monrad-Krohn, G. H. (1947). Dysprosody or altered melody of language. Brain, 70(Pt 4), 405-415.

Muñoz, C., y Jiménez, A. (1990). La expresión de la emoción a través de la conducta vocal. Revista de psicología general y aplicada, 43(3), 289-299.

Ortego, C. (2009). Detección de emociones en voz espontánea. Madrid: Universidad Autónoma de Madrid. Departamento de Ingeniería Informática.

Pfaff, P. L. (1954). An experimental study of the communication of feeling without contextual material. Speech Monographs, 21, 155-156.

Pollack, I., Rubenstein, H., y Horowitz, A. (1960). Communication of verbal modes of expression. Language and Speech, 3, 121-130.

Puts, D. A., Jones, B. C., y DeBruine, L. M. (2012). Sexual selection on human faces and voices. Annual Review of Sex Research, 49(2-3), 227-243.

Quilis, A. (1997). Principios de fonología y fonética españolas. Madrid: Arco Libros.

Rodero, E. (2001). Los principales errores que debe evitar todo locutor de informativos radiofónicos: Un estudio práctico. En P. Martínez (Ed.), Reinventar la radio (pp. 307-315). Pamplona: Eunate.

Scherer, K. R. (1979). Personality markers in speech. In K. R. Scherer y H. Giles (Ed.), Social markers in speech (pp. 147-201). Cambridge: Cambridge University Press.

Scherer, K. R. (1982). Emotion as a process: Function, origin and regulation. Social Science Information, 21, 555-570.

Sheridan, M. R., y Flowers, K. A. (2010). Reaction Times and Deception - the Lying Constant. International Journal of Psychological Studies, 2(2).

Tomicic, A., Bauer, S., Martínez, C., Reinoso, A., y Guzmán, M. (2009). La voz como una herramienta psicoterapéutica: La perspectiva de los terapeutas. Revista Argentina de Clínica Psicológica, 18, 197-207.

Trankell, A. (1982). Reconstructing the past. Stockholm, Sweden: Norstedt & Söner.

Upchurch, C. M., y O'Connell, D. C. (2000). "Typical clinton: Brazen it out". Journal of Psycholinguistic Research, 29(4), 423-431.

Vrij, A. (2000). Detecting Lies and Deceit: The Psychology of Lying and Implications for Professional Practice. Chichester, United Kingdom: John Wiley & Sons.

Vrij, A. (2008). Detecting lies and deceit : Pitfalls and Opportunities (2nd ed.). Chichester, United Kingdom: John Wiley. & Sons.

Vrij, A., Edward, K., Roberts, K. P., y Bull, R. (2000). Detecting deceit via analysis of verbal and nonverbal behavior. Journal of Nonverbal Behavior, 24(4), 239-263.

Walczyk, J. J., Roper, K. S., Seemann, E., y Humphrey, A. M. (2003). Cognitive mechanisms underlying lying to questions: Response time as a cue to deception. Applied Cognitive Psychology, 17(7), 755-774.

Walters, S. B. (2003). Principles of kinesic interview and interrogation (2nd ed.). Boca Raton, Florida: CRC Press.

Zuckerman, M., y Sinicropi, V. (2011). When physical and vocal attractiveness differ: Effects on favorability of interpersonal impressions. Journal of Nonverbal Behavior, 35(2), 75-86.

REFERENCIAS FOTOGRAFÍAS

1- CUERPOHUMANO.INFO. El aparato fonador y sus partes (en línea). Disponible en http://www.cuerpohumano.info/2009/04/dibujos-del-aparato-fonador.html, (fecha de consulta: 20 Enero 2014)

2- WIKIPEDIA. Aparato fonador humano (en línea). Disponible en http://es.wikipedia.org/wiki/Se%C3%B1al_de_voz, (fecha de consulta: 20 Enero 2014)

3- MONOGRAFÍAS.COM. La función de relación I. El sistema nervioso humano (en línea). Disponible en http://www.monografias.com/trabajos89/funcion-relacion-i-sistema-nervioso-humano/funcion-relacion-i-sistema-nervioso-humano.shtml (fecha de consulta: 20 Enero 2014)

4- VANITY FAIR.it. Delitto di Cogne, Anna Maria Franzoni ammessa al lavoro esterno (en línea). Disponible en http://www.vanityfair.it/news/italia/13/10/10/delitto-cogne-franzoni-lavoro-fuori-dal-carcere (fecha de consulta: 20 Enero 2014)

5- DIARIOTEINTERSA.ES. Muere la dama de hierro. Las citas más célebres de Margaret Thatcher (en línea). Disponible en http://www.teinteresa.es/dinero/citas-celebres-Margaret-Thatcher_0_897511046.html (fecha de consulta: 20 Enero 2014)

Fecha de recepción: 23/05/2014. Fecha de aceptación: 24/06/2014

LA MUJER EXTRANJERA EN ESPAÑA Y LA VIOLENCIA DE GÉNERO

FRANCISCO MIGUEL RODRÍGUEZ RODRÍGUEZ

RESUMEN

La violencia de género es un problema de gran importancia en nuestro país y cuando se añade el factor extranjería relacionado con dicha violencia aún está poco tratado por la doctrina y todavía menos en cuanto a la labor e intervención estatal a través de las Fuerzas de Seguridad del Estado en la lucha contra la VG o el trabajo de los abogados especialistas en violencia de género, el Ministerio Fiscal y los Juzgados de Violencia de Género en la defensa de las víctimas.

La normativa europea[1] y la doctrina constitucional han incidido decisivamente para que el legislador español haya cambiado la normativa respecto a la mujer extranjera, en relación con las órdenes de expulsión por su condición de estancia irregular en el país, la denegación a la asistencia jurídica, también por esta condición de irregularidad, y la vulneración al derecho fundamental a la defensa del artículo 24 de nuestra Constitución.

Palabras clave: violencia de género, extranjería, abogados especialistas en violencia de género, Ministerio Fiscal, Juzgados de Violencia de Género.

ABSTRACT

Gender-based violence is a substantial problem in our country. When the key element of “immigration” is added in relation to violence, we are not able to find any help from the doctrine and even less from the State (through its Security Forces against this type of violence or from gender-based violence specialists), nor from the Public Prosecutor’s Office or either from the Gender-based Justice of the Peace Court for the protection of victims.

The European legislation and the constitutional doctrine have influenced in a decisive way on the Spanish legislator to change the regulations related to the immigrant woman concerning deportation orders because of their illegal residence in the country, as well as refusal of legal assistance -dued to the irregular residence- and infringement of the fundamental Right of Defence included in the Article 24 of the Constitution.

Key words: gender violence, immigration, Gender Violence attorneys, Prosecution, Courts of Domestic Violence.

1 Nuestro país ha ratificado el Convenio europeo contra la Violencia de Género, mediante el Instrumento de ratificación por el Reino de España, del Convenio del Consejo de Europa sobre prevención y lucha contra la violencia contra la mujer y la violencia doméstica, hecho en Estambul el 11 de mayo de 2011; publicado en el BOE Núm. 137 de fecha 6 de junio de 2014 Sec. I. Pág. 42946. El citado Convenio entra en vigor de forma general y para España el 1 de agosto de 2014, de conformidad con lo dispuesto en su artículo 75.

1. INTRODUCCIÓN

Las mujeres inmigrantes están más expuestas a la violencia, psíquica y física, ejercida por sus parejas o ex parejas de sexo masculino, bien a causa de su dependencia económica y legal, bien por factores culturales, porque las mujeres sin estatus legal están en una situación de mayor vulnerabilidad y esta aseveración es de aplicación en nuestro país[2].

La especial vulnerabilidad del colectivo de mujeres extranjeras frente a la violencia ha sido reconocida por diversos instrumentos internacionales: desde la exposición de motivos de la Declaración de Naciones Unidas sobre la eliminación de la violencia contra la mujer de 1993, que se declara «preocupada por el hecho de que algunos grupos de mujeres, como por ejemplo las inmigrantes, son particularmente vulnerables a la violencia», al apartado 116 de la IV Conferencia Mundial de Naciones Unidas sobre la Mujer, celebrada en Beijing, que indica que «algunos grupos de mujeres, como las mujeres que emigran, son también particularmente vulnerables a la violencia».

La primordial norma protectora de la mujer en el ámbito del maltrato existente en nuestro país, «la Ley Orgánica 1/2004, de 28 de diciembre, de Medidas de Protección Integral contra la Violencia de Género», define la violencia de género[3] como la violencia que, como manifestación de la discriminación, la situación de desigualdad y las relaciones de poder de los hombres sobre las mujeres, se ejerce sobre éstas por parte de quienes sean o hayan sido sus cónyuges o de quienes estén o hayan estado ligados a ellas por relaciones similares de afectividad, aun sin convivencia.

La definición, tal y como se halla enunciada, ha sido tomada de la IV Conferencia Mundial sobre el avance de las mujeres, celebrada en Pekín en 1995[4], en la que se

2 Vid., ampliamente sobre los factores condicionantes de la especial victimización de las mujeres de nacionalidad extranjera en España, ACALE SÁNCHEZ, M., «Tratamiento jurídico y social...», cit., págs. 206 y ss.; MOYA ESCUDERO, M., y RUIZ SUTIL, M., «La mujer extranjera...», cit., pág. 256; RODRÍGUEZ YAGÜE, C., «La mujer extranjera...», cit., págs. 146 y ss. Es de interés el informe de Amnistía Internacional sobre Mujeres Invisibles, abusos impunes. Mujeres inmigrantes indocumentadas en España ante la violencia de género en el ámbito familiar, de julio de 2003, disponible en la página web: http://www.malostratos.org/images/pdf/AI%20mujeres%20invisibles%20avisos%20impunes.pdf.

3 La expresión violencia de género también es definida en el art. 1 de la Declaración sobre la Eliminación de la Violencia contra la Mujer, Resolución de la Asamblea General ONU 48/104, de 20 de diciembre de 1993, donde se utiliza como concepto jurídico la violencia de género, definiéndola como «todo acto de violencia basado en la pertenencia al sexo femenino que tenga o pueda tener como resultado un daño o sufrimiento físico, sexual o psicológico para la mujer, así como las amenazas de tales actos, la coacción o la privación arbitraria de la libertad, tanto si se producen en la vida pública como en la vida privada».

4 En la actualidad la comunidad internacional ha reconocido que la violencia de género constituye una violación de los derechos humanos. Instrumentos internacionales fundamentales a este respecto son la Convención sobre Eliminación de todas las formas de Discriminación contra la Mujer, de 18 de diciembre de 1979; la Declaración de Naciones Unidas sobre la Eliminación de la Violencia sobre la Mujer, proclamada en 1993 por la Asamblea General con motivo de la Conferencia Mundial de los Derechos Humanos celebrada en Viena, y las Resoluciones de la IV Conferencia Mundial sobre las Mujeres, celebrada en Pekín en 1995, donde se obtuvo el reconocimiento de que cualquier forma de violencia que se ejerza contra las mujeres constituye una violación de los derechos humanos. También para el Consejo de Europa la lucha contra la violencia de género constituye una de sus prioridades, aprobando varias Recomendaciones, entre las que cabe destacar la Recomendación 2002/05 adoptada por el Comité de Ministros el 30 de abril de 2002 sobre la Protección de las mujeres contra la violencia. Por su parte el Parlamento Europeo promovió en

definió la violencia contra la mujer como «todo acto de violencia sexista que tiene como resultado posible o real un daño físico, sexual o psíquico, incluidas las amenazas, la coerción o la privación arbitraria de libertad, ya sea que ocurra en la vida pública o en la privada...».

En ambos casos (tanto en la Ley 1/2004, como en la IV Conferencia Mundial) se acoge todo tipo de violencia fruto de la desigualdad y así se pone de manifiesto en la citada Conferencia, en la que se sigue diciendo que «es una manifestación de las relaciones de poder históricamente desiguales entre hombres y mujeres, que han conducido a la dominación de la mujer por el hombre, la discriminación contra la mujer y a la interposición de obstáculos contra su pleno desarrollo».

La violencia de género en España y en otros países es un fenómeno que se da independientemente del grado de desarrollo del país en si y afecta a muchas mujeres de distintas clases sociales. El problema de la violencia de género es complejo y por tanto difícil de erradicar. Esta violencia se vincula al desequilibrio en las relaciones de poder en diferentes ámbitos, ya sea el social o el económico, y constituye un atentado contra el derecho a la vida, a la seguridad, a la libertad, a la dignidad y a la integridad física y psíquica de la víctima. A pesar de generar esta violencia un rechazo social, las víctimas por violencia de género se siguen produciendo.

Con el objetivo de combatir estos hechos, se ha aprobado en España la citada Ley Orgánica 1/2004, de 28 de diciembre, de Medidas de Protección Integral contra la Violencia de Género (en adelante LOIVG), con la finalidad de prevenir, sancionar y erradicar la violencia ejercida sobre las mujeres y prestar asistencia a las víctimas (importante apartado, fundamental para las mujeres maltratadas).

Los distintos organismos involucrados en la lucha contra la lacra de la violencia de género (con base a la LOIVG) han venido publicando su evolución en los últimos años, de ahí que se tengan datos fiables, como que el número de mujeres muertas a manos de su pareja o ex pareja, documentados mediante los datos proporcionados por los Informes del Observatorio Estatal de Violencia sobre la Mujer[5], cuya estadística más adelante se intentará reflejar, es mayor en la mujer extranjera, que es más maltratada y muere más que la española a manos de sus maltratadores, también extranjeros.

Si bien las mujeres españolas comparten con las extranjeras el riesgo a ser maltratadas o asesinadas por sus parejas o ex parejas, en los últimos diez años ha existido una sobre-exposición de estas últimas, ya que la proporción de mujeres extranjeras en España víctimas de violencia de género supone una sobre-representación respecto a

el año 1997 la Campaña de Tolerancia Cero frente a la violencia contra las mujeres, que comenzó en el mes de marzo de 1999, con objeto de movilizar a la opinión pública a favor de una actitud de no permitir la violencia. En el mismo año, 1997, puso en marcha la iniciativa DAPHNE para promover medidas preventivas destinadas a combatir la violencia ejercida sobre las/los niñas/os, las/os adolescentes y las mujeres.

5 El REAL DECRETO 253/2006, de 3 de marzo, por el que se establecen las funciones, el régimen de funcionamiento y la composición del Observatorio Estatal de Violencia sobre la Mujer y se modifica el Real Decreto 1600/2004, de 2 de julio, por el que se desarrolla la estructura orgánica básica del Ministerio de Trabajo y Asuntos Sociales, (BOE Nº 62 de fecha 14 de marzo de 2006). Disponible para su consulta en: http://www.observatorioviolencia.org/bbpp-proyecto.php?id_proyecto=87

su peso demográfico[6]. En otras palabras, la mujer inmigrada es más proclive a sufrir violencia de género que la mujer española.

Las cifras son realmente alarmantes, pero no podemos obviar el hecho de que, a partir del año 2000, España se ha configurado como un país receptor de una gran cantidad de población extranjera procedente de diversas partes del mundo. Así la población residente en España sufrió un importante crecimiento[7] debido, en gran medida, al incremento de la población extranjera y es en el marco de esta población donde las agresiones mortales de género muestran un amplio porcentaje, tanto de víctimas como de agresores extranjeros, tal y como se apuntaba en los párrafos anteriores.

Estas mujeres inmigrantes están rodeadas de una serie de circunstancias que aumentan su vulnerabilidad en relación con este delito y dificultan la ruptura del ciclo violento[8].

Así destaca la Relatoría[9] especial -sobre trabajadores migratorios-, de la Comisión Interamericana de Derechos Humanos el llamado «duelo migratorio», entendido como la situación psicológica especial que condiciona las percepciones y el comportamiento, al menos en un primer momento, de gran parte de las mujeres que deciden migrar. De hecho, las mujeres que migran, por el hecho de ser mujeres, están más expuestas a sufrir abusos añadidos, como la violencia física o psicológica y, a menudo, la expropiación de sus ingresos. Si a la situación de mujer inmigrante se une el que se halle en un estado de irregularidad, podría llegar a experimentar lo que Joseba Achotegui ha venido a llamar «el Síndrome de Ulises»[10], en cuanto que se encuentra en situaciones de especial estrés por la impotencia y fracaso de no poder acceder al mercado laboral, miedo a ser expulsada y a las mafias a las que puede estar vinculada, junto a un sentimiento muy intenso de lucha por la supervivencia. En tales circunstancias estas mujeres soportan situaciones de maltrato pues, entre otras razones, emprender acciones legales contra su pareja añadiría aún mayor carga traumática a sus vidas y un mayor sentimiento de desarraigo.

Tampoco hay que olvidar, como circunstancia que aumenta la vulnerabilidad, el «choque cultural» que, dependiendo de la nacionalidad, es más o menos importante, aunque en muchos supuestos provoca el que la concepción de la vida y de las relaciones de pareja sean distintas, de tal forma que la relación entre los sexos no se

6 INE (2011). Avance del Padrón municipal a 1 de enero de 2011. Datos provisionales. Disponible en: http://www.ine.es/prensa/np648.pdf . Las cifras consideran, únicamente, a la población extranjera empadronada, por lo que el porcentaje podría aumentar al considerar a las personas en situación de «irregularidad» o no empadronadas.

7 Al inicio de 2000 se hallaban empadronadas en España 40.499.791 personas y las cifras en enero de 2007 señalaban 45.116.964 personas empadronadas, lo que implica un incremento de la población del 11,4%. Actualmente los extranjeros representan el 12,13 por ciento de las 47,2 millones de personas empadronas en España. Datos publicados el 16 de enero de 2013 por el Instituto Nacional de Estadística (INE).

8 Vid. Mujeres inmigrantes y violencia de género. Aproximación diagnóstica a tres años de la existencia de la Ley de Medidas de Protección Integral contra la violencia de género, Otoño 2007 (Federación de Mujeres Progresistas).

9 Relatoría especial sobre trabajadores migratorios y miembros de sus familias. Comisión Interamericana de Derechos Humanos. Derechos Humanos de los Inmigrantes, Informe CN 4/2000/82, de 6 de enero de 2000.

10 Achotegui, Joseba. Artículo publicado en la Revista Norte de salud mental de la Sociedad Española de Neuropsiquiatría 2005 Volumen V, Nº 21. pág. 39-53.

desarrolla de forma igualitaria, ya no sólo en la práctica sino desde el concepto mismo del papel que socialmente se concede a uno y otra.

Asimismo, la falta de información es determinante en el comportamiento de estas mujeres: muchas inmigrantes se encuentran aisladas, sin el apoyo o la información suficientes para intentar salir de la situación de maltrato en la que viven. Además se percibe que existe desconfianza hacia los Cuerpos de Seguridad por su parte, sobre todo en aquellas que se hallan en situación irregular, ya que temen la expulsión.

Respecto a las víctimas inmigrantes que no denuncian cabría decir que existen dos razones fundamentales para no hacerlo: desconocimiento del sistema de protección arbitrado en España a través de la LOIVG, por un lado, y miedo a la expulsión cuando se hallan en situación irregular, por otro.

En cuanto a la primera cuestión, la ley reconoce de modo expreso el derecho de las mujeres extranjeras que se hallen en España, aun en situación irregular, a ser protegidas y tener acceso a los recursos en igualdad con las demás mujeres[11].

El derecho así reconocido lo desconocen muchas de ellas y además pueden tener cierta desconfianza a que el sistema funcione, poniendo el punto de mira en la actuación de las Fuerzas y Cuerpos de Seguridad del Estado. Sin embargo deben estar prevenidas en cuál ha de ser su proceder, pues el art. 31 de la citada Ley establece que, en su actuación, habrán de tener en cuenta el Protocolo de Actuación de las Fuerzas y Cuerpos de Seguridad y de Coordinación con los Órganos Judiciales para la protección de las víctimas de violencia de género. Por su parte el artículo siguiente señala que los planes de colaboración de los poderes públicos y los protocolos de actuación que los desarrollen han de contemplar la situación de las mujeres que puedan tener mayor riesgo de sufrir la violencia de género o mayores dificultades para acceder a los servicios previstos en esa ley, entre las cuales se cita a las inmigrantes.

Esta misma sensibilidad y especial protección hacia las mujeres inmigrantes víctimas de la violencia de género y doméstica ha sido recogida por el legislador español en la regulación de extranjería[12]. Así respecto de las que no se hallan regularmente en nuestro país, ha establecido la obtención de autorizaciones de residencia temporal por razones humanitarias desde la propia denuncia[13] en dependencias policiales, cuestión regulada en los art. 131 al 134 del nuevo Reglamento de la Ley Orgánica 4/2000, de 11 de enero, sobre derechos y libertades de los extranjeros en España y su integración social, en el que se determina que ninguna mujer inmigrante (aunque

11 Título II, Capítulo I, art. 17.1. LOIVG. «Todas las mujeres víctimas de violencia de género, con independencia de su origen, religión o cualquier otra condición o circunstancia personal o social, tienen garantizados los derechos reconocidos en esta Ley»

12 Real Decreto 557/2011, de 20 de abril, por el que se aprueba el Reglamento de la Ley Orgánica 4/2000, sobre derechos y libertades de los extranjeros en España y su integración social, tras su reforma por Ley Orgánica 2/2009.

13 El reglamento de la Ley de extranjería anterior (Real Decreto 2393/2004, de 30 de diciembre, por el que se aprueba el Reglamento de la Ley Orgánica 4/2000, de 11 de enero, sobre derechos y libertades de los extranjeros en España y su integración social), era más restrictivo puesto que solo permitía la posibilidad de documentación de residencia en España, después que hubiera recaído sentencia por los delitos de que se trate, habiendo podido presentar la solicitud cuando se haya dictado a favor de la víctima una orden judicial de protección. Por lo que con el nuevo reglamento RD 557/2011, la mujer extranjera víctima de violencia de género se ve fortalecida en sus derechos respecto a la anterior normativa.

ilegal) que sea presuntamente víctima de violencia de género será expulsada. Desde los ya citados artículos 131 al 134 la protección a las mujeres inmigrantes que son víctimas de maltrato se amplía y si están en situación administrativa irregular podrán acceder a un permiso de residencia provisional desde el momento en el que denuncie a su presunto agresor.

Lo recogido en el párrafo que antecede es motivo de la promulgación de la Ley Orgánica 2/2009, que, en su artículo 31, añadió el derecho a autorización de residencia temporal y trabajo por circunstancias excepcionales[14].

Con esta alteración al Reglamento sobre derechos y libertades de los extranjeros en España se modifica la Instrucción 14/2005[15] (criticada por Amnistía Internacional), que regula la aplicación de un procedimiento de control y sanción por infracciones previstas en la Ley Orgánica 4/2000 a las víctimas de violencia de género que acuden a una dependencia policial a denunciar las agresiones sufridas.

La Instrucción establecía que los funcionarios policiales, además de seguir el protocolo común de trato a víctimas de violencia de género, ante la llegada de una víctima extranjera averigüasen si su situación era irregular y, en ese caso, siguieran un procedimiento que podía derivar en un expediente sancionador, e incluso en una expulsión[16].

Otra cuestión que no cabe obviar es la relativa a que la legislación no tiene en cuenta la necesaria autonomía económica que resulta precisa a toda persona, y ello en cuanto que la ley sólo garantiza a las víctimas inmigrantes la «residencia en exclusiva» y no un permiso de trabajo, lo que explica que en muchos casos numerosas mujeres vuelvan con su agresor por su precaria situación económica, de la que no les es fácil salir por la imposibilidad de acceder a un trabajo.

Aunque las estadísticas indiquen que las mujeres inmigrantes estén muy expuestas a la violencia en la pareja, en comparación con las ciudadanas españolas, no se puede decir que España sea un país hostil para las víctimas inmigrantes (más adelante se hará mención a la encuesta realizada por la UE sobre el maltrato a la mujer).

En los últimos años, a raíz de la entrada en vigor de la LOIVG han sido implementadas una serie de medidas legales y otras que buscan proteger a estas mujeres y

14 Sobre esta autorización el Ministerio de Trabajo e Inmigración, a través de la Hoja Informativa n.º 42 (septiembre de 2011), aclara que esta es una autorización de residencia y trabajo por circunstancias excepcionales que podrán obtener las mujeres extranjeras víctimas de violencia de género que se encuentren en España en situación irregular. Además se explican otras cuestiones relativas a la tramitación de esta licencia. Disponible en Internet en: http://extranjeros.mtin.es/es/InformacionInteres/InformacionProcedimientos/documentos2/42.pdf . Estos y otros derechos de las mujeres inmigrantes están disponibles, en diez lenguas diferentes, en la página de Internet del Ministerio de Sanidad, Política Social e Igualdad en: http://www.migualdad.es/ss/Satellite?c=Page&cid=1193047406938&language=cas_ES&pagename=MinisterioIgualdad%2FPage%2FMIGU_contenidoFinal.

15 Instrucción número 14/2005, de la Secretaría de Estado de Seguridad, sobre actuación en dependencias policiales en relación con mujeres extranjeras víctimas de violencia doméstica o de género en situación administrativa irregular. Disponible en Internet en: http://www.icam.es/docs/ficheros/200602010020_6_4.pdf.

16 Paradoja con la que se encontraban los letrados del Turno de Oficio de Violencia de Género del Ilustre Colegio de Abogados de Madrid (ICAM), que al acudir en sus guardias a sede policial del CNP, a defender a mujeres maltratadas, se encontraban con que se les abría expediente de expulsión del territorio nacional por estancia irregular.

atenuar los factores de riesgo que les afectan de forma considerable. España posee mecanismos legales muy importantes para una protección efectiva de este colectivo de mujeres, incluso las indocumentadas, que la colocan en la vanguardia en este ámbito, respecto a otros países.

Mantener un trato discriminatorio, basado en la situación administrativa de la mujer víctima, en relación al acceso a medios en materia de protección, asistencia y rehabilitación establecidos, o exponer a las inmigrantes indocumentadas a procedimientos que pueden afectar a su decisión de buscar protección, con el consiguiente menoscabo de su derecho a acceder a la justicia, la reparación y a los mecanismos que garanticen su vida y su seguridad personal, no son compatibles con el principio de no discriminación en la protección de los derechos de las mujeres ante la violencia de género.

Las diferencias idiomáticas a la hora de solicitar información o pedir ayuda, la falta de redes de contacto (familia, amistades locales), la dependencia económica hacia el hombre, el miedo a la deportación o la desestructuración de la familia, en los casos en que el proceso migratorio tuvo como objetivo la reagrupación familiar, son factores que podrían estar determinando el gran aumento de los casos de femicidio en los colectivos de mujeres inmigradas. Todo ello hace que se encuentren en una situación de mayor vulnerabilidad económica, judicial, cultural y política, en relación a las autóctonas.

Con el paso del tiempo las autoridades españoles han sabido hacer frente a las críticas y han dado pasos importantes para una protección efectiva de este colectivo de mujeres. La Ley Orgánica 1/2004 prevé que una de las líneas prioritarias de actuación dirigida a prevenir, erradicar y sancionar la violencia de género, así como a proteger a sus víctimas, es la que aborda la situación específica de las mujeres inmigrantes.

En este sentido, en su artículo 17 (Garantía de los derechos de las víctimas) se protegen los derechos de «todas las mujeres víctimas de violencia, con independencia del origen, religión o cualquier otra circunstancia personal o social».

Asimismo, los servicios públicos han de considerar de forma especial el artículo 32, número 4, donde se establece que «en las actuaciones previstas en este artículo se considerará de forma especial la situación de las mujeres que, por sus circunstancias personales y sociales, puedan tener mayor riesgo de sufrir la violencia de género o mayores dificultades para acceder a los servicios previstos en esta Ley, tales como “las inmigrantes”».

En diciembre de 2006 fue aprobado el Plan Nacional de Sensibilización y Prevención de la Violencia de Género para 2007-2008[17], en el que se señala que para la consecución de sus objetivos debe prestarse una atención especial a aquellos grupos de mujeres que presentan mayor vulnerabilidad, entre los que se incluyen las mujeres extranjeras, quienes al hallarse en una situación de doble discriminación (es el propio Gobierno español el que reconoce la doble discriminación), requieren de un esfuerzo adicional en la remoción de los obstáculos que impiden el ejercicio real y efectivo de su estatuto de ciudadanía y repercuten en su calidad de vida.

17 Se puede consultar dicho Plan, estando disponible en la siguiente dirección: https://www.msssi.gob.es/ssi/violenciaGenero/Documentacion/medidasPlanes/DOC/Plan_nacional_sensibilizacion_prevencion_violencia_genero.pdf.

Como dice Vela Díaz, Raquel[18]: «el informe de evaluación de la aplicación de la Ley Orgánica 1/2004, de 28 de diciembre, de medidas de protección integral contra la violencia de género, presentado en julio de 2008, muestra que la proporción de mujeres extranjeras en España víctimas de violencia de género, al igual que la proporción de agresores extranjeros, suponen una sobre-representación respecto al peso demográfico de mujeres y varones extranjeros en España. Dicho informe también muestra que las mujeres extranjeras declaran ser víctimas de violencia de género en mayor proporción que el resto de las mujeres».

También en 2007 fue aprobado el Plan Estratégico de Ciudadanía e Integración 2007-2010, que incluye entre sus objetivos facilitar la integración de las mujeres extranjeras víctimas de la violencia de género[19].

Para el período 2009–2012 el Gobierno español aprobó el Plan de atención y prevención de la violencia de género en la población extranjera inmigrante, el cual plantea estrategias para superar las barreras de acceso a la información y los recursos existentes, así como para incrementar la sensibilización social.

Para el período 2013–2016 el Gobierno ha diseñado la «Estrategia Nacional para la erradicación de la violencia contra la mujer», como instrumento vertebrador de la actuación de los poderes públicos para acabar con la violencia que sufren las mujeres por el mero hecho de serlo. Constituye uno de los ejes fundamentales del proyecto político del Gobierno para hacer frente a esta lacra social y un plan de acción estable y duradero hasta 2016.

Por la relevancia que tienen en el ámbito de la protección de mujeres extranjeras es necesario mencionar la Ley Orgánica 2/2009, de 11 de diciembre, de Reforma de la Ley Orgánica 4/2000 de 11 de enero, sobre derechos y libertades de los extranjeros en España y su integración social, que modificó el artículo 19 en relación a la reagrupación familiar e introdujo el artículo 31 bis para facilitar la obtención del permiso de residencia a las mujeres extrajeras irregulares víctimas de violencia de género; y la Ley Orgánica 10/2011, de 27 de julio, por la que se modifican los art. 31 bis y 59 bis de la Ley Orgánica 4/2002.

Por otro lado, en España existen diversos protocolos de actuación en casos de violencia de género en los que se contempla la situación específica de las mujeres extranjeras. Así ocurre en el Protocolo de Actuación de las Fuerzas y Cuerpos de Seguridad del Estado y de Coordinación con los Órganos Judiciales para la Protección de las Víctimas de Violencia Doméstica y de Género (2005)[20], el Protocolo Común para la Actuación Sanitaria ante la Violencia de Género (2006)[21] y el Protocolo de Actuación y Coordinación de las Fuerzas y Cuerpos de Seguridad del Estado y Abogados y Abogadas ante la violencia de género (2007)[22].

18 La incidencia de la Violencia de Género en las mujeres extranjeras y la importancia del trabajo como factor de integración social. p 1. Tercer Congreso para el estudio de la violencia contra las Mujeres “Justicia y Seguridad, Nuevos Retos”, Granada 26 y 27 de noviembre de 2012.

19 Plan disponible en Internet en: http://ec.europa.eu/ewsi/UDRW/images/items/docl_1313_577775293.pdf

20 Disponible en Internet en: http://www.malostratos.org/images/pdf/prot%20actu.pdf

21 Plan disponible en Internet en: http://www.msc.es/organizacion/sns/planCalidadSNS/pdf/equidad/protocoloComun.pdf

22 Plan disponible en Internet en: http://www.migualdad.es/ss/Satellite?blobcol=urldata&blobheader=application%2Fpdf&blobheadername1=Contentdisposition&blobheadervalue1=inline&blobkey=id&blobtable=MungoBlobs&blobwhere=1244651958884&ssbinary=true.

El nuevo Reglamento de la Ley Orgánica 4/2000,de 11 de enero, sobre derechos y libertades de los extranjeros en España y su integración social -tras su reforma por Ley Orgánica 2/2009-, determina que ninguna mujer inmigrante (aunque ilegal) que sea presuntamente víctima de violencia de género será expulsada.

Desde el artículo 131 al 134 la protección a las mujeres inmigrantes que son víctimas de maltrato se amplía y si están en situación administrativa irregular podrán acceder a un permiso de residencia provisional desde el momento en el que denuncien a su presunto agresor. Con esta alteración se pretende también animar a perder el miedo a denunciar de las víctimas cuando estén en situación irregular, ya que podrán acudir a la policía o a los juzgados a denunciar sin ningún temor a ser expulsadas.

Como se ha reconocido en el Informe de la 28ª Conferencia de Ministros Europeos de Justicia[23], sobre problemas de acceso a la justicia para grupos vulnerables, «es innegable que los inmigrantes están en una situación diferente y poco ventajosa, en comparación con el resto de ciudadanos, en lo que se refiere al acceso a los tribunales u otros órganos de Justicia, ya sea para cuestiones administrativas o de intermediación (mediación y arbitraje). Las razones más obvias tienen que ver con las dificultades lingüísticas, ya que el inmigrante es incapaz de hablar la lengua local o lo hace con dificultad y, con mayor frecuencia, su falta de conocimiento de las leyes y sistemas judiciales del país europeo de acogida».

Como hemos visto las autoridades españolas han implementado una serie de medidas muy relevantes, dirigidas a la población extranjera, con el objeto de mejorar la atención y la prevención desde una perspectiva global, lo que ha propiciado una mejor respuesta frente a la violencia que afecta a las mujeres inmigrantes.

Se deberá apostar por una mayor difusión de información sobre los derechos de las mujeres inmigrantes y sobre todos los recursos que tienen a su disposición, en plan de igualdad con las ciudadanas españolas, porque solo así se conseguirá rebajar las estadísticas sobre muertes de mujeres por violencia de género.

2. ESTADÍSTICA DE MUERTES DE MUJERES POR VIOLENCIA DE GENERO

En España, desde 1999, han muerto 973 mujeres víctimas de violencia de género; en 2014, a fecha 31 de agosto, habían muerto 40 mujeres. La LOIVG entró en vigor en el año 2005 y en la siguiente tabla se observa que las muertes no descienden e incluso en algunos años como 2008-2010 aumentan, llegando a plantearse la influencia de esta ley en la erradicación de este problema. A continuación se recogen los datos en función del total de mujeres asesinadas, así como la diferenciación de las víctimas en función de la nacionalidad española o extranjera, así como de la nacionalidad de agresor asesino, estadística que, teniendo presente el porcentaje de población masculina y femenina en nuestro país, da un alto porcentaje de víctimas y agresores extranjeros (en relación con las víctimas y agresores de nacionalidad española). La dura realidad de las estadísticas oficiales, nos demuestran que el factor extranjería está muy presente en la vulneración de los derechos fundamentales de las mujeres, que mueren y

23 Informe del Consejo de Europa, disponible en Internet en: http://www.coe.int/t/dghl/standardsetting/minjust/mju28/MJU-28(2007)01ES-Espana.pdf

son agredidas en mayor medida que las mujeres españolas, aun siendo un importante número mayor de población.[24]

		2014	2013	2012	2011	2010	2009	2008	2007	2006	2005	2004	2003	2002	2001	2000	1999
VÍCTIMA	TOTAL	40	54	52	61	73	56	76	71	69	57	72	71	54	50	63	54
	Españolas	31	38	41	40	45	36	43	43	49	41	54	62	37	36	50	43
	Extranjeras	9	16	11	21	28	20	33	28	20	16	16	9	13	9	9	7
	No consta											2		4	5	4	4
	% Victimas extranjeras sobre total de víctimas de nacionalidad conocida	22,5	29,6	21,2	34,4	38,4	35,7	43,4	39,4	29	28,1	22,2	12,7	24,1	18	14,3	13
		2014	2013	2012	2011	2010	2009	2008	2007	2006	2005	2004	2003	2002	2001	2000	1999
AGRESOR	TOTAL	40	54	52	61	73	56	76	71	69	57	72	71	54	50	63	54
	Españoles	31	37	39	43	44	32	48	44	50	42	52	59	37	32	44	41
	Extranjeros	9	17	13	18	29	24	28	27	19	14	16	11	12	13	8	4
	No consta										1	4	1	5	5	11	9
	% Agresores extranjeros sobre total de agresores de nacionalidad conocida	22,5	31,5	25	29,5	39,7	42,9	36,8	38	27,5	24,6	22,2	15,5	22,2	26	12,7	7,4

Tabla actualizada a fecha 29 de agosto de 2014

3. EL ESTADO A TRAVÉS DE LAS FUERZAS Y CUERPOS DE SEGURIDAD (FCS) EN SU FUNCIÓN PROTECTORA DE LA MUJER INMIGRANTE Y LA VIOLENCIA DE GÉNERO

La violencia machista ejercida en el ámbito de una relación de pareja constituye una grave violación de los derechos humanos básicos de las mujeres. La definición actual de seguridad pública: «actividad dirigida a la protección de personas y bienes (seguridad en sentido estricto) y al mantenimiento de la tranquilidad u orden ciudadano, que son finalidades inseparables y mutuamente condicionadas» (Izu Belloso, 1988), nos conduce fácilmente a la conclusión de que, en consecuencia, la violencia machista tiene que ser un objetivo prioritario para cualquier política pública de seguridad.

La intervención del Estado en el territorio familiar está perfectamente legitimada, no como un modo de imponer determinados valores inherentes a la propia sociedad,

24 Fuente: Delegación del Gobierno para la Violencia de Género (Ministerio de Sanidad, Servicios Sociales e Igualdad) desde 2006. Los datos anteriores proceden del Instituto de la Mujer a partir de información de prensa y del Ministerio del Interior. Más información en: http://www.msssi.gob.es/ssi/violenciaGenero/portalEstadistico/home.htm.

pero si para garantizar los derechos humanos y proteger a las víctimas de la violencia, responsabilizar a los culpables, impartir justicia y otorgar recursos a las víctimas.

Un Gobierno debe ser considerado como un instrumento de defensa de los derechos fundamentales, en el que el derecho cívico más fundamental es el derecho a la vida y a la seguridad física. Este es el fundamento moral y normativo del Estado y, por consiguiente, su razón de ser. Los ciudadanos dejan en manos del Estado su derecho a legislar y gobernar, pero a la vez parten del supuesto de que el Estado está a la altura de sus compromisos básicos: proteger la vida, la libertad y los bienes de los ciudadanos.

La eliminación de la violencia contra la mujer exige que se elimine la violencia sexista en la familia, en la comunidad y dondequiera que sea perpetrada o tolerada por el Estado y pone de manifiesto el deber que tienen los gobiernos de evitar el empleo de la violencia contra la mujer y actuar con la necesaria diligencia para prevenir, investigar y, de conformidad con la legislación nacional, castigar los actos de violencia contra la mujer y adoptar medidas apropiadas y eficaces respecto de los actos violentos, ya se trate de actos perpetrados por el Estado, por particulares o por grupos armados o facciones en lucha, y proporcionar a las víctimas el acceso a unos medios de reparación justos y eficaces y a una asistencia especializada, incluida la asistencia médica[25].

La aplicación de la justicia a través de las FCS y de los tribunales es una herramienta fundamental para hacer frente a la violencia de género, proteger a las mujeres y castigar a los agresores. Esta es una intervención represiva y disuasoria, a posteriori, o prevención secundaria, que se traduce en una actuación del Estado que, habiendo fracasado con la prevención primaria, se tiene que enfrentar a comportamientos violentos en las relaciones conyugales, a los que tiene que dar una respuesta.

Con la interferencia del Estado en la esfera privada de la familia se intenta también que este tipo de violencia adquiera una mayor visibilidad, sin la cual difícilmente serán eficaces las medidas de prevención o de promoción del bienestar de las víctimas.

25 La eliminación de la violencia contra la mujer. Resolución de la Comisión de Derechos Humanos 2000/45. Recordando que en la Declaración y Programa de Acción de Viena, aprobados en junio de 1993 por la Conferencia Mundial de Derechos Humanos (A/CONF.157/23), se afirmó que la violencia sexista y todas las formas de explotación y acoso sexuales, en particular las derivadas de los prejuicios culturales y de la trata internacional, son incompatibles con la dignidad y el valor de la persona y debían ser eliminadas, se exhortó a que se adoptaran medidas para integrar la igualdad de condición de la mujer y sus derechos humanos en las principales actividades de todo el sistema de las Naciones Unidas, se subrayó la importancia de la labor destinada a eliminar la violencia contra la mujer en la vida pública y privada y se instó a la eliminación de todas las formas de discriminación contra la mujer. Profundamente preocupada porque algunos grupos de mujeres, como por ejemplo las mujeres pertenecientes a minorías, las mujeres indígenas, las refugiadas, las migrantes, las que viven en comunidades rurales o remotas, las indigentes, las recluidas en instituciones o detenidas, las niñas, las mujeres con discapacidades, las ancianas y las mujeres en situaciones de conflicto armado son objetivos especiales, particularmente vulnerables a la violencia. Resolución disponible en Internet en: http://www.acnur.org/t3/fileadmin/scripts/doc.php?file=biblioteca/pdf/0655

La lucha contra la violencia en la pareja tiene que ser un objetivo global y transversal que implique a las administraciones públicas de todos los ámbitos. Los organismos e instituciones públicas deben ser el motor para la implementación de los dictámenes que las leyes expresan, en orden a la igualdad y a la erradicación de la violencia en la pareja. Tienen la obligación de ejecutar medidas firmes que permitan implementar estrategias eficaces dirigidas a la prevención y erradicación de esta lacra, además de tener una responsabilidad en orden a prevenir, denunciar y sancionar las conductas violentas y discriminatorias.

Las FCS son la institución que interviene de forma más directa en la producción de la seguridad pública, tanto en su dimensión objetiva, mediante la prevención y el control de la delincuencia, como en su dimensión subjetiva en la gestión del miedo y el sentimiento de seguridad.

Como guardiana de los derechos y libertades de los ciudadanos, a las Fuerzas y Cuerpos de Seguridad les incumbe desempeñar un papel fundamental en la protección de las mujeres víctimas de violencia en la pareja. En lo que respecta a la protección de las mujeres eso significa, por ejemplo, que las FCS deben responder de forma no discriminatoria a las amenazas contra la vida, la libertad y la seguridad personal de las mujeres en el contexto de la violencia de género. Además, las FCS son uno de los símbolos más visibles de la intervención del Estado en el ámbito de la violencia de género. Muchas veces son la primera institución donde las víctimas se dirigen y es frecuentemente llamada para actuar en conflictos familiares.

El tratamiento integral de la violencia contra las mujeres exige articular protocolos[26] que aseguren la actuación global e integral de las distintas administraciones públicas y servicios implicados que coadyuven a mejorar la prevención, protección e incluso la actividad probatoria en los procesos que se sigan.

Asimismo, y dada la gravedad y persistencia de las infracciones cometidas en el ámbito familiar, y más concretamente en el de la violencia de género, el Estado ha creído necesario profundizar en las medidas de protección a las víctimas, a través de una gestión coordinada de las instituciones obligadas a protegerlas, para prevenir y evitar riesgos de nuevas agresiones.

Para ello consideró fundamental disponer de un registro con la información que permita realizar un seguimiento individualizado de las circunstancias de estas víctimas y

26 Protocolo médico-forense de valoración urgente del riesgo de violencia de género. Convenio del Consejo de Europa sobre prevención y lucha contra la violencia contra las mujeres y la violencia doméstica. Protocolo de actuación para la implantación del sistema de seguimiento por medios telemáticos del cumplimiento de las medidas de alejamiento en materia de violencia de género. Guía de criterios de actuación judicial frente a la violencia de género. Protocolo para la valoración policial del nivel de riesgo de violencia sobre la mujer en los supuestos de la Ley Orgánica 1/2004, de 28 de diciembre. Protocolo de actuación y coordinación de Fuerzas y Cuerpos de Seguridad del Estado y Abogados ante la violencia de género regulada en la Ley Orgánica 1/2004, de medidas de protección integral contra la violencia de género. Protocolo común para la actuación sanitaria ante la violencia de género .Protocolo de coordinación entre los órdenes jurisdiccional penal y civil para la protección de las víctimas de violencia doméstica. Protocolo de actuación de las Fuerzas y Cuerpos de Seguridad y coordinación con los órganos judiciales para víctimas de violencia doméstica y de género: (adaptado a la LO 1/2004, de Medidas de Protección Integral contra la Violencia de Género). Modelo de solicitud de la orden de protección. Protocolo para la implantación de la orden de protección de las víctimas de la violencia doméstica.

de la evolución del riesgo en que se encuentran, con objeto de aplicar las medidas de protección adecuadas a su situación de riesgo en cada momento.

Uno de los factores que inciden de forma más notable en la agravación de este riesgo objetivo es, justamente, la variación de la situación penitenciaria de los autores de este tipo de actos delictivos, en cuando que supone la concesión de permisos o la puesta en libertad (condicional o definitiva) de los internos que se encuentran sujetos a medidas judiciales de alejamiento o prohibición de comunicación con la víctima, por lo que resulta necesario disponer de la información proporcionada a este respecto por la Dirección General de Instituciones Penitenciarias.

En consonancia con la necesidad expuesta de mejorar la eficacia en la protección de las víctimas el Consejo de Ministros aprobó,el 15 de diciembre de 2006, el «Plan Nacional de Sensibilización y Prevención de la Violencia de Género» y un «Catálogo de medidas urgentes en la lucha contra la violencia de género».

Entre las medidas aprobadas se incluyen la creación de una nueva base de datos policial para mejorar la eficacia en el seguimiento de las circunstancias que concurren en cada una de las víctimas y cuyo objetivo es tener constancia permanente de su situación para evitar nuevas agresiones y la creación en las Delegaciones y Subdelegaciones del Gobierno de Unidades de Violencia contra la Mujer, con el fin de coordinar toda la información y recursos existentes destinados a proteger a las mujeres en situación de riesgo y posibilitar su seguimiento individualizado. Las Unidades de Violencia contra la Mujer, adscritas a las Delegaciones y Subdelegados del Gobierno -en su función de jefatura de los Cuerpos de Seguridad del Estado en su ámbito territorial- se constituyen como un elemento importante en esta protección.

El acceso a la información de la base de datos quedará limitado a: los órganos judiciales, el Ministerio Fiscal, la policía judicial y las unidades policiales especializadas en violencia de género, la Dirección General de Instituciones Penitenciarias, así como a las Delegaciones y Subdelegaciones del Gobierno. Las Fuerzas y Cuerpos de Seguridad y las Administraciones Penitenciarias serán las únicas competentes para introducir y modificar los datos.

Desde la Guardia Civil la problemática de la violencia de género se aborda de manera integral, para asegurar a las víctimas un tratamiento adecuado, personalizado y específico, por lo que no sólo implica a las Unidades especializadas, sino también a todas las Unidades relacionadas con la atención y seguridad ciudadana.

En primer lugar son todos los Puestos de la Guardia Civil los que tienen la inmediación de la atención a las víctimas. A ellos les corresponde, por tanto, recibir las denuncias, prestar el auxilio que precisen y garantizar su seguridad, ejecutando, a su vez, las medidas judiciales dictadas en las correspondientes órdenes de protección.

Además, como complemento a la actuación de las Unidades territoriales, desde 1995 se han ido constituyendo los Puntos de Atención Especializada (PAE,s) en diversos órganos de las Unidades Orgánicas de Policía Judicial (UOPJ), como son todas las Secciones a nivel provincial y Equipos Territoriales a nivel comarcal en un número creciente. Estos PAE,s están compuestos por agentes especializados en la atención y protección de las mujeres víctimas de la violencia de género (y de los menores, los conocidos Especialistas Mujer-Menor, EMUME), tanto si son víctimas como autores.

Además garantizan que se pueda atender de forma específica los casos más graves, así como prestar apoyo y asesoramiento a los Puestos y Unidades Territoriales. A tal efecto, todas las actuaciones de las Unidades Territoriales en esta materia son notificadas a los PAE,s, al objeto de valorar su posible intervención, realizando, a su vez, un seguimiento de la problemática a su nivel de actuación.

Existe un PAE central, en la Unidad Técnica de Policía Judicial, que realiza el análisis nacional de la casuística, coordina las actuaciones, establece las directrices técnicas de actuación, asesora a los PAE,s provinciales y organiza la actualización de la formación de los especialistas.

Hoy día existen 273 PAE,s y se cuenta con 638 EMUME,s, que se forman y actualizan a través de jornadas técnicas, que se convocan de manera periódica, también para formar a nuevos especialistas, con el objetivo de ampliar el despliegue. Y es que se encuentran distribuidos, tanto en número como en componentes que los integran, en función de los casos existentes en su demarcación de responsabilidad.

4. LOS JUZGADOS DE VIOLENCIA SOBRE LA MUJER / EL MINISTERIO FISCAL Y LA FORMACIÓN EN VIOLENCIA DE GENERO POR PARTE DE LOS LETRADOS DEL TURNO DE OFICIO

4.1. LA CREACIÓN DE LOS JUZGADOS DE VIOLENCIA SOBRE LA MUJER

Es una de las novedades más importantes introducidas por la LOIVG. Según prevé la Exposición de Motivos de la Ley, los Juzgados de Violencia sobre la Mujer conocerán de «la instrucción, y, en su caso, del fallo de las causas penales en materia de violencia sobre la mujer, así como de aquellas causas civiles relacionadas, de forma que una y otras en la primera instancia sean objeto de tratamiento procesal ante la misma sede».

Por tanto, podemos afirmar que una de las principales ventajas que tienen estos Juzgados de Violencia sobre la Mujer es que van a permitir que el mismo Juzgado tramite todas las denuncias interpuestas por la mujer víctima de violencia de género, aún en el supuesto de que dichas denuncias se interpongan en fechas distintas, lo que sin duda facilitará que el Juzgado tenga una visión global de la relación existente entre el agresor y la víctima.

En todos los partidos judiciales se han creado Juzgados de Violencia sobre la Mujer con la finalidad de agilizar el proceso y conseguir una respuesta penal más rápida y eficaz y, también, que estén más cerca de la víctima. Además, para garantizar esta proximidad se establece que será competente para tramitar los asuntos de violencia de género el Juzgado del lugar del domicilio de la víctima.

En aquellos partidos judiciales donde no se ha creado un juzgado exclusivo para la violencia de género serán los Juzgados de Instrucción o de Primera Instancia e Instrucción los que se encarguen de estos asuntos, debiendo compatibilizar las causas por actos de violencia de género con las demás competencias que les correspondan en materia penal, si son Juzgados de Instrucción, o en materia civil y penal si son de Primera Instancia e Instrucción. De esta forma se asegura que en todo partido judicial haya un juzgado especializado en violencia de género, ya sea dedicado en exclusiva

a tramitar estos asuntos o bien especializado en la materia, aunque también tramite otras cuestiones.

Ahora bien, la creación de estos Juzgados de Violencia sobre la Mujer no sería suficiente para frenar la violencia de género sin la dotación de los medios adecuados para que todo el personal que va a prestar sus servicios en ellos tenga la formación adecuada. Precisamente por este motivo el artículo 47 de la LOIVG ha previsto que el Gobierno, el Consejo General de Poder Judicial y las Comunidades Autónomas, en el ámbito de sus respectivas competencias, asegurarán una formación específica y obligatoria[27] relativa a la igualdad y no discriminación por razón de sexo y sobre violencia de género en los cursos de formación[28] de jueces y magistrados, fiscales, secretarios judiciales, Fuerzas y Cuerpos de Seguridad y médicos forenses.

4.2. EL MINISTERIO FISCAL EN SU FUNCIÓN DE LUCHA CONTRA LA VIOLENCIA DE GÉNERO

La creación de la figura del fiscal de Sala contra la Violencia sobre la Mujer representa un avance importante en la aportación del Ministerio Fiscal[29] en la lucha contra la delincuencia que tan nocivos efectos despliega en el círculo de sus víctimas. Se pretende lograrlo con la intensidad que permite la posición central del fiscal general del Estado, pero con la flexibilidad de su articulación mediante un fiscal delegado que,

27 De conformidad con lo dispuesto en el número tres bis del artículo 329 de la Ley Orgánica del Poder Judicial, cuando la plaza vacante a cubrir por los jueces que deban ser promovidos a la categoría de magistrado sea un Juzgado de Violencia sobre la Mujer o Penal con especialización en violencia sobre la mujer, antes de tomar posesión, habrán de participar en las actividades específicas y obligatorias de formación que periódicamente establezca el Consejo General del Poder Judicial. Asimismo, y si la plaza vacante en los Juzgados de Violencia sobre la Mujer o en un Juzgado de lo Penal o Sección penal o civil con especialización en violencia de género ha sido obtenida mediante concurso de traslado por la mayor antigüedad en el escalafón del concursante, antes de la toma de posesión deberá participar en las actividades de formación a que se refiere el párrafo anterior. Se puede consultar texto completo en: http://www.poderjudicial.es/cgpj/es/Temas/Compendio_de_Derecho_Judicial/Reglamentos/Reglamento_2_2011__de_28_de_abril__de_la_carrera_judicial.

28 http://www.poderjudicial.es/cgpj/es/Temas/Violencia_domestica_y_de_genero. En dicha dirección Web podremos encontrar los criterios básicos que han de regir las actividades obligatorias de formación para los jueces/zas y magistrados/as destinados en Juzgados de Violencia sobre la Mujer, en Juzgados de lo Penal especializados en violencia de género o en Secciones penales y civiles especializadas en violencia de género (aprobados por acuerdo del Pleno del CGPJ de 17 de mayo de 2010). En el año 2011 se logró implantar la formación obligatoria en violencia de género para todos/as los/as magistrados y magistradas que acceden a plazas de violencia sobre la mujer, con la finalidad de sensibilizar y dar a conocer a nuestros/as jueces y juezas los instrumentos legales y recursos existentes en la lucha contra estos crímenes.

29 Entre los instrumentos encaminados a fortalecer y garantizar el vigente marco penal y procesal de protección, la Ley Orgánica 1/2004, de 28 de diciembre, de Medidas de Protección Integral contra la Violencia de Género, ha creado la figura del «fiscal contra la Violencia sobre la Mujer» como delegado del fiscal general del Estado, y en las Fiscalías territoriales la «Sección contra la Violencia sobre la Mujer», que intervienen en las materias y procedimientos penales y civiles que conozcan los Juzgados de Violencia sobre la Mujer. La Sección contra la Violencia estará integrada por un fiscal delegado de la Jefatura, que “asume las funciones de dirección y coordinación que específicamente le son encomendadas”, y los fiscales adscritos que se determinen pertenecientes a las respectivas plantillas. Disponible texto completo en la siguiente dirección: http://www.fiscal.es/cs/Satellite?c=Page&cid=1240559967690&pagename=PFiscal%2FPage%2FFGE_contenidoFinal&vest=1240559967690

a nivel estatal, se encargará de supervisar y coordinar la actuación de las Secciones contra la Violencia sobre la Mujer de todas las Fiscalías.

La LOIVG dibuja para el fiscal de Sala una nueva función: supervisar y coordinar a nivel estatal las Secciones contra la Violencia sobre la Mujer de las Fiscalías y sus criterios de actuación, superponiéndose a la actividad coordinadora que sobre las mismas ejercen también los delegados de la Jefatura en la Sección, pretendiendo con ello no sólo una respuesta eficaz en estos graves hechos, sino mantener la unidad de actuación, que es la base de la seguridad jurídica que debe amparar a la ciudadanía a la hora de someterse a un procedimiento penal en que se reclama la reparación del daño.

Entre las diferentes funciones que se acometen por la Fiscalía de Sala se incluyen las variadas y necesarias relaciones interinstitucionales que se llevan a cabo con la Delegación de Gobierno de Violencia de Género del Ministerio de Igualdad y con el Observatorio Estatal, dependiente de esta Institución; con el Ministerio de Justicia, Ministerio de Interior, Ministerio de Sanidad, Observatorio de Violencia Doméstica y de Género del C.G.P.J., así como con la participación en reuniones de ámbito nacional e internacional.

4.3. EL ACCESO AL TURNO DE OFICIO DE VIOLENCIA DE GÉNERO POR PARTE DE LOS LETRADOS

En el caso del Ilustre Colegio de Abogados de Madrid (ICAM), para la prestación de los Servicios de Asistencia Jurídica Gratuita[30] deben acreditar más de tres años en el ejercicio de la profesión y estar en posesión del diploma del curso de Escuela de Práctica Jurídica o de cursos equivalentes homologados por el Colegio, o, en su caso, haber superado los cursos o pruebas de acceso a los servicios de turno de oficio y asistencia letrada al detenido establecidos por las Juntas de Gobierno. Además, para el acceso a los turnos más especializados se requiere formación adicional y más años de antigüedad en el ejercicio profesional. Estos requisitos específicos vienen establecidos en las Normas Reguladoras de Turno de Oficio, de «la extranjería y la Violencia de Género»:

Turno de extranjería: Cinco años de antigüedad en el ejercicio de la profesión y curso específico en la materia.

Violencia de género: Tres años de antigüedad y curso específico en la materia.

La necesidad absoluta de que la defensa jurídica de las víctimas de Violencia de Género sea inmediata y especializada exige una organización del servicio por parte de los Colegios de Abogados, que han de designar profesionales para un servicio de guardia de 24 horas de atención inmediata a estas víctimas.

El Protocolo establece los parámetros de comportamiento de estos abogados de guardia en materia de violencia de género, entre los que están la obligación de estar localizable las 24 horas; no poder ausentarse del ámbito territorial en el que presta la asistencia a las víctimas; disponer siempre del impreso de solicitud del derecho de

30 http://www.icam.es/web3/cache/NS_TO_cf_incorporacion.html. Las mujeres extranjeras víctimas de violencia de género que sean asistidas por letrados del Turno de Oficio del ICAM están defendidas por profesionales cualificados, con un plus de antigüedad y formación previa en la materia, antes de poder ejercer la defensa especializada en dichos Turnos de Oficio.

asistencia jurídica gratuita para la defensa y representación letrada a la mujer víctima de Violencia de Género, etc.

Además, el abogado de guardia deberá realizar una labor de asistencia y asesoría a la víctima, informándola desde el primer momento de todas las posibilidades de protección (orden de protección y otras medidas cautelares penales y civiles), personación y los derechos que le asisten (información, asistencia social integral, asistencia jurídica gratuita, derechos laborales, económicos, etc.). Igualmente, el abogado informará de la posibilidad que tiene la mujer víctima de ser atendida en el Servicio Público de Asistencia Móvil para las víctimas de Violencia de Género (Teléfonos 900 22 22 92 y 96 369 50 37), obligación que también tienen las Fuerzas y Cuerpos de Seguridad.

5. DERECHO A LA ASISTENCIA JURÍDICA GRATUITA A LOS EXTRANJEROS, BAJO LA DOCTRINA CONSTITUCIONAL

El art. 24 CE hace referencia al derecho a la tutela judicial efectiva y el reconocimiento constitucional, así como la jurisprudencia constitucional, cuando afirma que es imprescindible la vinculación del derecho a la tutela[31] judicial efectiva y a la dignidad humana[32].

El derecho a la Justicia Gratuita no solo es un mandato específico de la Constitución que en su artículo 119 señala que «la justicia será gratuita cuando así lo disponga la ley y, en todo caso, para quienes acrediten insuficiencia de recursos para litigar», sino una cuestión que han respaldado el Tribunal Europeo de Derechos Humanos y el propio Tribunal Constitucional español en diversas sentencias, alguna de las cuales señala que aunque la configuración concreta de ese derecho corresponde al legislador, éste «no goza de una libertad absoluta, sino que en todo caso debe respetar un contenido constitucional indispensable».

La aportación que la Justicia Gratuita supone para la sociedad española es enorme en términos de paz y vertebración social y de promoción de la igualdad entre los ciudadanos como Derechos Fundamentales; en definitiva, dicho derecho a la tutela judicial efectiva, amparado por nuestra Constitución, no sería nada sin el derecho de Justicia Gratuita. La defensa del más débil y la búsqueda de la igualdad efectiva de las partes en el proceso explica su esencia profunda y expresa la conquista del Estado de Derecho y del supremo valor de la Justicia. No es discutible por tanto que la cobertura de este servicio público es una obligación de los poderes públicos, donde se debe incluir no solo al nacional, sino también a todo

31 Analizo los estrictamente relacionados o interrelacionados con el derecho a la asistencia jurídica y que inciden en interdependencia con estos derechos fundamentales en sentido estricto, tales derechos son: “se garantiza la asistencia de abogado al detenido en las diligencias policiales y judiciales, en los términos que la ley establezca (art. 17 CE), el derecho a obtener la tutela efectiva de los jueces y a los derechos procesales fundamentales (art. 24 CE)”. De plena aplicación en el tema de la mujer extranjera víctima de violencia de género (su derecho legal a ser asistida por abogado especializado como parte de la atención integral, desde ese mismo instante, para que pueda prestarle asesoramiento jurídico con carácter previo a la formulación de la denuncia y de la solicitud de la orden de protección).

32 El art. 10 de la Declaración Universal de Derechos Humanos (DUDH); el art. 6.1 del Convenio de Roma, y el art. 14.1 del Pacto Internacional de Derechos Civiles y Políticos (PIDCP), impiden diferencia de trato entre nacionales y extranjeros, con independencia de que estos tengan regularizada su estancia en nuestro país.

extranjero independientemente de la situación en que se encuentre residiendo en nuestro país.

El Tribunal Constitucional ha resuelto diversos recursos de inconstitucionalidad, entre otros, en las sentencias 236/2007, de 7 de noviembre, y 259/2007, de 19 de diciembre, reconociendo que la exigencia que la indicada Ley imponía a los extranjeros para el ejercicio de los derechos fundamentales de reunión, asociación, sindicación y huelga, de que tuvieran residencia legal en España, constituía una restricción injustificada y, por tanto, contraria a la Constitución, ya que según la misma los indicados derechos alcanzan a todas las personas por el hecho de serlo. Consecuentemente con ello, el Tribunal Constitucional ha declarado la inconstitucionalidad de los artículos de la Ley Orgánica 4/2000 que regulaban los indicados derechos fundamentales. Este párrafo se incluye dado que tiene una clara relación con el hecho de estar en nuestro país de forma legal, es decir, con la documentación preceptiva de extranjero o ilegal, sin la referida documentación de extranjería que ampara la residencia en España; y la Ley 1/1996, de 10 de enero, de Asistencia Jurídica Gratuita (en adelante LAJG) reconoce a los extranjeros ilegales en nuestro país, que se encontraban privados de la misma si carecían de los ingresos económicos suficientes para litigar.

Así las cosas, y en cumplimiento a la Jurisprudencia Constitucional, el Legislativo se ha visto obligado a promulgar una serie de Leyes que dieran cumplimiento a dicha Jurisprudencia relacionada con el derecho a la Asistencia Jurídica Gratuita de extranjeros irregulares en nuestro país; por ello la Ley Orgánica 2/2009, de 11 de diciembre, de reforma de la Ley Orgánica 4/2000, de 11 de enero, sobre derechos y libertades de los extranjeros en España y su integración social, preceptúa en su art. 22 «Derecho a la asistencia jurídica gratuita»:

"Los extranjeros que se hallen en España tienen derecho a la asistencia jurídica gratuita en los procesos en los que sean parte, cualquiera que sea la jurisdicción en la que se sigan, en las mismas condiciones que los ciudadanos españoles."

El criterio sustentado por el TC en Sentencia[33] 95/2003, de 22 de mayo, contra el art. 2 de la LAJG, al manifestar que «la expresión que residan (en España) habrá que entenderse referida a la situación puramente fáctica»... afirmando que «los extranjeros que se encuentren en España y reúnan las condiciones requeridas legalmente para ello, podrán acceder a la asistencia jurídica gratuita en relación con cualquier tipo de procesos a efectos del cual gocen de la preceptiva legitimación».

La regulación de esta materia se encuentra en la LAJG[34], la cual puso fin a la dispersión normativa hasta entonces existente y tuvo como principal novedad la

33 La propia Constitución Española en su artículo 119 dispone que la justicia será gratuita cuando así lo disponga la ley y, en todo caso, respecto de quienes acrediten insuficiencia de recursos para litigar. De acuerdo con la Jurisprudencia del Tribunal Constitucional, anterior a la que ahora se analiza "STC 95 / 2003" (puesta de manifiesto en sentencias como la 30/1981, 77/1983 ó 216/1988), la gratuidad de la justicia se configura como un derecho subjetivo cuya finalidad es asegurar la igualdad de defensa y representación procesal al que carece de medios económicos, constituyendo al tiempo una garantía para los intereses de la Justicia.

34 A tenor del artículo 2 de la Ley 1/1996, de asistencia jurídica gratuita, disponía que, si el extranjero no residente legalmente en España no dispone de recursos suficientes para procurarse abogado y procurador, veía cerrado su acceso a la jurisdicción, lo que supone, sin duda, una vulneración del derecho a la tutela judicial efectiva que, al resultar de la propia norma legal, hace que ésta incida en el vicio de inconstitucionalidad.

desjudicialización del procedimiento del reconocimiento de este derecho. Existen derechos que corresponden por igual a españoles y extranjeros y cuya regulación ha de ser igual para ambos, así sucede con aquellos derechos fundamentales que son imprescindibles para la garantía de la dignidad humana[35] que constituye fundamento del orden político español (STC 107/1984).

La expresión «que residan (en España)» habrá de entenderse referida a la situación puramente fáctica de los que se hallan en territorio español pues, de lo contrario, se vaciaría por completo el sentido y alcance de la declaración de inconstitucionalidad que el TC debe realizar.

El Real Decreto Ley 3/2013, de 22 de febrero, por el que se modifica el régimen de las tasas en el ámbito de la Administración de Justicia y el sistema de asistencia jurídica gratuita[36], reconoce el beneficio a la asistencia jurídica gratuita, universalmente y con independencia de sus recursos económicos, a todas las víctimas de violencia de género y trata de seres humanos.

A las víctimas de violencia de género se les reconoce este derecho con independencia de la existencia de recursos para litigar. La prestación de este derecho es inmediata y les reconocen aquellos procesos que tengan vinculación, deriven o sean consecuencia de su condición de víctimas. La condición de víctima a los efectos del reconocimiento del derecho a la asistencia jurídica gratuita se adquiere a partir de los siguientes supuestos: formulación de denuncia o querella o iniciar un procedimiento penal por alguno de los delitos descritos al definir a las víctimas. El mantenimiento de este derecho se dará mientras permanezca en vigor el procedimiento penal o cuando, tras su finalización, se hubiera dictado sentencia condenatoria.

Este beneficio se pierde en caso de sentencia absolutoria firme o archivo firme del procedimiento penal, pero sin la obligación de abonar el coste de las prestaciones disfrutadas gratuitamente hasta ese momento. Es decir, en el caso de que se dieran estos supuestos, con relación a los casos en los que se les ha reconocido este derecho y han estado exentas del pago de la tasa judicial, no deberán abonarla a posteriori como consecuencia de la pérdida de la condición de víctima.

6. CONCLUSIONES

La LOIVG ha supuesto un avance sumamente importante en la prevención, tratamiento y sanción de las conductas de violencia de género. Su largamente esperada coordinación con la normativa de extranjería[37] no puede sino ser beneficiosa para las mujeres. Tras las últimas reformas en el ámbito del Derecho de Extranjería hay que destacar que las medidas adoptadas son muy novedosas en el marco internacional,

35 La Declaración universal de derechos humanos, el Convenio de Roma de 4 de noviembre de 1950 y el Pacto internacional de derechos civiles y políticos de Nueva York de 19 de diciembre de 1966 establecen un derecho equivalente al derecho a la tutela judicial efectiva, que es reconocido a todas las personas, sin atención a su nacionalidad». (STC 99/1985).

36 Letra g) y h) del artículo 2 de la Ley 1/1996, de asistencia jurídica gratuita, introducida por el número uno del artículo 2 del R.D.-Ley 3/2013, de 22 de febrero, por el que se modifica el régimen de las tasas en el ámbito de la Administración de Justicia y el sistema de asistencia jurídica gratuita («B.O.E.» 23 febrero).Vigencia: 24 febrero 2013.

37 Cfr., RODRÍGUEZ YAGÜE, C., «La mujer extranjera...», cit., págs. 154-155.

ya que, con carácter general, los textos internacionales y comunitarios relativos a la violencia contra la mujer promueven la adopción de medidas relativas a la formación de los agentes implicados en su erradicación, sobre tutela civil y penal de las víctimas, pero no tenían referencia alguna al impacto de la situación de violencia sobre la mujer extranjera hasta el año 2011, con el convenio europeo sobre violencia contra las mujeres particularmente vulnerables por su doble condición de mujer y de extranjeras[38], aspectos de los que sí se ocupaba la normativa española antes del citado convenio europeo, lo que merece una valoración positiva. Cuestión distinta es entrar a valorar cómo lo ha hecho, pues la aplicación práctica que se está haciendo de las posibilidades de tutela de las mujeres extranjeras víctimas de violencia de género muestran la existencia de carencias que conviene proceder a corregir cuanto antes. Una de estas carencias es, sin duda, que haya supuestos en que se prevean como mecanismos de acreditación de la condición de víctima de violencia de género dos medios tan limitados como la orden de protección o el informe del Ministerio Fiscal. Urge una modificación legislativa que tenga en cuenta los problemas prácticos que ambos mecanismos plantean, abriendo el abanico a otras formas posibles de acreditar la situación de violencia que pueden garantizar la seguridad jurídica de forma tan efectiva como las citadas y que se admiten en otros casos, como los informes de los servicios sociales. A ello hay que añadir en todos los casos la sentencia definitiva como mecanismo concluyente de acreditación de la condición de víctima (sin exigir que sea condenatoria, para no excluir los supuestos en que se declaran probados los hechos pero el autor es declarado inimputable o concurre una causa de extinción de la responsabilidad penal).

Con ello se lograría unificar la forma de acreditación de la condición de víctima de violencia de género a los efectos que nos ocupan, lo que redundaría en una mayor protección de las mujeres extranjeras, cumpliendo mejor el mandato de la LOIVG en el sentido de evitar toda discriminación en el acceso a los derechos que reconoce, que el art. 31 bis 1 de la Ley 4/2000

ha extendido expresamente al colectivo que nos ocupa[39], al disponer que «las mujeres extranjeras víctimas de violencia de género, cualquiera que sea su situación administrativa, tienen garantizados los derechos reconocidos en la LOIVG, así como las medidas de protección y seguridad establecidas en la legislación vigente»[40].

38 Sobre el entrecruzamiento de las dos dimensiones de género e inmigración como factor que ahonda en la desigualdad y la discriminación, vid., MARTÍN SÁNCHEZ, M., «La mujer inmigrante: espacios de doble discriminación», en RODRÍGUEZ YAGÜE, C. (ed.), Estudios sobre género y extranjería, Bomarzo, Albacete, 2011, págs. 61-90; RODRÍGUEZ YAGÜE, C., «La mujer extranjera...», cit., págs. 137 y ss.; RAMOS QUINTANA, M. I., «Mujeres inmigrantes...», cit., pág. 17; TRIGUERO MARTÍNEZ, L. A., «Tratamiento jurídico-legal...», cit., págs. 191 y ss.; VILLAR CAÑADA, I. M., «Empleo y protección social de las mujeres inmigrantes. Una doble discriminación de partida», en BLÁZQUEZ VILAPLANA, B., y VILLAR CAÑADA, I. M. (coords.), La mejora de la empleabilidad de las mujeres inmigrantes en Andalucía, Literalia, Jaén, 2009, pág. 47.

39 Críticamente sobre esta remisión, TRIGUERO MARTÍNEZ, L. A., «Tratamiento jurídico-legal...», cit., pág. 200. Más en positivo, RODRÍGUEZ YAGÜE, C., «La mujer extranjera...», cit., págs. 163-164.

40 Con ello se supera la diferencia de trato que permite el art. 13.1 de la Constitución Española cuando apunta que «los extranjeros gozarán en España de las libertades públicas que garantiza el presente Título en los términos que establezcan los Tratados y la Ley (...)». La normativa de extranjería, pese a haber convertido la igualdad en el disfrute de los derechos y libertades reconocidos en el Título I de la Constitución en un mero «criterio interpretativo general» (vid., el art. 3.1 LEx), reconoce la igualdad de trato de las mujeres extranjeras víctimas de violencia de género y

Y es que de los datos disponibles se desprende que el uso que se está haciendo de los mecanismos favorables a la víctima de violencia de género en la normativa de extranjería es, como poco, escaso, sobre todo si se pone en la balanza con el riesgo que corren las mujeres en situación irregular en caso de que la denuncia presentada no llegue a buen puerto, p. ej. por no conseguir orden de protección o porque la sentencia definitiva no considere probados los hechos denunciados.

A modo de cierre, podemos decir que el aumento de la migración femenina, en conjunto con los factores estructurales mencionados anteriormente, podría actuar como caldo de cultivo para el aumento de los casos de violencia de género y femicidios contra mujeres inmigradas en España, de ahí la importancia de continuar trabajando desde diversos campos de acción para visibilizar y prevenir la violencia de género, independiente de la procedencia de las personas involucradas.

En este sentido podría contar con policia judicial adscrita para estos Juzgados de Violencia Contra la Mujer, en número proporcional a los procedimientos que se tramitan, psicólogos, asistentes sociales y médicos forenses adscritos, siendo preciso que se cuente con una formación y sensibilidad especial para evitar lo que se ha denominado «la victimización secundaria» de la mujer que acude por fin a denunciar y se encuentra con «profesionales» que no le dan a la víctima el trato especial que debe tener dadas las especiales características de los hechos que va a denunciar.

España está contribuyendo a mejorar las condiciones de vida de las mujeres migrantes que residen en nuestro país y Europa ya regula la condición de extranjera y la violencia de género, incluida asistencia letrada, con el reciente Convenio[41] del

las españolas.

41 Convenio del Consejo de Europa sobre prevención y lucha contra la violencia contra las mujeres y la violencia doméstica, Hecho en Estambul, el 11 de mayo de 2011. Artículo 57 – "Asistencia jurídica". Las Partes velarán porque las víctimas tengan derecho a asistencia jurídica y ayuda legal gratuita según las condiciones previstas en su derecho interno. Capítulo VII – Migración y asilo.- Artículo 59–" Estatuto de residente" 1 Las Partes adoptarán las medidas legislativas o de otro tipo necesarias para garantizar que se conceda a las víctimas, cuyo estatuto de residente dependa del de su cónyuge o de su pareja de hecho, de conformidad con su derecho interno, previa petición, un permiso de residencia autónomo, en el caso de disolución del matrimonio o de la relación en situaciones particularmente difíciles, con independencia de la duración del matrimonio o de la relación. Las condiciones relativas a la concesión y a la duración del permiso de residencia autónomo se establecerán de conformidad con el derecho interno. 2 Las Partes adoptarán las medidas legislativas o de otro tipo necesarias para que las víctimas puedan obtener la suspensión de los procedimientos de expulsión iniciados por causa de que su estatuto de residente dependa del de su cónyuge o de su pareja de hecho, de conformidad con su derecho interno, con el fin de permitirles solicitar un permiso de residencia autónomo. 3 Las Partes expedirán un permiso de residencia renovable a las víctimas, en al menos una de las situaciones siguientes: a) cuando la autoridad competente considere que su estancia es necesaria con respecto a su situación personal; b) cuando la autoridad competente considere que su estancia es necesaria a los fines de cooperación con las autoridades competentes en el marco de una investigación o de procedimientos penales. 4 Las Partes adoptarán las medidas legislativas o de otro tipo necesarias para que las víctimas de matrimonios forzosos llevadas a otro país a fines de celebración de dichos matrimonios y que pierdan, en consecuencia, su estatuto de residente en el país en que residan habitualmente, puedan recuperar este estatuto. Artículo 60 – "Solicitudes de asilo basadas en el género" 1 Las Partes adoptarán las medidas legislativas o de otro tipo necesarias para que la violencia contra las mujeres basada en el género pueda reconocerse como una forma de persecución en el sentido del artículo 1, A (2) del Convenio, relativo al estatuto de los refugiados de 1951 y como una forma de daño grave que da lugar a una protección complementaria o subsidiaria. 2 Las Partes velarán por la aplicación a cada uno de los motivos del Convenio de una interpretación sensible con respecto al género y porque

Consejo de Europa sobre prevención y lucha contra la violencia contra las mujeres y la violencia doméstica.

BIBLIOGRAFÍA

Acale, M. (2000), EL delito de malos tratos físicos y psíquicos en el ámbito familiar. Valencia: Tirant Lo Blanch.

Achotegui, J. (2005) “El Síndrome de Ulises”, Revista Norte de salud mental de la Sociedad Española de Neuropsiquiatría, 21, 39-53.

Chocrón, A. M. (2010).Tutela procesal de la mujer extranjera en el marco de violencia de género. En C. Sánchez-Rodas (coord.), Inmigración, mujeres y menores (p. 152). Murcia: Laborum.

Izu, M. J. (1988). Los conceptos de orden público y seguridad ciudadana tras la Constitución de 1978. Revista Española de Derecho Administrativo, 58, 233-252.

Martín, M., (2011). La mujer inmigrante: espacios de doble discriminación. En C. Rodríguez y J. de Paz (coords.), Estudios sobre género y extranjería (pp. 61-90). Albacete: Bomarzo.

Triguero, L. A. (2010). “La mujer extranjera víctima de violencia de género: residencia temporal y trabajo. Medidas de tutela protectoras sociolaborales”. En J. L. Monereo (dir.), Los Derechos de los Extranjeros en España. Estudio de la LO 2/2009, de 11 de diciembre, de reforma de la LO 4/2000 (pp. 487-551). Madrid: La Ley.

Vela, R. (2012). La incidencia de la Violencia de Género en las mujeres extranjeras y la importancia del trabajo como factor de integración social. Jaén: Universidad de Jaén.

Villar, I. M. (2009). Empleo y protección social de las mujeres inmigrantes. Una doble discriminación de partida. En B. BLÁZQUEZ e I. M. VILLAR (coords.), La mejora de la empleabilidad de las mujeres inmigrantes en Andalucía (p. 47). Jaén: Literalia.

Fecha de recepción: 07/05/2014. Fecha de aceptación: 24/06/2014

los solicitantes de asilo puedan obtener el estatuto de refugiado en los casos en que haya quedado establecido que el riesgo de persecución está basado en uno o varios de esos motivos, conforme a los instrumentos pertinentes aplicables. 3 Las Partes adoptarán las medidas legislativas o de otro tipo necesarias para desarrollar procedimientos de acogida sensibles al género y servicios de apoyo a los solicitantes de asilo, así como directrices basadas en el género y procedimientos de asilo sensibles al género, incluidos los relativos a la obtención del estatuto de refugiado y a la solicitud de protección internacional.

LA RESPUESTA POLÍTICA A LOS TRÁGICOS SUCESOS DE LAMPEDUSA 3-O 2013

¿HACIA UN NUEVO CONCEPTO DEL CONTROL DE LOS FLUJOS MIGRATORIOS IRREGULARES POR MAR EN LA POLÍTICA DE LA UE?

FRANCISCO JAVIER VÉLEZ ALCALDE

RESUMEN

Tan solo dos años y medio más tarde de iniciarse las salidas masivas por mar de inmigrantes desde el norte de África hacia Italia, como consecuencia de la denominada "primavera árabe", el 3 de octubre de 2013 estuvo marcado por la tragedia de Lampedusa. Esta vez Italia consiguió poner en marcha los mecanismos de solidaridad europeos. Es cierto que la situación en Italia ha cambiado significativamente. Ya no llegan tunecinos a sus costas que pueden ser repatriados, sino sirios con derecho a protección internacional. Ha cambiado la composición de los flujos migratorios. Pasar de la migración económica a la migración de asilo ha dado la excusa perfecta a Italia para seguir pidiendo solidaridad y un cambio político. La respuesta de la UE fue la creación de una Task Force para el Mediterráneo conteniendo 38 acciones operativas en el marco de cuatro ejes principales señalados por el Consejo. El discurso político de la Comisión de la UE está ahora centrado en convertir la dimensión exterior de las políticas de interior en la principal herramienta de la lucha contra la inmigración irregular por mar; en poner en marcha operaciones aeromarítimas con medios aeronavales militares, devolviendo al debate europeo la participación de los recursos militares en operaciones de Law Enforcement y, con el apoyo de Italia, transformar las operaciones de vigilancia y control en la mar en un potente sistema de salvamento y rescate de inmigrantes en la mar, generando un peligroso efecto llamada en el Mediterráneo central.

Palabras Clave: inmigración irregular marítima, política migratoria europea, fronteras marítimas, Frontex, Task Force Mediterráneo.

ABSTRACT

Just two and a half years after the massive flows of migrants by sea from North Africa to Italy that took place as a result of the so-called "Arab Spring", the third of October 2013 was marked by the tragedy of Lampedusa. This time Italy could implement European solidarity mechanisms. It is true that the situation in Italy has changed significantly. Tunisians no longer reach their shores and may be repatriated, but Syrians entitled to international protection. It has changed the composition of migration flows. Moving from economic migration to asylum migration has given the perfect excuse to Italy to claim for solidarity and political change. The EU response was the creation of a Task Force for the Mediterranean containing 38 operational actions under four main areas identified by the Council. The political discourse of the EU Commission is now focused on turning the external dimension of the policies of interior on the main tool in the fight against illegal immigration by sea; on launching military operations with naval means, returning with that decision to the European debate on the use of military assets in Law

Enforcement operations, and with the support of Italy, on turning around monitoring and control operations at sea in a powerful system of search and rescue of immigrants at sea, generating so a dangerous “pull factor” in the central Mediterranean.

Key words: irregular migration by sea, european migration policy, sea borders, Frontex, Mediterranean Task Force.

1. LA GESTIÓN ITALIANA DE LOS FLUJOS MIGRATORIOS MASIVOS EN LA PRIMAVERA DE 2011

1.1. CRONOLOGÍA DE LA RESPUESTA POLÍTICA A LA CRISIS MIGRATORIA

En el primer trimestre de 2011, y como consecuencia directa de los episodios revolucionarios que comenzaron en Túnez el 17 de diciembre de 2010 con la autoinmolación de Mohamed Bouazizi y la caída del Gobierno de Zine el Abidine Ben Alí, el 14 de enero de 2011, 20.000 irregulares, casi todos tunecinos, fueron detenidos en el mar y las costas italianas, dando lugar a una crisis humanitaria de grandes proporciones (Frontex, 2011).

La comisaria de Interior de la UE, Cecilia Malmström, ya había adelantado en febrero de ese año que la mejor solución para la crisis de los “inmigrantes económicos tunecinos” era tratar de llegar a acuerdos con Túnez para que los inmigrantes fueran repatriados. Italia podía esperar una respuesta solidaria de la UE mediante la cooperación de la Agencia Frontex en la gestión de los flujos excepcionales de inmigración de Túnez a Lampedusa.

La voluntad política de la Comisión tuvo su reflejo en el lanzamiento de la operación “Hermes” el 20 de febrero de 2011, proporcionando medios de apoyo aéreos y navales al control de las fronteras marítimas, así como el inicio de la cooperación con las autoridades tunecinas y la identificación de acciones de financiación por parte de Europol.

Sin embargo, el 11 de abril de 2011 los ministros de Interior de la UE rechazaron en Luxemburgo la propuesta del ministro italiano Roberto Maroni para que se repartieran solidariamente los inmigrantes irregulares llegados a Italia. Si bien el entonces primer ministro italiano, Silvio Berlusconi, aseguró que la principal solución para los miles de tunecinos llegados a Lampedusa y al sur de Italia era su repatriación, apeló a la solidaridad europea, ya que el acuerdo alcanzado el 4 de abril de 2011 entre Italia-Túnez, durante su viaje de urgencia a este país para la devolución de 100 inmigrantes irregulares diarios[1], entraba en vigor el 5 de abril de 2011, dejando fuera de los términos acordados los llegados masivamente en el primer tercio del año.

La respuesta de la UE fue negativa a la propuesta italiana, pero no se reflejó por escrito en las conclusiones del Consejo de Justicia y Asuntos de Interior del 11-12 de abril de 2011, mientras que sí se aceptó, sin embargo, el reparto solidario entre Estados de los inmigrantes llegados a Malta desde Libia, solicitándoles además una mayor

1 “Berlusconi: La solución para los inmigrantes de Lampedusa es repatriarlos”. Italia concedió una ayuda de 80 millones de euros para la adquisición de los equipos utilizados para vigilancia y control, así como otros 150 millones para la recuperación de la economía tunecina. Disponible en http://www.elmundo.es/elmundo/2011/04/01/internacional/1301657628

contribución al fondo de apoyo a las operaciones de Frontex y transmitiéndoles la urgente necesidad de dotar a esta Agencia de mayor operatividad mediante una modificación de su Reglamento. Esta propuesta fue contestada con desaire por el Gobierno italiano, afirmando que Italia había sido abandonada y llegando incluso a señalar que era inevitable preguntarse por el sentido de pertenecer a la UE.

La UE respondió que Italia debía gestionar por sí misma la crisis de los inmigrantes económicos tunecinos negociando con Túnez ya que no revestía la gravedad anunciada para las dimensiones económicas y demográficas de un país como Italia (González, 2011:1-6).

Como consecuencia, el Gobierno italiano decidió otorgar a los inmigrantes tunecinos, aplicando su interpretación de la Directiva comunitaria del 2001 prevista para el flujo masivo de refugiados[2], permisos de residencia temporales por razones humanitarias y documentos de viaje de extranjeros con los que podrían viajar a otros Estados del espacio Schengen (Diario El Mundo, 2011).

A esta medida se mostraron contrarios Francia, que el 17 de abril de 2011 suspendió el tráfico ferroviario en su frontera con Italia para evitar la entrada masiva de tunecinos (Diario El Mundo, 2011), y Alemania, cuyo ministro federal de Interior manifestó públicamente que el problema de los inmigrantes de Túnez era un asunto que en primera instancia debía ser abordado por Roma, tratando de llegar a un acuerdo con Túnez para su repatriación, y de ninguna manera por la UE, ya que 23.000 inmigrantes de tipo económico no representaban un flujo masivo para un país desarrollado y de la población de Italia (Ministerio Federal alemán de Interior, 2011).

El apoyo de la UE se consideró por Alemania como subsidiario una vez que Italia asumiera su responsabilidad. También adoptaron la misma postura Austria y Suecia, advirtiendo Alemania y Austria a Italia del refuerzo en la vigilancia y control de sus fronteras para impedir el acceso de los inmigrantes tunecinos a sus respectivos territorios (Diario alemán Der Spiegel, 2011). La Comisión, con Cecilia Malmström a la cabeza, no mantuvo una posición de liderazgo clara y firme en la gestión de esta crisis y la interpretación de las normas Schengen que superara el conflicto entre Italia y Francia, esperando su resolución entre ambos países de forma bilateral. La Comisión aceptó tanto la validez de la expedición masiva de los documentos de viaje por parte de Italia como el cierre por parte de Francia de algunos pasos fronterizos de forma temporal y por razones de orden público, según está previsto en el Tratado de Schengen. Además, en opinión de la Comisión, sobre la base del Tratado Schengen el documento de viaje no sería suficiente para permitir la libre circulación, ya que también son exigibles a los inmigrantes no comunitarios medios económicos de subsistencia, una dirección concreta y la garantía de que regresarán a su país al término de seis meses (Diario ABC, 2011).

En la cumbre bilateral entre Francia e Italia en Roma el 26 de abril de 2011, los presidentes Sarkozy y Berlusconi, en sorprendente sintonía en parte relacionada con asuntos ajenos a la política migratoria como la participación italiana en los ataques a

2 DIRECTIVA 2001/55/CE DEL CONSEJO de 20 de julio de 2001 publicada en el Diario Oficial de las Comunidades Europeas el 7.08.2001, L 212/12, relativa a las normas mínimas para la concesión de protección temporal en caso de afluencia masiva de personas desplazadas y a medidas de fomento de un esfuerzo equitativo entre los Estados miembros para acoger a dichas personas y asumir las consecuencias de su acogida.

la Libia de Gadafi (González, 2011: 4), decidieron enviar una carta conjunta a los presidentes de la Comisión y del Consejo Europeo en la que exponían como propuestas principales en materia de política migratoria la posibilidad de restablecer provisionalmente los controles en las fronteras internas, la necesidad de llegar a un acuerdo global con los países africanos origen y tránsito de la inmigración, la necesaria evolución hacia un régimen europeo común en materia de asilo y el fortalecimiento de la agencia Frontex (Ministerio de Asuntos Exteriores de Francia).

El 4 de mayo de 2011 la Comisión, ante esta grave crisis humanitaria, manifestó la necesidad de la UE de avanzar de manera urgente en la gestión común y solidaria de los flujos masivos de inmigración[3]. Para avanzar en la gestión correcta de los flujos migratorios, un documento de la Comisión en mayo de 2011 (MEMO/11/273) y la correspondiente nota de prensa de la comisaria de Asuntos de Interior, Cecilia Malmström, se refirieron a varios instrumentos de control de fronteras y de la gobernanza del espacio Schengen que era necesario mejorar y/o implementar urgentemente. Muchos de ellos ya habían sido propuestos en 2008, como el refuerzo del mandato de Frontex, la implementación de los acuerdos de readmisión y una nueva estrategia negociadora de los mismos, una intensificación de la dimensión exterior de las políticas migratorias, la creación de asociaciones migratorias y de movilidad con terceros países y la mejora de la gobernanza del espacio Schengen[4].

El 16 de septiembre de 2011 la Comisión propuso dos medidas legislativas (IP/11/1036). La primera fortaleciendo los mecanismos de evaluación Schengen[5], con el objetivo de mejorar el control del cumplimiento de las normas Schengen por parte de los Estados miembros. La segunda: dotar a los Estados miembros de un mecanismo común de respuesta coordinada y toma de decisiones para la reintroducción temporal de controles fronterizos internos en situaciones de amenaza grave al orden público y a la seguridad interior. Además, este mecanismo incorporó también la posibilidad de que los Estados miembros puedan actuar unilateralmente reintroduciendo controles interiores cuando tengan que hacer frente a situaciones de emergencia imprevistas, en las que sea necesario actuar inmediatamente, si bien esta medida puede adoptarse solo por un periodo máximo de cinco días, tras el cual la prórroga debería

3 "La Comisión propone una mejor gestión de la emigración a la UE". Bruselas, 4 de mayo de 2011. IP/11/532: "Más de 25.000 emigrantes, principalmente procedentes de Túnez y, en menor medida, de otros países africanos, han huido hacia la UE y han alcanzado las costas de Italia (la mayoría la isla italiana de Lampedusa) y Malta; ambos países se hallan actualmente bajo una fuerte presión migratoria. Además de los desplazados y los emigrantes, un número considerable de refugiados de distintas nacionalidades, (incluidos somalíes, eritreos y sudaneses) han abandonado Libia y algunos de ellos han conseguido llegar también a Italia y Malta. Estos acontecimientos han sometido a los sistemas de protección y recepción de algunos de los Estados miembros de la UE a una tensión creciente".

4 El 13 de septiembre de 2011 los ministros de Interior de Alemania, Francia y España, en declaración conjunta, apoyaron la necesidad de permitir que los Estados de la Unión, en el ejercicio de su soberanía nacional, puedan adoptar la decisión de reinstaurar los controles fronterizos internos en situaciones excepcionales, cuando la valoración del estado de la amenaza en sus territorios, elaborada por sus autoridades de seguridad competentes, así lo aconsejen para mantener el orden público y la seguridad de las que son políticamente responsables ante sus ciudadanos.

5 La Comisión ya expresó la necesidad de controlar el cumplimiento de las normas Schengen un año antes en 2010 como queda de manifiesto en la nota de prensa " Viajar sin fronteras: la Comisión propone controlar de manera más rigurosa el cumplimiento de las normas de Schengen" IP/10/1493 de 16.11.2010. Disponible en http://europa.eu/rapid/press-release_IP-10-1493_es.htm?locale=fr. Consultado el 17.02.2013.

asumirse a nivel de la UE. También quedaron reguladas medidas de apoyo económico y/o técnico a través de la intervención de agencias europeas como Frontex, Europol o la Oficina Europea de Apoyo al Asilo en aquellos casos en los que los Estados miembros no puedan afrontar correctamente la protección de la correspondiente frontera exterior de la UE e incluso las de reintroducción temporal de los controles fronterizos, si esto no fuera suficiente.

1.2. ANÁLISIS DE LA RESPUESTA POLÍTICA A LA GESTIÓN DE LA CRISIS MIGRATORIA EN 2011

Tras esta serie concatenada de acontecimientos descritos en el punto anterior, y analizadas las respuestas en su conjunto a la crisis migratoria que se produjo desde el norte de África hacia Europa, se hace necesario destacar los aspectos más importantes. En primer lugar, en opinión de la profesora González Enríquez, la evidente "crisis del europeísmo", con el descrédito de las Instituciones ocasionado por las respuestas contradictorias que hubo, poniendo en peligro el espacio Schengen y el avance en materia de políticas comunes. Por un lado, se puso de manifiesto la debilidad política de la Comisión ante los Estados miembros, al no obligar a Italia a asumir su responsabilidad en la gestión de los flujos de inmigración irregular procedentes del norte de África, dando el visto bueno a sus decisiones políticas e instándole a acercamientos bilaterales que solucionaran el problema. Por otro, esta reacción de la Comisión contrasta con el mensaje contundente del Consejo de Ministros de Interior que exigía a Italia asumir su responsabilidad en la gestión migratoria. Además, quedó demostrado que los acuerdos de repatriación firmados con Túnez y Libia hasta ese momento eran frágiles, obligando a la Unión Europea a renegociar dichos acuerdos con la consiguiente inversión financiera y de medios. Por último, la necesidad de que los Estados miembros den un tratamiento homogéneo a la inmigración irregular para crear confianza en el sistema y lograr una solidaridad efectiva ante las crisis migratorias (González 2011: 5).

Un mes más tarde, el 25 de octubre de 2011, vio la luz la primera respuesta a las conclusiones del Consejo Europeo de 24 de junio de 2011, en las que se pedía avanzar en materia de "Fronteras Inteligentes"[6] para conseguir una mejor gestión de flujos de viajeros en las fronteras exteriores mediante la implementación de un sistema de control de entradas y salidas (SES) y un programa de viajeros registrados (PVR).

Además, la gestión de esta crisis humanitaria puso de manifiesto determinados aspectos que debían ser mejorados como el necesario refuerzo en la dotación de los fondos de refugiados, de retorno, de integración y de fronteras para abordar una situación de emergencia, y la materialización de la solidaridad de los Estados miembros con los Estados que reciban mayor presión migratoria.

No solo hubo respuestas a la crisis de alguna manera controvertidas en el seno de la Unión. Alemania aceptó unos meses más tarde, en noviembre de 2011 y por razones humanitarias, acoger a 147 nacionales de Eritrea, Somalia, Sudán y Etiopía llegados desde Libia a las costas de Malta a principios de ese año, basando su razonamiento en

6 «Fronteras Inteligentes» de la UE: la Comisión desea un acceso más fácil y una mayor seguridad. IP/11/1234 de 25 de octubre de 2011. Disponible en http://europa.eu/rapid/press-release_IP-11-1234_es.htm?locale=fr Consultado el 17 de febrero de 2013.

que estas personas necesitadas de ayuda, no tratándose de inmigrantes económicos, con seguridad serían reconocidas más adelante como solicitantes de asilo y, además, debido a su situación geográfica y su pequeño número de habitantes, Malta se veía desbordada por movimientos migratorios de ese tipo, por lo que en este caso era necesario el apoyo de los Estados miembros[7]. En este sentido hay autores que consideran la política de asilo de Alemania y Suecia como un factor de atracción o "pull factor" de la inmigración irregular.

Otra de las consecuencias de la Primavera Árabe y la gestión de la crisis en el Mediterráneo en 2011 fue la necesidad manifiesta de revisar el Enfoque Global de la Migración adoptado en 2005 y la publicación en 2011, por parte de la Comisión, del nuevo Enfoque Global de la Migración y la Movilidad (GAMM), más estratégico, amplio, eficaz y no limitado geográficamente, vinculando las políticas externas e internas de la Unión. En esta Comunicación (COM (2011) 743 final), la Comisión destaca la importancia del refuerzo de la política exterior migratoria, incluida la cooperación al desarrollo y la política de vecindad de la UE, como prioridad para establecer diálogos a nivel regional, nacional y local sobre migración, movilidad y seguridad con terceros países, con los que se debe llegar a Asociaciones de Movilidad directamente o a través de los Programas comunes sobre migración y movilidad. Los cuatro pilares sobre los que se desarrolla este enfoque Global son la ordenación de los flujos migratorios legales, incluyendo el concepto más general de movilidad; la lucha contra la inmigración irregular; el refuerzo de la protección internacional de los migrantes y de la dimensión exterior de la política de asilo de la UE.

2. LA RESPUESTA DE LA UE Y LA GESTIÓN ITALIANA DE LOS FLUJOS MIGRATORIOS MASIVOS EN EL OTOÑO DE 2013

2.1. LA CRISIS DE LAMPEDUSA COMO PUNTO DE INFLEXIÓN EN LA POLÍTICA MIGRATORIA DE CONTROL FRONTERIZO

"Non è più un'emergenza: è un tempo della storia che ci consegna quello dell'immigrazione come un fenomeno immanente a questo tempo della storia. E non vi sarà mai un reticolato burocratico, un reticolato normativo, che potrà fermare il vento della storia. Perché? Perché è cambiata l'idea della frontiera, è cambiata completamente l'idea della frontiera, in questo tempo di globalizzazione dei diritti, ma anche di globalizzazione delle povertà. Almeno in una parte del mondo, l'istinto, la spinta ad andare fuori nasce dalla povertà, nasce dall'assenza di democrazia, nasce dall'assenza di benessere"

Ministro del Interior Italiano Angelino Alfano. Lampedusa 4/10/2013[8]

La política de control de las fronteras marítimas exteriores de la UE tiene como punto de inflexión los hechos acaecidos en Lampedusa en octubre de 2013.

Tan solo dos años y medio más tarde de iniciarse las salidas por mar de inmigrantes como consecuencia de la denominada "primavera árabe", el 3 de octubre de 2013

7 "Aufnahme von nach Malta geflüchteten Nordafrikanern", 29.11.2011, „Malta ist aufgrund seiner geografischen Lage und im Hinblick auf seine geringe Einwohnerzahl in besonderer Weise durch die Migrationsbewegungen aus Nordafrika belastet. Mit dieser erneuten humanitären Aufnahme von Flüchtlingen aus Malta tragen wir zur Entlastung des europäischen Partnerstaates bei". Disponible en http://www.bmi.bund.de

8 http://www.governo.it/Notizie/Palazzo%20Chigi/testo_int.asp?d=73129

estuvo marcado por la tragedia de Lampedusa. Una embarcación con cerca de 500 inmigrantes irregulares de Somalia, Eritrea y Ghana que había salido de Libia se incendió a media milla de la isla de los conejos y, tras arrojarse al mar, perecieron ahogados más de 360 inmigrantes (Diario italiano La Stampa, 2013). El profundo impacto mediático y social que estas imágenes produjeron, agravado por la indignación social ante la presunta inacción de barcos pesqueros que no auxiliaron a los inmigrantes en peligro por temor a ser acusados de favorecer la inmigración irregular según la Ley de 2008 aprobada por el Gobierno de Silvio Berlusconi y actualmente derogada, centraron el discurso político de la Comisión de la UE y del Gobierno italiano en la voluntad decidida de convertir las operaciones de vigilancia y control en la mar en un potente sistema de salvamento y rescate de inmigrantes en la mar.

Desde el comienzo de 2013 hasta noviembre de ese año cerca de 32.000 inmigrantes cruzaron el Mediterráneo central hacia la UE principalmente desde Libia y Túnez, representando aproximadamente un 70% del total de inmigrantes que cruzaron este mar utilizando las diferentes rutas mediterráneas. Un total de 45.000 inmigrantes cruzaron o intentaron cruzar el Mediterráneo en 2013, lo que supone un notable incremento de aproximadamente un 311% respecto a 2012 en los flujos migratorios totales y una concentración en las rutas centrales[9]. Sin embargo, en opinión de De Bruycker, Di Bartolomeo y Fargues (De Bruycker et al., 2013: 2-27) esta situación no supone una nueva tendencia migratoria ya que la inmigración por mar hacia la UE, en términos globales, se puede calificar como de fenómeno estructural con una media de 40.000 inmigrantes por año que han tratado de alcanzar las costas de la UE en el periodo comprendido de 1998 a 2013, no obstante la probabilidad de morir en las rutas marítimas se ha incrementado en ese periodo más de un 3%.

Una de las diferencias con la crisis migratoria de 2011 antes analizada es que esta vez Italia ha conseguido poner en marcha los mecanismos de solidaridad europeos. Es cierto que su situación ha cambiado significativamente. Ya no llegan tunecinos a sus costas que pueden ser repatriados sino sirios con derecho a protección internacional. Ha cambiado la composición de los flujos migratorios. Pasar de la migración económica a la migración de asilo ha dado la excusa perfecta a Italia para seguir pidiendo solidaridad y un cambio político.

Sin embargo, De Bruycker, Di Bartolomeo y Fargues (De Bruycker et al., 2013: 2-27) creen que si los flujos migratorios por mar, fundamentalmente los que utilizan las rutas hacia Italia, se clasifican habitualmente como “mixtos” por ser utilizados por “inmigrantes económicos”, mientras que otro gran número de inmigrantes trata de solicitar “asilo y protección internacional”, puede concluirse con los datos actualmente disponibles que la migración por mar no es el procedimiento más habitual entre los peticionarios de asilo que llegan a la UE.

La situación de inseguridad en Libia, donde no hay fuerzas de seguridad organizadas y el crimen organizado aumenta, así como la falta de control en las fronteras, propicia las salidas de embarcaciones desde este lugar. A esta situación se suma como factor de empuje o “push factor” la inestabilidad política generalizada en la zona, en

9 Council of the European Union. “Migration Flows in the Southern Neighbourhood and their External Relations perspectiva-Possible Avenues for Dialogue and Cooperation with Partner Countries, including Options for a CSDP Operation”. Bruselas, 19 de noviembre de 2013.p-4. Disponible en http://register.consilium.europa.eu/pdf/en/13/st16/st16394.en13.pdf

países como Egipto. Por otro lado, como ya se ha apuntado anteriormente, algunos analistas opinan que la política de asilo que mantienen países europeos como Suecia y Alemania podría estar actuando como factor de atracción o "pull factor"[10].

Así, los dramáticos sucesos ocurridos en Lampedusa el 3 de octubre de 2013 han vuelto a poner sobre la mesa los debates sobre el fenómeno migratorio irregular por mar y la manera en la que la UE lo afronta a través de sus políticas de gestión integrada de las fronteras marítimas del sur, su política migratoria y de asilo. También se han centrado estos debates en la definición conceptual del salvamento y rescate en la mar y el peso específico que estas operaciones de salvamento y rescate (SAR) tienen en el contexto del control migratorio irregular, así como el nuevo papel de apoyo de las operaciones desarrolladas en el marco de la Política Común de Seguridad y Defensa (PCSD) en el control de las fronteras marítimas.

2.2. LA RESPUESTA POLÍTICA A LA GESTIÓN DE LA CRISIS MIGRATORIA EN LAMPEDUSA 2013: LA "TASK FORCE" MEDITERRÁNEA

La reacción de la Unión Europea (UE) a la crisis no se hizo esperar. La Agencia Europea para la Gestión de la Cooperación Operativa en las Fronteras Exteriores de los Estados miembros de la Unión (FRONTEX) reforzó sus operaciones en curso HERMES[11] y AENEAS[12] en el Mediterráneo Central[13] con financiación de la Comisión.

En el Consejo de la Unión Europea (Justicia y Asuntos de Interior) del 7 y 8 de octubre de 2013 en Luxemburgo[14], el ministro del Interior italiano, refiriéndose a los trágicos sucesos ocurridos en Lampedusa, pidió a la Comisión la creación de una "Task Force Mediterranean (TFM)" liderada por la Comisión/DG HOME y con la participación del Servicio de Acción Exterior de la UE (SEAE), los Estados miembros de la UE, así como numerosas Agencias relevantes de la UE como FRONTEX, la Oficina Europea de Apoyo al Asilo (EASO) y la Oficina Europea de Policía (EUROPOL), con el objetivo de definir acciones concretas para afrontar la situación en el Mediterráneo y evitar tragedias futuras.

10 El ministro de Interior alemán durante la crisis de Lampedusa, Dr. Hans-Peter Friedrich, afirmaba en 2013 que Alemania era el país de la UE más solidario en materia de asilo y en opinión de Günter Burkhardt, director de la asociación pro asilo germana, el incremento de las peticiones de asilo en Alemania tiene lugar porque "viele Flüchtlinge vermeiden es, in Italien einen Asylantrag zu stellen, weil ihnen dort die Obdachlosigkeit droht. In Griechenland haben sie überhaupt keine Chance, einen Antrag zu stellen. Deshalb versuchen viele, direkt in einem Land wie Deutschland oder Schweden einen Antrag zu stellen". Desde enero a octubre de 2013 el número de personas que solicitó asilo en la RF de Alemania pasó de 50.344 a 87.442 personas, lo que significa un aumento del 73,7 % respecto a 2012.

11 Operación de control en el mar para controlar los flujos migratorios desde Túnez hacia el sur de Italia, principalmente a Lampedusa y Cerdeña.

12 Combate de la inmigración ilegal en el mar Jónico desde Turquía y Egipto a Apulia y Calabria.

13 Desde noviembre de 2013 hasta abril de 2014, FRONTEX incluyó un despliegue permanente en el escenario mediterráneo de medios de los Estados Miembros. Los medios militares de las armadas han trabajado en apoyo de las autoridades civiles a las que están subordinadas en el cumplimiento de estas misiones.

14 Nota de prensa. 3260th Council meeting Justice and Home Affairs.14149/13. http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/en/jha/138925.pdf

En una rápida reacción de la UE, este grupo de trabajo recibió el encargo de presentar un informe (COM (2013) 869 final) sobre acciones concretas y prioritarias en el Mediterráneo para evitar incidentes como el ocurrido en Lampedusa y, tras ser debatido en Consejo JAI los días 5 y 6 de diciembre de 2013[15], fue presentado en el Consejo Europeo del 19-20 de diciembre de 2013.

Se trataba en definitiva de proporcionar soluciones a corto y largo plazo para evitar las muertes en la mar y este tipo de tragedias en el escenario Mediterráneo sobre la base de los principios de prevención, protección, solidaridad y responsabilidad compartida. En este punto es donde la dimensión exterior de la política migratoria, a través del fortalecimiento del diálogo y la cooperación con terceros países de la mano del Servicio de Acción Exterior, recobra todo su significado, habiéndose planteado la integración de soluciones bajo el paraguas de la PCSD y de las que trataremos más adelante.

Los trabajos de la TFM, desde un enfoque integral para la zona, dieron como fruto un conjunto de propuestas concretas, en el Marco del GAMM, como el diálogo permanente con los terceros países; la redefinición de conceptos como el de reasentamiento; la realización de propuestas novedosas como la búsqueda de nuevas vías legales para la inmigración a la UE y otras ya conocidas en el ámbito de la lucha contra la trata de seres humanos y el tráfico de inmigrantes irregulares, la repatriación, la gestión de la fronteras exteriores, a través de la herramienta de EUROSUR, o el apoyo a los países que reciben más presión migratoria.

En definitiva, este documento ha pretendido definir una operación marítima de FRONTEX en el Mediterráneo, atendiendo a los principios de responsabilidad compartida y solidaridad política y presupuestaria frente a las amenazas del tráfico y trata de seres humanos y el crimen organizado, basada en la cooperación con terceros países. Italia y la propia Comisión, considerando la de Lampedusa una de las mayores tragedias de los últimos tiempos en el Mediterráneo, buscaban que el documento diera un peso más específico si cabe a las operaciones de búsqueda y salvamento marítimo, además de reforzar las fórmulas de acceso a la protección internacional de los inmigrantes.

Las medidas adoptadas por la TFM se enmarcan en varias líneas de acción de las que pasaremos a analizar las más destacadas en el marco de este trabajo.

2.2.1. La cooperación con terceros países

En primer lugar se mencionan las acciones de cooperación con terceros países, a cargo principalmente del Servicio Europeo de Acción Exterior y basadas en acuerdos a corto y largo plazo en el Marco del GAMM. Nos encontramos en una nueva fase de la dimensión externa de las políticas de interior. Concretamente, se ha definido la puesta en marcha de campañas preventivas de información, iniciativas diplomáticas y medidas de cooperación técnica con los terceros países en el desarrollo de sus capacidades.

Es la primera vez que en una Comunicación de la Comisión se propone en primer lugar una medida de este tipo, destacándola como una de las formas más efectivas para prevenir la entrada irregular de inmigrantes en la UE y que emprendan viajes en

15 La TFM se reunió para elaborar este documento dos veces, el 24 de octubre y el 20 de noviembre de 2013 respectivamente.

los que ponen su vida en peligro. Esta idea destaca la importancia que se le va a dar en el futuro a la dimensión exterior de las políticas comunes de interior y supone un cambio estratégico en el enfoque político de control migratorio marítimo para la UE y por el que España lleva apostando desde su gestión de la crisis migratoria de los "cayucos" en 2006.

Definitivamente, se reconoce abiertamente que una lucha eficaz contra la inmigración irregular exige medidas de prevención en origen. No resulta eficaz la implementación de políticas reactivas, que abordan los aspectos más técnicos del control de las fronteras marítimas exteriores, sin la cooperación activa de los países origen y tránsito de la inmigración en ámbitos como el intercambio de información, la lucha contra las redes dedicadas a facilitar la inmigración irregular, las campañas informativas de prevención o el control de sus fronteras terrestres y marítimas.

No es posible el control de los flujos migratorios irregulares por mar sin la colaboración de los países origen y tránsito de la inmigración que prevengan e impidan las salidas irregulares desde sus costas. Sin embargo, existen los mismos obstáculos de siempre para avanzar en la consecución de acuerdos. Por un lado la visión que estos terceros países tienen de las políticas migratorias de la UE, hasta ahora más centradas en el enfoque de seguridad y control de la inmigración irregular y, por otro, el que estos países buscan incentivos como contraprestación a su apoyo al control migratorio.

Para lograr que esta cooperación sea eficaz es necesaria la construcción de una relación de confianza entre la UE y los terceros países. Es necesaria la cooperación de la UE en materias de apoyo técnico, formación, dotación de material y construcción de capacidades que les facilite la colaboración, garantizándose el respeto a los derechos humanos consagrados en las leyes internacionales. El GAMM vuelve a ser la referencia de la UE en donde circunscribir el diálogo y la cooperación con los terceros países.

Mención expresa se hace en el documento analizado de la necesidad de incentivar esta cooperación, sobre todo de los países de tránsito. Sin embargo en nuestra opinión parece razonable y, en este sentido, se echa en falta en el documento una referencia en términos de que la UE pudiera, si no condicionar los incentivos a los apoyos prestados, sí poder ejercer el necesario control del cumplimiento de los compromisos adquiridos, como por ejemplo en el ámbito de la readmisión. Sin embargo estas referencias a posturas algo controvertidas, en las que se vincula el apoyo técnico y la cooperación al desarrollo, a la eficacia y cumplimiento de los acuerdos alcanzados en materia de control y gestión migratoria, han desaparecido expresamente de los documentos políticos europeos desde el año 2011.

Así mismo, es muy importante destacar que esta colaboración con los terceros países se plantea tanto en el corto como en el largo plazo. A corto plazo, alcanzando acuerdos de colaboración operativa en el ámbito de los intercambios de información y apoyo técnico, como el Seahorse Mediterráneo, que incluyan medidas encaminadas a luchar contra la inmigración irregular y las redes criminales que la facilitan, identificando en estos ámbitos los Estados norteafricanos y de la región del Sahel que sean de interés como Túnez, Egipto, Sudán, Nigeria y Libia, y con los que se busca implementar acciones concretas para impedir que los viajes irregulares por mar puedan emprenderse y que incluyan también las campañas de información, tanto advirtiendo de los peligros de la inmigración irregular por mar como de los canales disponibles que favorecen la

inmigración legal; las iniciativas diplomáticas en el marco del GAMM[16]; los acuerdos de movilidad como los alcanzados con Túnez y Marruecos y los que se proyecta alcanzar con Jordania, Egipto, Libia, Argelia y Líbano, estudiando caso por caso el apoyo en la construcción de capacidades.

En el medio plazo, se propone el apoyo de la organización internacional de policía criminal (INTERPOL) a la mejora de las capacidades de intercambio de información con África y la creación de una comunidad de policías de África (AFRIPOL), así como el impulso a los programas de retorno voluntario asistido y finalmente, también en el largo plazo, centrándose la UE en el desarrollo de la dimensión exterior de las políticas buscando solucionar las causas origen de las migraciones.

El problema más acuciante se plantea en Italia, donde la composición de los flujos es mixta y no es fácil llegar a acuerdos con países como Libia, lugar en el que actualmente existe una situación de inestabilidad política e inseguridad que limita las posibilidades de alcanzar estos acuerdos. Por esta razón, la Comisión propone como primera prioridad el apoyo a Libia en su lucha contra el terrorismo, lo que permitirá sin duda mejorar su situación de seguridad y gobernabilidad alcanzando una mayor estabilidad, apoyando a la vez la implementación en este país de la legislación internacional en materia de asilo y de garantía de la protección internacional y los derechos humanos. En este ámbito es donde la reforma del sector seguridad libio, para crear las condiciones de seguridad necesarias en el país y la cooperación técnica en el ámbito de la gestión integrada de sus fronteras, alcanza su mayor significado. La operación en curso de asistencia fronteriza de la UE (EUBAM) y el proyecto Sahara-Mediterráneo se han configurado como dos herramientas de la vertiente exterior de la política migratoria de la UE de la máxima importancia, por lo que una mayor implicación de los Estados miembros y de FRONTEX a estas iniciativas sería muy deseable.

Sin embargo, es muy importante destacar la recomendación, aunque tímida y breve, para discutir la participación de los terceros países de salida en operaciones de control del mar en el marco de FRONTEX y del sistema europeo de vigilancia de fronteras (EUROSUR). La cooperación con los terceros países en el control de sus aguas territoriales, impidiendo la salida de la inmigración irregular mediante la puesta en marcha de patrullas conjuntas, recomendada en este documento, es una de las herramientas más eficaces de control de los flujos migratorios irregulares por mar, como así lo demuestran las operaciones puestas en marcha por la Guardia Civil española en el escenario Atlántico desde 2006 y que han permitido evitar muchas pérdidas de vidas humanas.

En efecto, estas medidas deben aplicarse simultáneamente a un control eficaz de las fronteras terrestres y las costas, que permitan poner en marcha operaciones de retorno de los inmigrantes a los lugares más cercanos y seguros, en cumplimiento de la legislación internacional, lo que exige apoyo de formación a los terceros países en estas capacidades y en materia de salvamento y rescate en la mar.

16 El documento menciona las „joint demarches“ como la acción diplomática conjunta de los representantes de la UE y de los diferentes Estados miembros en los países de origen y tránsito, coordinada por el Servicio de Acción Exterior y la Comisión que incluya la negociación de acuerdos de readmisión, de establecimientos de sistemas de protección internacional, de lucha contra las redes criminales que facilitan la inmigración irregular o de identificación y redocumentación de repatriados.

Sin embargo, a pesar de las referencias al papel de FRONTEX en el desarrollo de la participación de los terceros países en el Mediterráneo, éste resulta de alguna manera limitado a facilitar la cooperación operativa entre los Estados miembros y los terceros países en el marco de la política de relaciones exteriores de la Unión[17], quedando los cometidos negociadores en manos de las Instituciones europeas y/o los Estados miembros. Sin embargo, en materia negociadora, el Consejo de Administración de FRONTEX adoptó el 1 de septiembre de 2006 una Decisión[18], en virtud de la cual se precisa el procedimiento que debe seguir la Agencia para negociar y concluir acuerdos con terceros Estados y organizaciones internacionales[19].

En opinión de Mariola Urrea FRONTEX dispone de personalidad jurídica propia pero "carece por completo de subjetividad internacional, por lo que no dispone de capacidad para celebrar tratados internacionales" sino acuerdos de trabajo[20] o técnicos, no publicados en principio por razones de seguridad, con organismos de los Estados miembros, como pueden ser por ejemplo los Ministerios del Interior o las Agencias de vigilancia y protección de fronteras (Urrea, 2012:157-173). La consecuencia directa de esta limitación de la Agencia es que para poder realizar patrullas conjuntas en aguas territoriales de terceros países es necesario que los Estados miembros celebren acuerdos internacionales con aquéllos.

2.2.2. La lucha contra la trata y el tráfico de personas

Destaca en esta segunda línea de acción el que la Comisión pretende reforzar el papel de EUROPOL en los cometidos de análisis que ha recibido como mandato en el ámbito de los tráficos ilegales, incorporando un equipo dedicado al crimen organizado (tráfico de seres humanos), así como la puesta en marcha de dos planes de acción EMPACT[21] en materia de tráfico de seres humanos e inmigración irregular.

Se pone de manifiesto la necesidad de elaborar un plan integral de la UE y disponer de unas reglas de procedimiento operacional que, siendo respetuosos con la carta de

17 Artículo 14 del Reglamento (CE) 2007/2004 del Consejo en la nueva redacción que le otorga al mismo el Reglamento 1168/2011 del Parlamento Europeo y del Consejo de 25 de octubre de 2011.

18 La Decisión a la que hacemos mención puede ser consultada en http://www.frontex.europa.eu/minutes_and_decisions/decisions/page5.html. Sólo 20 días después de la aprobación de dicha Decisión el Consejo de Administración de FRONTEX autorizó al director ejecutivo la negociación de una cooperación operativa entre la Agencia y Croacia.

19 El citado procedimiento, disponible en la página web de FRONTEX, se articula básicamente de la forma siguiente. El director ejecutivo de la Agencia es el encargado de presentar un borrador de mandato al Consejo de Administración en el que se incluirán las directrices de negociación. Para ello, la Agencia consultará a los Estados miembros y a la Comisión. Una vez aprobado el mandato por el Consejo de Administración, el director ejecutivo negocia con las autoridades del país tercero o, en su caso, con la organización internacional. Una vez logrado el acuerdo, y tras ser nuevamente consultada la Comisión, el director ejecutivo lo trasladará al Consejo de Administración, que ofrecerá la versión definitiva. Corresponde la firma al director ejecutivo.

20 Se ponen de manifiesto también dudas jurídicas sobre la posibilidad de que una Agencia de la UE tenga competencias para celebrar acuerdos de esta naturaleza en MARTÍN Y PÉREZ DE NANCLARES, José. "Seguridad y acción exterior de la Unión Europea: la creciente relevancia de la dimensión exterior del espacio de libertad, seguridad y justicia". Revista del Instituto Español de Estudios Estratégicos. Núm. 0 / 2012.pp-135-154.

21 Plataforma multidisciplinaria europea contra las amenazas del crimen organizado (EMPACT-European Multidisciplinary Platform against Criminal Threats). Se trata de proyectos que pondrán en marcha planes de operaciones (OAPs) para luchar contra las amenazas prioritarias del crimen organizado.

los derechos fundamentales de la UE, desarrollen y apliquen una estrategia de lucha contra el tráfico de inmigrantes que implique a los Estados miembros, las agencias de la UE, terceros países, oficiales de enlace en los países de origen y tránsito y organizaciones internacionales y regionales relevantes. Señala al Comité permanente de Seguridad Interior (COSI)[22] como el responsable de la eficaz implementación de las operaciones conjuntas y la coordinación de aquellos aspectos concretos en este ámbito que se pretende recoger en la futura Estrategia de Seguridad Marítima europea.

Resulta fundamental en esta línea de acción la implementación efectiva de la herramienta de intercambio de información entre los Estados miembros y EUROPOL, exhortando la Comisión, además, a que las Agencias Frontex y Europol lleguen a un acuerdo operativo sin dilación de tiempo que contemple la posibilidad de intercambiar datos personales, fundamentalmente en la dirección EUROPOL a EUROSUR, con la finalidad de luchar contra el crimen transfronterizo. Sin embargo hay que tener en cuenta las restricciones reglamentarias que la Agencia Frontex tiene respecto al tratamiento de datos personales, aspecto que se ha puesto de manifiesto como una clara limitación operativa en el desarrollo del sistema EUROSUR.

2.2.3. Salvar las vidas de los inmigrantes en la mar

La cuarta línea de acción se refiere al refuerzo de la vigilancia fronteriza que contribuya a mejorar la situación en el escenario Mediterráneo y a proteger y salvar vidas de los inmigrantes. El refuerzo de las operaciones de FRONTEX y del papel que desempeña en la coordinación de operaciones de vigilancia y control de las fronteras marítimas no debe significar, sin embargo, que sus cometidos pasen a ser de salvamento y rescate por varias razones.

En primer lugar, porque esta función queda fuera del mandato inicial que ha recibido la Agencia. En segundo lugar porque la función genérica de salvamento y rescate en la mar es una competencia de los Estados miembros, para la que cuentan con organismos de salvamento marítimo competentes en esta materia, en la que colaboran todos los medios en la mar en aquellos casos contemplados en la legislación internacional específica, como el Convenio SOLAS, que nada prevé en el ámbito del control migratorio en operaciones marítimas. En tercer lugar, porque el salvamento y rescate en la mar nada tiene que ver con las operaciones policiales de seguridad pública o de “Law Enforcement” como el control de las fronteras marítimas y, por últi-

22 “Por el artículo 71 del Tratado de Funcionamiento de la Unión Europea (TFUE) se crea un Comité Permanente de Seguridad Interior (COSI) dentro del Consejo. Este está compuesto por miembros de los ministerios nacionales competentes, asistidos por representaciones permanentes de los Estados miembros frente a la Unión Europea (UE) en Bruselas, y por la secretaría del Consejo. El principal objetivo de este comité consiste en facilitar, promover y reforzar la coordinación de las acciones operativas entre los Estados miembros de la UE en el ámbito de la seguridad interior. Para ello actuará en los campos de la cooperación policial y aduanera, la protección de las fronteras exteriores y la cooperación judicial en materia penal, entre otros. Regularmente presentará un informe de sus actividades al Consejo, quien informará de ello al Parlamento Europeo y a los parlamentos nacionales. El COSI también será responsable, al igual que el Comité Político y de Seguridad (COPS), de asistir al Consejo en virtud de la “cláusula de solidaridad” (artículo 222 del TFUE). El COSI no participará en la elaboración de actos legislativos ni en la ejecución de operaciones.” Disponible en http://europa.eu/legislation_summaries/glossary/internal_security_committee_es.htm

mo, porque confundir los objetivos fundamentales de las operaciones de vigilancia y control de la frontera exterior marítima con las tareas de salvamento y rescate en la mar en cumplimiento de la legislación internacional supondría el peligro de enviar un mensaje equivocado a los organizadores y facilitadores de estos "viajes de la muerte" llevándoles al convencimiento de que el dispositivo aeromarítimo se refuerza con la idea de aumentar las capacidades de salvamento y no de cerrar las rutas marítimas de inmigración irregular a la UE.

Este refuerzo de la vigilancia fronteriza en el mar que realizan los Estados está basado en los propios esfuerzos nacionales y en la implementación de operaciones de la Agencia en el Mediterráneo, creándose una Red de Patrullas europeas que disponen del sistema de intercambio de información EUROSUR.

Sin embargo hay que poner de manifiesto algunas carencias que se observan en la decisión de la TFM. En primer lugar, y como así reconoce el documento, se hace muy necesario disponer de una regulación sobre los procedimientos de actuación en la vigilancia y control de las fronteras marítimas exteriores, o lo que es lo mismo de un Reglamento de operaciones marítimas FRONTEX[23].

En segundo lugar, otro problema en el que surgen dificultades es la financiación de las operaciones de vigilancia y control marítimo coordinadas por FRONTEX. Las operaciones de FRONTEX continúan basándose en un sistema voluntario de contribuciones de medios aeromarítimos de los Estados a las operaciones. A este respecto se ha propuesto como incentivo el que los Estados anfitriones, también de forma voluntaria, no exijan el pago del IVA a los Estados participantes durante las operaciones conjuntas.

Otro aspecto que no queda claro, en tercer lugar, son los términos reguladores de la participación de la EASO en las labores de identificación y evaluación de los solicitantes de asilo en los flujos migratorios "mixtos" en el marco de las operaciones coordinadas por FRONTEX. Y otra cuestión política que requiere un urgente desarrollo normativo práctico es el de la asistencia y solidaridad con los Estados miembros que se ven afectados por grandes presiones migratorias. La Unión Europea sigue sin tener claro qué hacer con los inmigrantes que ponen pie en suelo europeo. ¿Debe seguir siendo voluntaria la clausula de solidaridad?. Por un lado, en el caso de la crisis de Lampedusa 2013, la Comisión ha asignado unos fondos de 30 millones de euros extra a Italia y 20 millones de euros a otros Estados miembros que no tienen capacidad suficiente para asumir las presiones migratorias y para hacer frente a las operaciones de vigilancia de la frontera bajo mandato FRONTEX, así como mejorar las capacidades de acogida e identificación de inmigrantes, permitiéndose además en casos de entrada masiva de inmigrantes recurrir al mecanismo europeo de protección civil (EU-CPM). Por otro lado, se señala el necesario papel que en estos procesos deben tener Agencias como EASO, UNHCR e IOM, aunque tampoco queda definido.

23 El 26 de abril de 2010 se completó el Código de fronteras Schengen (Decisión del Consejo de 26 de abril de 2010; DOUE L.111/20, 4/5/2010) en la parte del ámbito de la vigilancia de las fronteras marítimas exteriores en operaciones coordinadas por Frontex. Sin embargo una sentencia del Tribunal de Justicia de la UE anuló esta Decisión del Consejo 2010/252/UE que completaba el Código de Fronteras, aun manteniendo los efectos de la misma hasta la entrada en vigor de una nueva normativa.

Por último, cabe mencionar que estos instrumentos descritos por la TFM requieren del impulso de la cooperación interagencias en el intercambio de información y datos de posicionamiento. En este marco resulta decisiva la importancia de EUROSUR y su integración en la tercera fase con el entorno de intercambio de información común para el dominio marítimo (CISE), desarrollado conjuntamente por la Comisión y los Estados miembros. Así mismo, el impulso de la Comisión a la integración de los sistemas de posicionamiento y vigilancia del mar compartiendo la información y permitiendo que este sistema sea alimentado por, entre otros, los proyectos Perseus y Closeye, liderados por la Guardia Civil, o el servicio proporcionado por la Agencia de Seguridad Marítima Europea (EMSA) y el centro de satélites de la UE.

2.3. LA PARTICIPACIÓN DE LOS RECURSOS MILITARES EN OPERACIONES AEROMARÍTIMAS DE LAW ENFORCEMENT Y LA DIMENSIÓN EXTERIOR DEL ESPACIO DE LIBERTAD SEGURIDAD Y JUSTICIA (ELSJ)

El 14 de octubre de 2013 el ministro del Interior Angelino Alfano dio luz verde a la operación “Mare Nostrum” calificada como “militar y humanitaria” y prevista para reforzar el dispositivo de vigilancia y salvamento en alta mar[24]. Esta operación, que comenzó el 18 de octubre de ese año, es coliderada por el Ministerio del Interior y la Armada italiana bajo el mando de ésta y está utilizando por primera vez una nave anfibia para el mando y control de las operaciones con helicópteros y capacidades hospitalarias y de alojamiento, embarcando además a expertos de diferentes agencias de seguridad italianas y representantes de organizaciones humanitarias y legales[25].

El dispositivo está formado por cuatro navíos, dos patrulleros y dos fragatas con la finalidad de disuadir a quienes piensen que pueden traficar con seres humanos impunemente, interceptar los llamados “barcos de la muerte” y detener a las tripulaciones. Definida como una misión militar humanitaria íntegramente italiana, el entonces primer ministro Enrico Letta, tras los acontecimientos desgraciados de octubre y la acusación a FRONTEX de dar más importancia a la gestión migratoria en otras fronteras, puso en marcha una operación en el canal de Sicilia triplicando el número de aviones y naves que patrullan esa zona del Mediterráneo, incluso introduciendo el uso de drones para la vigilancia del mar[26].

Esta operación ha debido ser coordinada para evitar duplicidades con la operación marítima de vigilancia de fronteras puesta en marcha en el Mediterráneo en las áreas de Lampedusa e islas Pelagicas, el sur de Sicilia y Malta y el sudeste de Siracusa, impulsada por la Comisión y basada en la Red Europea de Patrullas (EPN) para reforzar la misión de protección y salvamento de las vidas de los inmigrantes.

Italia ha apostado en su política de vigilancia y control de los flujos migratorios en el mar por que las operaciones en el Mediterráneo Central se basen fundamentalmente en el salvamento y rescate en la mar. El argumento principal de Italia es que el tipo de los flujos migratorios con destino a Italia ha cambiado. La primavera árabe y los flujos migratorios procedentes de Túnez se consideraron migraciones económicas.

24 http://www.governo.it/Notizie/Palazzo%20Chigi/dettaglio.asp?d=73282
25 Disponible en http://www.interno.gov.it/mininterno/site/it/sezioni/sala_stampa/notizie/immigrazione/2013_10_15_mare_nostrum.html
26 http://www.abc.es/internacional/20131014/abcp-italia-militariza-mediterraneo-para-20131014.html

Los últimos acontecimientos de Italia, con la llegada masiva de ciudadanos sirios, sitúan los flujos en el Mediterráneo central de carácter eminentemente mixto.

Esta nueva situación y tanto la postura de la Comisión como las medidas emprendidas por Italia tienen un doble efecto, por un lado pueden provocar un efecto llamada ya que el mensaje que se envía a las organizaciones criminales es el de que se va a tratar de salvar a todos los que emprendan el viaje por mar, aumentando las posibilidades de quedarse en territorio europeo con protección internacional, y por otro se desvirtúan las misiones que FRONTEX tiene encomendadas de coordinación de operaciones de vigilancia y control, pero no de salvamento y rescate, funciones que son competencia nacional de los Estados, que cuentan con Unidades específicas para ello.

Los datos disponibles actualmente refuerzan la hipótesis de este efecto llamada. Según declaraciones del ministro de Interior Angelino Alfano el 28 de mayo pasado ante el Comité Parlamentario italiano del Acuerdo Schengen, de Vigilancia de la Actividad de Europol, Control y Vigilancia en materia de inmigración, casi 54.000 inmigrantes irregulares han llegado a Italia en los primeros cinco meses de 2014 frente a los 43.000 durante todo el año 2013.

Si bien otros Estados de la Unión como España han puesto en marcha en un principio operaciones exclusivamente militares en el ámbito de la lucha contra la inmigración irregular por mar, como fue la operación Noble Centinela, liderada por la Armada en 2006, resulta muy significativa en este contexto la posición de la Comisión en el documento de la TFM sobre la implementación de otras operaciones complementarias u otros medios militares aeronavales que refuercen la vigilancia y control en el mar. Se refiere el texto a aquellas contribuciones de los Estados con operaciones aeronavales militares complementarias a las desarrolladas por Frontex, como la italiana Mare Nostrum para aumentar la capacidad de detección temprana de inmigrantes irregulares en el mar y así ser más eficaces en la prevención de pérdida de vidas humanas. De estas operaciones aeronavales dice que tienen que ser respetuosas en sus procedimientos con los derechos fundamentales y el principio de no devolución (non-refoulement), deberán estar coordinadas con las operaciones de Frontex y se les aplicará la regulación dispuesta en el marco legal de Frontex y Eurosur. El nivel de consenso sobre estos aspectos en la UE se ha alcanzado solo gracias a abrir la puerta a las contribuciones de medios militares en operaciones policiales, siempre que lo permitan las legislaciones nacionales. En este punto encontramos posiciones antagónicas. Italia no ha dudado en poner en marcha la operación Mare Nostrum y, sin embargo, países como Alemania, por razones históricas, políticas y jurídicas, no permite el empleo de medios militares en operaciones de seguridad pública o Law Enforcement.

Los principales problemas a los que se enfrenta el empleo de medios militares en este tipo de operaciones, siempre y cuando las legislaciones nacionales lo permitan, son los necesarios consensos que hay que alcanzar sobre los detalles de la subordinación de estas operaciones complementarias con medios militares a los Planes de operaciones del ámbito de la Law Enforcement, los problemas de confidencialidad de la información que es necesario compartir y que afectan a aspectos relacionados con el tipo y posicionamiento de medios de defensa, como se hace constar en la regulación de EUROSUR, así como el alto coste de su empleo con el consiguiente gasto del

presupuesto; como ejemplo la operación Mare Nostrum, que tiene un coste de cuatro millones de euros mensuales[27].

Tras la llamada de atención de Italia a la Comisión el 24 de octubre sobre las iniciativas que era necesario abordar por parte de la UE para hacer frente a la inmigración irregular en el Mediterráneo central, se comenzó de nuevo a plantear en el ámbito de la política de seguridad y defensa común la posibilidad de aportar soluciones complementarias a la acción global de la UE[28].

En materia de control de flujos migratorios por mar no podemos olvidar que a pesar de ser un tema tratado en el ámbito de la política común del espacio de Libertad, Justicia y Seguridad (ELSJ), como aspecto de seguridad pública o "Law Enforcement", la Unión Europea trata de desarrollar la estrategia de seguridad marítima común (EESM) bajo el paraguas de la política común de seguridad y defensa (PCSD), cuyo proyecto está ya aprobado en el ámbito del Consejo de la UE. Esta EESM tiene como reto llegar a concretar el marco jurídico y político en el que será desarrollada, respetando los diferentes modelos nacionales de seguridad pública y las competencias de los distintos Organismos e Instituciones involucrados en la seguridad marítima en los Estados miembros. En opinión de José Martín y Pérez de Nanclares (Martín, 2012: 135-154), la dimensión exterior del ELSJ reunía hasta la entrada en vigor del Tratado de Lisboa dos características: por un lado, la parte fundamental de la cooperación internacional con terceros países en materia de Justicia e Interior recaía en los Estados miembros y, por otro, el complejo sistema de toma de dicisiones y procedimientos legislativos basado en los tres "pilares", anterior al Tratado de Lisboa, obstaculizaba una acción exterior eficaz. Sin embargo, sigue afirmando este autor, "con la entrada en vigor del Tratado de Lisboa, se ha cerrado un largo proceso que, a diferencia de lo ocurrido con la Política Europea de Seguridad Común (PESC), concluye con la plena "comunitarización" (competencial, institucional y normativa) de los asuntos de Justicia e Interior en el contexto del espacio de Libertad, Seguridad y Justicia. Por tanto, como en todas las demás competencias de la Unión, esta acción tiene una acción interior (en relación con los Estados miembros), pero también proyecta una acción exterior". Desde la puesta en marcha del Programa de Estocolmo la dimensión externa de las políticas del ELSJ es una prioridad para la UE y una necesidad para cumplir sus objetivos en este ámbito. Sobre este último punto son varias las razones que apunta Martín y Pérez de Nanclares (Martín, 2002: 343-391): en primer lugar toda política comunitaria tiene una dimensión externa reconocida por el Tribunal de Justicia que "ha reconocido a través de su asentada doctrina in foro interno in foro externo[29]"; en segundo, en razón de la materia que trata el ELSJ, resulta indivisible la dimensión interior y exterior de sus políticas que, adoptadas en primer lugar para el ámbito interior, "ya poseen per se una cierta dimensión exterior que afecta a países terceros", como por ejemplo en materia de lucha contra la inmigración ilegal, los

27 http://www.publico.es/internacional/527705/la-marina-italiana-rescata-a-1-812-inmigrantes-en-el-canal-de-sicilia

28 Council of the European Union. "Migration Flows in the Southern Neighbourhood and their External Relations perspectiva-Possible Avenues for Dialogue and Cooperation with Partner Countries, including Options for a CSDP Operation". Bruselas, 19 de noviembre de 2013. Disponible en http://register.consilium.europa.eu/pdf/en/13/st16/st16394.en13.pdf

29 Sentencia de 3 de marzo de 1971, ASUNTO 22/70 que reconoce que la Comunidad en todos aquellos ámbitos en que el Tratado le atribuya una competencia expresa (in foro interno) ostentará también una competencia externa implícita (in foro externo) en ese mismo ámbito. Disponible en http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:61970CJ0022:ES:PDF

acuerdos de cooperación policial, los intercambios de información o los de repatriación de los inmigrantes en situación irregular a sus países de origen. La finalidad de la PCSD en este ámbito debe ser, por tanto, reforzar las capacidades en seguridad marítima de la UE y definir el concepto de apoyo a una Gestión Integral de Fronteras.

El punto de acercamiento entre las dos políticas se ha venido tratando en los foros del COSI, donde se ha hablado de los flujos migratorios en los países del sur y sus relaciones exteriores, buscando el diálogo y la cooperación entre los países implicados, incluyendo el estudio de las opciones en el marco de la PCSD.

Tras los sucesos de Lampedusa, encontramos también diferentes posiciones en el seno de las Instituciones de la UE sobre la finalidad de las operaciones.

La Comisión se muestra en general favorable a que las operaciones de FRONTEX en el Mediterráneo central tengan como objetivo esencial el salvamento y rescate en la mar y que se refuercen las fórmulas de acceso a la protección internacional de los inmigrantes. En esta línea tanto la Comisión como Italia, impulsadas por el impacto político de este tipo de crisis, pretenden definir medidas a corto plazo de inmediata implantación. Sin embargo el problema de los flujos migratorios irregulares exige la adopción de estrategias a medio y largo plazo y, por supuesto, acciones inmediatas de choque que consigan hacer frente a la situación en el Mediterráneo. Esta última visión es la de una mayoría de países de la UE como España, Alemania o Francia, que desean impulsar la participación de FRONTEX, la mejora de las capacidades de vigilancia y control del mar, así como las de salvamento y rescate. España reconoce que el elemento fundamental para evitar los flujos ilegales reside en la prevención en origen. Este elemento es el que no se define y recoge como esencial en el documento de la TFM. El Servicio de Acción Exterior de la UE (SEAE), por su parte, considera que es hora de alejarse del enfoque que centra las soluciones en los aspectos de la seguridad de las fronteras y volcarse más en la puesta en marcha de políticas que impulsen las relaciones exteriores con terceros países, donde hay que afrontar las causas directas que producen los movimientos migratorios y propugnar que los países origen y tránsito inicien reformas de sus marcos legales y administrativos en el ámbito migratorio.

El SEAE tiene claro que cualquier iniciativa que se adopte en materia migratoria por la Unión Europea debe situarse en el contexto de las relaciones de la Unión con terceros países y estar coordinada con los principios de actuación marcados en la política general migratoria de la Unión definidos en la política de vecindad y en el GAMM.

La complejidad del escenario mediterráneo central es evidente por tres razones: los flujos migratorios son mixtos, existe actualmente un marcado enfoque del fenómeno migratorio desde los aspectos vinculados a la seguridad y hay una situación política inestable y de inseguridad en el escenario Mediterráneo.

En este escenario está previsto que a largo plazo los flujos de tipo mixto crezcan, aumentando las necesidades de asilo y protección internacional, lo que ocasiona a su vez un incremento de la actividad criminal y proliferación de redes dedicadas al tráfico de personas. A diferencia del año 2011, en el que los flujos migratorios como consecuencia de la primavera árabe los constituían ciudadanos procedentes de Túnez (definiéndose como migración económica), en 2013 estos flujos se convirtieron fundamentalmente en flujos migratorios de personas procedentes de Siria (15.700 sirios entre enero y septiembre de 2013 entraron en la UE y de ellos 5.904 utilizando

la ruta marítima del Mediterráneo central), Somalia y Eritrea que, necesitadas de protección internacional o solicitantes de asilo, utilizan fundamentalmente la ruta del Mediterráneo central. Esta situación se ha producido por el aumento del número de ciudadanos somalíes y eritreos en esta ruta como consecuencia del cierre de la ruta del Sinaí, tras el levantamiento de la muralla entre el Líbano e Israel en 2012.

Por otro lado, estos terceros países en general tienen un interés limitado en abordar el fenómeno migratorio, desde el punto de vista de la seguridad y el control de la inmigración irregular, con políticas estables de cooperación activa de larga duración, ya sea por que no comparten del todo la visión que del control de los movimientos migratorios tiene la Unión Europea, demasiado enfocada en impedir el cruce de las fronteras exteriores y la política de repatriaciones; ya sea por que no ven compensada suficientemente o incentivada su colaboración con políticas simultáneas de la UE de amplio espectro, que favorezcan las migraciones legales de sus nacionales; ya sea por que no tienen plena voluntad de aplicar marcos legales internacionales en materia migratoria y de asilo, así como cooperar con UNHCR, buscando que los Estados miembros compartan solidariamente cupos de personas con derecho a ser protegidas internacionalmente, asentándolos en sus territorios. De cualquier manera es necesario tener en cuenta las diferentes perspectivas, sensibilidades e intereses de los terceros países a la hora de explorar voluntades y diseñar las políticas de acercamiento y negociación de acuerdos de cooperación globales.

En esta línea, el Servicio de Acción Exterior propone, en el marco del diálogo con los terceros países origen y tránsito de la inmigración irregular, establecer una relación de confianza en donde se traten de abordar las migraciones como elemento especialmente relevante, pero desde un enfoque global y a largo plazo de la UE. Para ello la Unión Europea tiene que aprovechar las oportunidades que le ofrecen los países del Mediterráneo en la actual situación de inestabilidad política y social e inseguridad ciudadana por la que pasan. Hay que buscar el marco global de la cooperación adecuado en el que se integren tanto las capacidades militares con las policiales en misiones de apoyo técnico en ámbitos como el de las reformas del sector seguridad de estos países, el apoyo a la gestión de sus fronteras o de los flujos migratorios y el refuerzo de las capacidades de las Instituciones para el “Rule of Law”, como los diálogos sobre migraciones, movilidad y seguridad. Buen ejemplo de esto es la misión sobre fronteras EUBAM Libia[30], que nació con el objetivo de asistir a las autoridades libias en el fortalecimiento de la seguridad en las fronteras terrestres, aéreas y marítimas (Díez, 2013: 1-8). El SEAE propone que la PCSD apoye las capacidades locales de lucha contra el tráfico de seres humanos, el tráfico ilegal en el mar, el contrabando de seres humanos y la inmigración ilegal, así como reforzar las capacidades de vigilancia e interceptación con las que simultáneamente se incrementarían las capacidades para salvar personas en peligro. Asímismo, se sugiere la implementación de operaciones marítimas en alta mar con medios militares, complementarias a las desarrolladas por FRONTEX y por las autoridades militares italianas, como la operación Mare Nostrum, en el marco de la lucha contra la inmigración irregular en alta mar para disuadir el tráfico de seres humanos mediante el control, interceptación y detención de facilitadores de inmigración irregular, aumentando la capacidad de respuesta en materia de interceptación, así como de salvamento y

30 Misión a la que el Consejo de la Unión Europea dio luz verde el 22 de mayo de 2013, con un mandato inicial de dos años, en el marco de la Política Común de Seguridad y Defensa.

rescate en la mar y potenciando el intercambio de información. La PCSD propone cooperar entre actores de la seguridad interna y externa, reforzando las operaciones de FRONTEX con medios principalmente militares de los que la Agencia no dispone, para el control de fronteras como aviones de patrulla de largo alcance. No serían operaciones PCSD propiamente dichas. No plantearían problemas de duplicación de sistemas de mando y control, así como de los procedimientos operativos y el marco legal en donde se desarrollan, pues quedaría regulado por los planeamientos operacionales de FRONTEX. Se incrementarían de esta manera las capacidades de vigilancia y por lo tanto las de salvamento y rescate de personas en peligro en la mar.

Sin embargo, la implicación de poner en marcha operaciones marítimas en alta mar en el marco de la PCSD, para la lucha contra la inmigración irregular por mar, no está exenta de problemas, como afirma el propio Servicio de Acción Exterior. Y es que algunos Estados miembros ven con recelo el empleo de medios militares en el ámbito de las operaciones de lucha contra la inmigración irregular, aunque la acción conjunta implique que embarque personal de las fuerzas de seguridad en los medios navales militares. La implementación de estas operaciones se considera con frecuencia una respuesta desproporcionada y una reiteración de esfuerzos en el Mediterráneo central, donde se desarrollan actualmente las operaciones HERMES y AENEAS bajo mandato de FRONTEX, con procedimientos y estructuras de mando, control y planeamiento específicas. Además debe valorarse el impacto que podría tener en la opinión pública la “militarización” de la respuesta a la inmigración irregular en el mar. FRONTEX se opone a la inclusión en su despliegue de medios militares por dos razones fundamentales: son excesivamente caros de mantener en operaciones, lo que supone una parte importante del presupuesto total, y en general muestran recelos para integrarse bajo mando y coordinación de los Centros de Coordinación Nacional de las operaciones (NCC) quienes, según dispone el Reglamento de EUROSUR, son los responsables de coordinar las acciones operativas en la mar y los intercambios de información dirigidos a luchar contra la inmigración irregular, de determinar los niveles de impacto a las zonas fronterizas exteriores y de fijar las medidas a adoptar según estos niveles de impacto.

De tal forma que la definición concreta del marco legal, además de los procedimientos específicos en los que se desarrollaría una operación propia de “Law Enforcement” con medios militares, responsabilidad por tanto de los Ministerios del Interior, la delimitación de funciones de los actores con participación en las operaciones, la aplicación del principio de non-refoulement y los procedimientos específicos de interceptación en el marco del cumplimiento de las leyes internacionales sobre asilo y protección de refugiados son los nuevos retos a los que van a enfrentarse los Estados de la UE en un futuro muy cercano.

BIBLIOGRAFÍA

Agencia Efe. Los inmigrantes de Túnez llegados a Italia podrán ir a los países del área “Schengen”. El Mundo. 07/04/2011. Disponible en: http://www.elmundo.es/elmundo/2011/04/06/internacional/1302113673.html

Agencia Efe. Francia suspende los trenes desde Italia para frenar la entrada de inmigrantes. El Mundo. 17/04/2011. Disponible en: http://www.elmundo.es/elmundo/2011/04/17/internacional/1303045656.html

De Bruycker, P., Di Bartolomeo, A., y Fargues, P. (2013). Migrants smuggled by sea to the EU: facts, laws and policy options. MPC Research Report 2013/09, 2-27. Disponible en: http://www.migrationpolicycentre.eu/docs/MPC-RR-2013-009.pdf

Der Spiegel. Flüchtlinge aus Nordafrika: Deutschland will Grenzen stärker kontrollieren": "Die Bundesregierung reagiert auf den Flüchtlingsstrom aus Nordafrika nach Europa: Innenminister Friedrich kündigt verschärfte Grenzkontrollen an - und warnt Italien, Vertriebene nach Frankreich oder Deutschland ausreisen zu lassen. 11/04/2011. Disponible en: http://www.spiegel.de/politik/deutschland/fluechtlinge-aus-nordafrika-deutschland-will-grenzen-staerker-kontrollieren-a-756242.html

Díez, J. (2013). EUBAM Libia: seguridad fronteriza para la estabilización nacional y regional. Documento de Análisis del Instituto Español de Estudios Estratégicos, 36/2013, 1-8. Disponible en: http://www.ieee.es/Galerias/fichero/docs_analisis/2013/DIEEEA36-2013_EUBAM_Lybia_JDA.pdf

European Commission. Frequently Asked Questions: Addressing the Migratory Crisis. MEMO/11/273. 04/05/2011. Disponible en: http://europa.eu/rapid/press-release_MEMO-11-273_en.htm?locale=en

European Commission. Schengen: La Comisión de la UE propone un enfoque europeo para proteger mejor la libre circulación de los ciudadanos. IP/11/1036. 16/09/2011. Disponible en: http://europa.eu/rapid/press-release_IP-11-1036_es.htm?locale=en

European Commission. Communication from the Commission to the European Parliament and the Council on the work of the Task Force Mediterranean. COM(2013) 869 final. 04/12/2013. Disponible en: http://ec.europa.eu/dgs/home-affairs/what-is-new/news/news/docs/20131204_communication_on_the_work_of_the_task_force_mediterranean_en.pdf

European Commission. Communication from the European Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: The Global approach to migration and mobility. COM(2011) 743 final. 18/11/2011. Disponible en: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52011DC0743&from=EN

González, C. (2011). ¿Schengen en peligro?. Real Instituto Elcano, ARI 88/2011, 1-6. Disponible en: http://www.realinstitutoelcano.org/wps/wcm/connect/c98ebb0046cde98888ebbbc4d090bb2e/ARI88-2011_Gonzalez_Enriquez_Shengen_peligro.pdf?MOD=AJPERES&CACHEID=c98ebb0046cde98888ebbbc4d090bb2e

Martín, J. (2012). Seguridad y acción exterior de la unión europea: la creciente relevancia de la dimensión exterior del espacio de libertad, seguridad y justicia. Revista del Instituto Español de Estudios Estratégicos, 0/2012, 135-154. Disponible en: http://revista.ieee.es/index.php/ieee/article/view/13/14

Martín, J. (2002). La delimitación de competencias entre la unión europea y los estados miembros: sobre el difícil equilibrio entre la flexibilidad, la eficacia y la transparencia. Revista de Derecho Comunitario Europeo, 12, 343-391. Disponible en: http://repositori.uji.es/xmlui/bitstream/handle/10234/101907/Martin%20y%20Perez%20Nanclares_Delimitacion_2002.pdf?sequence=1

Ministerio de Asuntos Exteriores de Francia. Nota de prensa sobre la 29 cumbre bilateral Francia-Italia y sus relaciones políticas en general. 1/10/2012. Disponible en: http://www.diplomatie.gouv.fr/es/spip.php?page=rubrique_imprim&id_rubrique=1291

Ministerio Federal del Interior de Alemania. Entrevista al Ministro federal alemán de interior Dr. Hans-Peter Friedrich: Von Massenflucht kann derzeit keine Rede sein. 11/04/2011. Disponible en: http://www.bmi.bund.de

Serbeto, E. Bruselas apoya el bloqueo de Francia a los inmigrantes tunecinos. ABC. 19.04.2011. Disponible en: http://www.abc.es/20110419/internacional/abcp-bruselas-apoya-bloqueo-francia-20110419.html

Unidad de análisis de riesgos de FRONTEX. (2011). Annual Risks analysis 2011, 4591, 1-64. Disponible en: http://frontex.europa.eu/assets/Publications/Risk_Analysis/Annual_Risk_Analysis_2011.pdf

Urrea, M. (2012). El control de fronteras exteriores como instrumento para la seguridad: una aproximación al nuevo marco jurídico de FRONTEX. Revista del Instituto Español de Estudios Estratégicos, 0 / 2012, 155-174. Disponible en: http://revista.ieee.es/index.php/ieee/article/viewFile/14/12

Fecha de recepción: 19/05/2014. Fecha de aceptación: 24/06/2014

LA AMENAZA TERRORISTA
¿HACIA LA TERCERA GUERRA MUNDIAL?

ÁNGEL GARCÍA-FRAILE GASCÓN

Editorial Actas S.L. 28709 San Sebastián de los Reyes, Madrid 2014, 765 páginas

ISBN 9788497391405

Datos, reflexiones, análisis. Este trabajo es una puesta al día, una visión global y limitada de este fenómeno que se ha convertido en una modalidad de guerra moderna. Por su extensión y profundidad aporta una visión necesaria para fuerzas armadas y de seguridad, políticos, diplomáticos, profesores, alumnos e incluso para el gran público. El conocimiento adquirido durante su carrera profesional le hace tener una visión práctica de los acontecimientos que expone en esta obra.

Ángel García-Fraile Gascón es un general de División que durante el desarrollo de su carrera profesional compiló ardua experiencia en materia de seguridad e inteligencia. Subdirector general de Apoyo, subdirector de Planificación en la Secretaría de Estado, consejero de la presidencia de la multinacional GMV son algunos de los puestos directivos en los que desarrolló sus conocimientos y habilidades. Piloto fundador de Helicópteros y jefe del Servicio Aéreo con experiencia operativa, doctor en Ciencias Económicas e investigador operativo.

Partiendo del concepto de terrorismo, tras analizar las diferentes definiciones propuestas, el autor ve la peligrosa evolución del mismo, desde la terminación de la II Guerra Mundial, como una forma de conflicto asimétrico extendido por todo el mundo cada vez más peligroso. Las bajas que produce son cuantiosas y al afectar a múltiples países podría asimilarse a una moderna forma de guerra mundial. Recorre las situaciones conflictivas que se han ido produciendo hasta llegar a nuestros días. Transporta a los lectores a los continentes del planeta mostrándoles la evolución y los distintos comportamientos y peculiaridades del fenómeno terrorista desde una perspectiva que permite analizar los cambios profundos en la operativa violenta y el número de grupos que han surgido en todo tipo de circunstancias.

El expansionismo de la doctrina soviética y la descolonización de múltiples países hacen aparecer grupos terroristas en Latinoamérica, tras la revolución cubana, desde los montoneros argentinos y uruguayos a los peruanos de Sendero Luminoso, pasando por Brasil, Guatemala y la Venezuela de los sesenta que permite comprender la situación actual de esta última y las tensiones del cono sur. En Europa, la guerra fría fue causa de que se reactivaran viejos conflictos como el del IRA y la aparición de grupos terroristas como la Baader-Meinhof, las Brigadas Rojas o Acción Directa que tienen reflejo hasta en Japón con el Ejército Rojo Japonés. En España ETA tiene esa ideología marxista-leninista pero une un etnonacionalismo y constituye un capítulo destacado dentro del texto que contiene la génesis, el desarrollo y la situación actual.

Paralelo en el tiempo, la creación del Estado de Israel, el desplazamiento de la población palestina, la guerra de árabes e israelitas reavivando el conflicto bíblico, tiene como consecuencia la aparición de un nuevo terrorismo que pretende atraer

la atención mundial con los nuevos medios de información de masas y con ataques violentos con explosivos que aumentaban la letalidad de las acciones. Son claves del terrorismo moderno.

El conflicto kurdo repartido en cuatro Estados, Turquía, Iraq, Irán y Siria que reivindican un territorio y un estado propio, con peligrosos grupos terroristas como el PKK. También en Armenia, Chechenia y Daguestán se crean conflictos, sobre todo los chechenos con Rusia, potencia que tiene 50 millones de musulmanes en sus fronteras del sur del territorio y teme el expansionismo del islamismo radical. La mitad de las fuerzas armadas rusas son de credo musulmán. La revolución iraní provocó el ataque de Iraq por miedo al contagio. La invasión de Afganistán por los rusos apoyando al gobierno comunista dio pie a la resistencia afgana y a la formación del brigadismo árabe internacional en los campos de entrenamiento del primer núcleo de al-Qaeda (La Base), con instrucción militar y la utilización del suicidio, convertido en martirio, como forma de inmolación para llegar al Paraíso. Bin Laden era el líder, sin embargo Egipto, con larga tradición terrorista, proporcionó los primeros jefes a Al-Qaeda. Hoy actúan los “lobos solitarios” y la actividad de las células durmientes no cesa.

Los brigadistas que lucharon contra los rusos, al regresar a sus países de origen, crearon nuevos grupos terroristas en Marruecos, Argelia, Túnez, Libia, Níger, que con el tiempo van avanzando desde Mali hacia Nigeria, país con petróleo, poniendo en peligro los intereses occidentales, sobre todo los de las antiguas potencias coloniales. Al-Qaeda en el Magreb es una amenaza para el sur de Europa por su proximidad y especialmente para España con Canarias, Ceuta y Melilla en sus fronteras.

Las guerras tras la invasión de Kuwait por las tropas de Saddam Husein, la invasión de Iraq por la coalición anglo-americana y Siria, en la actualidad, producen un terrorismo permanente por la insurgencia con ribetes religiosos entre chiíes y suníes, como Hezbollah en Líbano, apoyado por Teherán, con Hamas incluso en el gobierno de Gaza. Saddam utilizó el terrorismo contra los intereses occidentales, y en el Líbano, que sufrió una guerra civil entre musulmanes y cristianos, franceses y norteamericanos sufrieron crueles atentados con innumerables bajas. De estos surge una nueva generación de terroristas que son un peligro permanente en sus respectivos países y donde se recluta su relevo, muchos procedentes de Asia, donde Indonesia es una base importante. No se queda un espacio del planeta sin analizar ni describir haciendo que el lector adquiera una conciencia global de esta amenaza latente.

En otro orden de cosas se reflexiona sobre los atentados contra los aliados de las Azores y sus consecuencias y se describe la guerra sucia en la que participan algunos países para tratar de influir en las políticas de otros. Acciones encubiertas de soviéticos y occidentales durante la Guerra Fría, la lucha en las cloacas, la guerra sucia de los servicios secretos, la infiltración dentro de los aparatos del poder etc., para muchos terrorismo de Estado, y la importancia de las relaciones bilaterales, como la colaboración francesa a España y las compensaciones que se dieron a un buen vecino sin el cual no se hubiese frenado a ETA.

Un capítulo especial dedicado a España, que tiene tras de sí cincuenta años de terrorismo. Aborda los pilares de la lucha antiterrorista: la ley, el modelo policial, el papel de las fuerzas armadas, la tecnología de seguridad, y la industria de apoyo, con las necesidades de I+D policial así como los proyectos de colaboración internacional como las bases de datos de Schengen. La aplicación de la estadística, la investigación

operativa, la psicología y la sociología tecnifican el trabajo de los investigadores contraterroristas y sugiere su empleo.

El 11-S supuso un antes y un después en la lucha contra el terrorismo. Las reacciones que produjo, sobre todo las grandes coordinaciones como el Homeland Seccurity o el papel de los sistemas informáticos y las infraestructuras críticas, la necesidad de gabinetes de análisis y de directores nacionales en la lucha antiterrorista son consecuencia de ese atentado. El uso de las nuevas tecnologías y el ciberterrorismo juegan un papel fundamental en la amenaza terrorista.

A esta obra, que surge como el desarrollo de un artículo que le encargaron al autor desde Estados Unidos, ha dedicado los seis últimos años. Se trata de la ordenación de sus investigaciones, el análisis de las causas político-económicas de los conflictos que asolan el planeta. La Amenaza Terrorista advierte de los peligros que puede generar el terrorismo, estudiando el pasado y el presente y visionando el futuro.

Lali Castellanos
F.C.E. Jefe de Sección. Gabinete Técnico. ORIS-REVISTA
Licenciada en Ciencias de la Información

INTELIGENCIA Y ANÁLISIS RETROSPECTIVO LECCIONES DE HISTORIA Y LECTURAS RECOMENDADAS

DIEGO NAVARRO BONILLA

Inteligencia y Análisis Retrospectivo. Lecciones de Historia y Lecturas Recomendadas

Inteligencia y Seguridad. Tirant Lo Blanch. Valencia, 2014-08-27

ISBN: 9788490331729

Una vida entregada al estudio de la historia, la seguridad, la defensa y los servicios de inteligencia es el aval del que se sirve Diego Navarro Bonilla para componer "Inteligencia y Análisis Retrospectivo. Lecciones de historia y lecturas recomendadas". Una trayectoria vital conocida y reconocida que llegó a valerle en 2003 el Premio Nacional de Defensa en la modalidad de investigación en Ciencias Históricas en el ámbito militar. Un oficio convertido en estilo de vida que traslada a todos aquellos que tenemos la suerte de conocerle en las distancias cortas, en su labor de docente, de investigador, de escritor y de inconformista respecto a modelos y organizaciones obsoletas.

"Estudio inteligente del pasado" (Blanes, 2012) es una de las primeras citas utilizadas por Navarro y un magnífico y sencillo prefacio que aglutina en cuatro palabras la esencia de la obra aquí reseñada. Un texto que evidencia el efectivo aprovechamiento de las lecciones aprendidas en la gestión del conocimiento, en la creación de inteligencia y, en definitiva, en aquellos ámbitos organizacionales que requieren de un aprendizaje continuo.

Si bien las propuestas realizadas emanan de su amplio conocimiento del ámbito militar, la proposición metodológica y el resultado de su aplicación son de ineludible aprovechamiento para todo analista u organización que tengan por necesidad disponer de conocimiento con fines estratégicos. No se trata este de un conocimiento sin más, de un acercamiento superfluo a lo acaecido y menos de tener ligeras nociones sobre acontecimientos históricos. Es la capacidad de estudiar la historia de manera incisiva, desde sus más variadas aproximaciones, entender su desarrollo y comprender el desenlace del episodio concreto. Sólo así se puede diseñar de forma sistemática un estudio de casos que pueda ir en beneficio del aprendizaje continuo. Una extracción de las lecciones aprendidas orientada a la mejora de las dinámicas de gestión, análisis y decisión cuya aportación al proceso, punto este destacado, ha de ser evaluada de forma constante.

Para aquellos que no entendemos el tiempo de forma lineal, en tanto que presente y futuro en el momento actual ya son parte de nuestro pasado, el enfoque diacrónico de este tipo de análisis no perjudica en absoluto a la aplicación de sus resultados a escenarios imprevistos, nuevos e incluso posibles, la utilización del análisis retrospectivo toma fuerza y es utilizado como punto de partida para los análisis prospectivos. Es en esta utilidad dónde Navarro reflexiona con gran acierto sobre las aptitudes y actitudes de los analistas de inteligencia. El estudio de la historia, el registro de estudio de casos, la extracción de lecciones aprendidas y la sistematización de su uso y evaluación se encuentran de un lado de la balanza. Del otro, como única vía para que

la inteligencia que desciende de semejante aventura alcance su verdadero valor, se hace hincapié en la necesaria imaginación, plasticidad y creatividad del analista, una mente abierta, dispuesta y entrenada para entrelazar y relacionar una mayor sensibilidad hacia la búsqueda de respuestas. Imaginación, rigor, creatividad y crítica como forma de combatir la inteligencia anacrónica.

Como broche final, la obra expone una suerte de majestuosos trabajos, desde Furse (1985), pasando por Dulles (1963) o Heuer (2010), hasta nuestros días. Una meticulosa selección organizada en torno a diez temáticas de gran interés y continuo debate en el marco de la inteligencia. Otra forma de concienciar sobre la necesidad del estudio constante que subyace a todo analista. Es quizás este un compendio que no baste con leer una sola vez, una revisión literaria que obliga al lector más inconformista a releer en contadas ocasiones con el afán de intentar que ninguno de los múltiples detalles aportados se escapen. Una cuidada selección con detalladas conclusiones que incita a adquirir las obras citadas y emprender igual viaje.

Si he de concluir con un escueto resumen diría que la obra expone un pormenorizado estudio de algunos de los episodios más fascinantes de la historia para el más ávido de información; que se trata de una descripción de la evolución de la inteligencia para el que pretende dar contexto a una holística disciplina; que contribuye y da vigor a una necesaria visión para aquellos que se empeñan en que el aprendizaje ha de ser esencial e incesante; y que se viste de doctrina en tanto sistema, método y disciplina.

“La historia es un profeta con la mirada vuelta hacia atrás:
por lo que fue, y contra lo que fue,
anuncia lo que será.”

Eduardo Galeano

Jéssica Cohen Villaverde
Analista de Inteligencia

LA SEÑAL Y EL RUIDO

NATE SILVER

Península. Barcelona, 2014. 656 pp. 2014

ISBN: 9788499423234

Un estadístico se ahogó cruzando un río porque el mismo sólo tenía un metro de profundidad... de media.

Nate Silver trabajaba, tras su grado en económicas en el año 2000, como consultor en la empresa KPMG. En su tiempo libre comenzó a analizar datos sobre estadísticas de baseball, diseñando un sistema predictivo al que llamó Pecota. Posteriormente se dedicó al póker, dejando su trabajo tras ganar 15.000 dólares en seis meses (aunque se señala que al poco tiempo alcanzó las seis cifras). En 2008 su predicción sobre las elecciones norteamericanas supuso un acierto sobre el ganador en 49 de los 50 estados. Para ello supo identificar información demográfica (raza, edad, estructura, educación, etc.) que le permitió llegar a ese nivel predictivo. Pero en 2012, en su blog FiveThirtyEight.com, asociado al New York Times, predijo los ganadores de los 50 estados, con pleno acierto. El mismo día de las elecciones señaló que Obama tenía un 90,9% de probabilidad de victoria. La publicación de su libro "La señal y el ruido" se convirtió inmediatamente en un best seller y en objeto de atracción para analistas y futuristas.

En su libro trata de aplicar las técnicas predictivas a multitud de facetas, como los mercados de acciones, el baseball, la meteorología, los terremotos o los ataques terroristas, en base al principio básico de diferenciar "aquello que sabemos" de lo que "pensamos que sabemos".

Para el análisis y prospectiva sobre la realidad que nos rodea, o sobre cualquier fenómeno relacionado con la seguridad, es preciso acceder a multitud de fuentes que ofrecen básicamente datos e información. La gestión de la información se torna cada vez más compleja, debido a su volumen, a su velocidad y a su variedad de formatos. Ello plantea problemas claramente diagnosticados, como la infoxicación, la desinformación o las posibilidades de manipulación o engaño. Cada vez es más necesario adoptar criterios y modelos para la evaluación de la información, tratando de acreditar la fiabilidad de la fuente y la credibilidad de la propia información. Nate Silver señala la necesidad de separar la señal del ruido.

Podemos definir la señal, la información con la se puede trabajar en un análisis de inteligencia, como lo que es posible conocer, está determinado por una causa y organizado por un plan. Es la clase de datos que se pueden procesar y que implican sentido. La esencia de un buen análisis y una predicción adecuada es identificar la causa raíz del fenómeno, la señal. Cuando los datos tienen mucho ruido es virtualmente imposible identificar información relevante. El ruido, además, tiende a expandirse en periódicos, blogs, redes sociales, etc. reduciendo aun más la señal y reduciendo por tanto nuestra habilidad para su detección. Dicho ruido puede tener su origen en varios factores: la sobreabundancia de información, el carácter complejo, indeterminado y

difícilmente predecible de los problemas a tratar, los sesgos cognitivos que afectan al analista y la percepción errónea del azar en los acontecimientos.

Como señalaba el Centro de Análisis y Prospectiva de la Guardia Civil en su boletín de actualidad internacional del mes de enero de 2013, el estudio de Nate Silver se puede complementar con las aportaciones de Nassim Taleb (la subestimación de la importancia del azar en los acontecimientos), de Surowiecki (la inteligencia de las multitudes), de Tecklock (sobre las predicciones de los expertos), de Kahneman (sobre sesgos probabilísticos y toma de decisiones en situaciones de incertidumbre) o de Per Bak, Chao Tang y Kurt Wiesenfield (concepto de criticidad autoorganizada).

Nate Silver ofrece tres recomendaciones que pueden ser útiles en la elaboración de análisis de inteligencia prospectivos: pensamiento probabilístico (no hay un resultado único), necesidad de actualización de las predicciones (a medida que se incorpora nueva información o cambian las circunstancias) y potencial del consenso (el pronóstico agregado es más preciso que el del experto individual).

La propuesta de Silver se basa en el teorema de Bayes, que tiene en cuenta la probabilidad condicional: la probabilidad de que una hipótesis o teoría sea cierta si determinados eventos se han producido. De esta forma, aplicando este modelo a los atentados del 11S, estimaba que la probabilidad de que fuera un atentado terrorista el hecho de aviones estrellándose contra rascacielos en Manhattan era de un 0,005%. Tras el ataque a la primera Torre Gemela, la probabilidad de tratarse de un atentado terrorista pasaría a ser de un 38%. Pero, tras el segundo ataque, la probabilidad de un ataque intencionado se disparaba hasta un 99,99%. Un accidente, en un día despejado, es una posibilidad, pero dos seguidos sería imposible, señala Silver.

La inferencia bayesiana se basa en el método científico, que supone la incorporación continua de evidencias a favor o en contra de la hipótesis a demostrar. A medida que la evidencia se acumula el grado de creencia en una hipótesis se modifica.

Para evitar el ruido producido por todos estos sesgos, Nate Silver propone un sistema basado en mercados predictivos, en la creación de un mercado competitivo que oferte análisis prospectivos exactos y concretos. Desde el lado de la demanda se pretendería reducir la demanda de análisis inexactos y demasiado seguros de sí mismos. Ya existen diversas propuestas en ese sentido, algunas de ellas bajo patrocinio de la inteligencia norteamericana y basadas en incentivos intangibles como el prestigio del apostante más acertado.

Siendo una obra de indudable interés para investigadores y analistas en el ámbito de la seguridad, es preciso realizar una serie de críticas o consideraciones. La primera de ellas fue publicada en la revista The New Yorker. Señalan los profesores Marcus y Davis, de la Universidad de Nueva York, que el método bayesiano es útil cuando se dispone de un conocimiento previo potente sobre la materia y abogan por la aplicación de teorías posteriores a la de Bayes, especialmente por la aproximación de Fisher. Pone de manifiesto la tensión entre los tradicionalistas, que se guían por frecuencias (experimentos repetibles que tengan confirmación empírica) y los estadísticos bayesianos, que permiten incorporar al modelo probabilidades subjetivas.

Estas teorías están relacionadas con uno de los fenómenos de actualidad, el llamado Big Data, que permite la gestión y análisis de grandes cantidades de datos. Sobre

esta utilización de datos, de interés también en la Seguridad Nacional o en la Seguridad Interior (por ejemplo a la hora de trazar mapas calientes de zonas delictivas), existen algunas limitaciones:

- Se basan en datos del pasado. Que se pueda predecir el pasado no significa que se pueda hacer igual en el futuro, en base a dichos datos.
- Al basarse en datos pasados y presentes, difícilmente podrá predecir nuevos eventos, cisnes negros o disrupciones.
- Estos modelos pueden explicar qué está pasando en un fenómeno y expresar probabilidades de ocurrencia futura, que pueden llegar a ser muy acertadas. Pero no explican las causas. Las políticas públicas de seguridad necesitan disponer de diagnósticos, por supuesto, a cuyo fin los datos ayudan, pero deben diseñar medidas que actúen sobre las causas.

José María Blanco Navarro
Director del Centro de Análisis y Prospectiva

DATOS SOBRE LOS AUTORES DE ESTE VOLUMEN POR ORDEN ALFABÉTICO

Miguel Cañellas Vicens, comandante de la Guardia Civil, destinado en la Consejería de Interior de Brasil, ha sido miembro experto destacado del Comité de Seguridad del Séptimo Programa Marco de financiación de proyectos de innovación de la UE, miembro del Subgrupo Nacional sobre Seguridad para el Programa Marco 2014-2020 de la UE (Horizonte 2020) y miembro evaluador del Grupo de Evaluación Schengen en el ámbito de la cooperación policial UE. También es máster de Seguridad por la UNED, con formación en Investigación criminal por la Universidad de Virginia (EE. UU.) y tiene el curso internacional F.B.I. (Quantico, Va), entre otros. mcanellas@guardiacivil.es

Luis Fernando Hernández García, teniente coronel de la Guardia Civil, jefe de la Unidad de Ciberseguridad del Área Técnica de la Jefatura de Información. Es representante de la Institución ante los Grupos de Trabajo permanentes CIIP del Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC) y de Coordinación en Ciberseguridad de la Secretaría de Estado de Seguridad, además de punto de contacto oficial (POC) en materia de Ciberseguridad ante la División CIS del EMAD, el CIFAS y el Mando Conjunto de Ciberdefensa (MCCD) del Ministerio de Defensa, del Departamento de Seguridad Nacional (DSN) del Ministerio de Presidencia y del Consejo Rector del Centro Nacional de Excelencia en Ciberseguridad (CNEC) –Instituto de Ciencias Forenses y de la Seguridad de la UAM (ICFS). lf_hernandez@guardiacivil.es

Rafael Manuel López Pérez, doctor en Psicología, licenciado en Ciencias Económicas y Empresariales, presidente de la Fundación Universitaria Behavior & Law, director de los grupos de investigación científica “Nonverbal” y “ForensicResearchGroup”, editor de la Revista Científica Behavior & Law Journal, director del “Máster en Comportamiento no Verbal y Detección de la Mentira” de la Universidad Miguel Hernández, director del “Máster en Pericia Caligráfica y Documentoscopia” de la Universidad Miguel Hernández. Director de cursos de perfeccionamiento universitario en materia forense y de comportamiento. rlopez@behaviorandlaw.com

José Luis Mayorga Martín, comandante de la Guardia Civil, con destino en la Jefatura de Información desde el año 2008. Es licenciado en Derecho, diplomado en Informática Militar, máster en Sistemas de la Información y Comunicación para la Defensa y en Dirección de Sistemas y Tecnologías de la Información y las Comunicaciones para la Administración Pública, posee distintos cursos, como el Superior de Información, de Seguridad de las Tecnologías de la Información y Comunicaciones (STIC), de Gestión de la Seguridad de las Tecnologías de la Información y Comunicaciones, de Defensa NRBQ nivel III y de Policía Judicial para Oficiales. jlmayorga@guardiacivil.es

Jesús Narciso Núñez Calvo, teniente coronel de la Guardia Civil, jefe de Operaciones de la Comandancia de Cádiz, Diplomado en Estudios Avanzados de Historia Contemporánea por la UNED y doctorando en Historia Contemporánea por la Facultad de Geografía e Historia de la UNED, teniendo prevista su próxima defensa de la tesis “La Comandancia de la Guardia Civil de Cádiz en la Guerra Civil Española

1936-1939". Es colaborador del Servicio de Estudios Históricos de la Guardia Civil, así como autor y coautor de una decena de libros e innumerables artículos sobre Historia Militar y de la Guardia Civil en diferentes medios y revistas especializadas. jenunez@guardiacivil.es

José Manuel Petisco Rodríguez, jefe del Departamento de Formación y Perfeccionamiento de la Escuela Militar de Ciencias de la Educación (EMCE), licenciado en Psicología por la UAM, posee, entre otros, diploma en aptitud pedagógica, formación de evaluadores, comunicación social y certificado de aptitud en formación de tutores on-line. Ha colaborado como profesor en el programa de postgrado "Experto universitario en comportamiento no verbal" de la Universidad Camilo José Cela y, actualmente, en el nuevo "Máster en comportamiento no verbal y detección de la mentira", patrocinado por la Universidad Miguel Hernández de Elche (Universitas), seccif y otros organismos. Colaborador habitual de múltiples cursos de inteligencia, también lo hace altruistamente con Human Behavior Academy. Comportamiento.no.verbal@gmail.com

Francisco Miguel Rodríguez Rodríguez, destinado en el Área de Asuntos Legales de la Jefatura de Personal de la Dirección General de la Guardia Civil, es abogado del Estado Sustituto, máster universitario en Derechos Fundamentales "Especialidad en Protección Jurisdiccional de los Derechos" por la UNED, experto en Violencia de Género y Extranjería por el Ilustre Colegio de Abogados , diplomado en Investigación Criminal y en Biología Forense y Derecho por la Universidad Complutense de Madrid y experto universitario en Delincuencia Juvenil y Derecho Penal de Menores además de en Ciencias Forenses para miembros de las FCSE y Administración de Justicia y en Gestión y Técnicas de Policía Judicial por la UNED. frodriguez@guardiacivil.es

Francisco Javier Velez Alcalde, teniente coronel de la Guardia Civil, diplomado de Estado Mayor de las Fuerzas Armadas, está actualmente destinado en la Secretaría de Cooperación Internacional, dependiente de la Dirección Adjunta Operativa. Ha sido agregado de interior en la Embajada de España en Alemania y participó como comandante en la planificación y establecimiento del Centro de Coordinación Regional de Canarias, para el control de la inmigración ilegal vía marítima, como responsable del área de organización y planes. javiervelez@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 Y AUTORÍA. En la primera página constará el título, en mayúsculas y negrita, y, debajo, el nombre del autor (en mayúsculas), indicando puesto de trabajo o profesión.

Se adjuntará adicionalmente breve CV del autor.

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 "Key words".

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. Times New Roman de tamaño 12 puntos. Las notas y fuentes bibliográficas serán de la misma letra, tamaño 10 puntos.

CUADROS Y FIGURAS. Serán numerados e incluirán una breve titulación.

PÁRRAFOS. Sangrado de 5 espacios. Espacio interlineal 1,5.

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 del artículo 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.

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.

Entre sus actividades, en el plan para 2014, se incluye:

- La investigación. Ayudas/becas para la realización de trabajos según la convocatoria anual.
- La realización de seminarios y jornadas:
    - Seminario Duque de Ahumada. XXV Aniversario
    - Seminario Internacional
    - Seminario de Inteligencia y Seguridad
    - Seminario de Delincuencia Económica
    - Jornada sobre Radicalización y Conexiones Internacionales
    - Workshop de Prospectiva
    - Jornada de Liderazgo Estratégico
    - Jornada sobre Administración Electrónica
    - Taller Operaciones Conjuntas Internacionales Inmigración Irregular
    - Jornada sobre Polìtica de Seguridad de la Información
    - Jornada sobre Ley de Seguridad Ciudadana
    - Jornada sobre la Dimensión Transnacional de la Trata de Seres Humanos
    - Jornada sobre Modelos de Gestión Policial (Intelligence Policing)
- Otras acciones que se irán anunciando en su página web: www.iuisi.es