CIENCIA POLICIAL

182 | 2024

Ediciones Universidad Salamanca

CIENCIA POLICIAL

182
2024

CIENCIA POLICIAL, VOLUMEN 182, 2024

ISSN: 1886-5577 - ISSN en línea: 2254-0326 - Depósito Legal: M-39.360-1987
https://doi.org/10.14201/cp.2024182

Composición: Glaux Publicaciones Académicas

Impresión y encuadernación: Impreso en España – Printed in Spain

Normas de estilo para publicaciones: https://revistas.usal.es/documentos/cienciapolicial/normas.pdf

Guía de buenas prácticas: https://revistas.usal.es/Guia_buenas_practicas.pdf

Ediciones Universidad de Salamanca

Plaza de San Benito s/n – 37002 Salamanca (España)

eusal@usal.es – eusal.es

Ciencia Policial pretende divulgar publicaciones científicas de los productos resultantes de la investigación que sean de utilidad para las instituciones policiales, compartiendo conocimientos sobre métodos y técnicas que faciliten su formación, modernización y actualización.

Sumario

Presentación

En el año 1987 la revista *Ciencia Policial* nace como una publicación de carácter técnico y multidisciplinar de la Policía Nacional. En sus 181 números y 36 años de vida ha ofrecido a sus lectores un amplio espectro sobre los temas de interés policial en sus diferentes áreas de actuación en defensa de los derechos fundamentales y la seguridad ciudadana.

Las instituciones de educación superior que se precien como tales han de contemplar en sus líneas estratégicas tres pilares básicos: la formación, la investigación y la transmisión del conocimiento a través de las publicaciones en el ámbito de la comunidad científica internacional, como fomento de la ciencia abierta al colectivo policial, universitario y a la ciudadanía.

Con la creación del Centro Universitario de Formación de la Policía Nacional, surgen nuevas exigencias y premisas como institución de educación superior, con la adaptación del modelo policial a una sociedad cambiante, compleja y en continua evolución en el ámbito de la seguridad público-privada.

La publicación de este número implica el inicio un nuevo paradigma en su enfoque, dando carácter científico a la revista *Ciencia Policial*, con un formato digital y abierto, que garantice la libre circulación de los conocimientos relacionados con la actividad y función policial, sin excluir la colaboración y participación de otras organizaciones públicas o privadas.

Iniciamos esta singladura, como revista científica indexada, con la publicación de siete artículos que abordan las siguientes temáticas: los obstáculos procesales en la investigación de los ciberdelitos; el análisis jurisprudencial del uso de las armas de fuego; las garantías procesales en la interceptación de las comunicaciones telefónicas; la actuación policial con familiares y allegados de personas desaparecidas; las ciencias forenses en la investigación de delitos con agentes biológicos; el control de las armas químicas; el análisis de la huella digital de los criptoactivos.

Las directrices marcadas por el Consejo de Redacción, así como las pautas descritas por el Comité Científico, pretenden que Ciencia Policial se posicione en la comunidad científica internacional como referente en la difusión de investigaciones que tengan impacto en las actividades relacionadas con la función policial, lo que implica una alta exigencia en los estándares de calidad.

El Equipo de Redacción no quieren finalizar esta presentación sin dejar de expresar el agradecimiento a todas aquellas instituciones y personas que de alguna manera han contribuido a la evaluación, corrección, maquetación y publicación de los artículos de este primer número como revista científica indexada. A todos ellos nuestro más sincero reconocimiento. GRACIAS.

El Director de la Revista

ARTÍCULOS

Ciberseguridad *vs* ciberdelincuencia: obstáculos procesales en la persecución de la ciberdelincuencia organizada. Propuestas para una más eficaz represión de los ciberdelitos

Cybersecurity vs Cybercrime: Procedural Obstacles in the Prosecution of Organized Cybercrime. Proposals for a More Effective Repression of Cybercrime

María Luisa García Torres[1]
Universidad Alfonso X el Sabio.
mgarctor@uax.es | https://orcid.org/0000-0002-7638-9791

DOI: https://doi.org/10.14201/cp.31962
Recibido: 03-05-24 | Aceptado: 10-05-24

Resumen

La ciberseguridad y la ciberdelincuencia son dos caras de la misma moneda. Mientras que la ciberseguridad se refiere a las medidas diseñadas para proteger los sistemas informáticos, redes y datos contra los ataques cibernéticos, la ciberdelincuencia es aquella actividad criminal que se lleva a cabo mediante el uso de computadoras, redes y tecnologías de la información.

Los ciberdelincuentes son cada vez más, más fuertes y mejor organizados: se aprovechan de la transformación digital del mundo, y de la sociedad, del aumento de las transacciones por *Internet*, del anonimato en la navegación, del efecto multiplicador de sus acciones en la red, del desconocimiento de los ciudadanos sobre las medidas mínimas de ciberseguridad que deben adoptar en su vida diaria y de la proliferación de datos que se producen en el mundo cada día. Además, la persecución de la

1. Dra. en Derecho Procesal. Abogada del Ilustre Colegio de la Abogacía de Madrid. Directora del área jurídica de la Facultad Business & Tech, Universidad Alfonso X el Sabio.

ciberdelincuencia presenta numerosos obstáculos procesales: carácter extraterritorial de los delitos, escasez de recursos humanos y materiales, desconocimiento tecnológico de los jueces, dificultad para obtener las pruebas y la volatilidad de las evidencias son los más evidentes.

A pesar de los esfuerzos legislativos de la Unión Europea para garantizar el acceso a las pruebas electrónicas y para facilitar la investigación de estos crímenes, los resultados en la represión de la ciberdelincuencia han sido escasos hasta el momento. La cooperación internacional en materia penal se torna crucial en esta lucha.

El presente no es sencillo y el futuro una incógnita y es que la Inteligencia Artificial plantea nuevos y complejos retos para la ciberseguridad.

Palabras clave

Ciberseguridad; Ciberdelincuencia; Delincuencia organizada; Ciberdelincuencia organizada; Prueba electrónica; *Compliance*; *Behavioral compliance*.

Abstract

Cybersecurity and cybercrime are two sides of the same coin. While cybersecurity refers to measures designed to protect computer systems, networks, and data against cyber attacks, cybercrime is criminal activity carried out using computers, networks, and information technologies.

Cybercriminals are becoming increasingly powerful and they are better organized: they take advantage of the digital transformation of the world and society, the increase in online transactions, the anonymity of browsing, the multiplier effect of their actions on the network, the lack of awareness among citizens of the minimum cybersecurity measures they should adopt in their daily lives, and the proliferation of data produced in the world every day to commit crimes. Additionally, prosecuting cybercrime presents numerous procedural obstacles: the extraterritorial nature of crimes, scarcity of human and material resources, technological unfamiliarity among judges, difficulty in obtaining evidence, and the volatility of evidence.

Despite the legislative efforts of the European Union to ensure access to electronic evidence and facilitate the investigation of these crimes, results in the repression of cybercrime have

been scarce so far. International cooperation in criminal matters becomes crucial in this fight.

Keywords
Cybersecurity; Cybercrime; Organized crime; Organized cybercrime; Electronic evidence; Compliance; Behavioral compliance.

1 Algunas notas introductorias para entender el surgimiento de un nuevo término: «ciberdelincuencia organizada»

En primer lugar, debemos diferenciar ciberseguridad y ciberdelincuencia, pues, aunque son conceptos relacionados, resultan opuestos en su naturaleza y objeto:

La ciberseguridad se refiere a las medidas, prácticas y tecnologías diseñadas para proteger los sistemas informáticos, redes y datos contra accesos no autorizados, ataques cibernéticos, robo de información, daños o cualquier tipo de amenaza que pueda comprometer la seguridad de la información y la operación de los sistemas. La ciberseguridad se centra, por ende, en prevenir, detectar y responder a posibles riesgos y amenazas cibernéticas.

Sin embargo, la ciberdelincuencia es aquella actividad delictiva que se lleva a cabo mediante el uso de computadoras, redes y tecnologías de la información. La ciberdelincuencia implica el uso ilegal de la tecnología para cometer actos delictivos y causar daño a individuos, organizaciones o sistemas.

Así, la ciberseguridad busca proteger los sistemas y datos contra amenazas cibernéticas. La ciberdelincuencia representa las acciones criminales que se apoyan en las vulnerabilidades en esos sistemas y datos, todo ello con fines ilícitos. La ciberseguridad es proactiva y defensiva, mientras que la ciberdelincuencia es destructiva y criminal.

El fenómeno de la globalización ha tenido más beneficios que perjuicios para el mundo. Efectivamente, sus efectos han sido favorables para la economía, la tecnología, la sociedad y para la

cultura. Pero no podemos soslayar algunos efectos perniciosos, como el que tiene que ver con la delincuencia. La globalización, unida al imparable crecimiento de la tecnología y transformación que está produciendo en el mundo, han originado que los patrones de delincuencia hayan cambiado. De hecho, hoy hablamos de la delincuencia transnacional y de ciberdelincuencia, términos antes desconocidos.

¿Cómo podemos definir la delincuencia transnacional? ¿Son términos sinónimos los conceptos de delito internacional y de delito transnacional? No resulta tan sencillo dar una respuesta a estos interrogantes.

Podríamos intentar definir los delitos internacionales acudiendo al Estatuto de la Corte Penal Internacional, firmado, en Roma, el 17 de julio de 1998. Tanto de su Preámbulo, como de su arts. 1 y 5, podríamos inferir que un delito internacional es aquél que, siendo grave, tiene trascendencia para la comunidad internacional en su conjunto. Así serían delitos internacionales, según el art. 5 de la Norma citada, los siguientes crímenes: genocidio, lesa humanidad, crímenes de guerra y el de agresión. Se trataría, en definitiva, de graves violaciones de las normas imperativas de Derecho Internacional Público.

Sin embargo, no resulta tan claro el concepto, si atendemos a la clasificación de los crímenes internacionales que algunos autores realizan (Messuti, 2013). Los delitos internacionales se pueden agrupar en cuatro categorías diferentes: a) delitos de Derecho Internacional, por ejemplo, crímenes de guerra; b) delitos contra el Derecho Internacional, como son los delitos de piratería; c) delitos que interesan al Derecho Internacional, caracterizados por elementos jurídicos, sociológicos y antropológicos dispersos entre territorios, nacionalidades o razas diferentes, como es el caso de la trata de personas y; d) delitos según el Derecho Internacional, los cuales se fundamentan en el carácter universal del bien jurídico protegido, entre los que se encuentran el delito de abordaje marítimo o aéreo o la misma piratería. Los delitos transnacionales, según esta clasificación, podrían incluirse dentro de la tercera categoría (Zúñiga Rodríguez, 2016). Podemos observar que el delito de piratería resulta difícilmente subsumible en las categorías anteriores, lo que

evidencia la dificultad de deslindar las diferentes clases de delitos internacionales.

Sin perdernos en disquisiciones doctrinales y desde la perspectiva de Derecho positivo, en España, el principio de Justicia universal permite atribuir jurisdicción a los tribunales españoles mezclando dos grupos de delitos: los que deben perseguirse por existir un interés común, por tratarse de hechos de carácter trasnacional, que requieren el acuerdo de varios Estados para que sea posible y; aquéllos, en cuya protección están interesados todos los Estados de la Comunidad internacional, por fundamentarse en las normas de *ius cogens* del Derecho Internacional. Así, el art. 23.4 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial (en adelante, LOPJ), atribuye jurisdicción a los tribunales españoles, siempre que exista la concreta conexión que la Ley establece en cada caso (entre otras, víctima española, procedimiento dirigido frente a un español o frente a una persona que resida en territorio español) en delitos tan dispares como genocidio, lesa humanidad o contra las personas y bienes protegidos en caso de conflicto armado, tráfico ilegal de drogas tóxicas, estupefacientes o sustancias psicotrópicas o, entre otros, corrupción entre particulares. El precepto mencionado recoge así tanto las tesis universalistas como las pragmáticas, en la configuración del llamado principio de Justicia universal (Menéndez Rodríguez, 2014).

Aunque el art. 23.4 de la LOPJ española, incluya delitos propiamente internacionales como aquéllos que pueden calificarse de transnacionales, podemos definir los delitos internacionales, diferenciándolos de los segundos, como aquéllos afectantes a bienes jurídicos de carácter universal, teniendo su fundamento en los derechos humanos, afirmados por las normas imperativas de Derecho Internacional, tanto consuetudinarias como convencionales.

Por delito transnacional entendemos, sin embargo, aquellas acciones u omisiones que, siendo definidas como delito por las normas de cada uno de los Estados, se cometen o producen efectos en el territorio de más de un Estado. Los delitos transnacionales, por ende, no vienen definidos por el Derecho Internacional Público, sino por los ordenamientos jurídicos internos, lo que

sucede es que, a diferencia de los delitos nacionales, se cometen o repercuten en más de un ordenamiento jurídico. Se suelen caracterizar, además, por cometerse por medio de una estructura organizada, de ahí que se hable de una delincuencia transnacional organizada. Los delitos transnacionales más conocidos son el narcotráfico, el tráfico de armas, la trata de seres humanos, el blanqueo de capitales, etc. Su fundamento no radica en la afirmación de los derechos humanos inherentes a la dignidad del ser humano, sino en razones prácticas: el interés de los Estados en llegar a acuerdos para perseguir hechos delictivos que escapan de sus fronteras, pues se cometen en un ordenamiento jurídico, pero producen sus efectos en otro distinto o incluso se cometen allá donde su jurisdicción no alcanza (Zúñiga Rodríguez, 2016).

Hoy en día, resulta imposible aplicar los viejos cánones del Derecho Penal sobre los que éste se construyó, basados en la soberanía de los Estados, en la territorialidad de la norma penal y en la titularidad exclusiva de los Estados del *ius puniendi* (Zúñiga Rodríguez, 2016). La represión de los delitos de carácter transnacional requiere de la cooperación entre los Estados. Dado que se producen o tienen sus efectos en diferentes ordenamientos jurídicos, no es posible ni la prevención ni su castigo, si no es contando con la colaboración de todos los Estados. Manifestación concreta de la delincuencia transnacional, es la llamada ciberdelincuencia o, en inglés, *cybercrime*.

Se entiende por ciberdelincuencia aquélla en la que está involucrada un equipo informático o *Internet* y en la que el ordenador, el teléfono, la televisión (*smart tv*), el reproductor de audio o vídeo o el dispositivo electrónico puede ser usado para la comisión del delito o puede ser objeto del mismo delito (Rayón Ballesteros y Gómez Hernández, 2014).

Cabe trazar una línea diferenciadora entre el concepto de ciberdelito y el de delito informático. El primero está estrechamente vinculado a las tecnologías de la Información y la Comunicación (TIC). En ellos, interviene la comunicación telemática abierta (pública), cerrada (privada) o de uso restringido. El delito informático es el aquél que se vale de elementos informáticos para su perpetración (Romero Casabona, 2016). Por tanto,

implica el uso indebido de elementos informáticos o sistemas computacionales: se vale de elementos informáticos, como computadoras, dispositivos de almacenamiento, *software*, redes, para perpetrar la actividad delictiva, pero no tiene que ir ligado a la comunicación telemática, aunque puede utilizarla como medio para cometer el hecho.

De lo que se ha dicho en relación con la delincuencia transnacional queda claro que, en la actualidad, las fronteras no son un límite para la comisión de crímenes, siendo uno de los ámbitos donde más se plasma lo que cabe llamar la realidad «líquida» de las fronteras del ciberespacio (Zúñiga Rodríguez, 2016).

Si se unimos los conceptos de delincuencia organizada y ciberdelincuencia, obtenemos el término ciberdelincuencia organizada (Oficina de las Naciones Unidas Contra la Droga y El Delito, 2022). Tal y como reconoce Naciones Unidas no existe consenso para definir este nuevo término, ahora bien, hay ciertos parámetros de obligado cumplimiento como son los siguientes: el acto ilícito tiene que tener una dimensión cibernética, teniéndose que tratar bien de un delito facilitado por la cibernética o bien basado en la misma[2] y entrañar ya sea la participación de un grupo delictivo organizado (art. 2 de la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional) o un delito tipificado, conforme al art. 5 de la misma Convención (confabulación o asociación delictuosa).

Los ciberdelincuentes se amparan en la continua transformación digital del mundo, y de la sociedad, en el aumento vertiginoso de las transacciones económicas que se realizan a través de *Internet*, en el anonimato en la navegación, en el efecto multiplicador de sus acciones en la red, en el desconocimiento de los

2. La Oficina de las Naciones Unidas Contra la Droga y el Delito diferencia los delitos facilitados por la cibernética y los delitos basados en la cibernética. Los primeros son delitos tradicionales facilitados (de alguna manera) por las *TIC*. Así, «(…) las *TIC* desempeñan un papel fundamental en el método de operación, (es decir, el modus operandi) del delincuente o los delincuentes». Sin embargo, los delitos basados en la cibernética (quedan incluidos aquellos que solo se pueden cometer utilizando computadoras, redes informáticas u otras formas de tecnología de comunicación de la información, el objetivo de ese tipo de delitos son las *TIC*.

ciudadanos de las medidas mínimas de ciberseguridad que deben adoptar en su vida diaria y en la gran volumen de datos que se producen e intercambian en el mundo cada día, para delinquir. Son muchos y, como veremos a continuación bien organizados y ven multiplicadas sus acciones delictivas por el gran impacto que tienen en el ciberespacio.

Gracias a la investigación y a la cooperación internacional, podemos conocer los caracteres esenciales que definen a los grupos que cometen ciberdelitos de carácter transnacional, aunque ciertamente la ciberdelincuencia organizada es todavía muy desconocida. Ciertamente, los grupos de ciberdelincuentes muestran conductas similares a los de los grupos organizados que pueden calificarse de tradicionales, por cometer delitos no cibernéticos, pues usan una estructura y se valen de unos procedimientos especiales que tienden a preservar el anonimato de sus miembros y a evitar la detección por parte de la policía. Es tal la protección que crean para no ser vistos por las fuerzas policiales que, de hecho, los foros utilizados por los ciberdelincuentes (por ejemplo, los empleados para compartir fotografías sexuales de menores), tienen más protección y más medidas de seguridad que otras[3]. Pero, a diferencia de los grupos organizados tradicionales, las TIC permiten la agrupación de personas que no se conocen entre ellos y que nunca se han visto cara a cara y, por ende, se unen personas que residen en cualquier parte del mundo. La misma tecnología les dota de una infraestructura, de productos, de personal y de clientes, sin las barreras geográficas que existen en los delitos tradicionales. El anonimato es una característica propia de estos delitos, cometidos a través o por la red[4].

La investigación demuestra que los grupos varían en virtud de la complejidad estructural (Oficina de las Naciones Unidas Contra la Droga y el Delito, 2022): los hay con mayor jerarquización, que centralizan y dividen su trabajo, con líderes identificables,

3. A veces se obliga a una persona que quiere entrar en esos foros a hacerse miembro, exigiéndoles que aporten ellos mismos fotografías sexuales de menores, incluso se les exige pagar una cuota.
4. Véase a este respecto *Compendio de ciberdelincuencia organizada,* emitido por Oficina de las Naciones Unidas Contra la Droga y el Delito, 2022, pp. 1-3.

mientras que otros tienen redes transitorias, sin una naturaleza nítida, no vertical, sino lateral, sin una estructura fija y descentralizada. Ya sean de una clase o de otra utilizan foros y plataformas en línea para regular y controlar el suministro de bienes y servicios ilícitos. Esto quiere decir que entienden la delincuencia como un servicio y se basan en las aptitudes de sus individuos para realizar sus actividades.

Los grupos de ciberdelincuentes se pueden dividir en tres: los que operan principalmente en línea y cometen delitos cibernéticos; los que lo hacen fuera y en línea y cometen delitos cibernéticos y; los grupos que operan predominantemente fuera de línea y se dedican a la ciberdelincuencia para ampliar y facilitar sus actividades fuera de línea.

Dentro del primer grupo, a su vez se pueden distinguir los «enjambres» y los «nodos». Un «enjambre» es una fusión durante un espacio de tiempo de personas que se agrupan para realizar tareas para cometer un delito cibernético, pero después, una vez terminan y cumplen sus objetivos, desintegran el grupo. Son redes descentralizadas, que se componen por grupos efímeros de personas, y mínimas cadenas de mando. Cometen los delitos por razones ideológicas. Los «nodos» se integran por un núcleo de delincuentes, a los que se unen unos que se asocian, tienen más estructura y son más jerarquizados.

Los grupos que operan fuera de línea y en línea y se dedican a cometer delitos y delitos cibernéticos son llamados «híbridos», habiendo «híbridos agrupados» o «híbridos extendidos». Los primeros realizan determinadas actividades o utilizan métodos específicos para cometer ciberdelitos; se organizan como los «nodos», pero realizan sus actividades fuera y en línea, teniendo capacidad para ello. Tienen una táctica y operan en una ubicación concreta. Los grupos extendidos son mucho más especializados, menos centralizados y con un núcleo menos evidente; su composición es más compleja y su ámbito de operaciones es la llamada «red oscura».

Por último, el tercer grupo tienen una fuerte estructura jerárquica, se integran por grupos organizados tradicionales, pero amplían sus actividades ilícitas operando en línea, por ejemplo,

a través de los juegos de azar, extorsión, prostitución o trata de personas.

La estructura de todos los grupos supone que operen como una auténtica empresa con «trabajadores» que prestan sus servicios en ella. Existe personal técnico, personal de apoyo, personal de comercialización; encargados de pagar y cobrar los servicios y cuentan con reglas de conducta por las que se rigen. La organización depende de a la actividad ilícita que se dediquen. Los que se basan para delinquir en la cibernética se nutren de codificadores, piratas informáticos, responsables de apoyo técnico y anfitriones (los que alojan actividades ilícitas en servidores o en ubicaciones físicas fuera de la red.

Después de esto, podemos afirmar que son muchos y muy bien organizados.

Debe tenerse en cuenta que, en el año 2023, del total de delitos, 2 459 659, cometidos de enero a diciembre, 470 388 son ciberdelitos, lo que representa un 19,1 % del total. De este número 426 744 son ciberestafas. Para entender el aumento vertiginoso que la ciberdelincuencia ha tenido en nuestro país, debemos comparar ese dato con las 70 178 estafas cibernéticas registradas en el año 2016. En sólo ocho años ha habido un aumento de un 508,1 %[5].

Los ciberataques más frecuentes son los que tienen que ver con alguna de estas conductas: robo de identidad, piratería, *phishing*, *botnets*, ciberespionaje, extorsión en la red, *malware*, *ransomware*, pornografía infantil, acoso y amenazas cibernéticas.

El robo de identidad sucede cuando una persona se apropia de la identidad de otra, en beneficio propio, actuando en el tráfico jurídico simulando ser la persona a la que suplanta.

La piratería supone una entrada ilegal en un sistema informático o la ruptura de las protecciones que impiden la copia de un programa. Se utiliza también para hacer referencia a las

5. Véase https://www.interior.gob.es/opencms/export/sites/default/.galleries/galeria-de-prensa/documentos-y-multimedia/balances-e-informes/2023/Balance-de-Criminalidad-Cuarto-Trimestre-2023.pdf (Consultado el 29/04/2024. Hora: 13:00).

copias ilegales de programas, discos o *DVDs*. El término inglés es *cracking*[6].

El *phishing* supone extraer información confidencial mediante suplantación de identidad por correo electrónico, sitios *web* o llamadas.

También es necesario explicar el término *botnet*, que tiene lugar cuando una red de computadoras es infectada con *malware*, conectándolas a un centro de comando y control central. Los ciberatacantes lo utilizan para enviar correos electrónicos no deseados o realizar ataques *DDoS*, que consisten en producir una denegación de servicio por una sobrecarga en un sitio *web*, un servidor o un recurso, lo que lleva a un bloqueo o falta de funcionamiento y, al mismo tiempo, a una denegación de un servicio a los usuarios legítimos.

Las *botnet* se utilizan también para hacer lo que se denomina *clic* en fraude, esto es *clics* falsos que tienen como objetivo aumentar la calificación de búsqueda de una página *web* o inflar de manera artificial la popularidad de una publicación en las redes sociales.

El ciberespionaje es aquella actividad a través de la cual se obtiene información confidencial, secreta o estratégica de individuos, organizaciones, o gobiernos a través de medios electrónicos y digitales. Esto puede incluir la infiltración en sistemas informáticos, el robo de datos, el monitoreo de comunicaciones en línea, y el uso de *malware* u otras técnicas de *craking* para acceder a información sensible. Por ejemplo, a través de un programa se espían las comunicaciones de *Internet*, para encontrar números de tarjetas de crédito.

La ciberextorsión es un tipo de delito por el que se amenaza a una persona, empresa u organización con revelar información comprometedora, filtrar datos sensibles, dañar sistemas informáticos o realizar otras acciones perjudiciales a menos que se cumpla con una demanda específica, normalmente el pago de una cantidad de dinero, generalmente en criptomonedas u otra

6. El término hacking hace referencia a una habilidad, pero no supone ilegalidad.

forma de pago digital, aunque también puede incluir otras condiciones, como la realización de acciones específicas o la entrega de bienes o servicios. Los métodos utilizados para llevar a cabo la extorsión en línea pueden variar, desde el envío de correos electrónicos amenazantes (conocidos como «emails de sextorsión»), hasta el uso de *ransomware* para cifrar archivos y exigir un rescate por su liberación.

La ciberextorsión puede tener graves consecuencias tanto para individuos como para empresas, ya que puede causar daños financieros, reputacionales y emocionales significativos.

El *malware* es un *software* malicioso que se utiliza para dañar computadoras y sistemas informáticos sin el conocimiento del propietario, por ejemplo, a través de *spyware*, virus, gusanos o troyanos.

El ciberataque que, con más frecuencia se produce, es el que se conoce como *ransomware*. El año 2023 ha supuesto un récord y es que, en el tercer trimestre de ese año, se constataron 1278 víctimas de este tipo de ataque, lo que ha supuesto un aumento del 11,22 % con respecto al segundo trimestre del mismo año y un aumento interanual del 95,41 %[7].

Este *software* está diseñado para bloquear el acceso a un sistema informático, archivos o datos, generalmente mediante su cifrado, para luego exigir un rescate económico a cambio de restaurar el acceso. Una vez que el *ransomware* infecta un sistema, muestra mensajes intimidatorios o instrucciones sobre cómo pagar el rescate, siendo habitual que sea solicitado en forma de criptomonedas, con la finalidad de dificultar el rastreo del pago.

Los *ransomware* suelen propagarse a través de correos electrónicos de *phishing*, descargas de archivos maliciosos, vulnerabilidades en el *software* o sistemas desactualizados, y en algunos casos, a través de *exploits* de seguridad. Una vez que el

7. Véase el Informe presentado por CORVUS (2023, 24 d octubre), en https://www.corvusinsurance.com/blog/q3-ransomware-report (Consultado el 24/04/2024. Hora: 13:00).

ransomware infecta un sistema, puede cifrar archivos de gran importancia para el usuario o la organización, como sucede con los documentos, las fotos, las bases de datos o incluso con todo el disco duro.

El *ransomware* puede causar graves daños y pérdidas económicas, además de afectar la reputación de las organizaciones que son víctimas de estos ataques. La prevención del *ransomware* implica la adopción de buenas prácticas de seguridad cibernética, como la actualización regular del *software*, la concienciación sobre seguridad entre los empleados, el uso de *software* de seguridad confiable y la realización de copias de seguridad frecuentes y almacenadas de forma segura.

La pornografía infantil se produce cunando se distribuye, produce y consume material sexualmente explícito que involucra a menores de edad. En *Internet* puede manifestarse en diversas formas, como imágenes, videos o cualquier otro tipo de material que muestre a menores en situaciones sexualmente explícitas o sugestivas. Esta actividad criminal suele estar asociada con redes de explotación sexual infantil, donde los perpetradores pueden producir este tipo de contenido para su propio beneficio o con fines de lucro.

El acoso y amenazas como ciberdelitos son formas de abuso que se llevan a cabo a través de medios electrónicos, *Internet*, redes sociales, mensajes de texto, correo electrónico, entre otros. Estas acciones pueden tener graves repercusiones emocionales, psicológicas y, en algunos casos, físicas para las víctimas. Aquí hay una definición detallada de cada uno.

A continuación, se enumeran los posibles ciberdelitos que pueden cometerse y que están tipificados en la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal (en adelante, CP[8]):

A) Descubrimiento y revelación de secretos: estos delitos lesionan la intimidad personal, familiar o la propia imagen

8. Para un conocimiento más profundo de los ciberdelitos, no ceñido exclusivamente al ordenamiento jurídico español, véase *Compendio de ciberdelincuencia organizada.* Incluso dicho Compendio incluye Resoluciones dictadas en distintos países.

de la víctima, mediante el apoderamiento de documentos o interceptación de telecomunicaciones (art. 197.1 del CP); o, el acceso, apoderamiento, utilización o modificación (sin permiso) de datos informáticos de carácter personal (197.2 CP); o, la difusión sin permiso de imágenes o documentos audiovisuales, obtenidos con autorización de la víctima en un lugar fuera del alcance público, cuando la difusión menoscabe gravemente la intimidad de ésta (197.7 CP); a este delito se le llama *sexting*.

B) Acceso ilícito a sistemas informáticos: se trata de los delitos que tienen que ver con el de revelación de secretos, bien por la permanencia o facilitación del acceso a un sistema informático vulnerando las medidas de seguridad impuestas por éste y contra la voluntad de un usuario legítimo (art. 197. Bis 1 del CP), bien por la interceptación de datos informáticos mediante herramientas o mediante expertos (*snifer)*, según lo previsto en el art. 197 bis 2 del CP. También se produce este delito por el acceso ilícito, por producción o facilitación de programas y/o contraseñas (art. 197 ter del CP).

C) Daños informáticos, como son borrar, dañar, deteriorar, alterar, suprimir o hacer inaccesibles datos informáticos, programas o documentos ajenos, sin autorización y de manera grave (264 del CP); obstaculizar o interrumpir el funcionamiento de un sistema informático (art. 264 bis del CP); producir, adquirir o facilitar programas (art. 264 ter del CP) y; facilitar contraseñas destinadas a cometer alguno de los delitos anteriores (art. 400 del CP)

D) Falsedades informáticas, como es la falsificación de moneda y timbre (386 a 389 CP); la de documento público, oficial y mercantil (390 a 394 del CP); de documento privado (395 a 396 del CP); de certificado (397 a 399 del CP); de tarjetas de crédito, débito o cheques de viaje (399 bis del CP) o; la fabricación, recepción, obtención o tenencia de instrumentos, datos o programas informáticos destinados a la comisión de los delitos indicados (400 del CP)

E) Estafa informática: es la utilización de un engaño, con ánimo de lucro y con la finalidad de obtener un beneficio o perjuicio a un tercero (art, 248 a 251 del CP). Es el art. 248.2 del CP el que recoge de forma expresa la llamada estafa informática, que consiste en valerse de manipulaciones

informáticas o mecanismos, como el *phishing,* para obtener de forma no consentida una transferencia patrimonial en perjuicio de un tercero. Tal y como hemos indicado es, con mucho, el ciberdelito más cometido en los últimos años. También se comete este delito por la fabricación, posesión o facilitación de programas informáticos, con el objetivo de realizar operaciones bancarias en perjuicio de su titular o de un tercero; esto es lo que en términos informáticos se llama *ransomware*.

F) Defraudaciones de telecomunicaciones y es que éstas, igual que sucede con el fluido eléctrico o agua, pueden ser objeto de defraudaciones a través de mecanismos que se utilizan al efecto, por ejemplo, alterando los contadores (art. 355 del CP); también cuando se utiliza un terminal de telecomunicaciones sin permiso de su titular, si se le causa un perjuicio económico.

G) Ciberdelitos sexuales: destaca el llamado *child grooming*, que consiste en ponerse en contacto con un menor de 16 años, para tener un encuentro con el fin de cometer los actos previstos en los arts. 181 a 189 del CP (art. 183.1 del CP). También, recibe esa denominación el delito cometido cuando el menor de 16 años facilita al autor material pornográfico o le muestra imágenes pornográficas en las que se represente o aparezca un menor (art, 183.2 del CP).

Cabe el acoso sexual, efectuado a través de las TIC (art. 184 CP) o el exhibicionismo ante menores de edad o discapacitados necesitados de especial protección (art. 185 del CP).

Asimismo, entra dentro de esta categoría la venta o difusión de material pornográfico a menores o discapacitados de especial atención (art. 186 del CP) o la prostitución, explotación sexual y corrupción de menores del art. 187 a 189 bis del CP.

H) Delitos contra la propiedad industrial, pues cabe la reproducción, plagio, distribución o comunicación pública de una obra con ánimo de lucro y sin autorización de los titulares de los derechos de propiedad intelectual (art. 270.1 del CP); la facilitación activa y con ánimo de lucro del acceso o localización en *Internet* de obras protegidas sin autorización de los titulares de los derechos de propiedad intelectual (art. 270 del CP). También, eliminar, modificar las medidas tecnológicas destinadas a proteger obras para favorecer la

comisión de alguna de las conductas de los tipos comentados (270.5 apartado C). Es posible que se cometa este tipo de delitos por la elusión o facilitación de medidas tecnológicas para facilitar a un tercero el acceso a una obra protegida (art. 270. 5 D).

La fabricación, importación, distribución o posesión con fines comerciales de cualquier medio destinado a neutralizar dispositivos técnicos utilizados para proteger programas informáticos u obras protegidas (270.6 CP) es un delito también cibernético contra la propiedad industrial.

I) Delitos contra el honor: y, dentro de éstos, encontramos la calumnia o la injuria, conductas agravadas por la publicidad, cuando, por ejemplo, se realizan en redes sociales o por grupos de mensajería (art. 208 del CP)

J) Amenazas y coacciones, siempre que se produzcan en el ciberespacio o entorno virtual (art. 271.2 del CP o art. 172 a 172 ter del CP). Tenemos el llamado ciberacoso o *ciberstalking* (art. 172 ter del CP), que supone el contacto de forma reiterada e insistente por parte del autor con la víctima, causándole graves alteraciones en el desarrollo de su vida diaria.

Cuando la acción la realiza un menor que es quien atormenta o amenaza o coacciona se llama bulling. Cabe que sea realizado mediante *Internet*, teléfonos móviles, videoconsolas *online*.

K) Delito de odio (art. 510 del CP) y apología del terrorismo, que tiene especial gravedad, cuando se difunde a través de medios telemáticos (art. 578 del CP)

L) Delito por usurpación o suplantación de la identidad: art. 401 del CP. Supone apropiarse una persona de la identidad de otra, en beneficio propio, actuando en el tráfico jurídico simulando ser la persona a la que suplanta. Este tipo de delitos es muy habitual en las llamadas «estafas del amor», pues como señuelo, se coloca la foto de una persona atractiva que es de otra persona.

El CP se ha ido modificando para adaptarse a la nueva realidad delictiva. La reforma más importante habida en este sentido ha sido la producida por la Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

Como puede entenderse, la cooperación en materia penal para la prevención y lucha contra la delincuencia transnacional y, en particular, contra la ciberdelincuencia, resulta, en virtud de lo anterior, de vital importancia.

La ciberdelincuencia proyecta sus consecuencias directamente sobre el proceso penal. Primeramente, porque la investigación de la ciberdelincuencia requiere de unidades investigación especializadas, dotadas de los medios técnicos necesarios para la efectividad de su trabajo.

En segundo lugar, los rastros que deja esta clase de delincuencia son de carácter electrónico, debiendo entonces referirnos a las evidencias electrónicas, difíciles de conseguir y altamente volátiles. En este sentido, la obtención transfronteriza de pruebas electrónicas se antoja extremadamente difícil, pues los proveedores de servicios de *Internet* suelen tener su sede en lugar distinto al de comisión de los hechos delictivos. La extraterritorialidad dificulta enormemente el acceso a dicha clase de prueba. La rápida alteración y destrucción de las evidencias digitales es uno de los grandes escollos que existen para el castigo de estos delitos.

Aunque en el seno de la Unión Europea (en adelante, UE) se ha legislado para evitar que los servidores de servicios de *Internet* impidan el acceso a la prueba electrónica, aún muchos Estados miembros se amparan en el necesario respeto de los derechos fundamentales para intentar impedir la obtención de las pruebas electrónicas.

Por último, tal y como se expondrá posteriormente, se hace necesaria la intervención de peritos especializados en la obtención y análisis de las evidencias encontradas.

A todos estos retos se une el uso de la Inteligencia Artificial (en adelante, IA) fundacional. Hemos pasado de la IA predictiva a la generativa y, dentro de ella, ya se habla del modelo fundacional. Que ¿de qué se trata? De redes neuronales *deep learning*. La IA que sigue este modelo se desarrolla a partir de un modelo fundacional que se utiliza como punto de partida para crear modelos de ML, que permite contar con aplicaciones nuevas de

manera rápida y poco costosa. Estos modelos fundacionales son entrenados a través de datos generalizados y sin etiquetar y que son capaces de realizar una gran variedad de tareas generales, entre ellas comprender el lenguaje, generar texto e imágenes y conversar en lenguaje natural.

Estos modelos fundacionales permiten crear archivos de voz o vídeos con imágenes como si fueran reales. ¿Qué les espera a los juzgadores si se les presenta una evidencia creada por IA fudacional sin que tengan posibilidad de conocer que dicha evidencia no es real?

2 Marco legal internacional de la delincuencia transnacional y de la ciberdelincuencia organizada

En diciembre de 2000, se firmó, en la ciudad de Palermo, la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional. La Comunidad internacional se percató de que la delincuencia transnacional se había convertido en un problema mundial, al atravesar las fronteras, siendo imposible atajarla a través de medios nacionales.

Dos Resoluciones de la Asamblea General fueron el origen de dicha Convención. En primer lugar, la Resolución 53/111, de 9 de diciembre de 1998, en la que decidió establecer un Comité especial intergubernamental de composición abierta, con la finalidad de elaborar una Convención internacional amplia contra la delincuencia organizada transnacional y de examinar, si procedía, la posibilidad de elaborar instrumentos internacionales sobre la trata de mujeres y niños, la lucha contra la fabricación y el tráfico ilícitos de armas de fuego, sus piezas y componentes y municiones, y el tráfico y el transporte ilícitos de migrantes, incluso por mar. La segunda fue la Resolución 54/126, de 17 de diciembre de 1999, en la que pidió al Comité Especial encargado de elaborar una Convención contra la delincuencia organizada transnacional que prosiguiera sus trabajos, de conformidad con las Resoluciones 53/111 y 53/114, de 9 de diciembre de 1998, y que intensificara esa labor, a fin de terminarla en el año 2000.

En esta Convención, se definieron conceptos claves tales como: a) grupo delictivo organizado, entendiendo por tal el estructurado por tres o más personas que exista durante cierto tiempo y que actúe concertadamente con el propósito de cometer uno o más delitos graves o delitos tipificados en la Convención, con miras a obtener, directa o indirectamente, un beneficio económico u otro beneficio de orden material; y; b) grupo estructurado, que es un grupo no formado fortuitamente para la comisión inmediata de un delito y en el que no necesariamente se haya asignado a sus miembros funciones formalmente definidas ni haya continuidad en la condición de miembro o exista una estructura desarrollada. La Convención se aplica a la prevención, la investigación y el enjuiciamiento cometidos por grupos organizados, blanqueo de capitales, corrupción y la obstrucción a la Justicia. Intenta que los Estados parte adopten medidas legislativas para el castigo de estos delitos y se decomisen bienes, producto de los mismos. Permite la presentación de la solicitud de la orden de decomiso de un Estado parte a otro, siempre que tenga jurisdicción para conocer de un delito comprendido en el Tratado.

Por otra parte y, ya en un ámbito regional, concretamente referido al Consejo de Europa, contamos con el Convenio sobre Ciberdelincuencia, firmado, en Budapest, el 23 de noviembre de 2001, mediante el cual se propone a los Estados firmantes adoptar las medidas legislativas necesarias para tipificar en sus respectivos ordenamientos jurídicos el acceso deliberado e ilegítimo a toda parte de un sistema informático; la interceptación deliberada e ilegítima por medios técnicos de datos informáticos en transmisiones no públicas dirigidas a un sistema informático, originadas en un sistema informático o efectuadas dentro del mismo, incluyendo las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos; los actos deliberados e ilegítimos que supongan ataques a los datos informáticos; ataques a la integridad de los sistemas; abusos de los dispositivos; la falsificación informática; el fraude informático; los delitos relacionados con la pornografía infantil y los delitos relacionados con infracciones de la propiedad intelectual y otras figuras afines.

Dicho Convenio permite la armonización penal y procesal penal en el ámbito de la ciberdelincuencia, regulando una cuestión

transcendental que provoca múltiples problemas en cuando a la persecución de este tipo de delitos, cometidos a través de servidores que se alojan en Estados diferentes de aquéllos en los produce efectos. Y es que el Convenio dispone que la jurisdicción quedará fijada a favor del Estado cometido en su territorio, incluyendo a bordo de un buque que tenga su pabellón o de una aeronave matriculada según sus leyes cometido por uno de sus nacionales, si el delito es está considerado como tal en el lugar en el que se cometió o si ningún otro Estado tuviera competencia territorial para conocer de aquél.

En 2003, se promulgó la firma del Protocolo Adicional al Convenio de Ciberdelincuencia del Consejo de Europa, criminalizando los actos de racismo y xenofobia, relacionados con las nuevas tecnologías.

Ambos Convenios ponen de manifiesto la importancia de la cooperación para la prevención y represión de los delitos transnacionales y de los ciberdelitos. Y es que las características propias de esta criminalidad dificultan enormemente su persecución.

España ratificó el Convenio en 2004 y el Protocolo Adicional en el año 2006. En 2024, son ya 69 Estados los firmantes de dicho Convenio.

3 La cooperación penal en la Unión Europea: especial referencia a la orden europea de investigación y a la obtención de pruebas electrónicas transfronterizas

La cooperación judicial en materia civil y judicial en la Unión Europea (en adelante, UE) comenzó con el Tratado de Maastricht, firmado el 7 de febrero de 1992, el cual que entró en vigor el 1 de noviembre de 1993. Dicho Tratado declaró la cooperación civil y mercantil cuestión de interés común. Fue el Tratado de Ámsterdam, firmado el 2 de octubre de 1997, en vigor desde el 1 de mayo de 1999, el que asoció la cooperación en ese ámbito con la libre circulación de personas.

La cooperación penal se antoja mucho más complicada pues, como sabemos, choca con la política criminal definida por cada Gobierno y, por tanto, con la soberanía de cada Estado. Los Estados son menos reticentes a cooperar en materia civil y mercantil, que en materia penal. Pero es cierto que la eliminación progresiva de las fronteras y la creación del espacio Schengen (1995), conquista de la UE y que nos permite pasar de un país a otro sin controles fronterizos dentro de la Unión, ha facilitado considerablemente la libre circulación de los ciudadanos europeos, pero también ha contribuido a que los delincuentes puedan actuar con mayor libertad a escala transnacional.

La UE, con el fin de afrontar el reto de la delincuencia transfronteriza y asegurar el espacio de libertad, seguridad y justicia ha incluido medidas para promover la cooperación judicial en materia penal.

Recordemos cuáles han sido los hitos conseguidos en la UE en materia de cooperación penal durante los últimos años:

El 29 de mayo de 2000, el Consejo de Ministros de la Unión adoptó el Convenio relativo a la Asistencia Judicial Mutua en materia penal, cuyo propósito es alentar la cooperación entre las autoridades judiciales, policiales y aduaneras dentro de la Unión, complementando las disposiciones relativas a los instrumentos jurídicos existentes y en aplicación del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales. Este Convenio se antoja clave pues permite la constitución de equipos conjuntos de investigación o la intervención de las telecomunicaciones previa solicitud de una autoridad competente de otro país de la UE, designada para ello en dicho país de la UE. Incluso, la intervención podrá también tener lugar en un país de la UE en que se encuentre la estación terrestre de comunicaciones por satélite correspondiente.

Conseguimos sustituir la extradición por la orden de detención europea, el 13 de junio de 2002, la cual permite, a través de un procedimiento judicial simplificado y transfronterizo, en un plazo de 60 días a partir de la fecha de la detención, la entrega de una persona para el enjuiciamiento y ejecución de pena o medida de seguridad privativa de libertad en otros Estado miembro

de la Unión distinto de aquél en el que se encuentra detenido. Se realiza a través de las autoridades judiciales de los Estados miembros, lo que evita las injerencias políticas propias de las extradiciones. Además, dicha Orden trata de evitar, en treinta y dos categorías de delitos, que el Estado miembro donde se encuentra la persona detenida y a la cual se ha ordenado la entrega, puede denegar la misma por no existir el delito por el que se le acusa tipificado en su ordenamiento jurídico.

Se han dictado Directivas que obligan a los Estados miembros de la UE a legislar sobre el estatuto de la víctima y sobre el estatuto del investigado. Así, tenemos la Directiva 2012/29/UE del Parlamento Europeo y del Consejo, de 25 de octubre de 2012 por la que se establecen normas mínimas sobre los derechos, el apoyo y la protección de las víctimas de delitos. La Directiva 2013/48/UE del Parlamento Europeo y del Consejo, de 22 de octubre de 2013, sobre el derecho a la asistencia de letrado en los procesos penales y en los procedimientos relativos a la orden de detención europea, y sobre el derecho a que se informe a un tercero en el momento de la privación de libertad y a comunicarse con terceros y con autoridades consulares durante la privación de libertad, también es muestra sobre ello.

Asimismo, a través de la Directiva 2014/41/UE, se ha adoptado también la orden europea de investigación en materia penal, aprobada bajo presidencia española, cuyo objetivo es simplificar la obtención de pruebas transfronterizas. A través de un formulario sencillo se permite que un Estado miembro emita una orden para la ejecución de una medida de investigación en otro Estado distinto, sin que éste, salvo en casos tasados, pueda negarse a ello.

La Directiva 2014/42/UE del Parlamento Europeo y del Consejo sobre el embargo y el decomiso de los instrumentos y del producto del delito en la UE, asimismo, establece normas comunes para los Estados miembros respecto al embargo y decomiso del producto de ciertos delitos, así como de propiedades cuya procedencia sea resultado de conductas delictivas, es lo que se denomina decomiso ampliado. Además, en diciembre de 2016, la Comisión propuso la adopción de un nuevo Reglamento sobre el reconocimiento mutuo de las resoluciones de embargo y

decomiso. De hecho, se ha dictado el Reglamento 2018/1805, de 14 de noviembre de 2018, sobre el reconocimiento mutuo de las resoluciones de embargo y decomiso.

Hemos logrado tener instituciones que son el adalid de la cooperación en materia penal. Así mencionamos *Europol*, *Eurojust,* la Red Judicial Europea, los Equipos Conjuntos de Investigación y la Fiscalía Europea. Por ejemplo, el Parlamento Europeo ha reformulado las funciones y estructuras de *Eurojust*, para mejorar la efectividad de este órgano de forma que se permita facilitar las investigaciones transfronterizas y el enjuiciamiento de los delitos graves en el seno de la UE. La Fiscalía europea ha surgido en 2018 para combatir el fraude contra las finanzas de la UE, pudiendo investigar los delitos que afecten a los intereses financieros de la UE y ejercer la acción penal en los procesos penales que se sustancien al efecto.

Los esfuerzos de la UE en cooperación penal se centran en lograr el respeto del principio de reconocimiento mutuo. La realización del espacio de libertad, seguridad y justicia en la Unión se basa en la confianza mutua y en una presunción del respeto, por parte de los demás Estados miembros, del Derecho de la Unión y, en particular, de los derechos fundamentales. Ya, en el Consejo Europeo de Tampere, en octubre de 1999, quedó definido que el reconocimiento mutuo debería constituir la piedra angular de la cooperación judicial en materia penal. El principio del reconocimiento mutuo fue confirmado en los Programas de La Haya, en 2005 y de Estocolmo, en 2009. Sólo a través de este reconocimiento mutuo se podrá logar la superación de los problemas que existen por la existencia de diferentes legislaciones en los distintos miembros de la UE y por las diferencias entre los sistemas judiciales nacionales. Recordemos que el sistema de integración europea no se basa en la uniformidad de las legislaciones, sino en la armonización de las mismas. El principio de reconocimiento mutuo no podrá lograrse si no existe un alto grado de confianza mutua entre los Estados miembros.

En julio de 2018, los ministros de Justicia de los distintos países de la UE trabajaron en la Agenda de Justicia para el año 2020 y dentro de la misma discutieron cómo facilitar la obtención transfronteriza de pruebas.

En 2023, se dicta el Reglamento 2023/1543 del Parlamento Europeo y del Consejo, de 12 de julio de 2023, sobre las órdenes europeas de producción y las órdenes europeas de conservación a efectos de prueba electrónica en procesos penales y de ejecución de penas privativas de libertad a raíz de procesos penales. Para la UE es cada vez más necesario regular las medidas para obtener y conservar pruebas electrónicas de cara a las investigaciones penales.

El Reglamento pone el acento en los prestadores de servicios como punto importante para la obtención de pruebas para procesos penales. A estos efectos, los prestadores de servicios más importantes son los proveedores de servicios de comunicaciones electrónicas y los prestadores de servicios de la sociedad de la información, que permite la interacción entre los usuarios.

Los proveedores de servicios de comunicaciones electrónicas se definen en la 2018/1972 del Parlamento Europeo y del Consejo y son los que prestan servicios de comunicaciones interpersonales, tales como servicios de voz sobre IP, servicios de mensajería instantánea y servicios de correo electrónico.

La Directiva 2015/1535 del Parlamento Europeo y del Consejo se refiere a los servicios que permiten a sus usuarios la capacidad de comunicarse entre sí o les ofrecen servicios que puedan utilizar para almacenar o tratar datos su nombre. Esto incluye a los mercados en línea que proporcionan a los consumidores y las empresas la capacidad de comunicarse entre sí, otros servicios de alojamiento de datos, y también a los datos alojados en la nube y a las plataformas de juegos y a los juegos de apuestas en línea.

Los entidades que prestan servicios de infraestructura de *Internet* y que asigna nombres y números, como ocurre con los registradores y registros de nombres de dominio y los prestadores de servicios de privacidad y representación o registros regionales de direcciones de protocolo de *Internet* (IP), pueden identificar a los creadores de páginas *web* maliciosas o comprometidas, pues poseen datos que permite identificar a la persona física o jurídica responsable de esos sitios y que los utilizan para cometer delitos o, también permite identificar a la víctima de dicha actividad.

El Reglamento define cuándo el prestador de servicios tiene una conexión sustancial con la UE. Esto ocurre si tiene un establecimiento en la Unión o en caso de no tenerlo, existe un número significativo de usuarios en uno o más Estados miembros, o si las actividades se orientan hacia uno o más Estados miembros.

Y es que las direcciones IP, los números de acceso y la información conexa, es sin lugar a dudas, un dato esencial en una investigación penal, cuando no se conoce la identidad del autor del delito. Además, la IP constituyen el registro de una serie de acontecimientos tales como el comienzo y el final de la sesión de acceso de un usuario a un servicio. Es la dirección IP el que indica la interfaz de red utilizada durante la sesión de acceso, aunque a veces se necesita información adicional sobre el comienzo y el fin de una sesión de acceso de un usuario a un servicio, pues resulta habitual que las direcciones IP sean compartidas entre usuarios.

La dirección IP constituye un dato personal y goza de la protección que dispensa la norma. Incluso, las direcciones IP pueden considerarse datos de tráfico. Asimismo, los números de acceso y la información conexa se consideran datos de tráfico en algunos Estados miembros.

Si se produce una investigación en el seno de un proceso penal, las Fuerzas y Cuerpos de Seguridad del Estado pueden solicitar las autoridades policiales una dirección IP y los números de acceso e información conexa, para poder identificar al usuario, antes de que puedan solicitarse al prestador de servicios los datos de los abonados relacionados con ese identificador. Además, la dirección IP puede ser solicitada para conseguir información aún más sensible y que incide más la vida privada, tal es el caso de los contactos y el paradero del usuario, lo que puede suponer establecer un perfil de la persona afectada.

A estos efectos, se crea la orden europea de producción y la orden europea de conservación. En ambos casos, serán emitidas por una autoridad judicial, aunque excepcionalmente, si lo único que se pretende a través de ellas es la identificación del usuario, también puede ser emitida por un fiscal.

La orden europea de producción se utiliza para obtener pruebas específicas, como documentos, objetos o datos almacenados electrónicamente, que sean necesarios para una investigación o un proceso penal en curso. La orden europea de conservación se usa para preservar pruebas o evidencias que puedan ser relevantes para una investigación penal.

Debe tenerse en cuenta que las pruebas de los ciberdelitos únicamente se encuentran en soporte electrónico y éstas, como ya se ha dicho, tienden a desaparecer con mucha facilidad. Esta es la finalidad del Reglamento, y requieren de un tratamiento distinto a las restantes clases de pruebas. Esta norma también se aplica a aquellas actividades delictivas que estén castigadas una pena máxima privativa de libertad inferior a tres años.

Las órdenes europeas de producción, que se tramita a través de un documento que se llama EPOC y las órdenes europeas de conservación, que se tramitan mediante un documento denominado EPOC-PR, se dirigen al prestador de servicios, que actúa como responsable del tratamiento. Una vez recibido, el destinatario debe conservar los datos solicitados durante un máximo de sesenta días, a menos que la autoridad emisora confirme que se ha emitido una solicitud posterior de entrega, en cuyo caso la conservación debe mantenerse.

Los motivos de denegación de una orden europea de protección son tasados. Cabe oponerse, por ejemplo, si supusiese una vulneración manifiesta de un derecho fundamental previsto en el artículo 6 del Tratado de la UE y en la Carta de derechos fundamentales.

En definitiva, el Reglamento permite dirigir de forma segura, peticiones a los prestadores de servicios de comunicaciones electrónicas directamente por las autoridades judiciales nacionales. De esta forma, se garantiza que dicho prestador no pueda negarse a colaborar con la investigación penal, salvo que concurra motivo tasado en el propio Reglamento. Dado el carácter volátil de las evidencias electrónicas de los delitos cibernéticos, la creación de estos instrumentos basados en la cooperación una muestra eficaz de por dónde deben transcurrir los caminos de persecución y represión de los ciberdelitos.

4 Las particularidades de la investigación y de los procesos penales contra la ciberdelincuencia organizada

Como conocemos, *Internet* está constituido por un gran número de ordenadores conectados entre sí, formando pequeñas redes que, a su vez, se enlazan en la llamada «red de redes».

¿Qué hace un usuario para entrar en la red? Pues bien, lo primero es comunicar su equipo con un proveedor de acceso a *Internet* (ISP), a través de un operador de telecomunicaciones. El proveedor es, en definitiva, la compañía que permite a un cliente tener servicios de *Internet*. Esta empresa asignará un identificador, denominado IP (*Internet Protocol*) que identifica a cada usuario. Los números IP son únicos y están compuestos por cuatro grupos de números naturales que puede adquirir el valor de 0 hasta 225, número que están separados entre sí por puntos. Existen unos 4.000 millones de combinaciones diferentes. Ahora bien, como después diremos, a pesar de que nos pueda parecer que esas múltiples combinaciones, permiten casi infinitas direcciones IP, debido al tan número de dispositivos conectados a la red, resultan actualmente insuficientes.

Dos computadores diferentes pueden intercambiar información entre sí a través de unos protocolos de comunicación. Esa información se agrupa en paquetes, que se denominan «datos del tráfico». Y, ahí radica la dificultad, pues estos datos de tráfico no siempre se localizan fácilmente. Normalmente, se almacenan por los sistemas y aplicaciones informáticas y su conservación y el tiempo de ésta es configurable por el usuario que maneja el sistema.

Si se ha cometido un delito, para conseguir las evidencias y obtener los datos para poderlos presentar posteriormente en un proceso, en definitiva, para poder comprobar que se ha perpetrado el delito y cómo se ha perpetrado, lo primero que se precisa es conocer el número IP, en el momento de conexión a *Internet*. Además, tendrá que saberse el momento concreto de acceso cuando se cometió el hecho delictivo, será necesario identificar el ordenador, su ubicación y el abonado de la línea telefónica.

Estos elementos permitirán, tras la investigación policial, conocer el equipo desde el cual se realizó la acción, la ubicación del mismo, incluso, identificar al abonado. Pero esta identificación no supone haber encontrado al autor de la acción delictiva. Primeramente, porque el usuario puede ser otra persona distinta a aquélla que contrató los servicios de *Internet*[9]. En segundo lugar, porque la determinación de la dirección del emisor puede haber sido manipulada. Por último, porque se puede haber accedido desde un lugar público. Existen muchos métodos para evitar que se conozca quién es la persona que navega por la red: están las redes privadas virtuales (VPN), TOR, redes *wifi* compartidas en lugares públicos, en los que los usuarios pueden compartir sesión o pueden registrarse con datos falsos (Barrera Ibañez, 2018).

Los proveedores de servicio de *Internet* deben colaborar con la investigación y dar a los peritos informáticos de la policía la dirección IP; los datos contractuales del abonado; la hora, la fecha y la duración de la comunicación; la concreta transacción o intercambio efectuado; la localización geográfica desde la que se conecta el presunto autor con el proveedor; la cuenta corriente con la que se paga el servicio; el número de teléfono de origen y destino de las comunicaciones realizadas por sospechoso; la transacción o intercambio ilícito; la copia de los ficheros del presunto autor en su espacio web; las llamadas perdidas, hora, duración y frecuencia de las misma; los datos de fecha y el momento de activación de la tarjeta prepago de móviles y tantos otros datos necesarios para que el proceso penal pueda llevarse a cabo.

Por otra parte, en la investigación de un ciberdelito será preciso acceder a los servidores de *Internet*, los cuales suelen guardar un registro de sucesos de lo que ocurre en la navegación por la red, llamados *logs*.

9. Traemos en este punto a colación, la resolución del Tribunal de Justicia de la Unión Europea, el 18 de octubre de 2018. Según esta Sentencia, el titular de una conexión a *Internet*, a través de la que se han cometido infracciones de los derechos de autor mediante un intercambio de archivos, no puede quedar eximido de su responsabilidad designando simplemente a un miembro de su familia que tenía la posibilidad de acceder a dicha conexión.

Los profanos en materia informática, nos podemos preguntar qué son esos servidores y qué son esos *logs*. Un servidor es un equipo informático que forma parte de la red y que provee de servicios a otro equipo cliente. Es decir, un ordenador que provee de ciertos servicios a otros ordenadores. Los hay de diferentes tipos: servidor de archivos, de directorio, de impresión, de correo, de fax, *proxy, web,* de base de datos, DNS, etc. El servidor *web* o de *Internet* tiene como función almacenar páginas *web,* normalmente escritas en HTML (*HyperText Transfer Protocol*), poniéndolas al servicio de los usuarios que las necesitan. Así pues, los servidores de *Internet* almacenan ficheros que componen una página *web* y contienen diferentes fragmentos que controlan la forma en la que los usuarios pueden acceder a estos ficheros, información toda ella de vital importancia para la investigación de un ciberdelito.

Se ha dicho que los servidores suelen almacenar un registro de sucesos, llamados *logs*. ¿Qué es un *log*? Un historial o un registro, una grabación secuencial en un archivo o en una base de datos de todos los acontecimientos que se realizan en la navegación por *Internet*. Así, un *log se* constituye en una evidencia del comportamiento del usuario en la red.

Los equipos informáticos personales no suelen guardar, a diferencia de los servidores, *logs*. En este supuesto, si se quisiera investigar los rastros de un delito, directamente en un ordenador personal, será necesario incautar, registrar y realizar un posterior *back-up* de la información contenida en aquél, para investigar las evidencias del mismo.

Además, de todo lo anterior, debemos referirnos a la tecnología *Network Address Translation* (NAT). Expliquemos en breves palabras qué significado tienen estas palabras casi ininteligibles y la dificultad que supone para la investigación penal. Debido al gran número de dispositivos que se conectan a la red y sabiendo que cada usuario necesitará una IP diferente para cada aparato que acceda a *Internet*, en los últimos tiempos, se está produciendo el agotamiento de las direcciones IP. Por ello, se ha ideado un sistema que permite conectar varios terminales a través de una única dirección IP (IP pública). Esto permite que grandes compañías puedan acceder a *Internet* con esa única IP pública,

con independencia de los aparatos que tengan en la misma, incluso que la conexión que realizamos a *Internet* desde nuestros hogares se pueda hacer desde un *router* al cual queden unidos todos los dispositivos ubicados en el mismo. La identificación del ordenador concreto desde el que se cometió el delito, cuando dicho ordenador se conecta a la red a través de NAT, resultará, como puede suponerse, mucho más complejo.

Cuando se trata de conexiones desde dispositivos móviles, los problemas son aún mayores. Un celular es un receptor-transmisor, el cual permite la comunicación entre personas mediante ondas electromagnéticas de radiofrecuencia. En la actualidad, los celulares utilizan tecnología digital, es, por ello, por lo que los mensajes de voz son transformados en códigos de dígitos binarios, quedando convertidas las conversaciones en paquetes de datos agrupados, según un lenguaje preestablecido.

Para que se pueda producir una conexión inalámbrica, es necesario que, en cada tramo de terreno en el que se quiera que exista cobertura, llamado técnicamente «célula», se instale una antena. Esas antenas receptoras-emisoras, junto a la estación base y a otros equipos electrónicos, permiten hablar y conectarse a *Internet* a las personas que estén situadas en el momento de la conexión en el territorio de esa célula (Martil, 2017). En un mundo en continuo movimiento, donde las personas vamos y venimos de un lado a otro, nos podemos preguntar cuántas antenas a lo largo de un día han podido darnos cobertura en nuestras conexiones inalámbricas. A todo ello hemos de unir una dificultad más y es que los celulares se conectan a *Internet* con una IP pública (NAT). La investigación de la comisión de un hecho delictivo cometido desde un celular podrá permitir averiguar la última antena desde la que se conectó este teléfono, pero debemos tener presente que, al mismo tiempo, habrá habido otros miles de celulares conectados desde esa misma antena. Si todos esos miles de celulares se conectan a través de una misma IP pública, resultará del todo imposible individualizar desde cuál fue cometido el hecho delictivo.

La utilización del protocolo IPV6, en lugar del IPV4, permite asignar direcciones IP a cada uno de los dispositivos en cada una

de las conexiones. El protocolo IPV6 permite que un número ilimitado de dispositivos se puedan conectar a *Internet* al mismo tiempo. La UE ha luchado mucho para que sea obligatorio y hoy, ya es una realidad. (Barrera Ibáñez, 2018).

Como puede observarse, el control, el seguimiento y el acceso a los datos de la navegación *web* por parte de la policía supone la limitación de derechos fundamentales de los ciudadanos, en este caso, del derecho a la intimidad y del secreto de las comunicaciones. La policía deberá realizar intervenciones telefónicas, rastrear IP, acceder de forma remota a los dispositivos desde los cuales se realiza la navegación por la red, obtener datos de los proveedores de servicios de *Internet* y de los contenidos en servidores, incluso incautar y registrar dispositivos de almacenamiento masivo de información, para su posterior análisis de su contenido, actuaciones todas ellas que suponen una importante limitación de los derechos fundamentales. Podemos incluso, hablar del derecho a la inviolabilidad del domicilio, puesto que, para incautar un ordenador, será precisa la entrada y registro domiciliario, en el lugar en que se encuentren, para lo que será necesario la correspondiente autorización judicial.

Las dificultades de la investigación penal del cibercrimen no acaban aquí, pues es necesario el análisis de la información, posteriormente, la redacción del correspondiente dictamen pericial y la intervención del perito en el juicio. Para poder realizar el análisis de los datos será ineludible la realización de ciertas operaciones técnicas, entre ellas, el «volcado» de la información obtenida, que se realiza a través de una copia del soporte original, aunque siempre se deberá guardar el original. Asegurar la cadena de custodia es lo más importante en ese momento. Por ello, para garantizar que el original y la copia sean iguales, y no tener después problemas con la nulidad de la prueba, ese volcado se suele realizar en presencia de un fedatario público y de forma simultánea al registro domiciliario e incautación de los ordenadores. El Letrado de la Administración de Justicia, cuya presencia se exige como fedatario público, en una diligencia de entrada y registro domiciliario, podrá acreditar la autenticidad de la copia que se realice, si es que el volcado se efectúa en ese mismo momento. Si no fuera así, el Letrado de la Administración

de Justicia será el que habrá de remover los precintos impuestos durante la entrada y registro domiciliario y en la diligencia de incautación de los distintos equipos informáticos hallados en el lugar. Una vez realizado el volcado, los precintos deben mantenerse, para garantizar la cadena de custodia de la prueba (Rayón Ballesteros y Gómez Hernández, 2014).

La redacción del dictamen pericial y la posterior actuación en la vista oral del perito tiene también sus complejidades, que analizaremos posteriormente. Pero lo que nos importa en este momento es insistir en la necesidad de conservar siempre los dispositivos originales de donde se hayan extraído las pruebas. Por este motivo, deberán estar en custodia del Letrado de la Administración de Justicia, que garantizará su conservación y puesta a disposición del juez, si ésta fuera precisa.

Pero la ciberdelincuencia no sólo plantea problemas en la investigación del delito, sino también en cuanto al proceso mismo. Al tratarse de delitos transnacionales, puede ocurrir que la conducta delictiva produzca resultados en Estados distintos de aquéllos donde se cometió, incluso puede ser que el hecho delictivo tenga su origen en uno o varios países. Obviamente, todo ello afecta a cuestiones tan básicas como la jurisdicción, la competencia jurisdiccional, la ley penal aplicable y al procedimiento que se tramitará para su investigación y enjuiciamiento. Las reglas clásicas, tales como la relativa al principio de territorialidad, según la cual el hecho delictivo se enjuiciará en el lugar de su comisión (*locus comissi delicti*) ya no tienen cabida (Rayón Ballesteros y Gómez Hernández, 2014).

5 La prueba electrónica transfronteriza

5.1 Prueba electrónica: concepto y clases

Entendemos por prueba electrónica toda información que puede ser usada como prueba en un proceso, bien contenida en un medio electrónico o bien transmitida por ese medio (Delgado Martín, 2016).

El motivo por el que hablamos de esta clase de prueba no es otro, como se ha explicado anteriormente, que el hecho de que las evidencias que permiten demostrar la existencia de un ciberdelito son de carácter electrónico.

Resulta indiferente si la información se ha creado, se almacena o se transmite por medios electrónicos y también es intrascendente qué tipo de información sea. Lo relevante es que se encuentre contenida o sea transmitida por medios electrónicos y que sirva para acreditar los hechos dentro de un proceso penal. Como estamos analizando la ciberdelincuencia, hablamos de la prueba electrónica que permite probar la comisión de un hecho delictivo en un proceso penal.

Recodemos que, cuando nos referimos a la prueba, este concepto puede estar referido bien al resultado, bien al medio de prueba o bien a la actividad que realizan las partes para convencer al juez de la certeza de los hechos controvertidos en el proceso. Asimismo, se ha de diferenciar dos términos que no significan lo mismo: fuente y medio de prueba. Concretamente, en el ámbito de la prueba electrónica, se entiende fuente de prueba aquella información contenida o transmitida por medios electrónicos. El medio de prueba es, sin embargo, la forma a través de la que la fuente de prueba accede al proceso penal (Delgado Martín, 2016).

Hoy contamos con muy variados elementos electrónicos, que han ido evolucionando a gran velocidad en los últimos años. Cuando nos estábamos acostumbrando a los *Cd-Rom*, llegaron los *DVD*, para ser sustituidos rápidamente por las memorias *USB* y, éstas, posteriormente, por el almacenamiento de datos en la nube. Igual sucedió en el ámbito de la telefonía móvil. Los teléfonos que sólo servían para llamar, pasaron a mejor vida, pues todo el mundo accedió a los *smartphones* (con sistema *Android* o *iOS*), que permiten realizar llamadas, enviar mensajes, utilizar los sistemas de mensajería instantánea y la navegación por *Internet*. Los ordenadores de consola siguen existiendo, pero comparten vida con los portátiles, con las tabletas, los reproductores de MP3 o MP4 o, las PDAs. Quién de nosotros no lleva en su vehículo un sistema de navegación que le permite ser rastreado a través de GPS y conocer las carreteras y el camino por dónde llegar a los lugares. Estos elementos electrónicos nos

permiten hablar de diferentes fuentes de prueba electrónica, tales como el correo electrónico, el SMS, la mensajería instantánea o las redes sociales.

Por otra parte, los medios de prueba son los tradicionales en cualquier procedimiento: documental, interrogatorio de partes, testifical, pericial, reconocimiento judicial u otros medios que permiten la reproducción de imágenes, sonidos, etc. Tengamos presente, por ejemplo, que en la Ley española 1/2000, de 7 de enero, de Enjuiciamiento Civil (en adelante LEC), el art. 299, diferencia la prueba documental de los medios de reproducción de imágenes, sonido e imagen y otros que permiten archivar y conocer o reproducir palabras, datos, cifras y operaciones matemáticas llevadas a cabo con fines contables o de otra clase.

Además, existen dos clases de prueba electrónica: a) los datos o informaciones almacenados en un dispositivo electrónico; y, b) los que son transmitidos por cualesquiera redes de comunicación abiertas o restringidas como *Internet*, telefonía fija y móvil u otras.

5.2 Fases de la prueba electrónica

Las fases de esta clase de prueba no son diferentes a las de otro tipo. En primer lugar, ha de obtenerse; en segundo lugar, ha de incorporarse al proceso y; por último, ha de valorarse por el juez.

5.2.1 Obtención de la prueba electrónica

Para poder obtener la prueba electrónica, podrá ser precisa la aprehensión y registro del aparato en el que se encuentra la misma. Incluso puede ser necesaria la entrada y registro en lugares no públicos.

En España y, tras la entrada en vigor de la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, según el art. 588 *sexies* a, la aprehensión de ordenadores o de registro de dispositivos de almacenamiento masivo de información requiere ser

autorizada también por el juez, no estando permitido a las Fuerzas y Cuerpos de Seguridad del Estado aprovechar la entrada y registro domiciliarios para registrar dichos aparatos, sin que el juez haya motivado las razones que legitiman el acceso de los agentes facultados a la información contenida en tales dispositivos.

Otras veces la prueba electrónica de la comisión de un hecho delictivo será fruto del acceso a través de datos de identificación, códigos o por medio de la instalación de un *software*, que permitan, de forma remota y telemática, el examen a distancia y sin conocimiento de su titular o usuario del contenido de un ordenador, dispositivo electrónico, sistema informático, instrumento de almacenamiento masivo de datos informáticos o base de datos. Es aquí donde cobra importancia la obtención de la prueba electrónica en la delincuencia transfronteriza, pues cuando los datos se localizan en un servidor situado fuera del territorio de un Estado surgen las dificultades.

La prueba electrónica no sólo puede ser obtenida por la intervención de las Fuerzas y Cuerpos de Seguridad del Estado, sino en ocasiones por los propios particulares. Tengamos presente que las personas hoy día se comunican a través de correos electrónicos, *whastapps*, redes sociales, etc. Esas informaciones, que pueden contener pruebas de delitos, pueden ser obtenidas por uno de los propios comunicantes, por un tercero o, incluso por el acceso a información contenida en páginas *web*.

Dadas las especiales características de la prueba electrónica, lo importante es no vulnerar derechos fundamentales, pues si así fuera, estaríamos ante una prueba ilícita, que viciaría no sólo las obtenidas de forma directa sino también indirectamente, en aplicación de la teoría del árbol de los frutos envenenados. Son varios derechos fundamentales los que pueden quedar afectados: intimidad personal, propia imagen, secreto de las comunicaciones, la protección de los datos personales o la inviolabilidad del domicilio. En España, según el art. 11 de la LOPJ, no surtirán efecto las pruebas obtenidas, directa o indirectamente, violentando los derechos o libertades fundamentales.

Los derechos fundamentales no sólo deben de ser respetados por los poderes públicos, sino también por los particulares, a

esto se denomina eficacia horizontal de los derechos fundamentales o *Drittwirkung*, expresión alemana que significa eficacia hacia terceros. Nada impide que un sujeto aporte a un proceso judicial como prueba un correo electrónico, un *whastapp* o incluso, una grabación de una conversación telefónica, mantenida entre dos personas, siempre que la aportación se produzca por uno de los intervinientes en el proceso comunicativo. En el ordenamiento jurídico español, el derecho a la aportación al proceso de grabaciones de conversaciones particulares realizadas por uno de sus protagonistas no vulnera el derecho al secreto de las comunicaciones. Y, como han dejado dicho Sentencias, entre otras, del Tribunal Constitucional 114/1984, de 29 de noviembre y del Tribunal Supremo de 9 de julio de 1993, ese derecho no puede esgrimirse frente a los propios intervinientes en la conversación o, podemos decir, comunicación.

Pero para conocer, por ejemplo, si los derechos fundamentales quedan afectados por la obtención de la prueba electrónica y si, por ejemplo, la policía debe solicitar o no autorización judicial para acceder a una prueba electrónica sin que esta intromisión sea ilegítima o ilícita es preciso conocer si la comunicación o el medio a través del cual se está transmitiendo una información es de carácter público o privado. Esto no es tan sencillo como a *priori* pudiera parecer. Lo primero que se necesita es analizar el tipo de comunicación utilizado y determinar si éste es apto para mantener una comunicación privada, existiendo casos realmente dudosos. Pensemos, en una página *web*. En principio, parece una comunicación pública y, aunque el acceso sea restringido, la interceptación por la policía de su contenido sin autorización judicial no vulneraría el secreto de las comunicaciones. Las publicaciones que se realizan en abierto en *Facebook*, por ejemplo, han sido calificadas por algunos Tribunales españoles, como información pública y, por tanto, pueden ser aportadas como pruebas en los procesos[10].

Plantemos también el caso de aquellos supuestos en los que la comunicación es privada, no siendo completamente cerrada,

10. Véase, por ejemplo, la Sentencia del Tribunal Superior del Tribunal Superior de Justicia de Las Palmas de Gran Canaria 19/2016 de 22 de enero, aunque referida al ámbito laboral.

al requerir el conocimiento o intervención de un tercero, como ocurre con el caso de un correo electrónico. Pues bien, la interceptación de un correo electrónico, requiere en todo caso la autorización judicial, pues se trata de una comunicación privada, a pesar de que en esa clase de comunicación deba intervenir el servidor de prestación de servicios de *Internet* (Volpato, 2016).

Todos sabemos que la conversación mantenida entre dos personas a través de un teléfono celular es privada y, por ende, está protegida por el derecho al secreto de las comunicaciones, pero ha de tenerse en cuenta que el aparato también se utiliza para el acceso a páginas *web*, para intercambiar mensajes instantáneos, para realizar fotografías o consultar correos electrónicos. Está en juego el derecho a la intimidad. Por ello, la policía, para poder acceder y registrar el contenido de un teléfono celular y obtener así una prueba electrónica, necesitará igualmente autorización judicial. El juez debe autorizar, en su auto, el posible acceso de la policía a todos aquellos elementos que contiene, pues en ese dispositivo, se albergan datos de contactos, fotografías, mensajes, correos electrónicos, etc. Actualmente, el derecho a la intimidad incluye el «entorno virtual» de una persona, tal y como se afirma en la Sentencia del Tribunal Supremo español 786/2015, de 4 de diciembre. En esta Resolución se nos dice que «La jurisprudencia de esta Sala ha recordado la necesidad de que exista una resolución jurisdiccional habilitante para la invasión del derecho al entorno digital de todo investigado».

5.2.2 Incorporación de la prueba electrónica al proceso

La incorporación de la prueba electrónica en un proceso, en nuestro caso penal, requiere que dicha prueba cumpla con los requisitos generales concretados por la teoría general de la prueba: pertinencia, utilidad y licitud. No es el momento de tratarlos, pues son de carácter general y no sólo aplican a la prueba electrónica. Interesa mucho más referirnos al modo en que la prueba electrónica accede al proceso. Hablemos, pues de los medios de prueba.

Como conocemos, los medios de prueba son: documental, interrogatorio de partes, testifical, pericial, reconocimiento judicial u otros medios que permiten la reproducción de imágenes, sonidos, etc.

Hablemos de la prueba documental y de la prueba pericial que son la que presentan especificaciones más significativas en el ámbito de la prueba electrónica.

Los documentos pueden clasificarse en torno a tres categorías tradicionalmente: públicos, privados y oficiales. Los documentos públicos son aquéllos en los que ha intervenido un fedatario público. Los privados, por el contrario, en los que no hay dicha intervención. Los oficiales en los que ha intervenido un funcionario con facultad certificante de las Administraciones Públicas, en relación con los actos administrativos de éstas.

Una prueba electrónica podría acceder al proceso a través de un documento en formato papel, pero también en forma de documento electrónico. En este caso, la prueba se aporta al proceso en soporte electrónico, bien a través de una memoria *USB*, un *DVD* o cualquier otro medio que permita el almacenamiento de datos. Lo que sucede, por ejemplo, es que, tradicionalmente, por documento se entiende sólo aquél que se encuentra en soporte papel. Según la LEC española entrarían en el proceso, a través del art. 299.2 como otros medios de reproducción de imágenes, sonido e imagen y otros que permiten archivar y conocer o reproducir palabras, datos, cifras y operaciones matemáticas llevadas a cabo con fines contables o de otra clase.

Los documentos electrónicos, por su parte, también pueden ser públicos, privados u oficiales.

Entre los documentos electrónicos públicos se incluyen las resoluciones y diligencias de actuaciones judiciales de toda especie y los testimonios que de las mismas expidan los Letrados de la Administración de Justicia, pues hoy contamos con el procedimiento judicial electrónico y, de hecho en España, tras la entrada en vigor de la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en

la Administración de Justicia, el expediente judicial electrónico es una realidad en nuestro proceso. También existen los documentos notariales electrónicos, los cuales tienen el mismo valor que los expedidos en soporte papel[11]. La copia electrónica de los documentos notariales existe desde el año 2002, en España y, se regulan en el art. 17 *bis* de la Ley de 28 de mayo 1862, Orgánica del Notariado.

La Ley 11/2023, de 8 de mayo, de trasposición de Directivas de la UE en materia de accesibilidad de determinados productos y servicios, migración de personas altamente cualificadas, tributaria y digitalización de actuaciones notariales y registrales; y por la que se modifica la Ley 12/2011, de 27 de mayo, sobre responsabilidad civil por daños nucleares o producidos por materiales radiactivos, es la que regula el nuevo Protocolo electrónico notarial. Hoy día, la matriz digital es una realidad[12].

Los documentos oficiales, como se ha dicho, son los firmados por funcionarios en el ejercicio de sus funciones. Actualmente, podemos relacionarnos con la Administración Pública a través de documentos electrónicos, tal y como sucede en España, des-

11. El artículo 17 *bis* de la Ley de 28 de mayo 1862, Orgánica del Notariado asevera que «Los instrumentos públicos a que se refiere el art. 17 de esta Ley, no perderán dicho carácter por el solo hecho de estar redactados en soporte electrónico con la firma electrónica avanzada del notario y, en su caso, de los otorgantes o intervinientes, obtenida la de aquél de conformidad con la Ley reguladora del uso de firma electrónica por parte de notarios y demás normas complementarias». En el apartado 2, párrafo b), sigue diciendo «Los documentos públicos autorizados por Notario en soporte electrónico, al igual que los autorizados sobre papel, gozan de fe pública y su contenido se presume veraz e íntegro de acuerdo con lo dispuesto en esta u otras leyes».
12. El art. 17 ha sido modificado, adicionando un apartado 4, según el cual: «Las matrices de los instrumentos públicos tendrán igualmente reflejo informático en el correspondiente protocolo electrónico bajo la fe del notario. La incorporación al protocolo electrónico o libro registro de operaciones electrónico se producirá en cada caso con la autorización o intervención de la escritura pública o póliza, de lo que se dejará constancia mediante diligencia en la matriz en papel expresiva de su traslado informático. Los instrumentos incorporados al protocolo electrónico se considerarán asimismo originales o matrices. En caso de contradicción entre el contenido de la matriz en soporte papel y del protocolo electrónico prevalecerá el contenido de aquella sobre el de este».

de la entrada en vigor de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas[13].

Es claro que la comunicación entre particulares ha cambiado significativamente, pues hoy se generan cantidad de documentos electrónicos, como son los correos electrónicos. Esos son documentos electrónicos privados. Existen, también, las facturas electrónicas. El Real Decreto 1619/2012, de 30 de noviembre, por el que se aprueba el Reglamento por el que se regulan las obligaciones de facturación se refiere a las mismas.

Los documentos electrónicos privados presentan una seria dificultad, pues al no haber intervenido en su confección una autoridad que acredite su autenticidad resulta muy fácil alterar su contenido. El correo electrónico se puede aportar como documento en soporte papel o en soporte electrónico. Si se presentase en soporte papel, bastaría con usar una aplicación disponible en el sistema operativo *Windows*, para alterar su exactitud. Pero en ambos casos es muy fácil adulterar la autenticidad, su exactitud o su integridad, debiéndose practicar una prueba pericial, para averiguar todos estos extremos. La única posibilidad que existe para garantizar la autenticidad de un correo electrónico es el *email* certificado, que se envía a través de proveedores, que otorga veracidad al propio correo, al contenido, a la fecha de envío y de recepción, y a las direcciones IP de envío y de recepción[14].

Con el sistema de mensajería instantánea de *whatsapp* ocurre otro tanto de lo mismo. Y es que existen *apps* que, aunque creadas con una finalidad de diversión, permiten sustituir conversaciones reales por otras falsas, alterar la hora de envío, el

13. El art. 14 de dicha Ley contempla: «Las personas físicas podrán elegir en todo momento si se comunican con las Administraciones Públicas para el ejercicio de sus derechos y obligaciones a través de medios electrónicos o no, salvo que estén obligadas a relacionarse a través de medios electrónicos con las Administraciones Públicas. El medio elegido por la persona para comunicarse con las Administraciones Públicas podrá ser modificado por aquella en cualquier momento».
14. En España, existen varios proveedores como son *EGarante, MailCertificado, Lleida.NET.*

estado de recepción, modificar el emisor del mensaje, crear audios, vídeos y fotos como si hubieran sido enviados verdaderamente. También posibilitan alterar los ajustes de los perfiles y estados de las personas implicadas (Picón Rodríguez, 2017). Así, para que las pruebas contenidas en sistemas de mensajería instantánea puedan ser válidas en un proceso, éstas deben estar certificadas y autentificadas y ello sólo se consigue a través de un perito informático. En la Sentencia del Tribunal Supremo 300/2015, se afirma la necesidad de aportar una prueba pericial que identifique el origen real de la conversación, la identidad de los interlocutores y la integridad del contenido.

Los «pantallazos» son también pruebas electrónicas, pues son impresiones digitales de un escritorio o pantalla de un aparato electrónico. Estos pantallazos se puedan aportar en formato papel o bien de forma electrónica, pero sea como fueran aportados son fácilmente manipulables. Como todos conocemos, existen programas informáticos de edición de imágenes con los resulta bastante sencillo alterar esas representaciones.

Refirámonos ahora a la prueba pericial informática. Como se ha visto, las evidencias electrónicas resultan altamente manipulables. Por este motivo, en la mayoría de las ocasiones, resultará necesario practicar una prueba pericial informática en el proceso judicial que permita acreditar la autenticidad, exactitud y la integridad de una prueba electrónica, por ejemplo, de un correo electrónico o de un *whastapp*. Al mismo tiempo, cuando la Policía registra e interviene un ordenador a través del cual se ha cometido un hecho delictivo, se necesitará la intervención de un perito para extraer, preservar, analizar y documentar los datos allí almacenados.

Así la prueba pericial informática puede definirse como aquél medio de prueba, mediante el cual una persona experta en temas informáticos aporta al juez los conocimientos técnicos que le permitan valorar y tener como probados los hechos, en este caso, delictivos, que se encuentran en dispositivos electrónicos o informáticos. Este medio de prueba, tal y como se ha expuesto, puede resultar complementario de otros medios, tal y como sucede cuando lo que se quiere es acreditar la autenti-

cidad, exactitud e integridad de una prueba electrónica o puede ser autónomo.

¿Qué puede analizar un perito informático? Desde un soporte portátil, como puede ser una memoria *USB* o un disco duro extraíble, hasta un ordenador portátil o de sobremesa, incluyéndose los datos almacenados en los discos duros; también celulares, tanto la tarjeta *SIM*, como la memoria interna o memorias adicionales. Asimismo, *GPS* de los vehículos, tarjetas de televisión de pago, lectores de bandas magnéticas, teclados de cajeros bancarios o un clonador de tarjetas bancarias de crédito o de débito.

Esta prueba tiene una especial dificultad, primeramente, porque el perito debe obtener los datos.

Una vez obtenidos, debe realizar un clonado de los mismos, debiendo siempre conservarse el original hasta el momento del juicio. Será sobre la copia clonada, sobre la que el perito podrá realizar las intervenciones que necesite para elaborar el dictamen posterior que después se aportará en el proceso.

¿Qué significa clonar? El clonado supone una copia espejo o *bit a bit* de la información original contenida en el dispositivo. Además, realizará una segunda copia, que quedará en manos del titular de los datos, para que éste pueda seguir realizando su actividad. En definitiva, clonar se refiere al proceso de crear una copia exacta o duplicado de una información digital, pudiendo ser un dispositivo móvil o de un sistema operativo, *software* o conjunto de datos.

Clonar y copiar son términos distintos: clonar implica crear una réplica exacta, de modo que la copia sea idéntica al original, incluyendo configuraciones y datos. Copiar significa duplicar o reproducir un objeto, archivo o información, pero no necesariamente implica que la copia sea idéntica al original en todos los aspectos. En informática, por ejemplo, copiar un archivo simplemente implica duplicar su contenido en otro lugar, pero no necesariamente incluye configuraciones. Esas configuraciones son los llamados metadatos, que todo archivo digital tiene, y van asociados con el archivo original. Los metadatos son datos que

proporcionan información sobre otros datos, es decir, es la información adicional que acompaña a archivos, mensajes o recursos digitales, proporcionando detalles sobre su origen, contenido, formato, autoría y más[15]. Aquí tienes algunos ejemplos de metadatos comunes:

En el ámbito de la ciberdelincuencia, los peritos informáticos suelen pertenecer a unidades especializadas de la policía. En España, contamos con el Departamento de delitos telemáticos de la Guardia Civil y con la Brigada de Investigación Tecnológica de la Policía Nacional, de los cuales forman parte ingenieros o informáticos. Éstos técnicos son diferentes a quienes realizan la incautación de los dispositivos, pues son los que obtienen los datos, realizan el clonado y realizan el dictamen pericial. También son los que averiguan y analizan las IP de los usuarios que navegan por *Internet*.

En la investigación criminal existen tres cuestiones vitales a tener en cuenta. La primera tiene que ver con las actuaciones que realiza la Policía, pues tras la entrada y registro, es preciso que se identifiquen y se aíslen aquellos dispositivos desde los que se ha cometido la acción criminal. Asimismo, los agentes intervinientes deben precintarlos, de modo que cuando se realice el clonado, pueda acreditarse que la copia procede del dispositivo intervenido. Seguramente, la Policía tomará testimonios a los sujetos que puedan conocer datos relevantes, para después poder tener más evidencias sobre los hechos delictivos. La segunda cuestión tiene que ver con la cadena de custodia del material clonado por el técnico. En muchas ocasiones, el clonado se realiza en el mismo acto de la intervención policial, para asegurar la inmediatez y evitar así el borrado de datos que pudieran resultar de importancia para la investigación penal. Junto al técnico,

15. Refirámonos, por ejemplo, a los metadatos de un archivo de imagen: Fecha y hora de la creación o modificación, resolución de la imagen, modelo de cámara utilizado para capturar la imagen, configuración de la cámara (apertura, velocidad de obturación, ISO, etc.) y nombre del autor o fotógrafo. O a los metadatos de correos electrónicos: dirección de correo electrónico del remitente; direcciones de correo electrónico de los destinatarios, fecha y hora del envío; asunto del correo electrónico e información sobre los servidores de correo utilizados en la entrega del mensaje.

suele estar el fedatario público (Letrado de la Administración de Justicia), que es quien acredita que los datos están siendo extraídos del dispositivo que se ha intervenido y sólo cuando dicho fedatario ha removido los precintos. En tercer y último lugar, debe asegurarse que la copia clonada no sufra daños, para que, en caso de ser necesario, pueda accederse a ella. Es por esta cuestión, por la que quedará en custodia del Letrado de la Administración de Justicia, que es el encargado de preservar las piezas de convicción.

Tras todo este proceso el perito deberá redactar su dictamen, en el cual dejará constancia del método científico utilizado y de la fuente del que proceden los datos analizados (ordenador, teléfono celular, memoria *USB*, etc), de las operaciones que ha realizado, de su titulación y currículum, para que el juez pueda valorar la prueba. Como todos conocemos, el perito podrá intervenir en la vista oral, para exponer, explicar, aclarar o responder a preguntas, sobre método, premisas, conclusiones y otros aspectos del dictamen.

5.2.3 Valoración de la prueba electrónica

A la hora de valorar la prueba electrónica, se seguirán los criterios que las leyes procesales establezcan. Recordemos que, en la mayoría de las ocasiones, se aplicará el principio de libre valoración de la prueba, que supone la aplicación de las reglas de la sana crítica y de la experiencia general o especial, dada por el perito. En el ordenamiento jurídico español, el art. 741 del Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal (en adelante, LECr) nos dice que «El Tribunal, apreciando según su conciencia las pruebas practicadas en el juicio, las razones expuestas por la acusación y la defensa y lo manifestado por los mismos procesados, dictará sentencia dentro del término fijado en esta Ley», pero deja sin concretar las reglas de valoración de la prueba. Hemos de aplicar el derecho fundamental a la presunción de inocencia (art. 24.2 de la Constitución Española) y el principio *in dubio pro reo*.

En el proceso civil español, los documentos públicos, al haber sido intervenidos por fedatario público, se salen del criterio de libre valoración de la prueba y hacen prueba plena de los datos obrantes en ellos (art. 319 de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil, en adelante LEC). También, los documentos privados suelen tenerse por válidos siempre que la parte a quien perjudique no impugne su autenticidad. (art. 326 de la LEC).

Entendemos el primer caso de aplicación al proceso penal, dada el carácter supletorio de las normas procesales civiles en el seno de los procesos que se sustancian ante otros órdenes jurisdiccionales. Sin embargo, creemos que, dada la vigencia del principio de oficialidad en los procesos penales, el juez no esperará a la impugnación por la parte contraria de la autenticidad de un documento en papel o electrónico, sobre todo teniendo en cuenta la gran manipulación que puede darse de estos últimos. En la LECr, el art. 729.2 permite al juez o tribunal practicar las diligencias de prueba no propuestas por ninguna de las partes, que el Tribunal considere necesarias para la comprobación de cualquiera de los hechos que hayan sido objeto de los escritos de calificación. Cierto es que este precepto ha sido interpretado por el Tribunal Supremo, en Sentencias de 23 de septiembre de 1995 y de 7 de abril de 1999, según el principio acusatorio, permitiendo al juez practicar prueba cuando sea para corroborar o rebatir las pruebas propuestas por las partes. El Ministerio Público será seguramente el encargado de solicitar al juez practicar prueba sobre la autenticidad y exactitud de la evidencia electrónica.

6 Problemas para la prevención, la investigación y la represión de la ciberdelincuencia transnacional. Dificultades para la obtención de la prueba electrónica en la delincuencia transfronteriza europea

Enumeremos, a continuación, los problemas de la investigación y represión de la ciberdelincuencia organizada y transnacional.

- La tecnología facilita la perpetración de delitos y su rápida propagación, debido a los miles de personas que utilizan *Internet*.

- La tipificación de las conductas ilícitas resulta complicada, pues son hechos nuevos y de carácter tecnológico, que en muchas ocasiones cuentan con el desconocimiento del Legislador.

- El desconocimiento de los jueces, que no tienen conocimientos específicos en la materia. También, el de los demás operadores jurídicos.

- Por mucho que los instrumentos normativos permitan formar equipos conjuntos de investigación, falta de recursos humanos y materiales, para la prevención, la investigación y la represión. Los jueces llevan múltiples asuntos, si además de toda la carga de trabajo tienen que solicitar comisiones rogatorias o, aunque sea dentro de la UE una orden europea de investigación o una orden europea de conservación de una evidencia electrónica dejarán de atender otros asuntos.

- El anonimato de la navegación por la red y la dificultad de la investigación tecnológica y de la obtención, análisis y preservación de las evidencias. La navegación anónima permite, asimismo, la ocultación de los rastros de los delitos. Como se ha insistido las pruebas electrónicas desaparecen con mucha facilidad; en este sentido se habla de la volatilidad de las pruebas digitales.

- La navegación por *Internet* no permite controlar ni el flujo ni la transmisión de información.

- La extraterritorialidad, que supone problemas concretos para determinar la jurisdicción y competencia a la hora de iniciar un proceso penal.

- La falta de homogeneidad de las legislaciones, incluso europeas.

- La estructura y medios con los que cuentan los ciberdelincuentes.

Las dificultades procesales para luchar contra la ciberdelincuencia en Europa son menores, pues las órdenes de investigación europea, de producción y conservación de las pruebas digitales, así como el Convenio de asistencia judicial mutua han ayudado. La cooperación de órganos como *Europol o Eurojust*, también.

Sin embargo, los instrumentos legislativos enunciados no están exentos de problemas. Sin ánimo de ser exhaustivos podemos mencionar la amplitud de plazos para el reconocimiento y ejecución de una orden, pudiendo extenderse dicho plazo hasta ciento cincuenta días, produciendo la dilación del procedimiento y, en definitiva, la ineficacia de dicha orden. La volatilidad de las pruebas electrónicas hace que, por muy rápida que sea la tramitación de la orden europea de investigación, cuando ésta llegue pueda ser que la evidencia no exista (De Hoyos Santo, 2023, p. 102).

La necesidad de traducción de la orden es otra de las dificultades. Pensemos en lo necesario que resulta una clara comprensión o los problemas que pueden darse si se mal interpretan los hechos delictivos descritos.

Además, debe tenerse en cuenta la escasa formación de los distintos operadores jurídicos. Bienvenidos sean los instrumentos legales de cooperación, pero pensemos en quién los utilizan y aplican: jueces y abogados que no están acostumbrados a los mismos. El cambio de paradigma de la delincuencia que responde a los parámetros de transnacional, organizada y ciber hace necesaria la formación jurídica de los distintos operadores jurídicos acorde a ella. No todos los jueces son la Audiencia Nacional, órgano jurisdiccional altamente especializado.

Los problemas no sólo se derivan de la norma europea, pues si nos referimos a la transposición española, realizada a través de la Ley 3/2018, de 11 de junio, por la que se modifica la Ley 23/2014, de 20 de noviembre, de reconocimiento mutuo de resoluciones penales en la UE, para regular la orden europea de investigación. nos encontramos con otras dificultades distintas. En primer lugar, dicha Ley prevé un sistema de competencias que se distribuyen entre jueces y fiscales, tanto para la emisión

como para la ejecución de la orden, aunque ciertamente el sistema español confiere un especial protagonismo al fiscal en la parte de ejecución. Debe tenerse en cuenta que el Fiscal sólo podrá asumir dichas competencias cuando sea el que instruya y esto, en España, solo se produce en el procedimiento penal de menores, regulado por la Ley Orgánica 5/2000, de 12 de enero, reguladora de la responsabilidad penal de los menores.

En otro orden de cosas, se producen problemas en cuanto a la competencia para la ejecución de la orden. ¿Qué ocurre si la autoridad judicial se considera incompetente? Los tribunales españoles han adoptado ante estos problemas diversas soluciones[16].

Además, el régimen de confidencialidad de la orden europea de investigación también plantea interrogantes, pues el Ministerio Fiscal no puede decretar el secreto de las actuaciones. Como bien indica Laro González (2022), la fase de instrucción se caracteriza por el secreto de las actuaciones, en lugar de por el principio de publicidad. El Fiscal queda obligado a respetar dicho principio, aunque la norma no le permita decidir el secreto de las actuaciones[17].

A todo lo anterior, se añade el hecho de que los ordenamientos jurídicos de los distintos Estados miembros son demasiado rígidos o garantistas. No somos partidarios de prevenir, reprimir y castigar los delitos al margen de la Ley, evidentemente. Pero las instituciones y los países, incluso europeos, se atrincheran en el respeto a los derechos fundamentales, tales como la intimidad o el secreto de las comunicaciones, para impedir la investigación criminal. Recordemos que uno de los motivos que permite denegar la orden de protección de una prueba electrónica es justamente la vulneración de un derecho fundamental. De esta manera, a pesar de que, en Europa, todos los Estados están de acuerdo en el respeto y garantía de los derechos fundamentales

16. Ejemplos son Auto nº 1566/2019 del Juzgado Central de Instrucción nº 2, de 14 de junio y Auto nº 344/2019 de la Audiencia Nacional, de 1 de julio; Auto nº 668/2019 de la Audiencia Provincial de Gerona, de 10 de octubre y auto de la Audiencia Nacional nº 483/2021, de 22 de diciembre.
17. Cit., pág. 134. Véase también Aguilera Morales, 2019 y Rodríguez-Medel Nieto, 2014, p. 413.

inherentes a la dignidad del ser humano, el hecho de negarse a entregar una evidencia a una autoridad judicial que sustancia un proceso en un Estado distinto de aquéllos donde se albergan los datos, se convierte en una excusa que dificulta la represión y castigo de los ciberdelitos y para poner obstáculos a la hora de obtener la prueba electrónica.

El debate jurídico está servido: facilidad para obtener pruebas electrónicas o respeto máximo de los derechos fundamentales; en definitiva, lucha contra la delincuencia transfronteriza o garantías.

Creemos que la respuesta está en el principio de confianza mutua. Debemos entender que todos los Estados miembros afirman y respetan los derechos fundamentales y que ningún juez que solicite la prueba electrónica habida en otro Estado miembro quiere ni pretende que resulte conculcado ningún derecho. Todos los Estados de la UE, se sobreentiende, protegen y respetan derechos como el secreto de las comunicaciones y el derecho a la intimidad. Por ello, ningún proveedor de servicios de *Internet* debe negarse a entregar las evidencias electrónicas cuando se requiera por la autoridad judicial en el seno de un proceso penal, pues se debe creer y entender que todos los procesos judiciales seguidos en cualquier país con legislaciones similares son sustanciados según todas las garantías. Podemos decir: quien es un proveedor de servicios de *Internet* para negarse a entregar, por ejemplo, una prueba que obra en su poder a una autoridad judicial española cuando la requiera. ¿Acaso, en España, no se afirman en su Constitución los derechos fundamentales? ¿Acaso no se respetan los mismos por sus autoridades judiciales, igual que en el lugar donde se halla situado tal proveedor? Cuando una autoridad judicial lo exige lo hace a través de una resolución motivada y porque alguien está siendo investigado como sospechoso de haber cometido un delito. Da igual de que Estado hablemos, pues todos somos miembros de la UE y, en todos ellos, se respetan los mismos derechos. Aunque tenemos legislaciones diferentes, son similares, pues existen instrumentos de armonización (Reglamentos, Directivas y Decisiones). Esto permite confiar mutuamente los unos en los otros.

Por otra parte, en caso de resultar vulnerado algún derecho fundamental en un proceso, existe un sistema de recursos y medios extraordinarios. Incluso, como todos los Estados miembros de la UE forma parte del Consejo de Europa, se someten a las decisiones del Tribunal Europeo de Derechos Humanos. No hay, pues, excusa válida para entorpecer los procesos judiciales contra la delincuencia transfronteriza para impedir la obtención de las evidencias electrónicas.

7 Conclusiones y propuestas

Se han dado pasos de gigante, en la UE, pero aún hay mucho por hacer, pongamos sólo algunas propuestas sobre la mesa:

- Se pueden homogenizar aún más las legislaciones de los Estados miembros. Somos partidarios del instrumento legislativo Reglamento más que de la Directiva. Y ello se justifica de la siguiente manera: la libertad que se otorga a los Estados miembros a la hora de trasponer las Directivas de la UE provoca problemas añadidos a los de la misma norma europea, como hemos observado que ocurre en el caso español, en relación a la orden europea de investigación.

- Se deben mejorar los instrumentos legislativos de la UE, anteriormente descritos, perfeccionando aspectos entre otros el de la traducción. ¿Cómo no va a poderse facilitar la traducción, si hoy contamos con la IA que permite automatizar este proceso? Insistimos que la agilización en la tramitación de las órdenes de investigación, producción y conservación es fundamental dada la volatilidad de las evidencias digitales y su pronta desaparición

- Debe existir mayor cooperación policial y judicial. Refuércense las instituciones *Europol* y *Eurojust* o la Fiscalía Europea.

- Debe formarse a todos los operadores jurídicos (jueces, fiscales, abogados, procuradores) para que estén capacitados para utilizar las herramientas creadas por la UE. Pensemos que

una orden europea de investigación podría ser necesaria en un procedimiento penal por un abogado, que podemos denominar de «a pie» o por un juez de instrucción de un partido judicial cualquiera. Formemos no sólo a las Fuerzas y Cuerpos de Seguridad del Estado de las unidades especializadas, sino a cualquier agente. La ciberdelincuencia es tan habitual que cualquier abogado puede personarse en una causa como acusador particular o cualquier juez puede estar inmerso en su persecución.

- Sigamos ahondando en la fijación de criterios de jurisdicción que faciliten la sustanciación de los procedimientos lo más cerca posible del lugar de comisión del hecho delictivo o del lugar de localización del servidor en donde se encuentra la evidencia de la comisión del delito. De esta manera, se evitará tener que solicitar la entrega de pruebas cuando el servidor esté alojado en un Estado distinto.

- Hagamos uso de las figuras del decomiso y de los embargos preventivos. Si las organizaciones de ciberdelincuentes no cuentan con medios económicos tendrán más obstáculos para seguir delinquiendo.

- Proponemos que exista un Reglamento de la UE sobre ciberdelincuencia, a través del cual se regulen los medios de investigación y de prueba en los procesos judiciales abiertos contra la ciberdelincuencia organizada. Debido a que la vigilancia electrónica es una medida intrusiva y restrictiva de derechos fundamentales o la entrega vigilada o las operaciones encubiertas son medidas cuestionadas por la incitación al delito, su aplicación puede ocasionar reticencias en algunos Estados miembros. Inclúyase en dicho Reglamento la posibilidad de utilizar medios tales como *exploits* (códigos que permiten, gracias a la vulnerabilidad de los programas informáticos o defectos de seguridad, meter intrusos que tengan acceso a distancia a una red y adquieran privilegios elevados), o programas maliciosos. La investigación de la ciberdelincuencia organizada requiere medidas de investigación tecnológicas altamente especializadas y agresivas. Es lo que se denomina en EE. UU., «técnicas de investigación de redes» (Oficina de las Naciones Unidas Contra la Droga y el Delito, 2022).

Fuera de la UE, el panorama es considerablemente mucho más sombrío. Los instrumentos legislativos de la UE no existen fuera de este ámbito regional. Tampoco resulta tan eficaz la cooperación internacional. Los estándares de protección de los derechos fundamentales son diferentes; los ordenamientos jurídicos muy dispares; los procedimientos penales distintos; la formación de los operadores jurídicos diversa, los niveles de opacidad en la represión criminal obviamente también varían. La investigación se torna más compleja, al tener que solicitar la entrega de una prueba a través de comisiones rogatorias, lo que permite su rápida destrucción. Los decomisos ni los embargos son tan sencillos y la extradición también complica la situación. La asistencia judicial recíproca y la cooperación se torna imprescindible.

Comenzamos este artículo relacionando los términos de ciberseguridad y de ciberdelincuencia: relacionados entre sí, pero diferentes. Ante la complejidad de la lucha contra la ciberdelincuencia, enarbolamos la bandera de la prevención. Estamos seguros de que la ciberseguridad es el camino ideal y preventivo para evitar o, al menos minimizar, los ataques de los ciberdelincuentes.

En el caso de los ciudadanos, no cabe otra solución que la formación: unas cuantas reglas de conducta habituales (contraseñas variadas y seguras, vigilancia de los permisos que se otorgan a las *apps*, no abrir *whatsapp*, correos electrónicos, mensajes o no contestar llamadas sospechosas) son la mejor prevención.

En el caso de las empresas, la cuestión tiene que ver con la prevención y el análisis de riesgos: no sólo grandes empresas, sino también las medianas y pequeñas deben contar con un *chief information security officer* (CISO). Importante a este respecto resulta la Directiva NISS 2 (Directiva 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) nº 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148[18]. Además, todas las

18. Esta Directiva se aplica a las empresas públicas y privadas, no sólo grandes, sino también medianas que presten sus servicios o lleven sus actividades en la UE y, por

empresas deberían tener unas *compliance guides*, idóneas y adecuadas en materia de ciberseguridad y de protección de datos, pues estos dos ámbitos forman parte inescindible del *compliance* de una empresa y es garantía de seguridad para todos[19].

En definitiva, la mejor forma de enfrentarse a la ciberdelincuencia organizada es transformar el deber y la sanción en una cultura *behaviour*. Se habla ya de *behavioral compliance*, esto es, de aquella forma de pensar que entiende la ética como punto fundamental en la transformación de la cultura corporativa.

¿Seremos capaces de lograrlo? El presente no es sencillo y el futuro una incógnita y es que la IA plantea nuevos y complejos retos para la ciberseguridad.

Referencias bibliográficas

Aguilera Morales, M. (2019). La implementación de la orden europea de investigación: el dolor de la lucidez. En I. González Pulido y F. Bueno de Mata (dirs.), *La cooperación procesal internacional en la sociedad del conocimiento* (pp. 209-224). Atelier.

Barrera Ibáñez, S. (2018). Perseguir el rastro digital en la red: once años sin medidas legislativas. *Revista del Consejo General Abogacía española, 11*.

CORVUS (2023, 24 de octubre). Q3 Ransomware Report: Global Ransomware Attacks Up Over 95% in 2022. *Corvus*. https://www.

tanto, afecta a empresas de más de 50 empleados o con un volumen de negocio mayor de 10 millones de euros, incluidas aquellas que puedan tener inversiones públicas. Pero también se aplica a empresa pequeñas y microempresas, que tengan que un papel fundamental para la sociedad, la economía o para determinados sectores o tipos de servicios.

19. Véase la Circular de la Fiscalía General del Estado 1/2016 y la Sentencia del Tribunal Supremo de 29 de febrero de 2016, en relación al código de cumplimiento normativo que deben tener las personas jurídicas para quedar exoneradas de responsabilidad penal, conforme al art. 31 *bis* del CP.

corvusinsurance.com/blog/q3-ransomware-report (Consultado el 24/04/2024. Hora: 13:00).

De Hoyos Santo, M. (2023). Novedades en materia de obtención transfronteriza de información electrónica necesaria para la investigación y enjuiciamiento penal en el ámbito europeo. *Revista de Estudios Europeos, número Extraordinario monográfico 1*, 99-128.

Delgado Martín, J. (2016). *Investigación tecnológica y prueba digital en todas las jurisdicciones*. Wolters Kluwer. Extracto en «La valoración de la prueba digital», http://diariolaley.laley.es/home/DT0000245603/20170411/La-valoracion-de-la-prueba-digital (Consultado 1/04/2024. Hora: 12:00).

Laro González, E. (2022). Luces y sombras de la Orden Europea de investigación. *Revista de Estudios europeos, Número Extraordinario monográfico 1*, 129-144.

Martil, I. (2017). Cómo función las redes inalámbricas de telefonía móvil. *Público.* https://blogs.publico.es/ignacio-martil/2017/02/24/como-funcionan-las-redes-inalambricas-de-telefonia-movil/?doing_wp_cron=1541448078.7565820217132568359375 (Consultado 1/04/2024. Hora: 12:00).

Menéndez Rodríguez, C. (2014). Los delitos de pertenencia a organización criminal y grupo criminal y el delito de tráfico de drogas cometido por persona que pertenece a una organización delictiva. Crónica de un conflicto normativo anunciado y análisis jurisprudencial. *Estudios Penales y Criminológicos, 34*, 511-560.

Messuti, A. (2013). *Un deber ineludible. La obligación de los Estados de perseguir penalmente los crímenes internacionales*. Buenos Aires: Ediar.

Oficina de las Naciones Unidas Contra la Droga y el Delito. (2022). *Compendio de ciberdelincuencia organizada.* Viena.

Picón Rodríguez, E. (2017). *¿Por qué no es válida una conversación de Whastapp en juicio?* https://elderecho.com/por-que-no-es-valida-una-conversacion-de-whatsapp-en-juicio. (Consultado 1/04/2024. Hora: 12:00)

Rayón Ballesteros, M. C. y Gómez Hernández, J. A. (204). Cibercrimen: particularidades en su investigación y enjuiciamiento. *Anuario Jurídico y Económico Escurialense, 47,* 209-234. http://www.rcumariacristina.net:8080/ojs/index.php/AJEE/article/view/189/158

Rodríguez-Medel Nieto, C. (2014). *Prueba penal transfronteriza: su obtención y admisibilidad en España* (Tesis doctoral).

Romero Casabona, C. M. (2016). Delitos cometidos con la utilización de tarjetas de crédito, en especial en cajeros automáticos. *Nuevo Foro Penal, 12*(52), 147-169.

Volpato, S. (2016). *El derecho a la intimidad y las nuevas tecnologías de la información*. http://hdl.handle.net/11441/52298 (Consultado 1/04/2024. Hora: 12:00).

Zúñiga Rodríguez, L. (2016). El concepto de criminalidad organizada transnacional: problemas y propuestas. *Nuevo Foro Penal, 86*, 62-114. https://doi.org/10.17230/nfp.12.86.2

El uso de las armas de fuego por funcionarios policiales: análisis jurisprudencial

The Use of Firearms by Police Officers: Case Law Analysis

Julián Sánchez Melgar[1]
Tribunal Supremo.
spain.criminalistica@gmail.com

DOI: https://doi.org/10.14201/cp.31935
Recibido: 11-03-24 | Aceptado: 03-05-24

Resumen

Esta investigación está referida al adecuado uso de armas por parte de los funcionarios policiales, a la luz de los principios legales y de la jurisprudencia que los interpreta.

El uso de las armas por los agentes policiales está amparado por el ordenamiento constitucional español que le autoriza al uso de la fuerza legítima como garantes del libre ejercicio de los derechos y libertades y de garantizar la seguridad ciudadana. En ocasiones este uso de armas produce lesiones, de diferente índole, en los ciudadanos sobre los que se actúa o que se encuentran en el entorno de las actuaciones policiales.

Este uso de armas se enmarca generalmente en el cumplimiento del deber y/o en la legítima defensa, pero en ocasiones también pueden darse casos de extralimitaciones profesionales o personales que nos hace preguntarnos sobre si se ha actuado bajo los estrictos procedimientos técnico-operativos policiales, las normas constitucionales y las normas jurídico-penales de desarrollo.

En los diferentes supuestos a los que nos enfrentamos hay que tener en consideración multitud de circunstancias a analizar que nos determinarán lo lícito o ilícito de la actuación policial y nos permitirá afianzar los procedimientos de actuación o plantear-

1. Magistrado de la Sala de lo Penal del Tribunal Supremo. Doctor en Derecho. Ex Fiscal General del Estado.

nos su posible adecuación a lo dictaminado en las sentencias del Tribunal Supremo.

Palabras clave
Empleo de armas; Legítima defensa; Sentencias Tribunal Supremo; Actuaciones policiales con armas; Regla Tueller.

Abstract
This investigation refers to the appropriate use of weapons by police officers, in light of the legal principles and the jurisprudence that interprets them.

The use of weapons by police officers is protected by the Spanish constitutional order that authorizes the use of legitimate force as guarantors of the free exercise of rights and freedoms and to guarantee citizen security. Sometimes this use of weapons produces injuries, of different kinds, in the citizens on whom action is taken or who are in the environment of police actions.

This use of weapons is generally framed in the fulfillment of duty and/or self-defense, but sometimes there may also be cases of professional or personal excesses that make us wonder if they have acted under the strict police technical-operational procedures. constitutional norms and legal-criminal development norms.

In the different cases that we face, we must take into consideration a multitude of circumstances to analyze that will determine the legality or illicitness of the police action and will allow us to strengthen the action procedures or consider their possible adaptation to what was ruled in the sentences of the Supreme Court.

Keywords
Use of weapons; Legitimate self-defense; Supreme Court rulings; Police actions with weapons; Tueller rule.

1 Introducción

Comenzamos por recordar que, en todo caso, los funcionarios de Policía judicial están obligados a observar estrictamente las formalidades legales en cuantas diligencias practiquen, y se

abstendrán bajo su responsabilidad de usar medios de averiguación que la ley no autorice (Ley de Enjuiciamiento Criminal, art. 297, 1882). Este mandato nos sirve de reflexión y también de introducción al tema que tratamos en este estudio, que es el adecuado uso de armas por parte de los funcionarios policiales. Y ello a la luz de los principios legales y de la jurisprudencia que los interpreta.

Desde luego que la utilización de armas es posible, y para ello van dotados de tales dispositivos los agentes policiales, pues su uso no es sino una manifestación del uso de la fuerza legítima que el ordenamiento jurídico-constitucional concede a la fuerza pública como garante de los derechos fundamentales y de la seguridad ciudadana. Sobre este particular no existe duda alguna. La problemática surge cuando se han utilizado armas en el desempeño de su función, y surgen preguntas como las siguientes: ¿Se actuó con absoluto respeto a la normativa policial, jurídico-penal y, por ende, constitucional?; ¿Suponía la causación de la muerte o lesiones del sospechoso la única opción de la que disponían las fuerzas policiales?; ¿O más bien se actuó de manera precipitada, improvisada, excesiva, impidiendo dicha actuación policial la eventual neutralización, detención y posterior enjuiciamiento de tales sospechosos?

Las lesiones causadas con armas reglamentarias a terceros han oscilado, o bien en la legitimación del suceso, como consecuencia de apreciarse caso fortuito o bien el cumplimiento de un deber o el ejercicio legítimo de un oficio o cargo, o legítima defensa, en otros supuestos la imputación mediante un delito de imprudencia, leve o grave, y en muy escasos supuestos, y casi siempre como consecuencia de comportamientos con armas en asuntos privados, con dolo, bien directo o eventual.

En definitiva, hemos de precisar que cuando del uso de armas se trata, estamos en presencia, teóricamente, de una cuestión afectante al cumplimiento del deber, y en otros supuestos, de legítima defensa. Pero también, pueden darse casos de extralimitaciones. Por eso, trazar la línea entre lo lícito y lo ilícito siempre es difícil, es más, depende de tantas circunstancias que, en muchas ocasiones, es imprescindible tener en consideración todos los detalles del caso concreto.

Por ello, hemos de hacer un ejercicio de aplicación de los principios generales, y, sobre todo, su aplicación práctica, esto es, cómo los Tribunales han dado respuesta a los casos que se han presentado en la realidad. De manera que tenemos que estudiar cuándo han condenado y cuándo han absuelto al policía involucrado en una situación extrema, en la que ha decidido utilizar su arma reglamentaria.

Naturalmente, no nos referimos a la utilización de otros instrumentos, como las defensas o la contención o inmovilización para practicar una detención, pues el campo sería amplísimo. Sí que es necesario señalar aquí que son supuestos bien de extralimitaciones, o sencillamente de utilización correcta de los medios empleados durante, por ejemplo, una manifestación, con intervención de la fuerza pública. La Sentencia del Tribunal Supremo (STS) 561/2023, de 6 julio de 2023, ratifica una Sentencia absolutoria de todos los acusados que había decretado la Audiencia Provincial de Madrid. En el caso, se pretendía la condena de los policías por lesiones dolosas causadas como consecuencia de la rotura del cordón policial. El Tribunal Supremo (TS) analiza la sentencia recurrida y considera en punto a la tutela judicial efectiva que la motivación era suficiente y que no se había producido infracción legal alguna, sino una falta de respeto a los hechos probados por parte de los recurrentes. Se declara en esta resolución judicial que, ante la actitud hostil de los manifestantes y viendo la intención de continuar la marcha de los partícipes en la concentración, los funcionarios de policía y para evitar ser sobrepasados y teniendo en cuenta las órdenes recibidas de que la concentración de personas no discurriera hacia el Congreso de los Diputados, utilizaron la mínima fuerza indispensable para evitarlo. De esa manera hubo forcejeos entre los policías y las personas que resultaron detenidas, unos al objeto de no dejar pasar y los otros para continuar la marcha.

2 Definición de los objetivos de la investigación

Los objetivos se enmarcan en obtener conclusiones válidas para ofrecer unas propuestas de mejora en los procedimientos

de actuación operativa de los agentes policiales en las situaciones planteadas.

3 Método de recopilación y evaluación de datos

El método empleado se basa en el análisis de la legislación española y la recopilación de sentencias del Tribunal Supremo español que debidamente analizadas nos permitirán concluir propuestas de mejora en la actuación policial.

4 Uso de armas de fuego: supuestos más habituales

Nos referimos ahora al uso por parte de los funcionarios policiales de sus armas reglamentarias, tanto sean de fuego, como las más modernas de inmovilización. Nos encontramos, por consiguiente, en una situación excepcional. Ciertamente, muchos funcionarios no se han visto nunca en la tesitura de tener que disparar, únicamente han utilizado su arma de modo disuasorio, para intimidar al sujeto al que no había otro modo de contener, pero no han tenido necesidad que abrir fuego. A lo sumo, ha disparado al aire.

Estudiaremos en este trabajo los casos en que así se ha producido y las consecuencias que han tenido. Y me atrevo a señalar que este tema es necesario conocerlo bien, porque en una profesión de riesgo como es la policial, en cualquier momento puede producirse una situación extrema necesidad que obligue al uso del arma.

Los supuestos más habituales, dentro del desarrollo constitucional de la misión de proteger el libre ejercicio de los derechos y libertades y garantizar la seguridad ciudadana, son el uso del arma para el cumplimiento de un deber y el uso del arma como medio de defensa.

4.1 Cumplimiento de un deber

Respecto al cumplimiento de un deber están exentos de responsabilidad penal aquellos que obren en cumplimiento de un deber o en el ejercicio legítimo de un derecho, oficio o cargo. (Código Penal, art. 20, 2015).

Y aquí conviene remarcar que tal deber no solamente viene impuesto por la situación que así lo requiera sino también por el cumplimiento de las órdenes, teniendo en consideración que, los funcionarios policiales han de sujetarse en su actuación profesional, a los principios de jerarquía y subordinación, pero, en ningún caso, la obediencia debida podrá amparar órdenes que entrañen la ejecución de actos que manifiestamente constituyan delito o sean contrarios a la Constitución o a las Leyes (Ley Orgánica 2/1986 de Fuerzas y Cuerpos de Seguridad, art. quinto.1.d). 1986).

El que cumple un deber realiza una conducta lícita, al punto de ser tan obvio que en algunos Códigos europeos recientes no se incluye esta eximente (como es el caso del derecho penal alemán), por considerarla absolutamente superflua.

4.2 Legítima defensa

Respecto a la legítima defensa, la circunstancia cuarta del artículo 20 del Código Penal, exime de responsabilidad penal al que obre en defensa de la persona o derechos propios o ajenos, siempre que concurran los requisitos siguientes:

> **Primero.** Agresión ilegítima. En caso de defensa de los bienes se reputará agresión ilegítima el ataque a los mismos que constituya delito y los ponga en grave peligro de deterioro o pérdida inminentes. En caso de defensa de la morada o sus dependencias, se reputará agresión ilegítima la entrada indebida en aquélla o éstas.

Segundo. Necesidad racional del medio empleado para impedirla o repelerla.

Tercero. Falta de provocación suficiente por parte del defensor.

5 Entronque constitucional

El artículo 104 de la Constitución Española, es del tenor literal siguiente: «1. Las Fuerzas y Cuerpos de Seguridad, bajo la dependencia del Gobierno, tendrán como misión proteger el libre ejercicio de los derechos y libertades y garantizar la seguridad ciudadana. 2. Una ley orgánica determinará las funciones, principios básicos de actuación y estatutos de las Fuerzas y Cuerpos de Seguridad».

Esta ley es la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad (LOFCS), que en su artículo primero proclama que la seguridad pública es competencia exclusiva del Estado, correspondiendo su mantenimiento al Gobierno de la Nación, sin perjuicio de la participación de las Comunidades Autónomas y de las Corporaciones Locales en dicho mantenimiento, el cual se ejerce a través de las repetidas Fuerzas y Cuerpos de Seguridad del Estado.

En el Preámbulo de tan básica ley, se dispone que los principios básicos de actuación policial se establecen como un auténtico «Código Deontológico», que vincula a los miembros de todos los colectivos policiales, imponiendo el respeto:

- a la Constitución,
- al servicio permanente a la comunidad,
- la adecuación entre fines y medios, como criterio orientativo de actuación,

- el secreto profesional,
- el respeto al honor y a la dignidad de la persona,
- la subordinación a la autoridad
- y la responsabilidad en el ejercicio de su función.

Principios, obvio es decirlo, que guían la actuación de los funcionarios policiales. La doctrina más autorizada señala que no cabe duda de que esta auténtica declaración de principios contenida al comienzo de la LOFCS afecta –y de qué manera– a las líneas de actuación de los agentes de la autoridad a la hora de investigar y esclarecer la comisión de conductas delictivas, independientemente de su gravedad, así como en el contexto de la detención de personas sospechosas.

Sigue su estela la Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana, en cuyo artículo cuarto, y como principios rectores de la acción de los poderes públicos en relación con la seguridad ciudadana, se declara que el ejercicio de las potestades y facultades reconocidas por esta Ley a las administraciones públicas y, específicamente, a las autoridades y demás órganos competentes en materia de seguridad ciudadana y a los miembros de las Fuerzas y Cuerpos de Seguridad se regirá por los principios de legalidad, igualdad de trato y no discriminación, oportunidad, proporcionalidad, eficacia, eficiencia y responsabilidad, y se someterá al control administrativo y jurisdiccional.

En su apartado dos, se precisa que la actuación de los miembros de las Fuerzas y Cuerpos de Seguridad está sujeta a los principios básicos de actuación regulados en el artículo cinco de la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad.

Así mismo, el artículo 10. Código de conducta, de la Ley Orgánica 9/2015, de Régimen de Personal de la Policía Nacional, singulariza el cumplimento de las funciones encomendadas a los Policías Nacionales con fidelidad a los principios básicos de actuación contenidos en las leyes orgánicas anteriormente refe-

ridas, así como a las líneas marcadas por la Declaración sobre la Policía contenida en la Resolución de la asamblea parlamentaria del Consejo de Europa de 8 de mayo de 1979, y en la Resolución 169/34, de la Asamblea General de Naciones Unidas.

Específicamente el Código Ético del Cuerpo Nacional de Policía, publicado por Resolución de la Dirección General de la Policía, Orden General número 2006 de 6 de mayo de 2013, en su artículo 26.5, singulariza que el uso de las armas de fuego es el último recurso con el que cuenta el Policía Nacional ante intervenciones con grave riesgo para su persona o la de terceras personas, lo que constituye una auténtica doctrina policial como norma de obligado cumplimiento.

6 Porte de armas

El porte de armas por funcionarios policiales es una constante en nuestra historia de las fuerzas de seguridad. El funcionario policial tiene que ir armado, como lógica consecuencia de su función, que es el ejercicio legítimo de la fuerza. Entre otros, el Real Decreto 1484/1987, de fecha 4 de diciembre, dispone en su artículo 22.1 que: «los funcionarios del Cuerpo Nacional de Policía, en las situaciones de servicio activo y segunda actividad con destino, irán provistos obligatoriamente de alguna de las armas que se establezcan como reglamentarias, durante el tiempo que presten servicio, salvo que una causa justificada aconseje lo contrario».

También se dispone en el apartado dos del mencionado artículo, que cuando la operatividad de los servicios exija el empleo de una mayor protección o acción, los funcionarios podrán portar cualquier arma o medio coercitivo cuyo uso esté reglamentariamente establecido.

Y sustancialmente, para lo que estudiamos, que «Todo el personal deberá conocer, de forma técnica y práctica, la utilización y uso adecuado de las armas y demás medios coercitivos que se empleen en las actuaciones policiales, para lo cual recibirá

la formación y entrenamientos precisos» (apartado 3 del artículo 22).

Con respecto al personal jubilado, al cesar en sus funciones deberá proveerse de una nueva licencia para las armas que posea, conforme a lo establecido en los artículos 96, 99 y 165 del Real Decreto 137/1993, de 29 de enero[2].

7 Tipos de armas

Cada vez los funcionarios policiales portan más instrumentos a su alcance, de manera que tienen necesidad de multitud de anclajes en su uniforme reglamentario para poder efectuar su función con garantías de eficacia y legalidad. Grilletes, defensa, linterna, tableta electrónica, cámara videográfica, etc. no son sino algunos de los instrumentos que portan en su uniforme; nos referimos ahora que, aparte del arma de fuego convencional, regulado administrativamente y proporcionado a todos los funcionarios policiales, hoy también se destaca el uso moderno del inmovilizador eléctrico, que ha sido reconocido por la Resolución de la Dirección General de la Policía, de 21 de diciembre de 2020, por la que se imparten instrucciones sobre la utilización del inmovilizador eléctrico por parte de la policía nacional.

En convergencia con este marco ético y jurídico, la Dirección General de la Policía ha asumido el compromiso de prestar atención a cualquier avance o innovación tecnológica que pueda revertir en una mejora de los servicios, de los procedimientos y de las herramientas operativas, tanto a través de los estudios técnicos previos del Servicio de Armamento y Equipamiento Policial, como de la recopilación de experiencias de otros cuerpos

2. La licencia tipo «A», que ampara las licencias de tipo «B», «D» y «E», se extingue al perder el personal la condición de policía en su jubilación. El porte de armas queda condicionado a la expedición de la licencia tipo «B» por parte de la Dirección General de la Guardia Civil, sin perjuicio de la solicitud de las correspondientes licencias que amparen la tenencia de otro tipo de armas.

policiales de nuestro entorno europeo, dentro de la información que facilitan los estudios y análisis en todo lo referente al amplio espectro que recoge la Ciencia Policial.

Fruto de este compromiso de la Dirección General de la Policía y una vez evaluado en profundidad, el inmovilizador eléctrico ha sido adoptado como instrumento idóneo para el cumplimiento de la función policial, el cual se encuentra regulado en el artículo 5,1.j del Real Decreto 726/2020, de 4 de agosto, como arma de uso policial, cuya utilización estará reservada, previa dotación, al personal expresamente habilitado de la Policía Nacional. La regulación de este nuevo elemento de protección, por Resolución de la Dirección General de la Policía, de 21 de diciembre de 2020, por la que se imparten instrucciones sobre la utilización del inmovilizador eléctrico por parte de la Policía Nacional, introduce, en los procedimientos de actuación policial, un nuevo elemento de defensa de la integridad policial y de los ciudadanos en general, dando una mayor profundidad al empleo progresivo de los medios de dotación policial.

8 Principios básicos de actuación: especial referencia a la responsabilidad y sus tipos

Los denominados «principios básicos de actuación» de las Fuerzas y Cuerpos de Seguridad (FFCCS) son los ejes fundamentales en torno a los cuales gira el desarrollo de las funciones policiales.

En este sentido, el trascendental artículo cinco de la LOFCS agrupa dichos principios básicos de actuación de los miembros de las FFCCS, adquiriendo las letras c) y d) del apartado dos de la mencionada disposición una importancia trascendental cuando señalan respectivamente que las FFCCS, en el ejercicio de sus funciones:

«Deberán actuar con la decisión necesaria, y sin demora cuando de ello dependa evitar un daño grave, inmediato e irreparable; rigiéndose al hacerlo por los principios de congruencia,

oportunidad y proporcionalidad en la utilización de los medios a su alcance» (letra c);

Uso excepcional de las armas: «Solamente deberán utilizar las armas en las situaciones en que exista un riesgo racionalmente grave para su vida, su integridad física o las de terceras personas, o en aquellas circunstancias que puedan suponer un grave riesgo para la seguridad ciudadana y de conformidad con los principios a que se refiere el apartado anterior» (letra d).

Frente a la actuación policial con uso de armas, como para el resto de actuaciones policiales, el artículo 5.6 LOFCS establece que los funcionarios policiales son responsables «personal y directamente por los actos que en su actuación profesional llevaren a cabo, infringiendo o vulnerando las normas legales, así como las reglamentarias que rijan su profesión y los principios enunciados anteriormente, y todo ello sin perjuicio de la responsabilidad patrimonial que pueda corresponder a las Administraciones Públicas por las mismas».

En el ejercicio de sus competencias, los miembros de las FFCCS pueden incurrir en tres tipos de responsabilidad: (1) disciplinaria; (2) civil y (3) penal, en función de las circunstancias que concurran en cada caso concreto, sin olvidar la responsabilidad subsidiaria de la Administración en los casos en que proceda su aplicación.

La Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad (artículo octavo) determina, en su apartado uno, que la jurisdicción ordinaria será la competente para conocer de los delitos que se cometan contra miembros de las Fuerzas y Cuerpos de Seguridad, así como de los cometidos por éstos en el ejercicio de sus funciones. Y también disponía que «iniciadas unas actuaciones por los Jueces de Instrucción, cuando éstos entiendan que existen indicios racionales de criminalidad por la conducta de miembros de las Fuerzas y Cuerpos de Seguridad, suspenderán sus actuaciones y las remitirán a la Audiencia Provincial correspondiente, que será la competente para seguir la instrucción, ordenar, en su caso, el procesamiento y dictar el fallo que corresponda».

Pero este párrafo ha sido declarado inconstitucional y nulo en cuanto que atribuye la competencia para seguir la instrucción y ordenar, en su caso, el procesamiento de los miembros de las Fuerzas y Cuerpos de Seguridad por delitos cometidos en el ejercicio de sus funciones a la Audiencia correspondiente, por Sentencia del Tribunal Constitucional 55/1990, de 28 de marzo. No obstante, el enjuiciamiento se residencia en las Audiencias Provinciales.

9 Uso de la fuerza y criterios orientativos acordados por la Administración

El artículo tres del Código de Conducta para Funcionarios Encargados de Hacer Cumplir la Ley (Resolución 34/169, de 17 de diciembre de 1979, de la Asamblea General de las Naciones Unidas), declara que «los funcionarios encargados de hacer cumplir la ley podrán usar la fuerza sólo cuando sea estrictamente necesario y en la medida que lo requiera el desempeño de sus tareas».

Son muchos los instrumentos orientativos que ha dictado la Administración al respecto. Nosotros nos vamos a referir a la Instrucción de 14 de abril de 1983 de la Dirección de la Seguridad del Estado, sobre utilización de armas de fuego por miembros de los Cuerpos y Fuerzas de Seguridad del Estado, dictada con el fin de «llenar el vacío normativo existente en la materia, conseguir las mayores cotas de seguridad para la colectividad y garantías suficientes para los propios miembros de los Cuerpos y Fuerzas de Seguridad», estableciendo unas reglas para el uso de armas de fuego por parte de éstos para los casos que se produzca una agresión ilegítima contra el Agente de la Autoridad o terceras personas, siempre que concurran los siguientes elementos:

- Intensidad: Que la agresión sea de tal intensidad y violencia que ponga en peligro la vida o integridad corporal de la persona o personas atacadas.

- Necesidad: Que el agente de la autoridad considere necesario el uso de arma de fuego para impedir o repeler la agresión, en cuanto racionalmente no puedan ser utilizados otros medios, es decir, debe haber la debida adecuación y proporcionalidad entre el medio empleado por el agresor y el utilizado por la defensa.

- Aviso: El uso del arma de fuego ha de ir precedido, si las circunstancias concurrentes lo permiten, de conminaciones dirigidas al agresor para que abandone su actitud y de la advertencia de que se halla ante un agente de la autoridad, cuando este carácter fuera desconocido para el atacante.

- Secuencia: Si el agresor continúa o incrementa su actitud atacante, a pesar de las conminaciones, se debe efectuar por este orden, disparos al aire o al suelo, para que deponga su actitud.

- Mínima lesión: Ante el fracaso de los medios anteriores, o bien cuando por la rapidez, violencia y riesgo que entrañe la agresión no haya sido posible su empleo, se debe disparar sobre partes no vitales del cuerpo del agresor, atendiendo siempre al principio de que el uso del arma cause la menor lesividad posible.

- No extralimitación: La utilización de estos medios se rige por el principio no extralimitación en la utilización de la fuerza, del medio de contención o del uso del arma.

Finaliza la Instrucción del año 1983 dando unas recomendaciones sobre el uso de armas de fuego en los **casos de huida del delincuente**, disponiendo que sólo en supuestos de delito grave, los miembros de los Cuerpos y Fuerzas de Seguridad del Estado, ante la fuga de un presunto delincuente que huye, deben utilizar su arma de fuego con suma cautela, que, en mi opinión, creo que no debe utilizarse nunca, pues no existe ya agresión ilegítima, sino huida, y por tanto, ya no resulta necesaria su utilización.

Me apoyo para esta afirmación en la STS de 18 de enero de 1982, en la que se señala que los funcionarios de policía deben utilizar las armas de fuego «solamente en aquellos casos en que las circunstancias que concurran en las situaciones con que se enfrenten hagan racionalmente presumir una situación de peligro o riesgo real para ellos o terceras personas, únicamente superable mediante esta utilización, y lo hagan en la forma adecuada para evitar consecuencias irreparables que no vengan justificadas por la gravedad del contexto en que se encuentran», añadiendo asimismo que «la simple y pura huida de una persona, desatendiendo las órdenes de («alto policía») no autoriza sin más a ésta para utilizar sus armas de fuego».

No obstante, esta afirmación y nuestra opinión no han sido contempladas en la reciente Instrucción nº 1/2024 de la Secretaría de Estado de Seguridad por la que se aprueba «el procedimiento integral de la detención policial», pues en su apartado Tercero sobre el empleo de la fuerza en la detención nos reitera en el subapartado 5 que «*Solo podrán hacerse uso de los medios de dotación autorizados, tales como defensa, sprays o dispositivo eléctrico de inmovilización y, como último recurso, el arma de fuego.*

Para ello, en función del medio a utilizar, de menos lesivo a más lesivo, se respetará el Protocolo de actuación previsto al efecto por las Direcciones Generales de la Policía y de la Guardia Civil que se haya aprobado en esta materia. No obstante, cuando por las características del ataque o actitud amenazadora, pueda preverse objetivamente y de manera razonable un riesgo inminente, serio y grave para la vida o la integridad física del o de la agente, o de terceras personas, excepcionalmente podrá recurrirse directamente al arma de fuego sin necesidad de hacer un uso escalonado del resto de medios», que aligera las más concretas reglas que especificaba la Instrucción de 14 de abril de 1983, derogada por esta última, sin aportar nuevos elementos que afiancen una exitosa intervención policial en situaciones de gran estrés profesional, como la indicada de no usar el arma de fuego ante la huida de una persona que no atiende a las instrucciones de «alto policía» sin más.

10 Conocimiento del manejo de armas y principios de actuación en su uso

Anteriormente, en el Real Decreto 1484/1987, artículo 22. Tres, referíamos que «Todo el personal deberá conocer, de forma técnica y práctica, la utilización y uso adecuado de las armas y demás medios coercitivos que se empleen en las actuaciones policiales, para lo cual recibirá la formación y entrenamientos precisos», obligaciones que se cumplen ampliamente en los programas de formación para ingreso en las Escalas Ejecutiva y Básica de la Policía Nacional y que se mantienen a lo largo de su vida profesional en el cumplimiento del Plan Nacional de Tiro.

Los principios de actuación en el uso de las armas se especifican en:

Principio de menor lesividad

La doctrina recuerda que este principio viene recogido con carácter general en el art. 520.1 de la Ley de Enjuiciamiento la Criminal, con respecto a la práctica de la detención, señalando que ésta debe llevarse a cabo en la forma que menos perjudique al detenido. La jurisprudencia del TS a la hora de aplicar la eximente de obrar en el cumplimiento de un deber en los casos de uso de la fuerza por parte de las FFCCS exige unos requisitos. Así, en la STS de 20 de octubre de 1980, el Alto Tribunal señala que el uso de la fuerza policial debe ser «racionalmente imprescindible, con la consiguiente limitación implícita de la menor lesividad posible para conseguir el cumplimiento de la función».

Principio de oportunidad

Principio que se conecta con el principio de necesidad: solamente es oportuna la utilización del arma, cuando es necesaria. Pero este principio no puede ser analizado en abstracto, sino en concreto. En efecto, solamente deberán utilizarse en las situaciones en las que existe un riesgo racionalmente grave para la vida o

integridad de los agentes o terceras personas, o en aquellas circunstancias que puedan suponer un grave riesgo para la seguridad ciudadana. Claro que por peligro hay que entender la probabilidad suficiente de lesión de un bien jurídico, individual o colectivo.

Por consiguiente, un agente de policía ha de poder recurrir a su arma reglamentaria para evitar un delito de homicidio.

Principio de proporcionalidad. La regla de Tueller

Se ha dicho con razón que el principio de proporcionalidad se erige en piedra angular de toda actuación policial. Aun cuando resulte imprescindible el recurso a la violencia para cumplir con una específica función policial, sin que exista un medio eficaz menos lesivo que el que se representa el agente de policía, la legitimación para, por ejemplo, el uso de un arma de fuego no podrá justificarse cuando su utilización no guarde proporción con el interés privado o público que se pretende salvaguardar o, dicho de otra manera, cuando el bien jurídico lesionado prepondere de forma esencial sobre aquel.

El Tribunal Supremo español estima que los funcionarios policiales únicamente estarán legitimados a utilizarla cuando ello sea necesario para mantener el orden público y cumplir con los deberes estrictos del cargo, pero el uso de la fuerza «nunca debe ir más allá de lo necesario y guardando siempre la debida proporción en los medios empleados» (STS de 22 de noviembre de 1970 y 8 de marzo de 1974).

Por lo que se refiere al exceso cometido por agentes policiales en su actuación, la STS 785/1999, de 18 de mayo de 1999, tenía como trasfondo los siguientes hechos: dos agentes se abalanzaron sobre un conductor que, al ser requerido para someterse a la prueba de alcoholemia, golpeó en la mano al primero de ellos, que portaba el aparato de medición, propinando a su vez un golpe al segundo cuando intentaba reducirlo. Los agentes respondieron «golpeándole ambos con tal fuerza que le causaron fractura bilateral de mandíbula y contusión escrotal con hematoma secundario, sanando a los 45 días». Pues bien, en este caso el TS confirmó la sentencia de instancia, apreciando, como

eximente incompleta, la concurrencia de legítima defensa y cumplimiento de un deber, con el siguiente razonamiento: «si bien han de apreciarse los requisitos tanto respecto a la legítima defensa, como a la del cumplimiento de un deber, dada la agresión ilegítima de la víctima, no es menos cierto que tales eximentes han de aceptarse (...) con un carácter relativo, es decir, como incompletas, debido al exceso cometido por dichos Agentes al tratar de reducir al conductor rebelde» (FJ Único).

Asimismo, resulta de gran importancia conocer la **regla Tueller**, la cual establece el espacio mínimo para tener posibilidades defensivas eficaces con una pistola, enfundada y lista para realizar un disparo frente a la posible agresión por un arma blanca. La regla Tueller fue denominada de esta forma, en recuerdo de un sargento norteamericano que la enunció. Esta regla establece como la distancia mínima 21 pies, aproximadamente, 6,4 metros. Un policía necesita como mínimo 1,5 segundos para disparar su pistola, el tiempo en el que un agresor con un cuchillo puede recorrer más de seis metros. Esta regla la consideramos dentro de la Ciencia Policial, pero no es doctrina policial en las FFCCS españolas al no haberse incorporado a ningún procedimiento técnico-operativo de obligado cumplimiento, ni venir recogida en la última Instrucción de SES sobre el Procedimiento Integral de la Detención Policial, anteriormente referenciada, donde sí se podía haber incorporado como nuevo elemento en el empleo progresivo de los medios policiales. Esta regla sí viene siendo empleada por otros cuerpos policiales como los norteamericanos, donde es doctrina policial avalada ampliamente por la Corte Suprema de Estados Unidos de América, y se podría instituir como una especificidad del empleo de las armas de fuego, para los miembros de las Fuerzas y Cuerpos de Seguridad españolas, en la legítima defensa, como así ya viene reconocido en la STS 268/2023, de 19 de abril, sobre Recurso 10569/2022, en la disputa entre particulares con resultado de muerte de uno de ellos.

Principio de eficacia o de eficiencia

Resulta de los principios que se enmarcan en la Ley de Protección de la Seguridad Ciudadana. El ejercicio de las potestades y

facultades reconocidas por esta Ley a las administraciones públicas y, específicamente, a las autoridades y demás órganos competentes en materia de seguridad ciudadana y a los miembros de las Fuerzas y Cuerpos de Seguridad se regirá por los principios de legalidad, igualdad de trato y no discriminación, oportunidad, proporcionalidad, eficacia, eficiencia y responsabilidad, y se someterá al control administrativo y jurisdiccional.

Principio de congruencia

Se trata de combinar los principios anteriores, como modo de tomar una decisión. ¿Qué podemos entender por congruencia? Según el diccionario de la Real Academia de la Lengua Española, puede considerarse así la coherencia, relación lógica, cohesión, ilación, lógica, sensatez, racionalidad, pertinencia, conveniencia, congruidad. En Derecho, se trata de la correspondencia con lo pedido y lo decidido.

La congruencia es un conjunto de factores que debemos considerar antes de tomar una decisión, que la conviertan en lógica, y por tanto, en comprensible por terceros.

Principio de la formación profesional

Este principio suele enunciarse diciendo que, así como los particulares, ante una situación extrema e imprevista de fuerza o agresión, no están instruidos para actuar, los funcionarios de policía deben mantenerse fieles a los estándares objetivos de comportamiento, incluso cuando aparecen situaciones excepcionales en las que deben recurrir a la fuerza coactiva para cumplir con su función policial.

Principio de actuación inmediata

El funcionario de policía debe tomar una decisión en segundos, a veces, en milésimas de segundo, y por ello, todo juicio sobre un acontecimiento con utilización de armas debe ser enjuiciado desde la perspectiva «ex ante» y nunca «ex post».

Principio de la no extralimitación

Este principio debe regir toda actuación profesional de carácter policial, significando que en el uso de la fuerza nunca puede existir un exceso sino la justa proporción entre lo que se trata de conseguir y los medios que se utilicen para ello. Por ejemplo, si en un espectáculo deportivo alguien salta al campo, no puede ser contenido mediante un uso desproporcionado de la fuerza física que le cause graves lesiones, sino aplicando técnicas de contención que sirvan al objetivo deseado; lo propio ante la disolución de una manifestación no autorizada; y desde luego, lo mismo, y aquí todavía con más razón por el peligro que entraña, en el uso de las armas de fuego.

11 Breve análisis jurisprudencial

Veamos cómo actúan y se interpretan los principios que rigen el uso de las armas de fuego en nuestro Tribunal Supremo, con algunas sentencias.

La STS 1103/1996, de 31 de diciembre, trata de un caso de justificación del uso de armas por un agente policial. Se trataba de un caso de la actuación tras un atraco, con ataque con un cuchillo, por parte del atracador. El desenlace fue absolutorio. Y se razona en esta resolución judicial: «... es preciso tener en cuenta que la Audiencia ha establecido que el acusado no obró voluntariamente, sino que el arma se disparó como consecuencia del forcejeo que tuvo con la víctima, y que se ha podido probar una conducta del occiso que no es en modo alguno irrelevante respecto del disparo del arma. Tal situación de hecho no es modificable, dado que constituye una cuestión de hecho, ajena, por lo tanto, al recurso de casación. Si nos mantenemos dentro de los hechos probados, en consecuencia, es de aplicación el principio in dubio pro reo y éste impone considerar que, al no haberse podido descartar que la víctima haya sido causal del resultado, no es posible imputar el mismo al acusado».

Sentencia del Tribunal Supremo 292/2000, de 28 de febrero

Es otro caso de uso de armas por los Cuerpos de Seguridad, en un caso también de imprudencia, analizándose sus requisitos configuradores. En esta ocasión el caso procede de la Audiencia Provincial de Madrid. Tras una operación antidroga, aparece un vehículo, que se da a la fuga. Una vez ha rebasado a los agentes, uno de ellos dispara seis tiros, hiriendo a la conductora. Condena por delito de imprudencia profesional.

Sentencia del Tribunal Supremo de 10 julio de 1991

Sobre el Recurso de Casación nº 2149/1989, en el caso de una actuación de detención. Cuando se cachea al detenido, el agente interpreta que quiere marcharse y dispara el arma al aire, pero impacta en el registrado, que fallece inmediatamente. El supuesto de hecho es calificado de imprudencia profesional.

Sentencia del Tribunal Supremo 614/2022, de 22 de junio

En el caso enjuiciado, un agente de policía instructor, al realizar pruebas de manejo de armas, incluyó balas reales y efectuó un disparo a una alumna causándole graves lesiones, que le causaron inutilidad. El condenado en este caso incumplió su obligación de percatarse que el cargador estaba puesto y el arma quedó preparada para disparar, y fue cuando apuntó hacia delante donde estaba la alumna dentro de su trayectoria.

Sentencia del Tribunal Supremo 714/2023, de 28 de septiembre

En ella el TS confirma la pena de un año de prisión impuesta a un agente de la Policía Local por un homicidio imprudente grave que cometió durante una detención al considerar que «la

omisión del deber de cuidado y exceso» en la actuación del policía «fue evidente», «tanto que acabó con la vida de una persona» con un 'modus operandi' «desproporcionado».

El TS desestima el recurso de casación que presentó el agente y han confirmado la sentencia de la Audiencia Provincial, que incluye, no solo la condena a un año de prisión, sino también la inhabilitación especial para el desempeño de funciones policiales que se le impuso por tres años.

Los hechos se remontan a junio de 2014, cuando el agente recibió una llamada al teléfono de guardia. Una vigilante de seguridad de una empresa ubicada en el polígono industrial de la ciudad requería la presencia de la Policía toda vez que dos individuos habían entrado en la compañía mercantil sin permiso.

El agente acudió al lugar con su compañero de patrulla. Ambos advirtieron la presencia de un hombre que caminaba por la zona próxima a la empresa y le pidieron que se detuviera. Éste, sin embargo, optó por huir «a la carrera». El agente condenado lo persiguió, lo tiró al suelo y forcejeó con él. Intentando neutralizar «golpes y patadas», el agente condenado le inmovilizó por la zona del cuello. Su compañero intentó esposarle por delante. Según consta en la sentencia, «durante todo el proceso de reducción», el acusado «con omisión y desprecio a las más elementales técnicas en materia de reducción de personas» manipuló el cuello del hombre de tal forma que le «provocó una insuficiencia respiratoria aguda y asfixia». Las maniobras de reanimación tanto de los agentes policiales como de los servicios sanitarios no tuvieron éxito.

Sentencia del Tribunal Supremo 381/2023, de 22 de mayo

Absolución de un funcionario policial por el disparo de un arma de fuego, ante una situación de estrés, producida con el propósito de detención de un vehículo que había participado en el intento de un robo a una ferretería, siendo llamados tales agentes por un ciudadano, y pretendiendo los ladrones atropellarles con el vehículo que conducían, momento en que el

acusado, agente de policía, dispara un tiro a las ruedas para detener el coche, que viene directo a embestirlos, y errando el disparo, entra el proyectil en el habitáculo del coche y causa lesiones a uno de sus ocupantes.

La actuación de los agentes de policía en situaciones de estrés, tiene que ser enjuiciada en el contexto de tales acontecimientos, de manera que el grado de imprudencia tiene que ser clasificado en el correspondiente catálogo, como siempre ocurre en términos jurídicos, mediante el análisis ex ante de las condiciones reales en que producen las acciones humanas, valorando todas las circunstancias concurrentes, momento en el que, en décimas de segundo, hay que tomar una decisión, acompasada a lo que la realidad demanda en cada momento.

En estos términos, es evidente que el comportamiento del agente policial concernido en esta resolución judicial actuó en las condiciones citadas, y utilizó el arma en las circunstancias que se justifican en su legislación específica.

La actuación del agente estaba justificada, puesto que el riesgo vital que sufrió, tanto él, como su compañero, el oficial, puede encuadrarse sin ninguna duda en un riesgo racionalmente grave para su vida o su integridad física, pues así lo describe el juicio histórico de la sentencia recurrida, la que dibuja una situación inminente de ser atropellados por un vehículo que circula en línea recta hacia ellos, a gran velocidad, y el citado funcionario policial hubo de disparar para defenderse, es decir, para detenerlo, así figura igualmente en el factum, errando, sin embargo, el disparo que lo dirige, no, desde luego a ninguna persona, y menos a quien después resulta lesionado, sino a la rueda derecha del vehículo con el que se pretendía consumar la agresión, y siempre, repetimos, conforme al factum, con objeto de defenderse. Ese error del tiro producido resulta así fortuito, en modo alguno atribuible a la voluntad del agente, y producto de la situación vivida en sumo grado de estrés por el agente ante la inmediata trayectoria del vehículo conducido por los ladrones.

El TS declara que no ve la imprudencia grave que demanda el recurrente: todo lo contrario, este suceso, como otros muchos vividos y sufridos por las fuerzas de seguridad, denotan la pro-

fesionalidad con la que trabajan, en situaciones de estrés, tanto las fuerzas de seguridad del Estado, como las dependientes de las Comunidades autónomas, así como las policías locales, que era la integración del agente que aquí se acusa de imprudencia constitutiva de delito, y que debe ser absuelto, como ya lo hizo así la Audiencia en la sentencia recurrida. No obstante, esta resolución judicial cuenta con un voto particular interesando la condena del agente.

12 Conclusiones

Aun considerando las dificultades que entraña el ejercicio de las funciones policiales en situaciones de estrés, donde en segundos han de decidir, analizando la situación y circunstancias ante las que se enfrentan, sobre el empleo de las armas, hemos de concluir que se deben atender específicamente los principios de actuación policial: de congruencia, oportunidad y proporcionalidad en la utilización de los medios a su alcance» (letra c) del apartado2. del artículo cinco de la LOFCS); los principios de legalidad, igualdad de trato y no discriminación, oportunidad, proporcionalidad, eficacia, eficiencia y responsabilidad, por los que se verán sometidos al control administrativo y jurisdiccional (Ley Orgánica 4/2015, de 30 de marzo, artículo 4).

Todo el personal deberá conocer, de forma técnica y práctica, la utilización y uso adecuado de las armas y demás medios coercitivos que se empleen en las actuaciones policiales, para lo cual recibirá la formación y entrenamientos precisos» (apartado 3 del artículo 22 del Real Decreto 1484/1987, de fecha 4 de diciembre), lo que aconseja que los órganos de formación, actualización y perfeccionamiento de los cuerpos policiales deben diseñar programas de entrenamiento en el uso de las armas que mantenga permanentemente habilitados a los agentes policiales.

Los principios de actuación en el uso de las armas definidos en: de menor lesividad, oportunidad, proporcionalidad, eficacia o de eficiencia, congruencia, formación profesional, actuación inmediata y no extralimitación, son bien considerados en

el análisis de actuaciones y sus circunstancias que motivan las sentencias de nuestro Tribunal Supremo, avalando las intervenciones policiales y corrigiendo las extralimitaciones, por la responsabilidad personal de la actuación.

Del análisis de las sentencias se puede proponer la mejora de la reciente Instrucción de la SES sobre el Procedimiento Integral de la Detención Policial, de 16 de enero de 2024, donde se debería establecer el «no permitir disparos contra un presunto delincuente en huida», como así se avala por la STS de 18 de enero de 1982 y la STS 292/2000, de 28 de febrero, y la posibilidad de «determinar la distancia mínima entre agente actuante y presunto delincuente para el empleo de las armas», atendiendo a la regla Tueller, como sí viene siendo empleada por otros cuerpos policiales como los norteamericanos, donde es doctrina policial avalada ampliamente por la Corte Suprema de Estados Unidos de América, y se podría instituir como una especificidad, en la legítima defensa, del empleo de las armas de fuego, por los miembros de las Fuerzas y Cuerpos de Seguridad españolas como así viene reconocido en la STS 268/2023, de 19 de abril, sobre Recurso 10569/2022, en la disputa entre particulares con resultado de muerte de uno de ellos.

Referencias

Instrucción nº 1/2024 de la Secretaría de Estado de Seguridad sobre el Procedimiento Integral de la Detención Policial, de 16 de enero de 2024. https://de-pol.es/wp-content/uploads/2024/01/INSTRUCCION_No_1_2024_PROCEDIMIENTO_INTEGRAL_DE_LA_DETENCION_POLICIAL_DEPOL.pdf

Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad. Boletín Oficial del Estado número 63, de 14/03/1986. Disponible en: https://www.boe.es/eli/es/lo/1986/03/13/2/con

Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana. Boletín Oficial del Estado número 77, de 31 de marzo de 2015. Disponible en: https://www.boe.es/eli/es/lo/2015/03/30/4/con

Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. Boletín Oficial del Estado número 281, de 24/11/1995. Disponible en: https://www.boe.es/eli/es/lo/1995/11/23/10/con

Real Decreto 137/1993, de 29 de enero, por el que se aprueba el Reglamento de Armas. Boletín Oficial del Estado número 55, de 05 de marzo de 1993. Disponible en: https://www.boe.es/eli/es/rd/1993/01/29/137/con

Real Decreto 726/2020, de 4 de agosto, por el que se modifica el Reglamento de Armas, aprobado por el Real Decreto 137/1993, de 29 de enero. Disponible en: https://www.boe.es/eli/es/rd/2020/08/04/726

Real Decreto 1484/1987, de 4 de diciembre, sobre normas generales relativas a escalas, categorías, personal facultativo y técnico, uniformes, distintivos y armamento del Cuerpo Nacional de Policía. Boletín Oficial del Estado número 291, de 05 de diciembre 1987. Disponible en: https://www.boe.es/eli/es/rd/1987/12/04/1484/con

Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal. Gaceta de Madrid, 260, de 17 de septiembre de 1882. Disponible en: https://www.boe.es/eli/es/rd/1882/09/14/(1)/con

Resolución 34/169, de 17 de diciembre de 1979, de la Asamblea General de las Naciones Unidas. Disponible en: https://www.ohchr.org/es/instruments-mechanisms/instruments/code-conduct-law-enforcement-officials

Interceptación de comunicaciones telefónicas, seguridad(es) y garantías procesales

Interception of Telephone Communications, Security(s) and Procedural Safeguards

Adriano J. Alfonso Rodríguez[1]
UNED Lugo.
ajalfonsorodriguez@hotmail.com

DOI: https://doi.org/10.14201/cp.31812
Recibido: 23-04-24 | Aceptado: 12-05-24

Resumen

Los desafíos referidos a la seguridad debemos verlos en diferentes vertientes. Uno de ellos es la «seguridad pública» ligada al desarrollo de actividades de persecución del hecho delictivo, lo que motiva que las limitaciones de derechos fundamentales sigan una estela de rigor y control judicial bajo parámetros garantistas muy intensos. Frente a ella se encuentra la denominada «seguridad nacional», que es bastante distante de la investigación penal propiamente dicha, pero cuyas amenazas resultan en ocasiones coincidentes (por ejemplo, crimen organizado y terrorismo) y para ello es necesario, también, limitar los derechos fundamentales y establecer una garantía judicial, sólo que bajo un prisma diferente que resulta impuesto en el proceso penal. Esto impacta, necesariamente, cuando es la Policía la que solicita al Juez una medida de escuchas telefónicas, de cuando lo es nuestro servicio secreto que tiene un régimen distinto, aunque muy interesante de control judicial.

1. Doctor en Derecho-Graduado en Criminología y Seguridad Publica. Profesor UNED. Coordinador Prácticum Criminología UNED-Lugo. Juez (s) adscrito a la Audiencia Provincial A Coruña.

Palabras clave
Seguridad pública; Seguridad nacional; Policía; Servicio de inteligencia; Garantías procesales.

Abstract
We must see the challenges related to security in different aspects. One of them is «public security» linked to the development of activities to prosecute criminal acts, which motivates the limitations of fundamental rights to follow a trail of rigor and judicial control under very intense guarantee parameters. In front of it is the so-called «national security», which is quite distant from the criminal investigation itself, but whose threats are sometimes coincident (for example organized crime and terrorism) and for this it is also necessary to limit fundamental rights. and establish a judicial guarantee, only under a different prism that is imposed in the criminal process. This necessarily has an impact when it is the Police that requests a wiretapping measure from the Judge, when it is our secret service, which has a different but very interesting regime of judicial control.

Keywords
Public security; National security; Police; Intelligence service; procedural guarantees.

1 Ideas previas: factores desestabilizadores y dos escenarios

La criminalidad grave ha dejado de ser un factor de riesgo ceñido a una respuesta policial y procesal para pasar a ser algo más: Es un elemento permeable, que ha traspasado determinadas fronteras, y cuyo alcance como elemento de desestabilización política, social y económica está por ver en toda su extensión y alcance, pero que conviene analizar con detenimiento. Como pone de manifiesto la Estrategia de Seguridad Nacional (2021):

> El crimen organizado es una amenaza a la seguridad que se caracteriza por su finalidad esencialmente económica, su efecto horadador sobre la institucio-

> nes políticas y sociales, su carácter transnacional y su opacidad. Los grupos delictivos y las organizaciones criminales camuflan sus operaciones ilegales con negocios lícitos y se apoyan cada vez más en tecnologías digitales, como las cripto-monedas y la Internet oscura. Además de su dimensión económica, el crimen organizado tiene un relevante potencial desestabilizador. Sus estructuras se adaptan al entorno geoestratégico y repercuten en la gobernanza, la paz social y el normal funcionamiento de las instituciones. En cuanto a la delincuencia grave, actividades como la explotación de menores o la trata con fines de explotación sexual se dirigen hacia los colectivos vulnerables y violan gravemente los derechos humanos. El contrabando, el cibercrimen, el tráfico de drogas, de armas y de especies silvestres y la corrupción son amenazas tangibles para la Seguridad Nacional. La convergencia entre grupos terroristas y redes de crimen organizado va en aumento. Los modelos de organización cada vez más descentralizada de estos actores delictivos favorecen su cooperación y facilitan la financiación terrorista.

Lo expuesto anteriormente no deja de ser una advertencia, por cuanto ya no estamos en el marco estricto de la seguridad pública limitando el problema a una respuesta policial y judicial, sino que ahora trasciende e integra cuestiones de seguridad nacional, concepto distinto que va más allá de la persecución delictiva propiamente dicha y donde proteger el interés nacional resulta primordial, pudiendo afectar a campos muy variados y no necesariamente penales[2]. Como es lógico, el destacado

2. Como apunta la STS 367/2021, de 17 de marzo, de la Sala III (Contenciosa-Administrativa), Ponente: Sr. Herrero Pina, y en materia de nacionalidad y «seguridad nacional» resulta que «Ello para poder apreciar la incidencia *que en la concreta concesión de la nacionalidad española por residencia tienen las particularidades derivadas de la incorporación al orden público o interés nacional, del concepto de «seguridad nacional»* recogido entre otras en la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional. Un elemento esencial de ese concepto de seguridad nacional, que engloba riesgos y amenazas para el orden público, sujetos a elementos de inteligencia

impacto que en el Estado de Derecho tienen las amenazas expuestas trae consigo, correlativamente, la búsqueda de soluciones destinadas a lidiar con tales fenómenos. Es aquí donde la seguridad, en tanto concepto polisémico, se presenta como una exigencia indeclinable que puede entrar en colisión con los derechos fundamentales y sin que su cumplimiento pueda marginar al Estado constitucional (Vervaele, 2007, p.103). De modo, que ya estén las actuaciones destinadas a perseguir el crimen, u orientadas a proteger un interés nacional, y siempre que supongan penetrar en la esfera de los derechos fundamentales, es preciso, adicionalmente, establecer un sistema de garantías, que impidan «espacios ciegos», carentes de control, y donde el protagonismo judicial resulta clave. Si se limita un derecho fundamental, esencial, aunque no exclusivamente en el proceso de indagación penal, antes de que esa legítima conculcación se haga efectiva, resulta precisa una autorización judicial, pues tal y como ha señalado el ATC 47/94, de 8 de febrero, en su Fundamento Jurídico (FJ) 2º:

> ...Pero es claro que la instrucción, globalmente considerada, tiene, además de la faceta de esclarecimiento de los hechos y averiguación del culpable, otra vertiente de garantía de los derechos de los ciudadanos. Y más patente resulta aún que algunas diligencias concretas de las englobadas en la instrucción de una causa penal inciden sobre derechos —y, en no pocos casos, derechos fundamentales— de los encausados...[3].

Hay que reparar que, en nuestro ordenamiento jurídico, existe una suerte de desdoblamiento en la faceta judicial de garantía, dependiendo de si intervienen las agencias policiales, de ordinario actuando en la averiguación de un hecho o autoría criminal,

---

que, por su propia naturaleza, tiene carácter confidencial o se basa en información protegida por la Ley 9/1968, de 5 de abril, sobre secretos oficiales y que, sin embargo, *ha de poder integrarse en el concepto de «orden público o interés nacional» del art. 21.2 del Código Civil y, en consecuencia, tenerse en cuenta a la hora de conceder o denegar la nacionalidad* española por residencia» (FJ 2º). La cursiva es del autor.

3. La cursiva es del autor.

o si quien solicita la limitación del derecho fundamental (control de las comunicaciones o inviolabilidad domiciliaria) es el Centro Nacional de Inteligencia, (en adelante CNI), evidenciándose un procedimiento diferente a la hora de su hipotética concesión. La necesidad de la denominada «inteligencia criminal»[4] que responde esencialmente, aunque no exclusivamente, al desafío exigido en materia de seguridad pública y destinada a surtir sus efectos en el marco del proceso penal, contrasta con la «inteligencia estratégica»[5]alojada en el recipiente de la «seguridad

4. Se trata de una inteligencia destinada para «obtener, evaluar e interpretar» información destinadas a defender la neutralización de amenazas delictivas que atenten contra el estado constitucional y los derechos fundamentales y libertades. (*Vid*. Sansó-Rubert, 2011, p. 214). Surge así la denominada «pericial de inteligencia», informe en el que se vuelcan conocimientos fruto de la obtención de datos policiales destinados a surtir efectos en el proceso penal. Haciendo un acopio de jurisprudencia reciente, resulta la STS 65/2019, de 7 de febrero de 2019, de la Sala II (Ponente: Sr. Magro Servet) que apunta en su FJ 2º «En este sentido se ha pronunciado esta Sala del Tribunal Supremo, en varias sentencias (SSTS de 31 de marzo de 2010; de 1 de octubre de 2010; de 29 de mayo de 2003; de 13 de diciembre de 2001 y de 17 de julio de 1998) señalando que «A este respecto debemos destacar nuestras sentencias..., *que han declarado que tal prueba pericial de inteligencia policial cuya utilización en los supuestos de delincuencia organizada es cada vez más frecuente, está reconocida en nuestro sistema penal pues, en definitiva, no es más que una variante de la pericial a que se refieren tanto los arts. 456 LECrim como el 335 LEC , cuya finalidad no es otra que la de suministrar al Juzgado una serie de conocimientos técnicos, científicos, artísticos o prácticos cuya finalidad es fijar una realidad no constatable directamente por el Juez y que, obviamente, no es vinculante para él, sino que como el resto de probanzas, quedan sometidas a la valoración crítica, debidamente fundada en los términos del art. 741 LECrim. La prueba pericial es una variante de las pruebas personales integrada por testimonios de conocimiento emitidos con tal carácter por especialistas del ramo correspondiente de más o menos alta calificación científica, para valorar por el Tribunal de instancia conforme a los arts. 741 y 632 LECrim. y 117 CE. Dicho de otro modo: la prueba pericial es una prueba personal, pues el medio debe ser interrogado por la opinión o dictamen de una persona y al mismo tiempo, una prueba indirecta en tanto proporciona conocimientos técnicos para valorar los hechos controvertidos, pero no un conocimiento directo sobre cómo ocurrieron los hechos*». La cursiva es del autor.
5. Este tipo de inteligencia se recopila fundamentalmente para la toma de decisiones políticas destinadas a la defensa de los intereses nacionales. (*Cfr*. Pinto, 2019, pp. 51 y ss). Los apuntes del autor son autorizados dada su condición de ex miembro del CESID y del CNI. En todo caso, podría servir para garantizar la política de seguridad

nacional», que opera en un marco más bien político y donde las actuaciones, esencialmente, poseen una naturaleza clandestina (*covert action*). Ambas responden a finalidades recopilatorias en campos que, en principio, no deberían mezclarse, (*Cfr.* Feijoo, 2006, p.820), de ahí que, como vamos a explicar, existe una distancia regulatoria evidente cuando una u otra llaman a la puerta de un Juez solicitando una limitación de derechos fundamentales, singularmente el acceso a las comunicaciones telefónicas o telemáticas, que permita recabar elementos ciertos de conocimiento, pero cuya obtención responde a finalidades distintas.

No obstante, y pese a lo señalado en las líneas anteriores, nos encontramos con la paradoja de una posible confluencia entre hechos susceptibles de ser perseguidos penalmente que son objeto de conocimiento en el desarrollo de actividades de obtención de inteligencia estratégica, lo que determina el qué hacer con esas informaciones, máxime cuando los requisitos de su obtención, pese a la autorización judicial, nada tienen que ver con las exigencias procesales que se derivan en los supuestos de investigación policial, algo que no está resuelto legislativamente en nuestro país, aunque jurisprudencialmente se han abordado los supuestos de comunicación a las FCSE por parte de autoridades policiales o servicios extranjeros de información y que sirven para iniciar procedimientos penales[6]. Asimismo, es preciso tener

y exterior, verificar las amenazas externas, conseguir información militar o coadyuvar a operaciones de esta naturaleza o recopilar inteligencia económica entre otras. (*Cfr*: Centre for the Democratic control of armed forces -Intelligence Working Group, 2003, pp. 24-28).

6. Paradigmática nos resulta la STS 445/2014, de 29 de mayo, de la Sala II (Ponente: Ferrer García), en la que se cuestionaban oficios remitidos por la agencia antidroga norteamericana (DEA) que sirvió para iniciar investigaciones por parte de la Policía Nacional, objeciones que fueron repelidas señalando, en su FJ 2º que «En definitiva, no se aprecien motivos que permitan cuestionar la validez de las intervenciones acordadas. Esa validez no queda empañada por la falta de ratificación de los agentes de la DEA que el recurso denuncia. En todo caso esa información que la policía recibió por cauces oficiales sirvió como denuncia (art. 262 LECrim), que motivó la actuación investigadora de la policía española que, no olvidemos, antes de solicitar la intervención, inició actuaciones encaminadas a la corroboración, dentro de lo posible, en atención las circunstancias de los hechos y la inminencia de la llegada del

en cuenta que si bien cuando las agencias policiales desarrollan esa tarea de recopilación informativa de manera secreta, lo cierto es que una vez resulta pertinente alzar la situación de secreto (art. 302 LECrim) y facilitar el acceso a los elementos esenciales de la causa penal, se produce el conocimiento por los investigados, acabando con la clandestinidad de la indagación penal, algo que no ocurre en los supuestos de actuación del CNI donde tal acceso, con el consabido desconocimiento por el interesado, no se produce, aunque tampoco, esto es preciso señalarlo, hay un proceso judicial abierto de ninguna clase y ello porque la información se obtiene para propósitos ajenos a unas diligencias penales. Son perceptibles, a simple vista, algunas de las aristas que la situación escenifica. Veamos los diferentes aspectos.

2 La seguridad pública en el contexto del proceso penal

El concepto de «seguridad pública» ha sido abordado desde diversas perspectivas. Por un lado, legislativamente, y así aparece ya delimitado en la Constitución (CE) al establecer el cometido de las fuerzas policiales de garantizar la «seguridad ciudadana» (art. 104.1) o la titularidad estatal exclusiva, en el reparto

barco que trasladaba la droga, de los datos que se le suministraban. Y así aportó datos suficientemente fundados, teniendo en cuenta el estado incipiente de la investigación, para sustentar la medida que solicitaba y fue concedida. Datos que además se fueron completando en los días sucesivos. Como dijo la STS 884/2012, de 12 de noviembre, «*cuando servicios de información extranjeros proporcionan datos a las fuerzas y cuerpos de seguridad españoles, la exigencia de que la fuente de conocimiento precise también sus propias fuentes de conocimiento, no se integra en el contenido del derecho a un proceso con todas las garantías. Lo decisivo, además de la constancia oficial, no necesariamente documentada, de que esa comunicación se produjo, es que el intercambio de datos sirva para lo que puede servir, esto es, para desencadenar una investigación llamada a proporcionar a los Tribunales españoles los medios de prueba precisos para el enjuiciamiento de los hechos». «Como consecuencia de todo lo argumentado, procede desestimar este motivo de impugnación*». La cursiva es del autor. Más recientemente y en la misma línea la STS 312/2021, de 13 de abril, de la Sala II (Ponente: Sr. Llarena Conde), FJ 1.11.

de competencias, de la denominada «seguridad pública» (art. 149.1.29ª), situación que liga a la creación de policías autonómicas, sin olvidar el art. 126 donde se establece la dependencia de la «Policía Judicial» de Jueces y Fiscales, dentro de cometidos relacionados con el «Poder Judicial», en cuanto a la averiguación del delito y del delincuente.

Y así, en sintonía con la anterior reflexión, la satisfacción de las funciones de «seguridad pública» puede desarrollarse en un plano «gubernativo» —no procesal, salvo ulterior revisión— sustanciado por la Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana (LOPSC), que sirve de marco de actuación administrativa y que permite la adopción de una suerte de medidas de intervención muy variadas para el cumplimiento de sus cometidos (la entrada y registro en domicilio, identificaciones personales, comprobaciones y registros en lugares y vías públicas, entre otras) cuyo empleo debe ser limitado a funciones de sanción, no por tanto, y en principio, de persecución penal y si se usan, para acabar desembocando en una actuación procesal, entonces es preciso dotarlas de las garantías constitucionales previstas en la LECrim. (*vid.* STS 6/2021, de 13 de enero, de la Sala II, Ponente: Sr. Puente Segura, FJ 3. 2º y 3. 3º, en relación al uso inadecuado de la LOPSC y los derechos fundamentales, aunque toda la resolución es de sumo interés).

En todo caso, jurisprudencialmente, el TC ha deslindado tempranamente el concepto de «seguridad pública», «*...entendido como actividad dirigida a la protección de personas y bienes y al mantenimiento de la tranquilidad y el orden ciudadano*, según pusimos de relieve en las SSTC 33/1982, 117/1984, 123/1984 y 59/1985, engloba, como se deduce de estos pronunciamientos, *un conjunto plural y diversificado de actuaciones, distintas por su naturaleza y contenido, aunque orientadas a una misma finalidad tuitiva del bien jurídico así definido*» (STC 104/1989, de 8 de junio, FJ 3º) y dentro de aquella se incluye la «actividad policial» como uno de sus contenidos (STC 175/1999, de 30 de septiembre, FJ 7º o la STC 86/2014, de 29 de mayo, FJ 4º), donde se encuentra la investigación de los delitos con actividades cuya finalidad es la determinación del hecho punible y de su autoría (STC 303/1993, de 25 de octubre, FJ 4º) y sin que exista una identidad plena entre «Policía» y «Seguridad Pública» (STC 174/2000, 1 de

junio, FJ 6º) . En suma, como ha señalado la STC 55/90, de 28 de marzo, «*De la Constitución se deduce que las Fuerzas de Policía están al servicio de la comunidad para garantizar al ciudadano el libre y pacífico ejercicio de los derechos que la Constitución y la Ley les reconocen y este es el sentido del art. 104.1 CE*, que puede considerarse directamente heredero del art. 12 de la Declaración de Derechos del Hombre y del Ciudadano, *configurando a la policía como un servicio público para la Comunidad, lucha contra la criminalidad, el mantenimiento del orden y la seguridad pública y la protección del libre ejercicio de los derechos y libertades*...» (FJ 5º).

Procesalmente, en materia de persecución delictiva, las fuerzas policiales, y específicamente la denominada «Policía Judicial» (art. 283 LECrim), llevan a cabo la investigación del hecho penal entendida al modo del art. 282 LECrim —en relación con el art. 299 del mismo texto— comprendiendo «*averiguar los delitos públicos que se cometieren en su territorio o demarcación; practicar, según sus atribuciones, las diligencias necesarias para comprobarlos y descubrir a los delincuentes, y recoger todos los efectos, instrumentos o pruebas del delito de cuya desaparición hubiere peligro, poniéndolos a disposición de la autoridad judicial.*», todo ello junto con la atención, información y valoración de la víctima (arts. 4 b), 5.1, 10 II, 11, 19 de la Ley 4/2015, 27 de abril, Estatuto de la Víctima).

En el curso de su actividad preparatoria e indagatoria, los investigadores policiales pueden desarrollar, con relativa autonomía, una serie de diligencias *no invasivas de los derechos fundamentales* para cumplir con las exigencias del precepto antes visto y así, grosso modo, pueden identificar a los sospechosos, víctimas o testigos e interrogarlos, llevar a cabo reconocimientos fotográficos o por medio de fotografías o grabaciones, reconocimiento de voz e identificación por dactiloscopia, recogida de vestigios de ADN abandonados o con entrega consentida, obtención de determinados datos personales, de comunicaciones, telefonía y archivos informáticos bajo determinados presupuestos, acordar la entrega y circulación vigilada con ulterior dación de cuenta al Juez, practicar una inspección ocular policial, o la recogida de efectos, medios, objetos o instrumentos del hecho delictivo. Asimismo, en cuanto *medidas estrictas limitativas o*

que pueden afectar a los derechos fundamentales, la Policía puede detener a quien sea sospechoso de un hecho delictivo (art. 17.3 CE), *entrar en un domicilio en supuestos de flagrancia delictiva* (art. 18.2 CE) y *realizar inspecciones corporales leves* (arts. 15 y 18.1 CE) como desarrollaremos más adelante, tampoco sin intervención judicial.

El desarrollo de su trabajo, que debe estar guiado por una absoluta objetividad, al margen de visiones particulares (*Vid.* como paradigmática STS 78/2021, 1 de febrero de la Sala II, (Ponente: Sr. Marchena Gómez), FJ 2.3º), concluye con la elaboración del atestado, documento técnico con categoría de mera denuncia sin valor probatorio per se (*Cfr.* STS 120/2021, 11 de febrero, Sala II (Ponente: Sra. Polo García), FJ 3.3º; SSTC 217/1989, de 21 de diciembre, FJ 2º; 303/1993, de 25 de octubre, FJ 4º; 79/1994, de 14 de marzo, FJ 3º; 22/2000, de 14 de febrero, FJ 5º; 188/2002, de 14 de octubre, FJ 2 º) sin perjuicio de aquellos datos objetivos y verificables de imposible reproducción en el acto de juicio oral, introducidos como prueba documental, y sujetos a contradicción (SSTC 107/1983, de 29 de noviembre, FJ 3º; 303/1993, de 25 de octubre, FJ 2 b); 173/1997, de 14 de octubre, FJ 2 b); 33/2000, FJ 5º; 188/2002, FJ 2º).

No hay que olvidar que en la persecución del delito, como herramienta procesal de satisfacción de la «seguridad pública», confluyen legítimas políticas, igualmente públicas, referidas a la criminalidad con lo que a la vez que se satisfacen aquellas (*Vid.* Fernández-Rodríguez, 2007, p. 8) [7], también se desarrolla una actividad inicialmente preprocesal, y luego procesal, con el propósito de delimitar la responsabilidad delictiva por parte de los agentes policiales, y luego por el Juez Instructor, configurando una causa, con los elementos de importancia para ella (art. 315

7. En todo caso, la EM de la LOPSC 4/2015 señala «*Para garantizar la seguridad ciudadana*, que es una de las prioridades de la acción de los poderes públicos, *el modelo de Estado de Derecho instaurado por la Constitución dispone de tres mecanismos*: un ordenamiento jurídico adecuado para dar respuesta a los diversos fenómenos ilícitos, *un Poder Judicial que asegure su aplicación*, *y unas Fuerzas y Cuerpos de Seguridad eficaces en la prevención y persecución de las infracciones*». La cursiva es del autor.

LECrim), destinada a una hipotética valoración de los rasgos indiciarios, que afloran en la superficie, con relación al ilícito investigado y que puede motivar la exigencia de responsabilidades penales, mediante la apertura de un eventual juicio, donde se practican las pruebas propiamente dichas (*Cfr*. STS 447/2015, de 29 de junio, de la Sala II (Ponente: Sr. Jorge Barreiro), FJ 1º; STC 31/1981, de 28 de julio, FJ 4º ya tempranamente, y luego reiteradamente SSTC 213/2007 de 8 de octubre, FJ 2º; 64/2008 de 26 de mayo, FJ 3º; 115/2008 de 29 de septiembre FJ 1º; 49/2009 de 23 de febrero, FJ 2º; 120/2009 de 18 de mayo, FFJJ 2º a 4 º o 132/2009 de 1 de junio, FJ 2º).

Por tanto, a través de la investigación policial se satisfacen los presupuestos propios de una política criminal en cuanto la persecución del delito como herramienta para la protección de los derechos de los ciudadanos y la búsqueda, legítima, de la tranquilidad pública, y a la vez, en un terreno estrictamente procesal, se depuran responsabilidades penales con la averiguación de los hechos y de su autoría bajo una dirección judicial. La «seguridad pública» opera en el contexto del proceso penal que coadyuva para su satisfacción pese a que la autoridad judicial queda al margen, lógicamente, pues no es su función satisfacer tal objetivo (*Cfr.* Conde-Pumpido, 1992, p. 18)[8], existiendo una

8. Esto ha servido, a la vez para intentar mutar el proceso penal otorgando al Ministerio Fiscal la dirección del proceso de investigación al acomodarse mejor a la satisfacción de esos objetivos de política criminal. Así institucionalmente la Memoria de la Fiscalía General del año 1992 señalaba que «La atribución de la investigación criminal al Ministerio Fiscal es en estos momentos algo más que una pura alternativa o una conveniencia atendible. Se trata con toda probabilidad de una necesidad de política criminal, a cuyo impulso deben dirigirse todos los esfuerzos de los poderes públicos(…) Debe aceptarse que la renovación del proceso sólo parece posible si partimos de la diferenciación entre las fases de investigación del hecho criminal, de la exclusiva dirección del Ministerio Fiscal, regido por los indicados dogmas de legalidad e imparcialidad, pivotando sobre la actividad profesionalizada, científica y especializada de la Policía Judicial, dotada de una mayor autonomía. Así delimitadas las bases del proceso, cuyo impulso corresponde al Ministerio Público, compete a Jueces y Tribunales ejercer su función jurisdiccional, con estricta sujeción al imperio de la ley y en el ámbito legalmente previsto dictado de su conciencia racional». (*Vid.* Fiscalía General del Estado. 1993, pp. 25-27). Igualmente, la Recomendación (2000)

doble dependencia de las fuerzas policiales indagadoras tanto respecto del Ejecutivo (orgánica) como del Juez (funcional) que se encarga de la investigación en cada momento (STS 14/2018, 16 de enero, de la Sala II (Ponente: Sr. Marchena Gómez), FJ 2º.1 y 6º) .

2.1 La garantía judicial en la investigación penal policial

Si hay un campo de tensión entre derechos (del investigado) y fines (de la investigación), sin duda, ese es el que enmarca el proceso penal, situando frente a las intervenciones gubernativas un muro infranqueable que es la necesaria actividad policial bajo autorización del Juez quien actúa como garante de los derechos señalados como fundamentales y cuya función resulta determinada constitucionalmente (art. 117.4 CE), algo que ha explicado con suma claridad la STS 79/2012, de 9 de febrero, de la Sala II (Ponente: Colmenero Menéndez de Luarca), en su FJ 11º, donde deja claro que: Al instructor en el proceso penal, a quien compete la dirección de la investigación, *no le corresponde ocupar una posición propia o característica de un enemigo del investigado, estando, por el contrario, obligado a «...consignar y apreciar las circunstancias así adversas como favorables al presunto reo...», (artículo 2 de la LECrim). Además, resulta encargado de la protección de los derechos fundamentales del imputado*, en tanto que la Constitución, ordinariamente, condiciona su restricción a la existencia de una resolución judicial debidamente motivada[9].

19 del Comité de Ministros del Consejo de Europa, de 6 de octubre de 2000, ya señala el protagonismo del Ministerio Fiscal en la política penal definida por el Ejecutivo, o el Legislativo, indicando que es quien la «lleva a la práctica».

9. La cursiva es del autor. No obstante, con anterioridad el ATS 3773/1992, de 18 de junio, de la Sala II (Ponente: Ruíz Vadillo) en su FJ 8º apuntó que «*El Juez, garante esencial de los Derechos Fundamentales y de las libertades públicas, debe examinar cada infracción con las circunstancias que la acompañan y decidir, valorando si los objetivos legítimos de las investigación,* enjuiciamiento y, en su caso, condena merecen en ese concreto supuesto el sacrificio de otro bien jurídico, especialmente valioso como es la dignidad, la intimidad la libertad de la persona, como esta Sala viene fijando en sus resoluciones en orden a la defensa siempre y para todos de estos valores esenciales» . La cursiva es del autor.

Y en este sentido, el Juez en primer lugar debe garantizar el derecho de defensa[10] que asiste a todo investigado en el curso de la instrucción conforme el *art. 24.2 CE* (STC 87/2001, de 2 de abril, FJ 3º). Esencialmente por cuanto no cabe el desarrollo de una actividad inquisitiva (SSTC 135/1989, 19 de julio, FJ 3º; 186/90, de 15 de noviembre, FJ 5º; STS 14/2018, 16 de enero, de la Sala II (Ponente: Sr. Marchena Gómez), FJ 2.1) y para ello se genera un estatus, el de investigado, que permite que la plenitud de derechos reaccionales que posee opere frente a los investigadores. Inicialmente, se produce una imputación no procesal[11] extrajudicial-policial, que podríamos calificar como la atribución al sujeto de la categoría de «sospechoso», que despliega ya de-

10. En una síntesis interesante que hace el decaído Anteproyecto de Ley Orgánica de Defensa, en su art. 3 al señalar que «1. El derecho de defensa comprende la prestación de asistencia letrada o asesoramiento en Derecho y la defensa de los intereses legítimos de la persona a través de los procedimientos previstos legalmente. 2. El derecho de defensa incluye, en todo caso, el derecho al libre acceso a los Tribunales de Justicia, a un proceso sin dilaciones indebidas, a que se dicte una resolución congruente y fundada en Derecho por el juez ordinario e imparcial predeterminado por la ley, así como a la invariabilidad de las resoluciones firmes y a su ejecución en sus propios términos. El derecho de defensa incluye, también, las facultades precisas para conocer y oponerse a las pretensiones que se formulen de contrario, para utilizar los medios de prueba pertinentes en apoyo de las propias, la garantía de indemnidad y al acceso a un proceso público con todas las garantías, sin que en ningún caso pueda producirse situación alguna de indefensión. 3. En las causas penales, el derecho de defensa integra, además, el derecho a ser informado de la acusación, a no declarar contra uno mismo, a no confesarse culpable, a la presunción de inocencia y a la doble instancia, de conformidad con la Ley de Enjuiciamiento Criminal, la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, la Ley Orgánica 2/1989, de 13 de abril, Procesal Militar, y la Ley Orgánica 5/2000, de 12 de enero, reguladora de la responsabilidad penal de los menores. Estos derechos resultarán de aplicación al procedimiento administrativo sancionador y al procedimiento disciplinario de acuerdo con las leyes que los regulen...».
11. La STC 18/2005, de 1 de febrero. ha señalado que «*…en el seno del proceso penal es el Juez de Instrucción* y no-como parece reclamar el recurrente- los funcionarios de la Administración Tributaria, a quien corresponde el otorgamiento de la condición de imputado de un ciudadano desde el momento en que considere verosímil o tenga fundadas sospechas de un ilícito penal» (SSTC 14/1999, de 22 de febrero, FJ 6 c); 149/1997, de 29 de septiembre, FJ 2; y 118/2001, de 21 de mayo FJ 3º, FJ 4º). La cursiva es del autor,

terminados derechos de defensa en sede policial (arts. 118 y 520 LECrim) , para luego recibir dicha imputación de manera judicial dando entrada al sujeto en el seno del proceso penal, sobre el que pesan indicios racionales de criminalidad (SSTC 47/2000, de 17 de febrero, FJ 6º, 108/1994, de 11 de abril, FJ 3º) permitiendo la situación de conocimiento, contradicción y confrontación con las acusaciones (STS 527/2021, de 16 de junio, de la Sala II (Ponente: Sr. Martínez Arrieta), FJ 2º).

Sin embargo, esa función de garantía se extiende a otros derechos fundamentales en el proceso penal y que en hipótesis pueden verse afectados en el marco de una investigación como la *libertad personal* (art. 17 CE)[12], *la intimidad* (art.18.1 CE)[13], la *inviolabilidad domiciliaria* (art.18.2 CE)[14], *el secreto de las comu-*

12. *Vid.* la SSTC 106/1989, de 8 de junio, FJ 4º; 98/1997, de 20 de mayo, FJ 4º y 5º en torno a la denominada prisión preventiva.
13. *Vid.* la STC 123/2002, 19 de junio, FJ 4º en relación a la necesidad de autorización judicial como regla general cuando se afecta a la intimidad.
14. Ha señalado la STS 423/2016, 18 de mayo, de la Sala II, (Ponente: Sra. Ferrer García) «Como hemos recordado en otras ocasiones (SSTS 727/2003 16 de mayo , 530/2009 13 de mayo , 478/2013 de 6 de junio o 103/2015 de 24 de febrero), e*l derecho a la inviolabilidad del domicilio es un derecho fundamental del individuo que, según el artículo 18.2 de la Constitución sólo cede en caso de consentimiento del titular; cuando se trate de un delito flagrante, o cuando medie resolución judicial*.». La Declaración Universal de los Derechos Humanos proscribe en su art. 12 las injerencias arbitrarias en el domicilio de las personas, reconociendo el derecho de éstas a la protección de la ley contra las mismas. En la misma forma se manifiesta el Pacto Internacional de Derechos Civiles y Políticos en su art. 17. Y el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, dispone en su artículo 8 que, «1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia. 2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás. *Se trata, por lo tanto, en cuanto recogido con ese carácter en la Constitución, de un derecho fundamental que protege una de las esferas más íntimas del individuo, donde desarrolla su vida privada sin estar sujeto necesariamente a los usos y convenciones sociales, a salvo de invasiones o agresiones procedentes de otras personas o de la autoridad pública,*

nicaciones (art. 18.3 CE) y también *la libertad de circulación o movimientos* (art. 19 CE)[15].

En todo, caso, se produce un claro contrapunto por cuanto, como antes apuntamos, cabe la posibilidad que los agentes policiales practiquen una *detención* en los supuestos previstos en los arts. 490 y 492 LECrim, privación de libertad limitada temporalmente (SSTC 31/1996, de 27 de febrero, FJ 8º; 21/1997, de 10 de febrero, FJ 4º; 174/1999, de 27 de septiembre, FJ 4º; 179/2000, de 26 de junio, FJ 2º) y en todo caso destinada a una puesta en libertad policial o en su caso a poner al sujeto a disposición de la autoridad judicial para que decida sobre su situación personal con plazos preclusivos de 72 horas que no pueden ser agotados bajo cualquier presupuesto, salvo la prórroga del art. 520 bis.

La *entrada y registro en domicilio de personas físicas en los supuestos de flagrante delito* (arts. 553 en relación con el 795.1.1º LECrim; STC 341/1993, de 18 de noviembre, en su FJ 8º o STS 71/2017, de 8 de febrero, de la Sala II, (Ponente: Sr. Berdugo Gómez de la Torre), en su FJ 8º) constituye una excepción a la autorización judicial bajo un presupuesto igualmente de apreciación estricta (STS 423/2016, de 18 de mayo, de la Sala II (Ponente: Sra. Ferrer García), FJ 4º). No podemos perder de vista, tampoco, la previsión que se establece (arts. 553 y 384 bis LECrim) en los supuestos de terrorismo si bien en relación a este

aunque puede ceder ante la presencia de intereses que se consideran prevalentes en una sociedad democrática» (FJ 4º). La cursiva es del autor.

15. La STC 85/1989, de 10 de mayo, en su fundamento jurídico tercero, ha señalado la limitación de libertad de movimientos bajo los presupuestos legales, pero mediante control judicial previo, así: «..). *Y, de otra parte, como este Tribunal ha dicho en supuestos similares al que nos ocupa (ATC 650/1984), la presentación ante el Juzgado, por ser una medida cautelar legalmente prevista, aunque ciertamente significa una restricción del derecho de libre elección de residencia, no constituye una vulneración al mismo aquella resolución judicial que, como ocurre en el presente caso, impone tal obligación dentro de los supuestos legales y en forma razonada en términos de Derecho*…». La cursiva es del autor. Debemos destacar la importancia de medidas cautelares en el ámbito de la violencia de género como la denominada orden de protección (art. 544 ter LECrim) o la «orden de alejamiento con prohibiciones de comunicación» (art. 544 bis LECrim.).

supuesto resulta que su habilitación radica en la detención de terroristas y solamente, una vez practicada la detención, cabría el registro (STC 199/1987, 10 de diciembre, FJ 9º). Autorización judicial extensiva para el domicilio de *personas jurídicas imputadas* entendido como «*el espacio físico que constituya el centro de dirección de las mismas, ya se trate de su domicilio social o de un establecimiento dependiente, o aquellos otros lugares en que se custodien documentos u otros soportes de su vida diaria que quedan reservados al conocimiento de terceros*» (art. 554.4 LECrim) sin que podamos confundir esta diligencia con la posibilidad de entrada y registro en espacios cerrados no constitutivos de domicilio o se traten de locales abiertos al público o domicilios de personas jurídicas no imputadas en el procedimiento penal (STS 150/2022, 22 de febrero de la Sala II, Ponente: Sr. Palomo del Arco, FJ 4º. 3).

Finalmente, a la Policía se le permite la práctica de *inspecciones corporales leves*[16] bajo razones de urgencia, proporcionalidad y razonabilidad (STC 207/96, de 16 de diciembre, FJ 2º y 4º) que si bien no pueden implicar una afectación del art. 15 CE en cuanto aquellas medidas invasivas[17] que necesariamente requie-

16. Con relación al denominado «cacheo» ya había señalado nuestro TS la pluralidad de derechos fundamentales que resultaban «tocados» y así «El cacheo, acompañado de la identificación, constituye por lo general la primera y más frecuente medida de intervención policial que indudablemente i*mplica una medida coactiva que afecta, de alguna forma, tanto a la libertad (art. 17 CE), como a la libre circulación (art. 19 CE), en tanto que, como la identificación misma, comportan inevitablemente, la inmovilización durante el tiempo imprescindible para su práctica, y además, puede afectar a la intimidad personal (art. 18 CE),* en la medida que sea practicado con exceso en cuanto a la justificación de su necesidad, al lugar en que se efectué o el trato vejatorio y abusivo dispensado en él por lo agentes actuantes, o *incluso en la integridad corporal (art. 15 CE)*, en función de la violencia o vis coactiva aplicado en su práctica» (STS 156/2013, 7 de marzo, de Sala II, Ponente: Sr. Berdugo Gómez de la Torre, FJ 1º A).

17. Jurisprudencialmente, en relación a la perspectiva garantista y la coerción física, *vid*. las SSTS 12748/91, de 26 de noviembre, FJ 1º, 6630/91, de 26 de noviembre, FJ 1º, 6635/91, de 26 de noviembre, FJ 1º, de la Sala II, (Ponente: Sr. Ruiz Vadillo). Con anterioridad destaca la STS de la Sala II de 22 de mayo de 1982 (RJ 1982/2702) en su considerando quinto (Ponente: Latour Brotons).

ren de autorización judicial, sí pueden afectar a su intimidad (art. 18.1 CE). En todo caso, no hay que olvidar la prueba de alcoholemia y de detección de drogas en relación con los delitos contra la seguridad vial que configura policialmente una prueba preconstituida (STC 173/1997, de 14 de octubre, FJ 2º), sin intervención judicial.

En suma, es preciso indicar que las vulneraciones más agresivas que implican una afectación a los derechos fundamentales más relevantes (integridad, intimidad, inviolabilidad del espacio domiciliario y comunicaciones o la libertad) están monopolizadas por la autoridad judicial que actúa en funciones de garantía, evitando injerencias no justificadas frente a actuaciones de investigación, sin perjuicio de la existencia de determinadas diligencias para cuya práctica sí están habilitados los agentes policiales aunque pudieran colisionar con los mismos derechos que la autoridad judicial está obligada a proteger pero bajo determinados presupuestos, ligados en ocasiones, a situaciones de urgencia[18] que necesariamente tiene que ser justificada debi-

18. Como puso de manifiesto la STC173/2011, de 7 de noviembre, «Esa regla general se excepciona en los supuestos en que existan razones de necesidad de intervención policial inmediata, para la prevención y averiguación del delito, el descubrimiento de los delincuentes y la obtención de pruebas incriminatorias. En esos casos estará justificada la intervención policial sin autorización judicial, siempre que la misma se realice también desde el respeto al principio de proporcionalidad» [FJ 10 b) 3]. Bien entendido que «la valoración de la urgencia y necesidad de la intervención policial ha de realizarse ex ante y es susceptible de control judicial ex post, al igual que el respeto al principio de proporcionalidad. La constatación ex post de la falta del presupuesto habilitante o del respeto al principio de proporcionalidad implicaría la vulneración del derecho fundamental y tendría efectos procesales en cuanto a la ilicitud de la prueba en su caso obtenida, por haberlo sido con vulneración de derechos fundamentales» [FJ 10 b) 5]. *En esta línea en la STC 206/2007, de 24 de septiembre, FJ 8,* a*firmábamos que «la regla general es que sólo mediante una resolución judicial motivada se pueden adoptar tales medidas y que, de adoptarse sin consentimiento del afectado y sin autorización judicial, han de acreditarse razones de urgencia y necesidad que hagan imprescindible la intervención inmediata y respetarse estrictamente los principios de proporcionalidad y razonabilidad» ...*» (FJ 2º). La cursiva es mía. En todo caso, verificar los arts. 579.3, 588 ter d). 3, 588 quinquies b). 4, 588 sexies c. 3. y 4, de la LECrim.

damente para impedir que la excepción se convierta en regla general.

2.2 La interceptación de comunicaciones y actividad policial

En el marco de la investigación penal y con relación a la inviolabilidad de las comunicaciones (art. 18.3 CE) jurisprudencialmente se ha puesto de manifiesto, en la STS 497/2016, de 9 de junio, de la Sala II (Ponente: Berdugo Gómez de la Torre), en su FJ 1º que: *El derecho al secreto de las comunicaciones puede considerarse una plasmación singular de la dignidad de la persona y del libre desarrollo de su personalidad, que constituyen el fundamento del orden político y de la paz social* (STC núm. 281/2006, de 9 de octubre y STS núm. 766/2008, de 27 de noviembre), por lo que trasciende de mera garantía de la libertad individual, para constituirse en medio necesario para ejercer otros derechos fundamentales. Por ello la *protección constitucional del secreto de las comunicaciones abarca todos los medios de comunicación conocidos en el momento de aprobarse la norma fundamental, y también los que han ido apareciendo o puedan aparecer en el futuro, no teniendo limitaciones derivadas de los diferentes sistemas técnicos que puedan emplearse* (SSTS núm. 367/2001, de 22 de marzo y núm. 1377/1999, de 8 de febrero). *El derecho al secreto es independiente del contenido de la comunicación, debiendo respetarse, aunque lo comunicado no se integre en el ámbito de la privacidad (SSTC núm. 70/2002, de 3 de abril y núm. 114/1984, de 29 de noviembre). Pero, sin embargo, este derecho no es absoluto, ya que en toda sociedad democrática existen determinados valores que pueden justificar, con las debidas garantías, su limitación* (art. 8º del Convenio Europeo). Entre estos valores *se encuentra la prevención del delito*, que constituye un interés constitucionalmente legítimo y que incluye la investigación y el castigo de los hechos delictivos cometidos, orientándose su punición por fines de prevención general y especial. El propio art 18.3 CE prevé la limitación del derecho al secreto de las comunicaciones mediante resolución judicial (STS núm. 246/1995, de 20 de febrero, entre otras muchas). *En nuestro ordenamiento la principal garantía para la validez constitucional de una intervención telefónica es, por disposición constitucional expresa, la*

exclusividad jurisdiccional de su autorización, lo que acentúa el papel del Juez Instructor como Juez de garantías, ya que lejos de actuar en esta materia con criterio inquisitivo impulsando de oficio la investigación contra un determinado imputado, la Constitución le sitúa en el reforzado y trascendental papel de máxima e imparcial garantía jurisdiccional de los derechos fundamentales de los ciudadanos[19].

En este sentido lo que resulta de importancia vital *es la existencia de un proceso comunicativo que permita desvelar datos de contenido y desarrollo de ese mismo proceso* ya sea telefónico, a través de mensajería o de medios de internet como el correo electrónico, incluso aquellos mensajes que ya fueran leídos, conociendo los datos subjetivos de los participantes, duración, destino o listado de llamadas e interceptación de comunicaciones de terceros ajenos a la investigación. Queda al margen la difusión de grabaciones efectuadas por uno de los partícipes, el acceso policial al listado (agenda) de contactos, las rellamadas efectuadas policialmente a un teléfono que, a su vez, llama insistentemente al del detenido, identificación de una llamada entrante con visionado directo del teléfono o conversaciones que son escuchadas por los agentes con permiso de uno de los interlocutores al activar mecanismos de altavoz o las conversaciones radiofónicas (Circular 2/2019, de 6 de marzo, FGE y Circular 1/2013 FGE sobre pautas en relación con la diligencia de intervención de las comunicaciones telefónicas).

Hay que señalar que la regulación operada por la Ley 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, establece un nuevo y riguroso marco[20] que acaba con una situación

19. La cursiva es del autor.

20. Como indica la STC 99/2021, de 10 de mayo, «Desde este mismo punto de vista, es decir, desde las exigencias de seguridad jurídica y certeza del Derecho, hemos proclamado el principio de legalidad en el marco de la injerencia en el derecho a la intimidad. Así, en la STC 37/1989, afirmamos que lo que la protección de la intimidad reclama es una decisión judicial motivada en una inexcusable previsión

de clara deficiencia legislativa procesal en la materia propia de la interceptación de comunicaciones, procediendo a desarrollar una regulación que resultaba imperiosa (SSTEDH Prado Bugallo contra España de 18 de febrero de 2003, Valenzuela Contreras contra España de 30 de julio de 1998, antes, en todo caso, STEDH Malone contra Reino Unido de 2 de agosto de 1984). En este sentido, la autorización judicial resulta esencial y su planteamiento deriva de la previsión contenida, en cuanto condiciones generales habilitantes, en la LECrim (Título VIII, Capítulo IV arts. 588 bis a)- bis k)), con sujeción a una serie de requisitos que también jurisprudencialmente, y con anterioridad a la reforma, se habían establecido: exclusividad jurisdiccional, uso para determinar el hecho delictivo y su autoría, excepcionalidad, temporalidad, proporcionalidad (delitos graves), especialidad, indicios de responsabilidad penal en el afectado, aplicación de la medida sobre los medios de los presuntos autores, existencia de una investigación penal en curso y resolución motivada con rigor, junto con el control judicial de la medida acordada (STS 1541/2003, de 7 de marzo, de la Sala II (Ponente: Sr. Sánchez Melgar), FJ 1º).

Ahondando en los requisitos exigibles para llevar a cabo la interceptación telefónica (o telemática), ello se traduce en el dictado de un *auto motivado* (art. 588 bis b) en relación con el art. 588 bis a LECrim), LECrim), no mediante providencia (STC 123/2002, de 19 de junio, FJ 7º), en un plazo perentorio desde la solicitud de 24 horas (art. 588 bis c), que podrá acordar de oficio el Juez o a instancia de la Fiscalía o la Policía Judicial —cuyos requisitos analizaremos a renglón seguido—, donde se ponga de

legislativa (fundamento jurídico 7). Con ello, afirmábamos, no solo que la existencia de una previsión legal es inexcusable; *sino que la resolución judicial que autorice la injerencia en la intimidad ha de hallarse fundamentada en la ley, de lo cual se infiere que la ley ha de expresar todos y cada uno de los presupuestos y condiciones de la intervención. Y en términos semejantes nos expresamos en el ámbito específico del derecho al secreto de las comunicaciones, afirmando que la injerencia estatal en dicho secreto ha de estar presidida por el principio de legalidad* (ATC 344/1990 —que invoca la doctrina sentada en la STC 150/1989—, y SSTC 85/1994, FJ 3; 34/1996, FJ 5; 49/1996, FJ 3; 54/1996, FJ 7,y 123/1997, FJ 4), especificando que el respeto a dicho principio requiere, en este caso, «una ley de singular precisión» (STC 49/1996, FJ 3)» (FJ 3º). La cursiva es del autor.

manifiesto la existencia de un hecho delictivo concreto —no un ilícito administrativo— objeto de investigación (*especialidad)*, rechazándose la idea de la prospección (STC 49/1999, de 5 de abril, FJ 8º), de modo que no es posible solicitar medidas para interceptar comunicaciones bajo el pretexto de verificar si hay o no un hecho delictivo susceptible de ser investigado, con lo que la presentación de indicios delictivos para acordar tal medida se presenta como indeclinable[21] (*necesidad*), de manera que sirva para el objetivo propuesto (*idoneidad*) es decir la *razonabilidad* de la medida, e implique el respeto al principio de *proporcionalidad* (SSTC 200/1997, 24 de noviembre, FJ 4º; 166/1999, 27 de septiembre, FJ 8º; 171/1999, 27, de septiembre FJ 8º; 126/2000, 16 de mayo, FJ 8º) de modo que el sacrificio en los derechos fundamentales sea menor que el beneficio que se pretende obtener.

El anterior escenario exige *la existencia de una investigación penal abierta*, con un procedimiento judicial también abierto y en el marco de un hecho delictivo grave que resulta, a los efectos de llevar a cabo la intervención, en delitos dolosos castigados con pena con límite máximo de, al menos, tres años, delitos cometidos en el seno de organizaciones criminales o delitos de terrorismo (art. 579. 1 en relación con el art. 588 ter a LECrim). Hay que descartar la adopción de una medida de interceptación en delitos leves o imprudentes, debiendo tenerse en cuenta la pena en abstracto, subtipo agravado incluido que pudiese ser aplicado siempre que se den indicios de su comisión, su aplicación a supuestos de concurrencia de organizaciones crimina-

21. Señala la STS 822/2022, 18 de octubre de la Sala II (Ponente: Sr. Palomo del Arco) «a) se proporcionan y recogen indicios incipientes que sobrepasan la mera subjetividad e integran un conjunto objetivo de datos que conducen a una sospecha razonable; lógicamente desde su ponderación no disgregada y fragmentada, sino global, que desdice la finalidad prospectiva alegada. *La adopción de esta injerencia requiere que se cuente con indicios suficientes, con "buenas razones"; no que se practiquen todos los posibles medios de averiguación que podían corroborar o no esa base indiciaria*. Postergar las escuchas a la realización de todas las imaginables informaciones que podrían colateralmente coadyuvar al esclarecimiento de los hechos o robustecer los indicios carece de lógica. No es necesaria una a modo de "mini-instrucción" previa judicial que siga a la investigación policial y preceda a la injerencia (a STS núm. 298/2020, de 11 de junio)» (FJ 1º.3. a). La cursiva es del autor.

les en función de su actuación, no del tipo de delito cometido y los delitos de terrorismo donde habrá que hacer una valoración ex ante por parte de la autoridad judicial (Circular 2/2019, 6 de marzo, FGE). A estos se añaden, por la gravedad del medio, «delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la comunicación o servicio de comunicación» (art. 588 ter a in fine LECrim).

Si bien cabe la posible adopción de oficio por el Juez, lo que implica un cierto comportamiento inquisitivo, la petición de una medida invasiva de estas características está sujeta a un procedimiento de solicitud motivado con una serie de requisitos que debe comprender *identificación de hechos con una calificación jurídica, sujetos sobre los que recae*[22] *y fundamento de la medida, con la justificación y motivación oportuna, qué tipo de medida se interesa y sobre qué medio, quién la va a ejecutar policialmente y quién la va a ejecutar en colaboración con la decisión judicial con sujeción a responsabilidad penal* (arts. 556.1, 465.2 y 466.3 CP) *y durante cuánto tiempo* (art. 588 bis b LECrim)[23].

22. Como apunta la Circular 1/2019, de 6 de marzo, FGE «En la resolución judicial que acuerde la medida deberá reflejarse la identidad del afectado, si fuere conocido. No conociéndose la identidad, deberán indicarse los datos de los que se tenga conocimiento y que permitan su individualización (número de teléfono, domicilio, señas de identidad física, apodo o sobrenombre, etc.). La identidad que ha de reflejarse en la resolución es la del afectado por la medida, cuyo derecho se ve limitado, que puede no coincidir con el titular formal del medio sobre el que ésta recaiga (teléfono, ordenador, vehículo en el que se instalen dispositivos, etc.). Los errores padecidos en la identificación subjetiva no tienen por qué viciar la resolución. Es posible adoptar medidas de investigación que afecten directamente a un tercero no investigado con la finalidad de obtener datos relevantes».

23. Como con anterioridad había señalado con precisión la STS 1078/2009, de 5 de noviembre, de la Sala II (Ponente: Sr. Varela Castro), FJ 1.2 «Sobre esa base, el Tribunal ha considerado insuficiente la mera afirmación de la existencia de una investigación previa, sin especificar en qué consiste, ni cuál ha sido su resultado por muy provisional que éste pueda ser, *afirmando también que la concreción del delito que se investiga, las personas a investigar, los teléfonos a intervenir y el plazo de intervención no pueden suplir la carencia fundamental de la expresión de los elementos objetivos indiciarios que pudieran servir de soporte a la investigación, ni la falta de esos indispensables datos pueda ser justificada a posteriori por el éxito de la investigación misma* (SSTC 299/2000, de 11 de diciembre, FJ 5; 138/2001, de

A estos elementos configuradores de la fisonomía de la solicitud que se dirige al Juez hay que incluir otros —atendiendo al Capítulo V— como «*a) la identificación del número de abonado, del terminal o de la etiqueta técnica, b) la identificación de la conexión objeto de la intervención o c) los datos necesarios para identificar el medio de telecomunicación de que se trate*» junto con «*a) El registro y la grabación del contenido de la comunicación, con indicación de la forma o tipo de comunicaciones a las que afecta. b) El conocimiento de su origen o destino, en el momento en el que la comunicación se realiza. c) La localización geográfica del origen o destino de la comunicación. d) El conocimiento de otros datos de tráfico asociados o no asociados, pero de valor añadido a la comunicación*» (art. 588 ter d).1 y 2 LECrim). En este sentido, la solicitud deberá precisar si lo que pretende es la intervención de la comunicación oral o también la mensajería que pueda generarse (SMS, MMS.), sobre los datos electrónicos de tráfico o asociados (identidades internacionales del móvil o del abonado móvil, direcciones, geolocalización, datos de facturación...).

La medida de interceptación de comunicaciones cuando es solicitada policialmente, requiere del informe del Ministerio Fiscal (art. 588 bis c) LECrim) lo que implica acentuar las medidas de garantía al tratarse de un órgano dictaminador en materia

18 de junio, FJ 4; 167/2002, de 18 de septiembre, FJ 3; 165/2005, de 20 de junio, FJ 5; 259/2005, de 24 de octubre, FJ 4; 253/2006, de 11 de septiembre, FJ 4). También ha destacado el Tribunal que "la idea de dato objetivo indiciario tiene que ver con la fuente de conocimiento del presunto delito, cuya existencia puede ser conocida a través de ella. De ahí que el hecho en que el presunto delito puede consistir no pueda servir como fuente de conocimiento de su existencia. La fuente del conocimiento y el hecho conocido no pueden ser la misma cosa" (STC 299/2000, de 11 de diciembre, FJ 5; citándola STC 138/2001, de 18 de junio, FJ 4). *Asimismo, debe determinarse con precisión el número o números de teléfono que deben ser intervenidos, el tiempo de duración de la intervención, quién ha de llevarla a cabo y los períodos en los que deba darse cuenta al Juez de sus resultados a los efectos de que éste controle su ejecución* (por todas SSTC 49/1996 , de 26 de marzo, FJ 3: 49/1999, de 5 de abril, FJ 7 y siguientes; 167/2002, de 18 de septiembre, FJ 2; STC 184/2003, de 23 de octubre, FJ 9; 259/2005, de 24 de octubre, FJ 2; 136/2006, de 8 de mayo, FJ 4)». La cursiva es del autor.

de limitación de derechos fundamentales como se prevé en el art. 3.3 del Estatuto Orgánico del Ministerio Fiscal (en adelante EOMF). Por tanto, y esto no es una cuestión menor, existe un órgano que ante la petición policial, no si lo solicita el propio acusador público, se encarga de analizar la regularidad de la petición al existir un subyacente interés público que motiva tal defensa (STC 65/1983, de 21 de julio, FJ 4º). Existiendo un doble control, por tanto, a nivel judicial, ante la solicitud, que se escenifica en la resolución que en su caso dicte, pero con previo dictamen de Fiscalía que resulta ya un primer filtro[24]. Hay que significar que un sujeto/s está potencialmente afectado/s por la investigación que se desarrolla secretamente y cuyos derechos fundamentales se pueden ver vulnerados, justificadamente, con lo que se procede a un riguroso control *ex ante* por dos órganos que se guían bajo principios de imparcialidad y objetividad, con lo que se acentúa el manto protector.

En todo caso, no podemos olvidar que los investigadores policiales, al amparo de la LECrim, pueden acceder por propia iniciativa a una *dirección IP abierta* (art. 588 ter k), proceder a la *captación del IMSI e IMEI de un teléfono* (art. 588 ter l.1), a *la identificación de titulares o terminales o dispositivos de conectividad* (art. 588 ter m) u *ordenar la conservación de datos* (art. 588 octíes) junto con la *observación directa policial de los denominados chats y foros en abierto*.

Hay un control judicial inicial, como antes señalamos, cuando, de ordinario, policialmente se le presenta una petición de interceptación. Sin embargo, ese control se mantiene sostenido en el tiempo. En primer lugar, por la *duración limitada de la medida* que se fija en un máximo absoluto de dieciocho meses (art. 588 ter g LECrim), por plazos prorrogables de tres meses —aunque es posible acordar por plazos más cortos— lo que im-

24. Como apuntaba la Circular 1/2013. FGE «En caso de incumplimiento o de un cumplimiento no satisfactorio de la exigencia legal de aportación de indicios es improcedente denegar sin más la diligencia solicitada por la Policía. Los Sres. Fiscales promoverán que por el Juez de Instrucción se oficie a la Policía a fin de que proceda a una ampliación de los datos».

pide duración de la intervención invasiva *sine die* en su dimensión temporal.

En segundo lugar, el *control se hace desde la autorización judicial* y «El cómputo, además, deberá hacerse en relación con cada investigado cuyo derecho fundamental se vea limitado, sin que sea procedente un cómputo total para todo el procedimiento o un cómputo para cada concreto medio de comunicación intervenido. Así, por ejemplo, el cambio de terminal de teléfono móvil que realice un investigado no debe motivar que se inicie de nuevo el cómputo del plazo, del mismo modo que, si se cesa temporalmente en la medida para después reanudarla, el cómputo no deberá iniciarse de nuevo, sino que continuará el anterior. Por el contrario, si se inicia una nueva investigación sobre el mismo sujeto por hechos diferentes a los que motivaron la intervención de sus comunicaciones, dando lugar a un nuevo procedimiento, deberá reiniciarse el cómputo del plazo de los dieciocho meses, al tener que renovarse también completamente la motivación y fundamentación de la resolución judicial que autorice la medida» (*Vid.* Circular 2/2019, 6 de marzo, FGE).

El tercer lugar, a la vista del desarrollo de la investigación, el Juez decidirá la continuación de las intervenciones con lo que es preciso justificar la razonabilidad del mantenimiento de las escuchas o interceptaciones, con lo que la Policía Judicial debe informar del desarrollo y resultados, una vez finalizada la medida incluso, poniendo a disposición de la autoridad judicial los soportes digitales con las transcripciones y grabaciones indicando origen y destino «mediante un sistema de sellado o firma electrónica avanzado o sistema de adveración suficientemente fiable, la autenticidad e integridad de la información volcada desde el ordenador central a los soportes digitales en que las comunicaciones hubieran sido grabadas» (art. 588 ter f, LECrim).

Es claramente perceptible, a la vista de estas líneas, el riguroso sistema que motiva la interceptación de comunicaciones que precisa de una investigación policial precisa y relativamente sólida, un control judicial exigente *ab initio,* y con posterioridad, y una supervisión rigurosa de la acusación pública teniendo presente que la interceptación de las comunicaciones telefónicas se convierte en una pieza fundamental para llevar a buen puerto las

causas penales de cierta complejidad y en atención a la capacidad organizativa y de medios de los grupos y sujetos criminales. El sentido de las grabaciones propiamente dichas —las transcripciones no lo son— es servir de prueba, introduciéndola en el plenario para enervar la presunción de inocencia (art. 24.2 CE) y servir como elemento de cargo que puede fundar una condena, de modo que son aquellas las que tienen que estar a disposición del investigado en todo momento, y no la transcripción, que es auxiliar o accesoria de las grabaciones.

3 La seguridad nacional: intento de conceptuación

Definir el término «seguridad nacional» no es tarea sencilla. Lo que está claro es que actúa en un sentido distinto que el anterior de «seguridad pública» motivando actuaciones diferentes para su satisfacción. En este sentido, no han faltado textos internacionales, que han intentado definirlo, pero planteando que su uso no puede ser con propósito represivo[25] con lo que,

25. Por ejemplo, los *Principios de Siracusa sobre las disposiciones de limitación y derogación del Pacto Internacional de los Derechos Civiles y Políticos* de la ONU de 24 de agosto de 1984 —elaborados para confrontar situaciones de excepción en cuanto documento interpretativo— que ha definido «Seguridad Nacional» bajo los siguientes propósitos «19. Solamente se puede invocar la seguridad nacional para justificar las medidas que limiten ciertos derechos cuando estas medidas se adopten para proteger la existencia de la nación, su integridad territorial o su independencia política contra la fuerza o la amenaza de la fuerza. 20. No se podrá invocar la seguridad nacional como motivo para imponer limitaciones o impedir amenazas puramente locales o relativamente aisladas contra el orden público. 21. No se podrá utilizar la seguridad nacional como pretexto para imponer limitaciones vagas o arbitrarias y solamente se podrá invocar cuando existan garantías adecuadas y recursos eficaces contra los abusos. 22. La violación sistemática de los derechos humanos socava la seguridad nacional y puede poner en peligro la paz y la seguridad internacionales. Un Estado que sea responsable de una violación de este tipo no podrá invocar la seguridad nacional para justificar las medidas encaminadas a suprimir la oposición a dicha violación o a imponer prácticas represivas contra su población». *El Informe de la Relatora Especial sobre la promoción y protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo sobre el obstáculo para los derechos*

sin adentrarse en profundidad en la cuestión, da la sensación de llamar la atención sobre una herramienta que puede ser usada como coartada para eludir controles y garantías. Doctrinalmente, tampoco han faltado intentos de delimitar, con cierta claridad, a qué nos estamos refiriendo aunque más bien inciden en la gestión de «nuevas amenazas» que influyen en el uso de los recursos públicos o como presupuesto de coordinación administrativa de naturaleza trasversal (*Cfr.* Orgis, 2011; Fernández Alles, 2020; Revenga y Fernández, 2020, pp. 390-391), concluyendo que la seguridad nacional «es la situación en la que el normal desarrollo de la vida de la nación está protegido contra riesgos, peligros o amenazas exteriores e interiores y permite al país defender sus intereses nacionales, cumplir con sus compromisos internacionales y contribuir a la paz y estabilidad internacional» (*Vid.* Ballesteros, 2016, p. 63).

Entre nosotros, legislativamente con su promulgación, la Ley de Seguridad Nacional 36/2015, de 28 de septiembre (en adelante LSN), en su exposición de motivos (en adelante EM), señala que: «En este sentido, la Seguridad Nacional se entiende como la acción del Estado dirigida a proteger la libertad y el bienestar de sus ciudadanos, a garantizar la defensa de España y sus principios y valores constitucionales, así como a contribuir junto a nuestros socios y aliados a la seguridad internacional en cumplimiento de los compromisos asumidos; concepto que, hasta la fecha, no había sido objeto de una regulación normativa integral», concepto que reitera en su art. 3.

En suma, parece aunar el concepto diversos elementos que pivotan en torno a ideas como la «seguridad pública», la «defensa nacional» y la «política exterior y diplomática», que la STC 184/2016, de 13 de noviembre, ha encajado señalando que «*Por otra parte, siendo clara la competencia estatal, tanto en materia de*

humanos que suponen los estados de emergencia en el contexto de la lucha contra el terrorismo que fue presentado ante Consejo de Derechos Humanos de la ONU (37 período de sesiones), 26 de febrero a 23 de marzo de 2018, donde se establece la relación entre terrorismo y seguridad nacional haciendo una crítica a las situaciones de emergencia como herramienta que sirve para vulnerar derechos de la ciudadanía,

defensa como en materia de seguridad pública, no tendría sentido que, en un ámbito como la seguridad nacional, tan estrechamente vinculado a ambas, hasta el punto de identificarse sus fines y objetivos y los bienes jurídicos protegidos en la forma indicada, la competencia estatal pasara a ser puramente residual. En definitiva, la seguridad nacional no es una competencia nueva, sino que se integra en las competencias estatales de defensa y seguridad pública» (FJ 3º). Sin olvidar la necesaria protección que subyace del «interés nacional» y el respeto al «orden público» (STS 367/2021, de 17 de marzo, de la Sala III, FJ 2º, Ponente: Herrero Pina).

En segundo lugar, si el tradicional riesgo que confronta la seguridad pública es el delito y las formas graves de criminalidad[26], es cierto que esto también cabe dentro del concepto de seguridad nacional, pero no exclusivamente, por cuanto los riesgos pueden venir derivados de otras vertientes como la climática[27], sanitaria y económica pudiendo ambas, como ha evidenciado la pandemia de la COVID-19, estar estrechamente ligadas[28] sin olvi-

26. *Vid.* la Estrategia Nacional Contra el Crimen Organizado y la Delincuencia Grave (2019-2023) que sitúa al terrorismo y al crimen organizado como «dos de las mayores amenazas a la Seguridad Nacional cuya confluencia puede llevar a un escenario crítico a nivel mundial, así como reducir la interacción y retroalimentación mutua entre el crimen organizado y otras amenazas como son los conflictos armados, el espionaje y la proliferación de armas de destrucción masiva».
27. Algo que ya se evidencia en la Estrategia de Seguridad Nacional (2017) «El cambio climático es también una pieza clave de la seguridad con importantes repercusiones políticas, económicas y sociales en el corto y largo plazo. Factores relativos al cambio climático, junto con la degradación de los recursos hídricos, tienen un componente de seguridad innegable». Y que reitera la Estrategia de Seguridad Nacional (2021) cuando afirma que «En particular, los efectos del cambio climático pueden agudizar crisis económicas, políticas y geopolíticas derivadas de la escasez alimentaria e hídrica en muchas partes del mundo. Como consecuencia, podrían agravarse las situaciones de migraciones masivas, inestabilidad regional e incluso producirse nuevos conflictos armados. Asimismo, el calentamiento global tendrá repercusiones directas en España, pues provocará fenómenos meteorológicos adversos más extremos y frecuentes, sequías, olas de calor, inundaciones, escasez de agua y perjuicios para la biodiversidad».
28 Para la Estrategia de Seguridad Nacional (2021) «*La pandemia de la COVID-19 ha generado el mayor desplome del Producto Interior Bruto desde la Segunda Guerra Mundial*, lo que ha causado una nueva crisis económica con consecuencias aún inciertas en clave social. Aunque el impacto económico sea fundamentalmente

dar los conflictos y tensiones externas, la ciberseguridad[29] o ataques a infraestructuras críticas[30] o las actividades de espionaje. Por tanto, la «seguridad nacional» *es un concepto trasversal, dinámico y variable en función de las circunstancias, amenazas y exigencias que en cada momento se presenten*, y del que la «seguridad pública» forma parte como integrante de un todo. Esto nos lleva a determinar que su configuración no puede tener una definición estática, por cuanto las variables que entran en juego son diversas, con lo que codificarlo en términos estrictos es, cuando menos, una tarea compleja con arreglo a los diferentes escenarios implicados y ello por cuanto «*The threats of yesterday were predominantly of the symmetric type: static, predictable, homogenous, hierarchical, rigid and resistant to change. The new threats are more of the asymmetric type: dynamic, less predictable, networked, fluid, self-organising and constantly adapting and evolving*» (*Vid.* Schreier, 2006, p. 6).

Es esencial destacar que la «seguridad nacional» supone *un marco de protección de derechos*, es decir, es un contrapeso ante una situación de amenaza o riesgo a aquellos, pero es preciso tener en cuenta que la propia «seguridad nacional» es un factor que justifica la limitación —invasión— de alguno de los derechos fundamentales (*Cfr.* Aba, 2020, p. 228). y ello implica, igualmente, *establecer mecanismos de garantía* destinados a evitar que una conceptuación laxa y extensiva sirva, precisamente, como argumento para una vulneración sistemática e incontrolada[31].

transitorio y esté seguido de tasas de crecimiento relativamente elevadas, ha causado un *aumento de la situación de inestabilidad y desigualdad económica*». La cursiva es del autor.

29. A este desafío responde el reciente Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

30. Definida por la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas en su art. 2 e como «las infraestructuras estratégicas cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales».

31. Es decir, delimitación de amenazas que sirvan para justificar conductas invasivas. Tal y como puso de manifiesto la STEDH Big Brother Watch and Others v. the United Kingdom de 25 de mayo de 2021 en relación a la posibilidad de llevar a

Por otro lado, la defensa de la «seguridad nacional» *no es, de ordinario, una actividad policial* pese a que la criminalidad organizada grave y el terrorismo implican amenazas frente a ella. Y esto se fundamenta en que su efectividad no busca trascendencia procesal, es decir, no se trata de identificar necesariamente a un responsable/s de un hecho delictivo y ponerlo a disposición de las autoridades judiciales o del Ministerio Público, bajo un marco reglado, donde existen derechos de parte y una situación de contradicción, *sino que se trata de recopilar información para una adecuada toma de decisiones a nivel ejecutivo-político (inteligencia estratégica)*, para que esa «acción de gobierno» pueda elegir las mejores opciones, sean del tipo que sean. Y ello se consigue mediante la actividad de espionaje, que debe desarrollar el servicio de inteligencia, con una actividad encubierta que puede motivar intromisiones en el marco de determinados derechos fundamentales, entre ellos, el referido al control de las comunicaciones telefónicas y donde las categorías procesales, pese a la posible existencia de actividades invasivas, se presentan vacías en lo que respecta a los afectados pues no hay propiamente «investigados», ni «encausados», ni «acusados», ni derechos que les sean correlativos, generándose un caudal de «inteligencia estratégica» que, al contrario que la «inteligencia criminal», ni tiene una cronología precisa para su uso (puede almacenarse para un análisis o empleo ulterior) ni un fin preciso, desde un principio, en el que invertir su empleo (no busca deducir responsabilidades y procurar, en su caso, condenas).

Sin embargo, aunque sobre la anterior cuestión me detendré más profundamente en el siguiente epígrafe, lo que queda claro es que hacer frente a los desafíos que la «seguridad nacional» plantea supone una actividad previa de recolección de datos e informaciones que pueden implicar que por los servicios de in-

---

cabo, bajo el presupuesto de la seguridad nacional, interceptaciones «18. First, in contrast to targeted interception in crime prevention, bulk interception is largely used for purposes of national security. *It is difficult to see why one should not expect the domestic legislation to clearly define the possible national security threats and the circumstances in which those threats may trigger bulk interception*». La cursiva es el autor.

teligencia —no policiales— se puedan exigir vulneraciones de derechos fundamentales, lo que nos lleva a la cuestión de cómo se garantizan en este marco porque no estamos ante una situación procesal[32].

3.1 Comunidad de inteligencia, CNI y persecución delictiva

Nuestro país dispone de un modelo policial plural en el que conviven cuerpos de diferente naturaleza (estatal y autonómica): Policía Nacional, Guardia Civil, Servicio de Vigilancia Aduanera, y Policías Autonómicas con modelos integrales (STC 184/2016, de 3 noviembre, FJ 4º) que proceden a la recopilación de inteligencia criminal con sus servicios de información[33] y como órgano cen-

32. Como resulta del STEDH Weber y Saravia contra Alemania, de 29 de junio, señala que «106. The Court reiterates that, when balancing the interest of the respondent State in protecting its national security through secret surveillance measures against the seriousness of the interference with an applicant's right to respect for his or her private life, *it has consistently recognized that the national authorities enjoy a fairly wide margin of appreciation in choosing the means for achieving the legitimate aim of protecting national security* (see, inter alia, Klass and Others, cited above, § 49; Leander, cited above, § 59; and Malone, cited above, § 81). Nevertheless, in view of the risk that a system of secret surveillance for the protection of *national security may undermine or even destroy democracy under the cloak of defending it, the Court must be satisfied that there exist adequate and effective guarantees against abuse* (see Klass and Others, cited above, §§ 49-50; Leander, cited above, § 60; Camenzind v. Switzerland, 16 December 1997, § 45, Reports 1997-VIII; and Lambert, cited above, § 31). This assessment depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorize, carry out and supervise them, and the kind of remedy provided by the national law (see Klass and Others, cited above, § 50)». La cursiva es del autor.

33. Así, en el ejercicio de la función de «Policía Judicial» (art. 282 LECrim), y con una dependencia orgánica del Gobierno y funcional de Jueces y Fiscales (art. 126 CE), enmarcada en la ya señalada «Seguridad Publica», se nutre del trabajo operativo y recopilación de información por la Comisaria General de Información de la Policía Nacional (art. 3 a) RD 734/2020, de 4 de agosto) y Jefatura de Información de la Guardia Civil (art. 4.5 b) RD 734/2020, de 4 de agosto y RD 146/2021, 9 de marzo, art. 2) , del Servicio de Vigilancia Aduanera (RD 319/1982, de 12 de febrero y el Acuerdo no jurisdiccional de la Sala II del Tribunal Supremo, de 14 de noviembre de

tral, que actúa de puente, el Centro de Inteligencia para el Terrorismo y Crimen Organizado (en adelante CITCO), que se encuentra incardinado en el Ministerio del Interior, y que se encarga de «Recibir, integrar y analizar informaciones y análisis operativos que sean relevantes o necesarios para elaborar la correspondiente *inteligencia criminal estratégica* y de prospectiva, tanto en su proyección nacional como internacional, integrando y canalizando, de manera coordinada, a las Fuerzas y Cuerpos de Seguridad del Estado y, en su caso, a otros organismos que se determine, toda la información operativa que reciba o capte.» (art. 2.3 del RD 734/2020, de 4 de agosto, de estructura del Ministerio de Interior, en relación con el art. 2.3 del RD 146/2021, de 9 de marzo)[34].

Frente a la anterior «comunidad policial de inteligencia», nos encontramos con el Centro Nacional de Inteligencia (en adelante CNI) que se encarga de recopilar inteligencia en el ámbito de la «seguridad nacional». Es el órgano sucesor del Centro Superior de Información de la Defensa (en adelante CESID)[35] con un marco

2003). En relación a las Policías Autonómica, tenemos a Cataluña (art. 109 Decreto 57/2023 de 21 de marzo que establece la Comisaria General de Información), Navarra (Orden Foral 174/2016 de 11 de octubre, art. 1 y ss, que hace depender del Área de Investigación una unidad de información) y el País Vasco (Orden de 18 de noviembre de 2021 con la Oficina Central de Inteligencia).

34. La cursiva es del autor.

35. El surgimiento del CNI resulta de su Ley reguladora 11/2002, de 6 de mayo, que en su EM manifiesta una necesidad clara «La sociedad española demanda unos servicios de inteligencia eficaces, especializados y modernos, capaces de afrontar los nuevos retos del actual escenario nacional e internacional, regidos por los principios de control y pleno sometimiento al ordenamiento jurídico». En un resumen que se realiza por el Consejo de Estado en su dictamen de 3033/2011, de 25 de octubre, resulta el siguiente iter legislativo en la configuración de los que hoy consideramos nuestros servicios secretos «*El Centro Superior de Información de la Defensa (CESID) fue creado por Real Decreto 1558/1977, de 4 de julio. En virtud de dicho Real Decreto se dio nueva estructura a determinados órganos de la Administración Central del Estado, creándose el Ministerio de Defensa y el propio Centro Superior de Información de la Defensa bajo la dependencia directa del titular del Departamento (artículo 2.5).Por Real Decreto de 2 de noviembre, 2723/1977, se estableció que el CESID, órgano que sustituyó a los anteriores servicios de información, —Servicio Central de Información dependiente de la Presidencia del Gobierno (CESED) y Servicio de Información del Alto Estado Mayor (SIAM)—, sería el órgano encargado de obtener, evaluar, interpretar y facilitar al Ministro de Defensa «cuanta información sea*

legal muy limitado, en concreto la Ley 11/2002, de 6 de mayo, que es la organizativa y la Ley 2/2002, de 6 de mayo, sobre su control judicial, junto con RD 240/13, de 5 de abril, sobre el Estatuto de sus miembros. Es un órgano singular de la Administración General del Estado[36], cuya incardinación ha variado si bien en la actualidad se encuentra adscrito al Ministerio de Defensa (RD 372/2020, 18 de febrero, art. 1) pero que no se encarga propiamente de la inteligencia militar (competencia del CIFAS ex. art. 12

necesaria o interese a la Defensa Nacional, atendiendo prioritariamente las necesidades de la Junta de Jefes de Estado Mayor». Un posterior Real Decreto 726/1981, de 27 de marzo, redefinió las funciones del CESID configurándolo como el órgano encargado de obtener, evaluar, interpretar y facilitar al titular del Departamento de Defensa, no sólo la información que fuese necesaria o interese a la Defensa Nacional, sino también lo que interese al cumplimiento de las misiones que a las Fuerzas Armadas encomienda el artículo octavo de la Constitución. La Orden Ministerial 135/1982, de 30 de septiembre, del Ministerio de Defensa, estableció la estructura y misiones del Centro Superior de Información de la Defensa; Orden Ministerial a la que se remitía el artículo 17.2 del Real Decreto 135/1984, de 25 de enero, de reestructuración del Ministerio de Defensa y, más tarde el art. 83.2 del Real Decreto 1/1987, de 1 de enero, por el que se estableció la estructura básica de dicho Ministerio; Real Decreto que asimismo se remite a la Orden 135/1984 en cuanto a la estructura interna, relaciones, misiones y competencias del Centro. Con posterioridad a las indicadas disposiciones, y en cumplimiento de la disposición final octava de la Ley Orgánica 17/1989, de 19 de julio, reguladora del Régimen del Personal Militar Profesional, se aprobó el Real Decreto 1324/1995, de 28 de julio, que constituye el Estatuto del Personal del Centro, disposición de importancia significativa porque estableció un único régimen jurídico para todo el personal del Centro, cualquiera que fuese su procedencia, sometiendo a sus integrantes a los mismos derechos y obligaciones».

36. Como ha establecido la SAN 2632/2009, 27 de mayo, Sala de lo Contencioso (Ponente: Sr. Gil Ibáñez) «Esta Sección, con motivo de pronunciamientos relativos a miembros del Centro Superior de Información de la Defensa, *ha reconocido a dicho Centro un carácter y una naturaleza singular, que también se proyecta sobre el personal que en él presta sus servicios y las normas estatutarias que le regulan* (Sentencias de 22 de julio —recursos 1.775/1996 y 1.897/1996— y de 31 de julio —recurso 1.888/1996— de 1999 o de 21 de febrero de 2002 —recurso 102/2001—), idea que es perfectamente trasladable al actual Centro Nacional de Inteligencia, cuyo personal se sigue rigiendo, en tanto no se produzca el desarrollo reglamentario de la Ley 11/2002 y se apruebe un estatuto propio, por el Estatuto del Personal del Centro Superior de la Defensa, aprobado por el Real Decreto 1.324/1995, de 28 de julio (disposición transitoria única de la Ley 11/2002), que conjuga aspectos de la función pública militar y civil, matizándolos por la singularidad de dicho organismo» (FJ 1º). La cursiva es del autor.

RD 521/2020, de 19 de mayo, regulador de la organización básica de las Fuerzas Armadas), siendo responsable ante el Presidente del Gobierno de facilitarle información en campos muy variados, todos ellos correlacionados con la seguridad nacional, para la adopción de las mejores decisiones y en campos muy diversos[37]. De lo que no se encarga el CNI es de perseguir hechos delictivos, algo que ha dejado claro la STS 1140/2010, de 29 de diciembre, de la Sala II (Ponente: Sr. Berdugo Gómez de la Torre): «*Pues bien es algo conocido que todos los Gobiernos disponen de Servicios de inteligencia que pretenden obtener información relevante con objeto de garantizar su seguridad interior y exterior.* En nuestro país se ha regulado tal control mediante LO. 11/2002 de 6 mayo, reguladora del control judicial del Centro Nacional de Inteligencia, en aquellas actividades que afecten a los derechos fundamentales reconocidos en los arts. 18.2 y 3 CE. Respecto a este control judicial de los Servicios de Inteligencia, hay que distinguir, *ante todo, entre la investigación de un delito y la investigación de inteligencia. La primera —como ya se ha explicitado— se realiza con objeto de conseguir pruebas que acrediten la comisión de un delito. La investigación de inteligencia pretende facilitar al Presidente del Gobierno*

37. Conforme el art. 4 de la Ley 11/2002 es competencia del CNI «a) Obtener, evaluar e interpretar información y difundir la inteligencia necesaria para proteger y promover los intereses políticos, económicos, industriales, comerciales y estratégicos de España, pudiendo actuar dentro o fuera del territorio nacional. b) Prevenir, detectar y posibilitar la neutralización de aquellas actividades de servicios extranjeros, grupos o personas que pongan en riesgo, amenacen o atenten contra el ordenamiento constitucional, los derechos y libertades de los ciudadanos españoles, la soberanía, integridad y seguridad del Estado, la estabilidad de sus instituciones, los intereses económicos nacionales y el bienestar de la población. c) Promover las relaciones de cooperación y colaboración con servicios de inteligencia de otros países o de Organismos internacionales, para el mejor cumplimiento de sus objetivos. d) Obtener, evaluar e interpretar el tráfico de señales de carácter estratégico, para el cumplimiento de los objetivos de inteligencia señalados al Centro. e) Coordinar la acción de los diferentes organismos de la Administración que utilicen medios o procedimientos de cifra, garantizar la seguridad de las tecnologías de la información en ese ámbito, informar sobre la adquisición coordinada de material criptológico y formar al personal, propio o de otros servicios de la Administración, especialista en este campo para asegurar el adecuado cumplimiento de las misiones del Centro. f) Velar por el cumplimiento de la normativa relativa a la protección de la información clasificada. g) Garantizar la seguridad y protección de sus propias instalaciones, información y medios materiales y personales».

y al Gobierno de la Nación, las informaciones, análisis, estudios o propuestas, que permitan prevenir y evitar cualquier peligro, amenaza o agresión contra la independencia o integridad territorial de España, los intereses nacionales y la estabilidad del Estado de Derecho y sus instituciones (art. 1 Ley 11/2002). Para ello el Gobierno determina y aprueba anualmente los objetivos del Centro Nacional de Inteligencia, mediante una Directiva que tendrá carácter secreto (art. 3 de la Ley). *Por tanto, la función legal de este Servicio no es la investigación de delitos concretos, sin perjuicio de que si en el curso de sus labores averiguan o tienen indicios de acciones delictivas lo pongan en conocimiento de los órganos policiales y judiciales competentes, pero —se insiste— su actividad no va encaminada directamente al descubrimiento de delitos, ni tiene como condicionante la previa comisión de alguno*» (FJ 9º)[38].

La inteligencia, por tanto, que se recopila por el CNI no va destinada a la indagación penal sin perjuicio que el ámbito de sus actividades comprende la delincuencia grave y el terrorismo, en cuanto factores de desestabilización, que afectan a la seguridad nacional, existiendo ciertos puntos de coincidencia con las fuerzas policiales (STS 5277/2011, de 22 de julio, Sala III (Ponente: Sr. Herrero Pina), FJ 3º). La cuestión es qué ocurre con la obtención de las informaciones, muchas de las cuales se llevan a cabo a través de la interceptación de comunicaciones telefónicas y se confronta con el art. 18.3 CE, cuestión que en el caso de los servicios de inteligencia como el CNI no se encontraba regulado y que podía motivar dificultades en el trabajo de los agentes ante la situación ayuna de legislación, antes de la reforma de 2002, en la que se encontraban a la hora de interceptar teléfonos u otros medios de transmisión.

La necesidad de limitar los derechos fundamentales en el ejercicio de actividades de espionaje se planteaba como un imponderable, sin embargo, había que correlacionarla con una actividad encubierta en la que la persona/s afectadas no podían, ni tenían conocimiento ulterior, por cuanto el secretismo era (y es), la clave de toda su actuación. Y ello, en claro contraste con la obten-

38. La cursiva es del autor.

ción por la comunidad de inteligencia policial de información, que se canaliza en el marco del proceso penal, bajo un control judicial inicial y ulteriormente. Y dicha información puede transformarse en prueba en el marco del juicio oral y servir para obtener un pronunciamiento condenatorio, de ahí el rigorismo en el examen de la solicitud de una concesión de naturaleza invasiva. De modo que había que arbitrar un sistema que permitiese trabajar autorizadamente a los agentes de inteligencia existiendo una relativa supervisión judicial de su actividad, pero que no implicase un corsé que les hiciese perder operatividad, sin que se produzca el desarrollo de sus funciones en el marco del proceso penal, lo que añade indiscutible peculiaridad a su sistema[39].

3.2 El control judicial de operaciones de inteligencia del CNI

Como antes se puso de manifiesto la necesidad de un control sobre la actividad de los servicios secretos implicaba establecer un tipo de garantía judicial[40] —sin perjuicio del control parla-

39. Como apuntaba el CONSEJO DE ESTADO en su dictamen 3075/2001, de 15 de noviembre, a propósito de la Anteproyecto de Ley Orgánica reguladora del control judicial del Centro Nacional de Inteligencia «El anteproyecto de Ley sometido a consulta tiene por objeto establecer un régimen jurídico que permita conciliar la efectividad de derechos fundamentales como son la inviolabilidad del domicilio y el secreto de las comunicaciones, garantizadas, respectivamente, por lo dispuesto en los números 2 y 3 del artículo 18 de la Constitución, con las exigencias propias de la seguridad nacional y la defensa del Estado, que también son cometidos propios que se imponen en una sociedad democrática al Estado de Derecho. Finalidad evidentemente loable, *sin que quepa desconocer las dificultades que entraña la intervención de un órgano de procedencia judicial, pero al margen de un procedimiento jurisdiccional en trámite o por tramitar. Ello obliga, sin mengua de las peculiaridades de las actividades del Centro Nacional de Inteligencia, a extremar el respeto a la tutela judicial efectiva*». La cursiva es del autor.

40. Como indicó la Circular 1/2013 de la FGE «De acuerdo con una consolidada doctrina jurisprudencial, la única solución posible prevista en el art. 18.3 CE es la plena jurisdiccionalidad de la medida, conclusión que ha tenido derivaciones tanto a través de la promulgación de la Ley Orgánica 2/2002, de 6 de mayo, relativa al Control Judicial Previo del Centro Nacional de Inteligencia, complementaria de la Ley 11/2002, de 7 de mayo, con objeto de posibilitar y asegurar la jurisdiccionalidad

mentario o gubernativo— en sus actividades, dictándose para ello la Ley 2/2002, de 6 de mayo, que en un único artículo, impactando con su derecho transitorio en la Ley Orgánica del Poder Judicial 6/1985, de 1 de julio, (LOPJ, en su arts. 125, 127, 135 e introduce el art. 342 bis en el mismo texto), decide concentrar en un Juez del Tribunal Supremo (Sala de lo Penal o de lo Contencioso-Administrativo) las funciones de concesión y control en cuanto a las actividades del CNI que impliquen colisión con la *inviolabilidad domiciliaria* (art. 18.2 CE) y la *interceptación de comunicaciones* (art. 18.3 CE). Es, en definitiva, quien habilita para la adopción de medidas limitativas de derechos fundamentales por parte de los servicios secretos y que le son solicitadas por parte del Secretario de Estado-Director del CNI (en adelante SED) en una relación única entre ambos que no tiene paragón en el seno de nuestra administración, configurando un procedimiento que no puede, por menos, que calificarse de especial[41].

Hay que señalar que el Juez que se encarga de controlar la solicitud del CNI t*iene un mandato temporal de cinco años* (art. 342 bis LOPJ) *que coincide con el mandato del SED* como prevé el art. 9.1 de la Ley 11/2002, de 6 de mayo, que regula organizativamente nuestro servicio de inteligencia. El requisito que tiene que cumplir es ser Magistrado del TS con al menos tres años de servicios en la categoría (art. 342 bis LOPJ), siendo propuesto para su nombramiento por el Pleno del Consejo General del Po-

de la intervención de las comunicaciones realizadas a instancias del CNI, y en la Ley 25/2007, de Conservación de Datos Relativos a las Comunicaciones Electrónicas, que ha reservado al Juez ordinario la competencia para la concesión de autorizaciones para el acceso a este tipo de datos».

41. Ha señalado la STS 1094/2010, 10 de diciembre, de la Sala II (Ponente: Sr. Marchena Gómez) en FJ 2.A: «Es cierto que su naturaleza es objeto de controversia, probablemente alentada por el hecho de que se haya optado por un modelo de control judicial residenciado, no en un órgano jurisdiccional, sino en un Magistrado al que se atribuye una función previa de fiscalización a partir de un expediente (art. 117.4 de la CE) que *participa de algunas de las características del acto de jurisdicción voluntaria descrito en el art. 1811 de la LEC*. La exclusión de cualquier posibilidad impugnativa de la resolución habilitante y, sobre todo, la ausencia de un seguimiento ulterior de lo actuado a partir de la autorización, añaden mayores dosis de especialidad al régimen jurídico dibujado por el legislador español». La cursiva es del autor.

der Judicial (art. 127. 4 LOPJ). Es preciso señalar que nuestro modelo es bastante original en cuanto al control de operaciones de inteligencia al concentrar la responsabilidad en un juez único al que se «extrae» de su sala para el cumplimiento de esta función[42], constituyendo una centralización de toda solicitud procedente de nuestro servicio secreto con independencia del lugar geográfico en el que surta efecto o se ejecute.

Llama la poderosamente la atención que, pese a no encontrarnos ante un proceso penal, se establezca la presencia de un Magistrado de la Sala II, sin que pueda calificarse a la autoridad judicial interviniente como una suerte de Juez Instructor, algo que la propia jurisprudencia ha señalado[43]. La solicitud que se le

42. No han faltado pretensiones de cambio, que no han podido prosperar, por parte del Congreso evidenciada en la Proposición de Ley de modificación de la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia; y de la Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia llevada a cabo por el Grupo Parlamentario Vasco (EAJ-PNV), publicado en el Boletín Oficial de las Cortes Generales de 25 de noviembre de 2022 y así en su EM señala que «En segundo lugar, esta ley contempla una serie de modificaciones en relación con el control judicial regulado en la Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia con el objetivo de ampliar dicho control y de actuar sobre las garantías del Estado de derecho. Así, y en lo referente al control judicial de las actividades del Centro Nacional de Inteligencia, *será un órgano colegiado compuesto por tres Magistrados del Tribunal Supremo* quien, por unanimidad, acordará, mediante resolución motivada, la concesión o no de la autorización solicitada». La cursiva es del autor.

43. Como ha señalado la STS 1094/2010, 10 de diciembre, de la Sala II (Ponente: Marchena Gómez) en FJ 2.a «Cuando el cumplimiento de esas finalidades exige la restricción de los derechos a la inviolabilidad del domicilio y de las comunicaciones, se impone una singular fórmula de control judicial. La singularidad deriva, *claro es, del hecho de que el Magistrado autorizante ha de verificar una ponderación de bienes jurídicos que no se identifican con los que son valorados en el seno de un proceso penal. La posición institucional del Magistrado llamado al control previo no está exenta de dificultades*. De una parte, por cuanto que los parámetros a partir de los cuales ha de resolver la petición cursada por el Director del CNI, instando el sacrificio de derechos fundamentales, no son los ponderados con carácter general cuando se trata de la investigación de un hecho delictivo (...) *Resulta indudable, pues, que la función del Magistrado llamado al control previo de las actividades del CNI no es la de un anticipado coadyuvante del Juez de instrucción.* El expediente incoado con ocasión del ejercicio de las funciones propias

formule al Magistrado del TS por el SED debe estar debidamente motivada y así debe contener necesariamente los siguientes extremos: «*a) Especificación de las medidas que se solicitan. b) Hechos en que se apoya la solicitud, fines que la motivan y razones que aconsejan la adopción de las medidas solicitadas. c) Identificación de la persona o personas afectadas por las medidas, si fueren conocidas, y designación del lugar donde hayan de practicarse. d) Duración de las medidas solicitadas, que no podrá exceder de veinticuatro horas en el caso de afección a la inviolabilidad del domicilio y tres meses para la intervención o interceptación de las comunicaciones postales, telegráficas, telefónicas o de cualquier otra índole, ambos plazos prorrogables por sucesivos períodos iguales en caso de necesidad*».

En el supuesto del proceso penal se observa, cuando se hace una petición policial, claramente la necesidad de incluir un relato de hechos calificados jurídicamente, identificar a los sujetos presuntamente responsables del ilícito penal, especificar medidas restrictivas a imponer, su duración y la unidad responsable, así como el modo de ejecución, persona obligada a ejecutarla, y ello motivando sus razones con el propósito de permitir que el autorizante pueda también ponderar y valorar la proporcionalidad, necesidad, idoneidad, entre otros principios, como hemos visto (*cfr.* arts.588 bis a, b o ter d, en relación con el art. 579. 1 LECrim). Sin embargo, siendo fácilmente observable, las exigencias a las que se somete el CNI, si bien tienen puntos en común con la solicitud en el proceso penal, no son exactamente las mismas lo que obliga, en todo caso, a hacer una serie de precisiones.

En primer lugar, en cuanto a las medidas a solicitar, sólo pueden ser aquellas que afectan a la inviolabilidad domiciliaria y de las comunicaciones, de modo que podría pedirse por el CNI al Magistrado del TS *la vigilancia de las comunicaciones postales,*

---

de los servicios de inteligencia y las diligencias penales encaminadas a la investigación de un hecho punible, no están necesariamente llamados a converger en un hipotético proceso penal. Responden a principios distintos, su contenido es también diferente y, por tanto, el sacrificio de los derechos fundamentales que se producen en uno y otro ámbito, se justifica por razones no coincidentes». La cursiva es del autor.

telegráficas, telefónicas y las digitales (y también la grabación de comunicaciones orales). Si se solicita una entrada que afecte a la inviolabilidad domiciliaria no es para entrar y registrar, como en el supuesto policial[44], sino que tiene un carácter accesorio, pues dicha medida está destinada a instalar elementos de escucha, o a verificar lo que se encuentra en el domicilio, sin que pueda sustraerse o requisarse ningún elemento que en él se sitúe.

En segundo lugar, los hechos y razones deben incardinarse dentro de las funciones que el CNI tiene encomendadas en su protección de la «seguridad nacional» y que resulta del art. 4 de la Ley 11/2002, de 6 de mayo, en cuanto los cometidos a desarrollar y en especial su letra b para «*Prevenir, detectar y posibilitar la neutralización de aquellas actividades de servicios extranjeros, grupos o personas que pongan en riesgo, amenacen o atenten contra el ordenamiento constitucional, los derechos y libertades de los ciudadanos españoles, la soberanía, integridad y seguridad del Estado, la estabilidad de sus instituciones, los intereses económicos nacionales y el bienestar de la población*». Tal precepto obliga al Magistrado del TS a integrar conceptos como «estabilidad institucional», «bienestar de la población» o «seguridad del Estado» bajo el prisma de la existencia de una amenaza o riesgo que puede tener una fisonomía variable, en permanente evolución, sin estar bajo el estricto marco de un texto codificado, algo que dependerá, sin perjuicio de su indiscutible y seguro rigor, de la interpretación individual del autorizante. Por otro lado, el Ministerio Fiscal no emite informe alguno en este procedimiento.

En tercer lugar, la medida, en principio, debería recaer sobre aquellos sujetos relacionados directamente con la amenaza a la seguridad nacional, aunque no está debidamente precisado en la norma con lo que puede recaer sobre un circulo amplio de suje-

44. No hay que olvidar que cuando nos referimos a agentes del CNI estamos en presencia de *personal estatutari*o como prevé los arts. 13 y 14 del RD 240/2013. De hecho, tienen limitado el porte de armas como prevé el anterior RD (disposición adicional sexta). Asimismo, en virtud del art. 5.4 de la Ley 11/2002, de 6 de mayo, no tienen la consideración de *agentes de la autoridad*.

tos siempre que se puedan vincular al relato de hechos efectuado. Finalmente, la duración de la medida determina su carácter temporal (veinticuatro horas en el supuesto de un domicilio o tres meses en la interceptación de las comunicaciones) pero, a la vez, su naturaleza es indefinida en materia de prórroga al no establecer un límite máximo de duración («ambos plazos prorrogables por *sucesivos períodos* iguales en caso de necesidad»). La medida, lógicamente, no es notificada ni en ese momento ni en otro posterior, a los afectados, recordando que las actuaciones son secretas y que los resultados quedan a disposición del SED.

Recibida la solicitud del SED, el Magistrado del TS dispone de un plazo perentorio para dictar una resolución, seguramente un auto, aunque la norma no lo específica, de 72 horas (o 24 horas en función de la urgencia de la medida), salvaguardando sus actuaciones, que serán secretas. La resolución inicial y las ulteriores ni son recurribles, ni por tanto revisables, y ello porque los únicos actores de dicho procedimiento son el Magistrado y el Director del CNI. Es preciso indicar que si en el supuesto del proceso penal, la prórroga se liga a la obtención de resultados que obliguen al mantenimiento de la medida, y su necesidad, lógicamente hiladas con la existencia de un hecho delictivo grave y de su autoría que están destinados a acabar en un juicio que dilucide la responsabilidad penal de los acusados, lo cierto es que el mantenimiento de las medidas para el CNI, al no tener un fin concreto, se ligan necesariamente o bien a conocer con exactitud el riesgo o amenaza, o bien a conjurarla[45]. Y no es descartable que sus investigaciones, fruto por otro lado de las medidas limitativas de derechos, siquiera de modo indirecto puedan acabar siendo objeto de discusión en un plenario pese a que no son actos de prueba (*vid.* SSTS 1140/2010, de 29 de diciembre, de la

45. En la reforma que de la Ley pretendía el Grupo EAJ-PNV (Boletín Oficial de las Cortes Generales de 25 de noviembre de 2022) se proponía la siguiente adición en el artículo único de la Ley 2/2002, de 6 de mayo «5. Los Magistrados deberán ser informados por el Secretario o Secretaria de Estado Directora del Centro Nacional de Inteligencia *del grado de ejecución de cada autorización o prórroga en el momento en que finalicen estas, a fin de que puedan asegurarse de la adecuación a su contenido*». La cursiva es del autor.

Sala II (Ponente: Sr. Berdugo Gómez de la Torre); 1094/2010, de 10 de diciembre, de la Sala II (Ponente: Sr. Marchena Gómez)), sin olvidar, a mayor abundamiento, que las investigaciones desarrolladas por el CNI pueden tener impacto procesal de relevancia en otras jurisdicciones como la Contenciosa-Administrativa, singularmente en materia de nacionalidad con la importancia del informe «de idoneidad» del CNI sobre la persona solicitante y si es un riesgo para la «seguridad nacional», informe que resulta particularmente importante junto con el que emite el Ministerio de Interior (*vid.* SSTS 233/2022, 23 de febrero, de la Sala III, Ponente: Sr. Menéndez Pérez, FJ 4º; 395/2022, 29 de marzo, de la Sala III, Ponente: Sr. Roman García FJ 6º; 367/2021, de 17 de marzo, de la Sala III, Ponente: Sr. Herrero Pina FJ 2º,; 4376/2015, de 26 de octubre, de la Sala III, Ponente: Sr. Del Riego Valledor, FJ 4º; STS 2105/2014, de 26 de mayo, de la Sala III, Ponente: Sr. Del Riego Valledor, FJ 5º).

4 Conclusiones

La recopilación de información e inteligencia se ha convertido en una necesidad indeclinable ante el conjunto de amenazas que se ciernen sobre nuestra sociedad. Ese trabajo se desarrolla en dos planos diferentes y bajo condiciones igualmente distintas. La seguridad pública que converge en el proceso penal buscando depurar responsabilidades penales y el castigo de los culpables, y donde la conculcación de los derechos fundamentales se realiza bajo criterios que estrictamente marca la norma jurídico-procesal y conforme el paraguas garantista de un Juez que supervisa el desarrollo de las investigaciones. Éstas, inicialmente, se desarrollan en un espacio de naturaleza «clandestina» pues su conocimiento se limita a los investigadores policiales, a la autoridad judicial y a la acusación pública y con el propósito de recopilar indicios destinados a determinar la pertinencia de continuar con la investigación y en su caso transformar el procedimiento para, o bien clausurar la indagación, o bien decidir la apertura del juicio oral, donde se determinen el alcance de las responsabilidades y sus consecuencias, de modo que lo que inicialmente, y lógicamente dicho sea de paso, es desconocido

acaba necesariamente aflorando al primar la contradicción y defensa en un escenario procesal donde las pruebas, y singularmente los elementos acopiados en la investigación policial, son objeto de examen.

Pues bien, hay derechos fundamentales que necesariamente se confrontan con las finalidades de toda instrucción judicial y entre ellas la inviolabilidad de las comunicaciones que nuestra Constitución ha consagrado en su art. 18.3, convirtiéndose en un muro infranqueable que precisa de una autorización judicial para sortearla por cuanto su indisponibilidad no tiene un carácter absoluto. Aun así, los requisitos para llevar a cabo una inmisión legal en el campo de la interceptación de las comunicaciones telefónicas son técnicamente rigurosos en su planteamiento policial y examen judicial y ello por cuanto implican una restricción relevante que permite tener una cartografía exacta de la situación que es objeto de indagación. Que sea necesaria, útil, proporcionada e idónea juntamente con la existencia de un hecho delictivo calificado como grave bajo estándares legales, resultan presupuestos indeclinables para su adopción. Asimismo, la supervisión judicial se produce en un momento inicial, con la solicitud, y luego posteriormente, en cada prórroga, valorando la necesidad de su mantenimiento. De ahí depende el debate y valor procesal ulterior y la lectura que los afectados hagan bajo el prisma de las garantías en defensa de sus intereses.

La cuestión de la seguridad nacional es más espinosa, se mueve en ámbitos concéntricos con la seguridad pública, pero el abanico está más abierto, es asimétrico y responde a amenazas criminales pero también a riesgos de variado tipo (económico, energético, ambiental, cibernético...). También aquí, concretamente en el desarrollo de actividades de espionaje, es precisa una conculcación de derechos fundamentales y de ellos lo que afecta a las comunicaciones es de enorme trascendencia. Para ello, nuestro ordenamiento también ha establecido un control judicial con mimbres diferentes respecto de la investigación del hecho delictivo, en un marco regulatorio limitado, que frente al carácter difuso que implica la autorización en lo que a la investigación penal se refiere (cada Juez Instructor competente puede acordar medidas restrictivas y en su partido judicial que

delimita territorialmente su ámbito de actuación), cuando se refiere a los servicios secretos opta por la centralización atribuyendo la competencia a un Magistrado del TS con competencia, al menos, en todo el territorio nacional, y que puede limitar, a petición del responsable del CNI, la inviolabilidad domiciliaria y de las comunicaciones telefónicas bajo presupuestos no procesales penales, sino examinando lo solicitado bajo el prisma de la propia «seguridad nacional», que implica un concepto abstracto y dinámico, que no está destinado a ser discutido en una vista ni tampoco a hacerse público en sus resultados, cuando menos apriorísticamente. Frente al trinomio penal Policía- Juez- Fiscal, aquí hay un binomio de actuación, Magistrado del TS-Director del CNI, situación que busca, por la propia naturaleza del sistema, un blindaje informativo máximo y una relación temporal en virtud del plazo común de ambos mandatos.

En relación a la incógnita que implica la convergencia de actuaciones que pudiera existir en materia penal, ha sido reflejada por nuestro TS, señalando que ni los servicios secretos están para desarrollar una persecución delictiva, ni sus investigaciones tienen categoría probatoria, aunque no podemos perder de vista que su actividad, magnífica y rigurosa al igual que la de nuestra Policía, tiene relevancia o al menos puede llegar a tenerla y ser objeto de debate en un escenario jurisdiccional, algo que debería ser objeto de reflexión para que, absolutamente todos, empezando por los agentes que son esenciales, puedan desarrollar sus diferentes funciones en un marco operativo, teniendo presente lo singular de sus funciones, adecuado legalmente y que ampare sus actuaciones a la vez que respete, nuevamente teniendo presente lo singular del escenario, las garantías procesales y constitucionales.

Glosario de términos

ADN: Ácido desoxirribonucleico.

ATC: Auto del Tribunal Constitucional.

ATS: Auto del Tribunal Supremo.

CESED: Servicio Central de Información dependiente de la Presidencia del Gobierno

CESID: Centro Superior de Información de la Defensa.

CFR.: Confróntese.

CIFAS: Centro de Inteligencia de las Fuerzas Armadas.

CNI: Centro Nacional de Inteligencia.

DEA: Agencia Antidroga Norteamericana.

EM: Exposición de motivos.

EOMF: Estatuto Orgánico del Ministerio Fiscal.

ESN: Estrategia de Seguridad Nacional.

FCSE: Fuerzas y Cuerpos de Seguridad del Estado.

FGE: Fiscal General del Estado.

FJ: Fundamento Jurídico.

IMEI: Identidad Internacional de Equipo Móvil.

IMSI: Identidad Internacional del Abonado Móvil.

LECrim: Ley de Enjuiciamiento Criminal.

LOPSC: Ley Orgánica de Protección de la Seguridad Ciudadana.

LOPJ: Ley Orgánica del Poder Judicial.

LSN: Ley de Seguridad Nacional.

MMS: Servicio de mensajería multimedia.

SED: Secretario de Estado – Director del CNI

SIAM: Servicio de Información del Alto Estado Mayor.

SMS: Servicio de mensajes cortos.

STC: Sentencia del Tribunal Constitucional.

STEDH: Sentencia del Tribunal Europeo de Derechos Humanos.

STS: Sentencia del Tribunal Supremo.

TC: Tribunal Constitucional.

Vid.: Véase.

Referencias

Aba Catoira, A. (2020). Rendición de cuentas y servicios de inteligencia. En J. J. Fernández Rodríguez (coord.), *Seguridad y libertad en el sistema democrático* (pp. 209-237). Valencia: Tirant lo Blanch.

Ballesteros Martin, M. A. (2016.). *En busca de una Estrategia de Seguridad Nacional*. Madrid: Ministerio de Defensa.

Centre for the Democratic control of armed forces - Intelligence Working Group. (2003). *Intelligence practice and democratic oversight-A practitioner's view.* Geneva: Geneva Centre for the Democratic Control of Armed Forces.

Conde-Pumpido Ferreiro, C. (1992). El modelo constitucional de la policía judicial y su desarrollo normativo. *Cuaderno del Instituto Vasco de Criminologia (Eguzkilore), 6*, 13-20.

Departamento de Seguridad Nacional. (2021). *Estrategia de Seguridad Nacional*. Disponible en https://www.dsn.gob.es/es/estrategias-publicaciones/publicaciones.

Fernández Alles, J. J. (2020). El artículo 116 CE, la Ley de Seguridad Nacional y la Ley de Estabilidad Presupuestaria como medidas alternativas al artículo 155 CE. *Revista Española de Derecho Constitucional, 120*, 377-399. https://doi.org/10.18042/cepc/redc.120.13

Fernández Rodríguez, I. (2007). La Policía Judicial como función de investigación y su ejercicio por funcionarios no pertenecientes a las Fuerzas y Cuerpos de Seguridad. El caso de los Agentes Forestales. *Boletín de Información del Ministerio de Justicia, 2039*, 2429-2454.

Feijoo Sánchez, B. (2006). *El Derecho penal del enemigo y el Estado democrático de derecho.* En M. Cancio Meliá y Gómez-Jara Díez (coords.), *Derecho penal del enemigo. El discurso penal de la exclusión* (Vol. I, pp. 799-844). Madrid: Edisofer.

Fiscalía General del Estado. (1993). *Memoria elevada al Gobierno de S.M. presentada al inicio del año judicial por el Fiscal General Estado Excmo. Sr. don Eligio Hernández Gutiérrez*. Madrid.

Orgis, M. (2011). Operaciones impulsadas y guiadas por inteligencia, la mejor opción para combatir las amenazas preeminentes. En J. Fernández Rodríguez, D. Sanso-Rubert Pascual, J. Pulido Grajera y R. Monsalve (coords.), *Cuestiones de inteligencia en la sociedad contemporánea* (pp. 143-166). Madrid: Ministerio de Defensa.

Pinto Cebrián, F. (2019). *Manual de inteligencia y contrainteligencia* (terrorismo y contraterrorismo). Burgos: Amabar.

Revenga Sánchez, M. y Fernández Alles, J. J. (2020). El artículo 116 CE, la Ley de Seguridad Nacional y la Ley de Estabilidad Presupuestaria como medidas alternativas al artículo 155 CE. *Revista Española de Derecho Constitucional, 120*, 390-391. https://doi.org/10.18042/cepc/redc.120.13

Sansó-Rubert Pascual, D. (2011). Estrategias de seguridad, criminalidad e inteligencia criminal: Una apuesta de futuro. En J. Fernández Rodríguez, J. Pulido Grajera y R. Monsalve (coords.), *Seguridad*

y libertad en el sistema democrático (pp. 205-218). Madrid: Ministerio de Defensa.

Schreier, F. (2006). *Fighting the Pre-eminent Threats with Intelligence-led Operations.* Geneva: Geneva Centre for Security Sector Governance.

Vervaele, J. (2007). *La legislación antiterrorista en Estados Unidos ¿Inter arma silent leges?* Buenos Aires: Editores del Puerto.

La aplicación de las ciencias bioforenses a la investigación del bioterrorismo y biocrimen

The Application of Bioforensic Sciences to Bioterrorism and Biocrime Research

Desiderio José Ordoño Ballesteros[1]
Policía Nacional.
dordono0000@policia.es

DOI: https://doi.org/10.14201/cp.31804
Recibido: 08-11-23 | Aceptado: 19-04-24

Resumen

En los últimos años las técnicas de biología molecular han experimentado un avance enorme en todos sus campos. Esto hace que las capacidades de análisis cualitativo, cuantitativo y de tiempos de procesamiento hayan mejorado mucho, en especial con la aplicación de programas informáticos para el tratamiento de datos. Estos avances pueden ayudar en gran medida en el trabajo de la ciencia forense y en particular en la bioforense. El conocimiento de estas disciplinas y técnicas, así como lo que pueden aportar a las investigaciones sobre delitos de bioterrorismo o biocriminales, constituyen una gran herramienta para los policías dedicados a tareas de investigación, en especial para aquellos encargados de la elaboración de los informes periciales. Este conocimiento adquiere mayor importancia en la investigación de delitos terroristas donde el tiempo de respuesta policial puede ser clave para salvar vidas. En este trabajo se dan a conocer las últimas técnicas existentes, demostrando con los datos publicados en investigaciones científicas las grandes posibilidades que ofrecen.

1. Licenciado en Bioquímica UAM.

Palabras clave
Amerithrax; Bioforense; Bioterrorismo; Biocrimen; Bioincidente; Microbiología; Genómica; Proteómica; Bioinformática.

Abstract
In recent years, molecular biology techniques have experienced enormous progress in all their fields. As a result, the capabilities of qualitative, quantitative and processing time analysis have been greatly improved, especially with the application of data processing software. These advances can greatly help in the work of Forensic Science and in particular in Bioforensics. Knowledge of these disciplines and techniques and what they can contribute to the investigations into bioterrorism or biocriminal crimes, establishes a great tool for police officers dedicated to investigation, especially for those that make expert reports. This knowledge becomes more important in the case of terrorist crimes where police response time can be the key to saving lives. In this work, the latest existing techniques are presented, demonstrating with the data published in scientific research the great possibilities they offer.

Keywords
Amerithrax; Bioforensic; Bioterrorism; Biocrime; Bioincident; Microbiology; Genomics; Proteomics; Bioinformatics.

1 Introducción

Se entienden como agente biológico (AB) los microorganismos y endoparásitos humanos, susceptibles de originar cualquier tipo de infección, alergia o toxicidad (Real Decreto 664/1997), así como las toxinas producidas por éstos o por otros seres vivos. Un incidente biológico o bioincidente se puede definir como un suceso y sus posteriores consecuencias adversas, que tienen su origen en un AB. En función de la intencionalidad del "bioincidente", nos podemos referir a estos sucesos como:

- Biocrimen, cuando hay una liberación dolosa del agente, pero sin motivación terrorista.

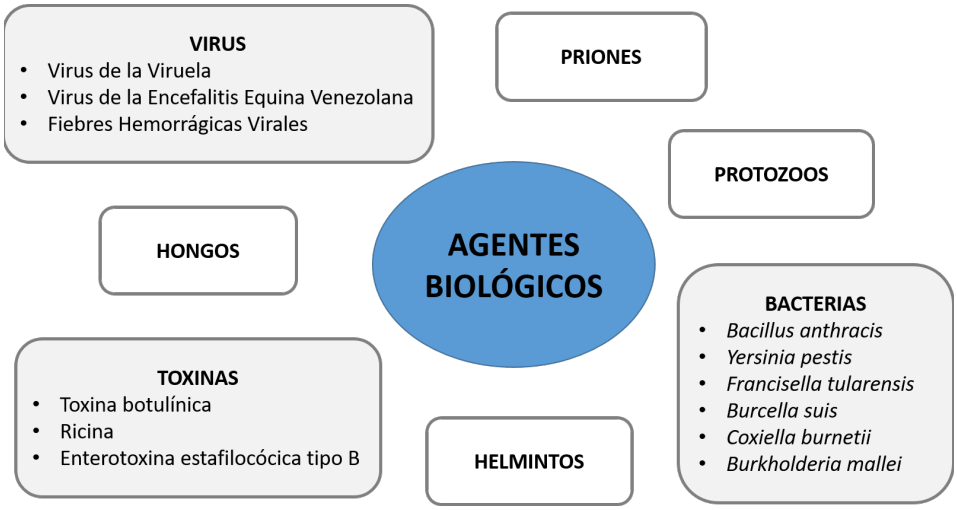
- Bioterrorismo, si la intención última es provocar un clima de miedo en una parte de la población.

- Emergencia sanitaria, si la liberación no ha sido intencional, pero las graves consecuencias ocasionadas por el AB requieren de la intervención de varios colectivos profesionales para hacerles frente.

Del amplio abanico de patógenos humanos, sólo algunos son aptos para ser utilizados como un arma biológica. En la Figura 1 se muestran los tipos de AB, y se pone de relieve que sólo algunas especies de virus, bacterias y toxinas son adecuadas para ser usadas como arma biológica, en concreto se enumera el grupo llamado *la docena sucia (Manual Curso Riesgos NBQ*, 2022), compuesto por aquellos que los diferentes programas militares de armamento biológico tomaron en consideración.

Según lo establecido en el artículo 11 de la *Ley Orgánica 2/86 de 13 de marzo de Fuerzas y Cuerpos de Seguridad* de España, las

Figura 1: Tipos de agentes biológicos; sombreados en gris aquellos AB con adecuadas características para ser usados como armas biológicas; dentro de estos tipos se enumeran aquellos pertenecientes a la denominada *docena sucia*.



Fuerzas y Cuerpos de Seguridad del Estado tienen como misión proteger el libre ejercicio de los derechos y libertades y garantizar la seguridad ciudadana, a través del desempeño de funciones como las de prevenir la comisión de actos delictivos e investigar los delitos y colaborar con los servicios de protección civil en los casos de grave riesgo, catástrofe o calamidad pública, en los términos que se establezcan en la legislación específica de protección civil.

En esta línea, y previendo actos cuya etiología fueran agentes nucleares, químicos o biológicos, se crearon en las instituciones estatales policiales sendas unidades de lucha contra agentes NRBQ, que se integraron en los servicios de desactivación de artefactos explosivos previamente existentes. En la Guardia Civil la unidad se denominó SEDEX-NRBQ, y en la Policía Nacional, se conoce como la Unidad TEDAX-NRBQ, cuyos integrantes son policías con una alta cualificación técnica, convirtiéndose en la punta de lanza ante la amenaza de artefactos explosivos o agentes NRBQ y su neutralización. Atendiendo a la Ley de Enjuiciamiento Criminal, estos técnicos especialistas están considerados como agentes de la Policía Judicial, especialmente formados en la toma de muestras de agentes NRBQ y su conservación como evidencia judicial, así como peritos con los necesarios conocimientos científicos y técnicos que les hacen capaces de la emisión de informes periciales con trascendencia jurídica que analicen las características de estos agentes. Las ciencias bioforenses (CB) engloban una serie de tecnologías y procedimientos, que se han desarrollado de una manera exponencial a lo largo de las dos primeras décadas del siglo XXI, ofreciendo cada vez más herramientas para el análisis de los AB, pudiendo por tanto resultar de gran ayuda para los especialistas NRBQ, en su labor en apoyo a los policías encargados de una investigación policial.

El objetivo del presente estudio es definir las ciencias bioforenses y analizar los grandes avances tecnológicos conseguidos en las técnicas de las CB en las últimas décadas, que posibilitan que estas puedan dar respuesta a las interrogantes claves en las investigaciones policiales de una manera muy rápida y precisa, erigiéndose como herramientas imprescindibles para los especialistas en bioincidentes. Este trabajo es una revisión acerca de las técnicas y procedimientos más novedosos usados en el

análisis de patógenos, ya sea desde un punto de vista sanitario, forense o de investigación científica.

2 Metodología

La aplicación de un punto de vista de policía judicial ha determinado la extracción de datos y su análisis, para alcanzar unas conclusiones muy concretas para el trabajo policial. El desarrollo del trabajo ha consistido en:

- Búsqueda en la base de datos PUBMED[2] de la *National Library of Medicine*, base de datos de biomedicina y biología molecular, donde se almacenan todas las referencias a artículos de investigación publicados en las revistas especializadas en estas materias.

- Búsqueda en la base de datos *Europol Platform of Experts* (EPE), concebida para el intercambio de información entre policías de países miembros de Europol, especializados en diferentes tipologías delictivas.

Ambas búsquedas se llevaron a cabo introduciendo las palabras clave de interés: bioforense, forense, bioterrorismo, biocrimen, bioincidente, microbiología, genómica, proteómica, bioinformática, metagenómica, NGS, secuenciación y una combinación de las mismas para poder hallar los artículos con la información precisa, prestando especial interés en aquellos más actuales y seleccionando aquellos más relevantes para el estudio.

- Solicitud de información a Dña. María del Carmen Cañavate, directora de la Red de Laboratorios de Alertas Biológicas (RE-LAB) del Instituto de Salud Carlos III, a través de un pliego de preguntas sobre las capacidades técnicas de la RE-LAB, para la identificación y análisis de las muestras enviadas por parte de las Fuerzas y Cuerpos de Seguridad con competencias en agentes biológicos.

2 https://pubmed.ncbi.nlm.nih.gov/

- Análisis de la información recopilada, definiendo y ordenando conceptos, uniéndolos en áreas temáticas, relacionando las técnicas científicas con las aplicaciones en el área policial y judicial, y extrayendo las conclusiones al respecto.

3 Las ciencias bioforenses y sus capacidades

La ciencia bioforense, conocida en sus inicios como microbiología forense, es un grupo de disciplinas científicas que permiten analizar muestras biológicas procedentes de escenarios con relevancia jurídica, con el fin de detectar e identificar el AB; discernir entre el tipo de liberación, ya sea natural, intencionada o accidental según su intencionalidad; rastrear la procedencia y atribuir una autoría del hecho. El uso de estos procedimientos racionales y científicos produce pruebas consistentes que no dan lugar a dudas para la elaboración de unas conclusiones en un procedimiento judicial.

Los procedimientos usados en esta rama científica pertenecen a disciplinas clásicas, que, sin embargo, han experimentado un importante desarrollo en los últimos años, constituyéndose como ejemplos de tecnología de vanguardia. Las técnicas o disciplinas en las que se agrupan los procedimientos de la CB son las siguientes:

- Cultivo celular
- Genómica
- Proteómica
- Bioinformática

El uso de varias de estas disciplinas en el análisis de una muestra genera una sinergia que da como resultado una gran cantidad de datos, los cuales es necesario que sean interpretados con la ayuda de herramientas de la bioinformática para obtener una información de calidad.

La información obtenida con las CB aporta una serie de puntos muy interesantes en una investigación sobre un bioincidente:

- Distinguir una liberación accidental de una intencional (Schmedes y Budowle, 2009; Merkley *et al*., 2020), al poder comparar el tipo de AB presente en un incidente con aquellos existentes de forma natural en el ambiente. La aparición de un patógeno no endémico en una región geográfica es un indicio de una posible liberación no natural. También sería un indicio que el análisis del genoma de un AB endémico de un lugar revelara que éste porta una modificación o serie de modificaciones que sean vistas como poco probables o sospechosas, en el sentido de que se salen de la tasa de mutación natural y que, además, estas modificaciones en el genoma provocan una mejora en las características de patogenicidad, infectividad, transmisibilidad, virulencia o resistencia. Estas técnicas permiten analizar el genoma al detalle, base por base, y concluir si un AB es de origen natural, de origen natural con modificaciones dirigidas o bien completamente artificial.

- Detección de patógenos presentes en muestras ambientales (Oliveira *et al*., 2020). El alto rendimiento de las nuevas tecnologías en el campo de las CB permitiría la adopción de un plan de bioseguridad y biodefensa, en el que se vigilaran de forma continua ciertos espacios sensibles de interés público, con el objeto de detectar de forma temprana una diseminación inadvertida de una amenaza biológica, para así responder de forma rápida y minimizar los efectos.

- Identificación rápida de un AB (Schmedes y Budowle, 2009). Dada una muestra de origen desconocido sospechosa de contener un patógeno, cobra una gran importancia una rápida identificación en el caso de haber personas expuestas, dado que es posible la necesidad de un tratamiento preventivo de las mismas, y con objeto de coordinar las medidas epidemiológicas adecuadas al caso concreto. Desde un punto de vista estrictamente policial, disponer del nombre del AB podría ayudar en gran medida a guiar el desarrollo de la investigación para la detención del culpable y evitar reiterados incidentes. Con la mejora de las técnicas bioforenses, se consigue

la identificación sin la necesidad de poseer material previo del mismo en el laboratorio, tan sólo es necesaria una potente base de datos. Además, es posible una identificación precisa en muestras contaminadas con otros tipos de AB, incluso si están relacionados filogenéticamente.

- Determinación del origen de un AB (Merkley *et al.*, 2020; Schmedes *et al.*, 2016). Por un lado, las técnicas de alto rendimiento de datos de la genómica pueden aportar la secuencia completa del microorganismo en un periodo de tiempo aceptable en el transcurso temporal de la investigación, lo que permite asociar AB hallados en distintos escenarios y, por consiguiente, convertir estas evidencias en pruebas de cargo contra un investigado. De manera complementaria, la proteómica es capaz de describir en qué condiciones ambientales se ha cultivado el microorganismo, así como la composición del medio de cultivo en el que crecía, dando la forma de vincular un AB recogido en una muestra con el lugar donde fue cultivado y la forma particular de crecerlo, sin necesidad de tener en ese escenario la presencia del mismo.

3.1 Cultivo celular

El cultivo celular es una técnica por la cual se consigue el crecimiento y mantenimiento de los diferentes tipos de células eucariotas y procariotas. La gran variedad celular en los seres vivos hace necesario que existan multitud de protocolos diferentes de cultivo para cada tipo celular. Esta dificultad, junto al gran número de técnicas asociadas para la observación y la caracterización celular, como la tinción celular o la microscopía, hace de estas técnicas algo complejo. El cultivo es un método tradicional de detección y caracterización de microorganismos, considerado como una prueba que revela la presencia de un microorganismo en una muestra dada, tal y como proponen los postulados de Henle-Koch. El hecho de que el AB tomado de la muestra pueda crecer y desarrollar su ciclo biológico demuestra que es viable y que tendría capacidad patogénica en presencia del huésped adecuado. Sin embargo, el crecimiento de un microorganismo del que no disponemos información previa es complicado, ya que

puede precisar condiciones especiales y, por tanto, si no se consigue la proliferación, puede dar un resultado de falso negativo.

Adicionalmente, el uso de esta técnica presenta limitaciones que le impiden aportar información necesaria en un procedimiento judicial. La observación del crecimiento del microorganismo no puede proporcionar una identificación con precisión del AB más allá de su género o especie, en el caso de que fuera posible, dado que en ocasiones el crecimiento diferencial y la observación al microscopio no bastan para la diferenciación con respecto a otros microorganismos relacionados filogenéticamente. En este nivel de identificación del AB, no se podría determinar la procedencia del mismo en un estudio comparativo con otra muestra obtenida en otro escenario en relación con la investigación. Así, esta técnica necesita de otras para completar una investigación bioforense.

3.2 Genómica

Los ataques terroristas con sobres postales, en cuyo interior había un polvo blanco con alto contenido de la bacteria *Bacillus anthracis*, ocurridos en el año 2001 en Estados Unidos fueron conocidos como el caso Amerithrax, nombre dado por el *Federal Bureau of Investigation* (FBI). Este bioincidente supuso un punto de inflexión para la ciencia forense y la genómica aplicada a este campo. De esta forma, hoy día la genómica es capaz de cumplir funciones de:

- biovigilancia ya que permite una detección rápida,
- bioforenses por identificar con precisión un AB,
- y sanitarias pues ayuda al tratamiento de la enfermedad,

determinando un diagnóstico sindrómico, en el que ante una enfermedad desconocida, y partiendo de los síntomas manifestados, se ejecuta una única prueba genómica, identificando el agente causal rápidamente, para así implementar las medidas necesarias tanto sanitarias, para el tratamiento médico a los

afectados, como policiales, para la implementación de medidas de seguridad y el desarrollo de la investigación sobre el hecho.

El análisis del genoma proporciona una identificación a nivel de aislado, definido como el conjunto de microorganismos individuales presentes en una muestra concreta, es decir, nos informa de la población clonal de cada especie, lo que permite determinar su origen. Un análisis más profundo de la secuencia del ADN podría aportar una relación filogenética entre los individuos de muestras de distintas cepas de la misma especie, obtenida de individuos infectados por el patógeno y en el que ya ha habido posibles cambios en el genoma debido a mutaciones naturales producto de la división del patógeno en el crecimiento (Schmedes y Budowle, 2009). También habría posibilidad de establecer una relación filogenética entre especies y cepas que han sido modificadas intencionalmente por técnicas de ingeniería genética, con intenciones delictivas. De este modo, se podría relacionar la presencia de un microorganismo concreto en un escenario con su hallazgo en otro lugar distinto del primero.

Desde la descripción molecular del ADN por Watson y Crick en el año 1953, las técnicas basadas en el estudio y manipulación del ADN se han multiplicado a lo largo de los años y el análisis del genoma hoy día se puede realizar utilizando diversos procedimientos. Las técnicas basadas en la PCR (*Polymerase Chain Reaction*) suponen una manera rápida y barata de conseguir la identificación diferencial de un agente biológico. Con estas técnicas se puede lograr una identificación a nivel de aislado, pero no hay una seguridad de alcanzar este nivel de resolución en todos los casos. La técnica PCR-DGGE (*Polymerase Chain Reaction – Denaturing Gradient Gel Electroforesis*), que consiste en la amplificación a partir de una secuencia inicial de oligonucleótidos y la separación posterior del producto de reacción en un gel de electroforesis, es la técnica más común para la identificación de especie de los AB, pero difícilmente sería capaz de ofrecer información más allá de la identificación de especie, y eso contando *a priori* con una sospecha de los microorganismos presentes en la muestra (Hyytiä-Trees, Cooper, Ribot y Gerner-Smidt, 2007). Estas limitaciones también las presentaría la técnica de PCR cuantitativa (qPCR), sin embargo, la qPCR puede ofrecer un

mayor rendimiento y velocidad, al practicarse con mayor automatismo y aceptar muy bien la simultaneidad de varias pruebas de PCR frente a varias secuencias de distintos AB, dando en un solo ensayo mayor cantidad de información del contenido de una mezcla de AB. Partiendo de este enfoque de multiplexación de PCR, la técnica MLVA (*Multi Locus VNTR Analysis*), que amplifica zonas del ADN que contienen secuencias repetidas de pares de bases presentes en los genomas de los seres vivos, da un paso más y consigue aportar una identificación en el nivel de cepa del AB (Hyytiä-Trees *et al.*, 2007). Una identificación a este nivel podría diferenciar con suficiencia diferentes muestras obtenidas en el curso de una investigación, pero en ocasiones es necesaria una mayor precisión entre los distintos aislados.

Para alcanzar un nivel de individualización dentro de una cepa de un AB, hay que recurrir a las técnicas de secuenciación del ADN. Esta es un conjunto de procedimientos bioquímicos cuya finalidad es la determinación del orden de los nucleótidos en una cadena de material genético. El conocimiento de la secuencia genética permite analizar diversos sitios del mismo como SNP (*Single Nucleotide Polymorphisms*), inserciones, sitios de restricción, factores de virulencia, plásmidos, duplicaciones o ausencias, caracterizando así al AB, y extrayendo información con la que conocer la huella genética de éste, donde se revelen evidencias de la práctica de técnicas de ingeniería genética y se señale el origen exacto del AB. La secuenciación presenta una ventaja adicional frente a las técnicas de PCR o de hibridación, puesto que no necesita un conocimiento previo y material de análisis basado en este conocimiento, analizando cualquier tipo de muestra con los mismos reactivos iniciales. Sin embargo, inicialmente eran técnicas muy caras y tardaban mucho tiempo en ofrecer los resultados, debido a que se trataba de procedimientos secuenciales, no realizados en paralelo como ocurre hoy día. La técnica WGSS (*Whole Genome Shotgun Sequence*) consta de varias fases en las que se trocea previamente el genoma, luego se clona en plásmidos, se secuencia a continuación y, por último, se construye la secuencia completa con el uso de programas informáticos como si de un rompecabezas se tratase. La información obtenida es del genoma completo, identificando por completo al AB y facilitando un exhaustivo análisis que pueda resolver las necesidades de la

investigación. Inicialmente se utilizaba el método Sanger, tardando meses en finalizar el trabajo y con alto coste económico (Gupta y Verma, 2019). Hoy día, con el gran desarrollo en el campo de la genómica, las técnicas denominadas NGS (*Next-Generation Sequencing*) consiguen reducir en gran medida tanto el tiempo de trabajo como los costes de los ensayos.

La primera técnica de secuenciación, la técnica Sanger, fue descrita en 1977, y hasta la primera década del 2000 no se desarrollaron otros procedimientos. Las tecnologías de secuenciación se multiplicaron con el comienzo del siglo XXI, llamándose NGS de segunda generación, que utilizan la amplificación clonal para fortalecer la señal de detección, mejorando en gran medida las prestaciones (Goodwin, McPherson y McCombie, 2016). Ya en la segunda década del 2000 se mejoran las técnicas con las NGS de tercera generación, las cuales no necesitan una fase de amplificación, lo que acorta los tiempos en la preparación de las muestras, evitando los errores en esta fase. También se reduce la cantidad de ADN necesario, muy importante en los casos en los que la muestra tenga poca cantidad de material genético. Los genomas más grandes pueden ser secuenciados al completo en cuestión de semanas y aquellos más pequeños como los bacterianos y los virales en tan sólo unos pocos días. Como ejemplo de esta velocidad de secuenciación, en tan sólo 62 horas se consiguió un borrador de la secuencia completa de la cepa de *Escherichia coli* responsable del brote causante de la muerte de 53 personas en Alemania en 2011 (Schmedes y Budowle, 2009), usando una tecnología NGS de segunda generación. Consecuentemente, las NGS generan una gran cantidad de datos en poco tiempo, que deben ser tratados con sistemas informáticos y revisados para evitar errores. Por ello es esencial que estos avances en secuenciación vayan acompañados con el desarrollo de la bioinformática.

Todas estas técnicas ya están siendo utilizadas en el análisis sin sesgo de muestras complejas en las que hay una mezcla de microorganismos, denominándose metagenómica esta rama de la genómica en la que se secuencian todos los genomas presentes en una muestra. Para una muestra que contenga principalmente una mezcla bacteriana, el problema se puede abordar desde dos puntos de vista, bien dirigiendo la secuenciación a ciertas

partes variables del genoma como puede ser el gen 16S rRNA de bacterias, o bien realizando un WGSS de todo el genoma. Con el primer enfoque se logra una amplia visión de las bacterias presentes en la muestra, mientras que con el segundo se tendría más detalle de aquellos detectados, pero se perdería sensibilidad en la detección de algunos de ellos, pudiendo pasar desapercibido aquel patógeno de interés, resultando en un falso negativo (Zheng, Qiu, Wan y Zhang, 2021).

3.3 Proteómica

La proteómica significa la caracterización del conjunto total de las proteínas presentes en una célula o tejido, llamado proteoma, y sus cambios, lo que incluye la expresión, su estructura, funciones, interacciones y modificaciones (Aslam, Basit, Nisar, Khurshid y Rasool, 2017). El proteoma de las células es un conjunto dinámico, que cambia su composición en una misma célula en función del entorno en la que está inmerso el individuo. Es decir, el proteoma de un microorganismo va a depender de los nutrientes que tenía disponibles para reproducirse, la temperatura, la presión, la composición del aire y otros factores presentes en el ciclo vital de este microorganismo. Así pues, el análisis del proteoma en una investigación forense puede, en primer lugar, detectar la presencia y determinar la identidad de un microorganismo hasta un nivel de cepa, e incluso en ocasiones de aislado, ya que el perfil proteico de expresión de un AB es característico del mismo tanto desde un punto de vista cualitativo como cuantitativo. No obstante, el hecho de que ese proteoma pueda variar dependiendo del entorno donde haya crecido el AB permite determinar si procede de un entorno natural o de un laboratorio, dando indicios de un acto accidental o deliberado (Merkley *et al.*, 2017). De igual forma, este cambio permite inferir en qué condiciones se creció el AB y qué precursores se usaron en ese proceso, pudiendo asociar una muestra objeto del delito con un lugar donde se haya practicado una diligencia de entrada y registro. Otro factor importante a tener en cuenta es la averiguación del procedimiento de diseminación del AB, bien por haber presentes en el proteoma de la muestra proteínas distintas del mismo, o bien porque el AB ha modificado su proteoma como consecuencia del proceso diseminador.

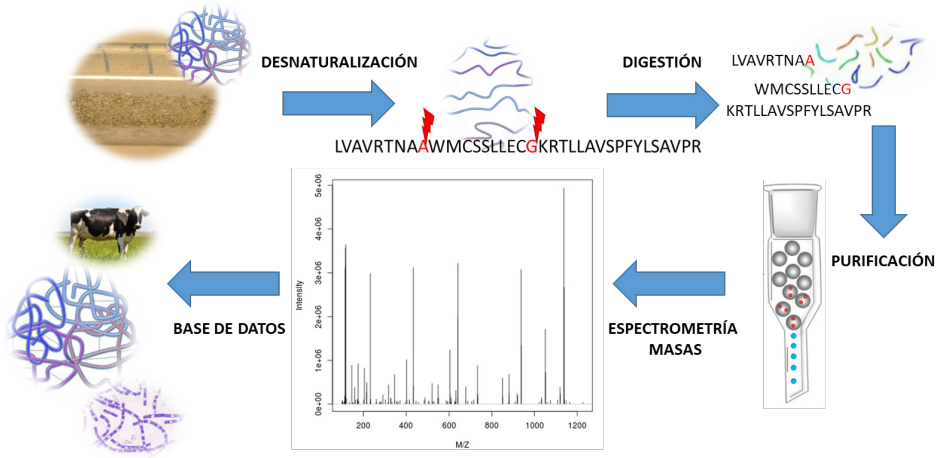
Las ventajas que ofrece la proteómica la hacen una disciplina complementaria a la genómica, que en unas ocasiones refuerza las conclusiones extraídas de la misma, en otras supone la única opción disponible si no hay material genético en la muestra de la evidencia y, por último, aporta una información adicional a la investigación que no es posible conseguir con las técnicas de la genómica.

La proteómica comprende multitud de técnicas con el fin de tratar y analizar las proteínas de una muestra. Los inmunoensayos están considerados técnicas convencionales, que, sin embargo, poseen una gran sensibilidad, sencillez, rapidez y eficacia. A día de hoy son conocidos por toda la población dada la importancia que han tenido en el diagnóstico de la enfermedad covid-19, en especial las técnicas de inmunocromatografía de aplicación comercial y autodiagnóstico y del ensayo ELISA (*Enzyme-Linked Immuno-Sorbent Assay*) utilizado como ensayo de referencia junto la PCR tanto para la confirmación de la presencia del virus como para analizar la concentración de anticuerpos contra el mismo en sangre. Con estos inmunoensayos se consigue la detección e identificación diferencial hasta nivel de cepa, con la condición de poseer información y material previo y la realización de un experimento dirigido hacia ciertos AB bajo sospecha. Los *microarrays* de proteína son una variante de inmunoensayo de alto rendimiento que acorta el tiempo de detección e identificación evaluando de forma simultánea varias proteínas dirigidamente en una muestra compleja, sin embargo, al igual que el ELISA precisa tener de antemano los anticuerpos contra las proteínas de los AB (Aslam *et al.*, 2017).

La necesidad de experimentos dirigidos hacia ciertos patógenos es salvada por las técnicas de espectrometría de masas. Esta tecnología de alto rendimiento es capaz del análisis de muestras complejas y la definición del proteoma completo de una muestra, de manera rápida y con mucha sensibilidad y precisión. Un paso previo que mejora el resultado de la espectrometría es la digestión con enzimas que cortan todas las proteínas en ciertas partes fijas de la secuencia de aminoácidos, generando péptidos cuyos extremos C y N terminales están prefijados. En el siguiente paso, se lleva a cabo la separación de los fragmentos peptídicos presentes en la mezcla, usando normalmente una cromatografía líquida (LC). Continúa el ensayo, transformando las moléculas

en iones en fase gaseosa, habitualmente usando como métodos de ionización el MALDI (*Matrix-Assisted Laser Desorption Ionization*), el SELDI (*Surface Enhanced Laser Desorption/Ionization*) o el ESI (*Electrospray Ionization*). El siguiente paso consiste en la separación de estas moléculas cargadas eléctricamente (z) en función de su peso molecular (m) en una cámara donde se ha aplicado un campo eléctrico o magnético. Finalmente, estas moléculas con un valor m/z son medidas, generando un espectro peptídico con m/z en el eje x y la abundancia relativa en el eje y dando unos picos característicos de cada muestra (Figura 2). Este espectro de la muestra contiene la información para la identificación de todas las proteínas presentes y, por tanto, el origen de cada una de ellas. La MS (*Mass Spectrometry*) es una tecnología de alto rendimiento que puede ofrecer un proteoma de muestras complejas en las que estén presentes varios AB y otras proteínas, pero necesita de la bioinformática para el análisis de los espectros que produce y del seguimiento de un experto en la materia, capaz de manejar los programas informáticos precisos, y que disponga de potentes bases de datos de proteínas y proteomas de AB con las que reconstruir el de la muestra de análisis.

Figura 2: Fases para la identificación del proteoma de una muestra en polvo mediante espectrometría de masas.



Nota. El análisis revela que hay una mezcla de proteínas de *Bacillus anthracis* y vaca, dando una pista acerca del origen de la muestra.

3.4 Bioinformática

Las técnicas de genómica y proteómica generan una gran cantidad de datos en bruto que necesitan ser tratados informáticamente. Las aplicaciones bioinformáticas usan algoritmos matemáticos, la estadística y procesos lógicos informáticos para organizar y analizar enormes cantidades de datos de origen biológico y darles un sentido. Para realizar estos cálculos, los programas de bioinformática se ayudan de bases de datos en las que previamente se han introducido la secuenciación del ADN o el proteoma completo de los microorganismos. Por este motivo, es necesario contar con potentes bases de datos que contengan el mayor número de agentes patógenos posibles, así como sus más cercanos familiares, con el fin de minimizar en lo posible la aparición tanto de falsos positivos, por la asignación de un microorganismo relacionado filogenéticamente con un patógeno, al no tenerlo incluido en la base de datos, así como de falsos negativos al no disponer de la información precisa de ese patógeno. Esta diferenciación entre microorganismos emparentados filogenéticamente es un reto que los propios programas de asignación pueden tener incluso con una buena base de datos, por ello la investigación y el desarrollo de nuevas plataformas continúa avanzando. Diversas agencias dedicadas a la vigilancia en biodefensa y epidemiológica han desarrollado aplicaciones de fuente abierta como SURPI (*Sequence-based UltraRapid Pathogen Identification*) o EDGE (*Enpowering the Development of Genomics Expertise*) (Minogue *et al.*, 2018), que ayudan a la interpretación de los datos de una secuencia genómica. Paralelamente, en proteómica podemos encontrar herramientas bioinformáticas como SEQUEST®, PRIDE, PEPTIDEATLAS o PROTEOME COMMONS y una variedad de bases de datos de secuencias de microorganismos (Aslam *et al.*, 2017). La selección de una base de datos enfocada al problema de interés es importante, de tal manera que sea lo bastante amplia para evitar falsos negativos, así como restringida, para evitar señuelos y falsos positivos en la identificación de un AB en una muestra.

Las bases de datos diseñadas con fines bioforenses deben contar adicionalmente con una información asociada a cada microor-

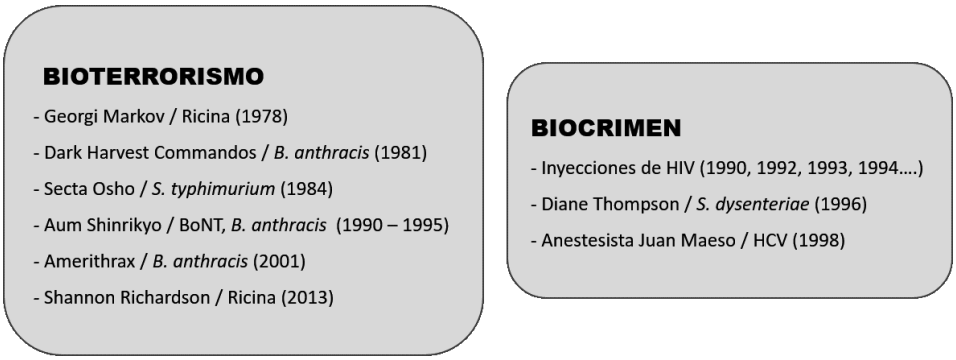
ganismo en el que se reflejen las muestras previas donde apareció, su localización, fecha, condiciones ambientales, concentración, tipo de muestra y la forma de recogida, método de secuenciación, virulencia de la cepa y otras anotaciones de interés. Este tipo de información es llamada metadata y es de gran importancia en estudios epidemiológicos y bioforenses, ya que ayudaría a la determinación de aspectos clave en la investigación de un brote.

La inteligencia artificial (IA) es la rama de la informática que dota a las máquinas de una imitación de la estructura cognitiva humana, dándoles capacidad de pensamiento analítico y de toma de decisiones (Mintz y Brodie, 2019). La IA ha demostrado ser una herramienta útil en el trabajo de las técnicas de cultivo celular; el algoritmo de "Chromogenic Media Image Detection" consigue discriminar cultivos celulares de un determinado microorganismo frente a otras especies (Rhoads, 2021), ayudando en la interpretación de placas de cultivo muy numerosas y limitando el componente subjetivo humano. La IA, aplicada a través de sus técnicas de *machine learning* y *deep learning*, mejora el tratamiento de esta ingente cantidad de datos generados por la genómica y la proteómica, incrementando la velocidad de análisis y minimizando los errores en los resultados (Mishra *et al.*, 2023). Estas máquinas inteligentes pueden ser diseñadas y entrenadas para que ejecuten análisis en las secuencias genéticas o proteómicas de los AB y extraigan información útil desde el punto de vista jurídico, en relación con la intencionalidad del uso, capacidad letal u origen del mismo, alimentando a la metadata asociada al bioincidente.

4 Uso de las ciencias bioforenses en bioincidentes

A lo largo de la historia ha habido numerosos actos malintencionados con la participación de AB (Figura 3) y el método científico se ha usado para la resolución de los mismos; sin embargo, fue en el bioincidente conocido como Amerithrax cuando las ciencias bioforenses tuvieron un uso más amplio, adaptándose a las necesidades planteadas, apoyando y definiendo las líneas de investigación policial y aportando evidencias judiciales de valor probatorio. En

Figura 3: Principales bioincidentes ocurridos desde finales del s. XX hasta hoy día en relación con: izquierda bioterrorismo, derecha biocrimen.



Nota. Elaboración propia a partir de un extracto de los hechos más relevantes de las citaciones.
Fuente. Medical Management of Biological Casualties Handbook, 8th edition; Schmedes *et al*., 2019).

el año 2001, una semana después del atentado en Nueva York del 11-S, una serie de cartas conteniendo en su interior polvo de *Bacillus anthracis* fueron enviadas en dos oleadas, en primer lugar, a medios de comunicación, y en segundo término a senadores del Partido Demócrata de los Estados Unidos. Como consecuencia de estos actos, se produjeron 22 casos de enfermedad de ántrax, de los cuales 5 personas fallecieron. Adicionalmente, otras 30 personas dieron positivo en las pruebas de detección del AB y otras 32.000 tuvieron que seguir un tratamiento profiláctico por un posible contacto con este microorganismo. El impacto económico de estos actos ascendió a 6 billones de dólares, de los cuales 320 millones de dólares se destinaron a la descontaminación de las esporas (Schmedes y Budowle, 2009). La investigación duró 10 años, y no fue hasta 7 años después del incidente que se tuvo certeza y pruebas de la autoría del hecho. Durante estos años la investigación del bioincidente maduró y la incorporación de diversas tecnologías fue una necesidad para dar respuesta a muchas preguntas.

El cultivo bacteriano en placas de agar de las muestras recogidas en los escenarios pudo determinar, tras los dos primeros días después del incidente, que las bacterias contenidas en la muestra eran del género *Bacillus*. Posteriormente, la observación de las colonias que crecieron y su cultivo diferencial, así como técnicas de tinción, reveló que entre todas las muestras había colonias con una morfología distinta (morfotipos A, B, C/D y E). En noviembre de 2001, se consigue identificar al *B. anthracis* a partir de muestras tomadas

de víctimas expuestas que presentaban síntomas. En paralelo los investigadores analizaban el contenido de la carta usando técnicas de microscopía electrónica y de cultivo celular como ya se ha indicado. Es decir, no se identificó el contenido de las cartas hasta que los afectados no presentaron síntomas casi un mes después de la exposición. Para una identificación más precisa a nivel de cepa hubo que esperar hasta septiembre de 2002, gracias a la aplicación de la tecnología MLVA de las colonias obtenidas en el laboratorio, pudiendo afirmar en ese momento que la cepa de *B. anthracis* contenida en las cartas era la llamada Ames. Para conocer de manera más precisa las diferencias genéticas entre los morfotipos y llegar en la identificación a un nivel de aislado, se practicaron las WGSS de las las colonias obtenidas, logrando su finalización en el año 2003.

Por otro lado, los investigadores se dieron cuenta de que la mezcla de polvo de las cartas enviadas a direcciones de Nueva York contenía una bacteria distinta de *B. anthracis*, en una proporción del 1 al 5 %. Para averiguar la especie concreta, se realizaron secuenciaciones del gen 16S rRNA, dando como resultado, en diciembre de 2001, que la identidad de la otra bacteria era *Bacillus subtilis*, una especie muy común en laboratorios de investigación e industriales, aportando una línea de investigación que finalmente fue corroborada. La secuenciación de la cepa finalizó en 2008, lo que permitió añadir un elemento probatorio más del origen de la mezcla en polvo usada en los ataques.

Con el objeto de hallar más pistas acerca del lugar de producción y los materiales usados, se usaron otras técnicas como microscopía electrónica, dispersión de rayos X, radioactividad del carbono y espectrometría de masas de moléculas inorgánicas y orgánicas. Todos estos análisis en unión a otras técnicas clásicas de la investigación forense y policial lograron descartar a un buen número de sospechosos y centrar la investigación en el Dr. Ivins. Finalmente, ya en el año 2007, los análisis filogenéticos de un aislado de la cepa Ames presente en su laboratorio llamada RMR-1209 en relación con las muestras de las cartas lograron determinar que el autor de los hechos había sido esta persona.

En otros casos más recientes, la secuenciación y el análisis filogenético de los agentes biológicos han resultado una pieza clave en el procedimiento judicial. Sirva de ejemplo el caso del

anestesista español Juan Maeso, que fue condenado por un delito de lesiones por imprudencia grave profesional, al demostrarse por medio de estudios filogenéticos que inyectó el virus de la hepatitis C a 275 pacientes, que enfermaron como consecuencia de esta infección, al usar la misma jeringuilla para inyectarse morfina y posteriormente tratar a sus pacientes (Schmedes y Budowle, 2009).

Una investigación policial, en especial en casos de terrorismo, exige una rápida respuesta y desarrollo para la toma de medidas de seguridad, evitar la pérdida de evidencias y prevenir futuras acciones criminales. En el caso del Amerithrax, el acto de bioterrorismo de mayor relevancia mundial, la investigación duró 10 años, en los cuales se tardó un mes en identificar el agente patógeno, tiempo en el que las personas expuestas no recibieron ningún tipo de tratamiento específico. Los ataques sucedieron en dos oleadas que pudieron ser muchas más, dado que el análisis del AB no consiguió dar información bastante hasta pasados 5 años, pudiendo detener al autor en 2007, es decir, 6 años después. Por fortuna, la motivación del causante era generar una gran alarma social alrededor de la peligrosidad de los AB, para no perder su financiación en la investigación sobre una vacuna efectiva para el ántrax, objetivo que alcanzó a la perfección; sin embargo, si la motivación hubiera sido la muerte indiscriminada, la catástrofe hubiera sido, sin duda, mucho mayor. Las nuevas técnicas de CB permitirán que los plazos en la respuesta del incidente se acorten, y así una toma de decisiones rápida que mejore las consecuencias del ataque.

Por otra parte, el procedimiento judicial requiere precisión en los datos aportados que se puedan constituir en evidencias con eficacia probatoria. Las nuevas tecnologías en el campo de las ciencias bioforenses mejoran a anteriores aplicaciones tanto en velocidad y capacidad de procesamiento como en calidad y fiabilidad de los datos. En la Tabla 1, se reflejan agrupadas por campo de conocimiento las principales técnicas usadas en la identificación y el estudio de muestras de origen biológico. Todas las técnicas pueden ser usadas para la detección de un AB, si bien este dato es muchas veces insuficiente. El siguiente paso es la identificación del agente, dentro de la cual hay tres niveles

Tabla 1: Las distintas disciplinas de las CB ofrecen información muy relevante en una investigación policial y/o judicial.

DISCIPLINA/TÉCNICA CIENTÍFICA	TECNOLOGÍA	DETECCIÓN	IDENTIFICACIÓN			ESTUDIO FILOGENÉTICO	DETERMINACIÓN PRECURSORES
			ESPECIE	CEPA	AISLADO		
CULTIVO	*Dependiente tipo AB*	+	+/-				
GENÓMICA	*"Microarrays" DNA*	+	+	+/-			
	PCR-DGGE	+	+	+/-			
	"Real-time" PCR	+	+	+/-			
	MLVA	+	+	+			
	WGSS	+	+	+	+	+	
	MPS (NGS)	+	+	+	+	+	
PROTEÓMICA	*ELISA*	+	+	+/-			
	"Microarray" de Proteína	+	+	+/-			
	Espectrometría de Masas	+	+	+	+/-		+

Nota. PCR: polymerase chain reaction; MLVA: multi-locus variable number tandem repeat VNTR analysis; WGSS: whole genome shotgun sequencing; MPS: massively parallel sequencing; NGS: new generation sequencing; ELISA: enzyme linked immunosorbent assay.
Fuente. Elaboración propia.

de precisión que diferencian unos agentes de otros. Sabiendo la especie del AB se pueden tomar medidas sanitarias y de seguridad, tales como elección de descontaminantes, medidas profilácticas, de tratamiento médico a personal expuesto y otras. A este nivel, casi todas las técnicas te ofrecen una respuesta, salvo el cultivo, que puede darla o no dependiendo de varios factores, muchos de ellos dependientes de la experiencia del científico. A nivel de identificación de cepa (conjunto de microorganismos de la misma especie que proceden de un mismo individuo), muchas de las técnicas están limitadas en su respuesta, dado que necesitan de información adicional previa para conseguir un resultado positivo; es lo que se conoce como ensayo con "sesgo", en el que se debe partir de un material específico por AB en el ensayo para comprobar su presencia. En el último nivel de aislado, tan sólo las secuenciaciones genéticas, WGSS y MPS, son capaces de dar una total precisión. El detalle ofrecido por la secuenciación genética permite la realización de estudios filogenéticos entre genomas de individuos, que, si bien no son idénticos, se puede inferir que unos proceden de otros por los cambios dados en sus secuencias genéticas. Las nuevas técnicas aumentan las tasas de

rendimiento respecto al tiempo empleado, disminuyendo su coste y acumulando un gran número de datos. Este gran volumen de datos que ofrecen estas tecnologías, una vez procesados con la ayuda de la informática, da respuesta a los interrogantes fundamentales que surgen en la investigación de un bioincidente: *qué*, identificación del AB; *cómo*, forma de producción y diseminación del AB; *dónde*, localización del laboratorio de producción; *quién*, productores del AB.

La Red de Laboratorios de Alerta Biológica (RE-LAB), creada por la Orden PCI/1381/2018, de 18 de diciembre, por la que se regula la Red de Laboratorios de Alerta Biológica, está formada por 13 laboratorios que disponen para diagnóstico de las más novedosas tecnologías, aquí comentadas. Dentro de esta red hay servicios de genómica, con las últimas tecnologías de NGS, como los sistemas Illumina® y Nanopore®, y de metagenómica, como el basado en el gen 16S rRNA. Actualmente se podría lograr la secuencia completa de un genoma bacteriano en tan sólo tres días. También existen unidades de proteómica que utilizan de modo habitual espectrometría de masas con ionización por MALDI-TOF y muchas otras técnicas analíticas asociadas. Por último, las unidades de bioinformática existentes darían el apoyo necesario en el tratamiento de los datos originados en un bioincidente.

Todas estas tecnologías están, por tanto, a disposición de una investigación policial, y aprovechar todas las ventajas que ofrecen es una decisión del instructor del atestado, el cual puede necesitar del asesoramiento de policías titulados y especializados en la materia, que son capaces de proponer soluciones que aportan estas tecnologías que los policías de investigación pudieran no conocer, y de elaborar los informes periciales pertinentes que darán respuesta a muchos de los interrogantes que surjan en la investigación, cumpliendo con lo indicado por la Ley de Enjuiciamiento Criminal sobre el informe pericial en el artículo 456 y siguientes. Este estudio pone de relieve las respuestas que la incorporación de estas tecnologías aportaría en la investigación de un bioincidente. El detalle alcanzado por la identificación del AB lograría asociar los microorganismos hallados en una muestra, obtenida en el lugar del incidente, con otra muestra tomada en una diligencia de entrada y registro, de manera que se establece-

ría un nexo causal entre el imputado y la acción terrorista. Otra utilidad muy llamativa la aporta el estudio con la proteómica, con el que dada una muestra de origen biológico, y elaborado el espectrograma del proteoma, se pueden inferir los medios nutricionales de crecimiento del patógeno, así como las condiciones de crecimiento, e incluso los mecanismos de dispersión. En el caso de que al hacer una entrada y registro en un local, donde haya un laboratorio y el material necesario para el crecimiento de AB, no se hallase ni rastro del mismo, la asociación del AB con sus precursores y útiles de crecimiento sería fundamental para imputar un delito con garantías de condena en un juicio oral. Los estudios filogenéticos ya han demostrado ser muy útiles en la investigación de infecciones de múltiples víctimas, como se vio en el caso Maeso. En el terreno preventivo, la instalación en infraestructuras críticas y ciertos eventos de alto riesgo de sistemas de toma de muestras automáticos, para la realización posterior de análisis sistemáticos de detección de AB, es hoy día factible e interesante en ciertos casos.

La validación de todas estas técnicas, desde el punto de vista jurídico, es muy conveniente para dotarlas de la eficacia necesaria en los procedimientos tanto policiales como judiciales. Pudiera resultar positivo que los protocolos de actuación existentes en relación con la RE-LAB fueran revisados y adaptados a estos nuevos métodos de análisis, con el objeto de fortalecer la coordinación entre los policías actuantes y el personal del laboratorio de referencia. El incidente del Amerithrax demostró que la coordinación entre las Fuerzas y Cuerpos de Seguridad y los laboratorios de análisis es muy importante. La toma de muestras es crucial, ya que debe ir enfocada a la tecnología que se va a utilizar y debe cubrir las necesidades del personal que las va a procesar en el laboratorio. Otro punto importante sería acreditar estas nuevas técnicas, a través de la Asociación Española de Normalización, generando normas UNE (Una Norma Española) para cada técnica, que garantizaría unos niveles altos de calidad, fiabilidad y seguridad jurídica, que repercutiría positivamente de cara a las pruebas en el proceso judicial.

5 Conclusiones

Los avances en las tecnologías han hecho de las CB una fuente muy importante de información para las investigaciones policiales y judiciales. Los resultados de gran parte de las técnicas de las CB generan informes con una precisión inequívoca, que de esta manera apoyan pruebas muy sólidas desde el punto de vista judicial.

El gran avance tecnológico alcanzado ha conseguido acortar los tiempos de obtención de la información surgida de las CB, beneficiando mucho el desarrollo de la investigación y de la toma de medidas de seguridad frente a la amenaza que supone la liberación de un AB. Esta aceleración de los procesos da la posibilidad de examinar de una manera más detallada las muestras obtenidas y así responder a un mayor número de preguntas acerca del bioincidente, logrando determinar qué, cómo, dónde y quién.

La ejecución de las técnicas de las CB debe ser llevada a cabo por personal altamente especializado, en instalaciones adecuadamente equipadas y con unas medidas de bioseguridad suficientes. Es por ello que es necesaria la colaboración con instituciones externas a las Fuerzas y Cuerpos de Seguridad que cumplan con estos requisitos. El Instituto de Salud Carlos III y la Red de Laboratorios ReLab se ajustan a la perfección a estos criterios, y a día de hoy ya hay firmados convenios de colaboración. Se deberían estrechar lazos y actualizar los protocolos operativos para adecuarlos a estas nuevas tecnologías, fortaleciendo así la eficacia ante una posible investigación de un bioincidente.

En el ámbito policial es muy importante la presencia de agentes que estén altamente formados en este tipo de amenazas de naturaleza biológica, como es el caso de la Unidad TEDAX-NRBQ en la Policía Nacional o el SEDEX-NRBQ de la Guardia Civil. Estos técnicos especialistas sirven de puente entre los laboratorios de referencia de análisis de muestras y los policías encargados de la investigación. Como primeros intervinientes en el escenario del crimen, toman las medidas de seguridad y de neutralización de

la amenaza, así como efectúan la recogida de indicios y muestras del AB, asesoran a los investigadores y emiten informes periciales para la instrucción del atestado y la autoridad judicial.

Las ventajas que aportan las CB hacen de ellas una herramienta jurídica imprescindible para la unidad policial de investigación y como una prueba de cargo en el procedimiento judicial correspondiente.

Glosario

AB: Agente biológico.

CB: Ciencias bioforenses.

EDGE: Enpowering the Development of Genomics Expertise.

ELISA: Enzyme-Linked Immuno-Sorbent Assay.

EPE: Europol Platform of Experts.

ESI: Electrospray Ionization.

MALDI: Matrix-Assisted Laser Desorption Ionization.

MLVA: Multi Locus VNTR Analysis.

MS: Mass Spectrometry.

NBQ: Nuclear, biológico y químico.

NGS: Next-Generation Sequencing.

NRBQ: Nuclear, radiológico, biológico y químico.

PUBMED®: base de datos de libre acceso a la National Medicine Library.

PCR: Polymerase Chain Reaction.

PCR-DGGE (Polymerase Chain Reaction – Denaturing Gradient Gel Electroforesis.

RE-LAB: Red de Laboratorios de Alertas Biológicas.

SEDEX: Servicio de Desactivación de Explosivos.

SELDI: Surface Enhanced Laser Desorption/Ionization.

SMRT: Single Molecule Real Time sequencing.

SNP: Single Nucleotide Polymorphisms.

SURPI: Sequence-based Ultra Rapid Pathogen Identification.

TEDAX: Técnico Especialista en Desactivación de Artefactos Explosivos.

VNTR: Variable Number of Tandem Repeats.

WGSS: Whole Genome Shotgun Sequence.

Referencias

Aslam, B., Basit, M., Nisar, M. A., Khurshid, M. y Rasool, M. H. (2017). Proteomics: Technologies and their Applications. *J Chromatogr Sci.*, *55*(2), 182-196. https://doi.org/10.1093/chromsci/bmw167

Budowle, B., Murch, R. y Chakraborty, R. (2005). Microbial forensics: the next forensic challenge. *Int J Legal Med.*, *119*(6), 317-30. https://doi.org/10.1007/s00414-005-0535-y

Escuela de Guerra del Ejército (2022). *Manual Curso Riesgos NBQ*.

Goodwin, S., McPherson, J. D. y McCombie, W. R. (2016). Coming of age: ten years of next-generation sequencing technologies. *Nat Rev Genet.*, *17*(6), 333-351. https://doi.org/10.1038/nrg.2016.49

Gupta, N. y Verma, V. K. (2019). Next-Generation Sequencing and Its Application: Empowering in Public Health Beyond Reality. *Sp Nat Sing*, 313-341. https://doi.org/10.1007/978-981-13-8844-6_15

Hyytiä-Trees, E. K., Cooper, K., Ribot, E. M. y Gerner-Smidt, P. (2007). Recent developments and future prospects in subtyping of foodborne bacterial pathogens. *Future Microbiol.*, *2*(2), 175-85. https://doi.org/10.2217/17460913.2.2.175

Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad.

Medical Management of Biological Casualties Handbook (2014). USAMRIID'S. 8th edition.

Merkley, E., Kaiser, B., Wunschel, D. y Wahl, K. (2020). Proteomics for Bioforensics. *Microbial Forensics* (pp. 251-264). 3th edition. https://doi.org/10.1016/B978-0-12-815379-6.00017-9

Merkley, E. D., Sego, L. H., Lin, A., Leiser, O. P., Kaiser, B. L. D., Adkins, J. N., Keim, P. S., Wagner, D. M. y Kreuzer, H. W. (2017). Protein abundances can distinguish between naturally-occurring and laboratory strains of Yersinia pestis, the causative agent of plague. *PLoS One*, *12*(8), e0183478. https://doi.org/10.1371/journal.pone.0183478

Mintz, Y. y Brodie, R. (2019). Introduction to artificial intelligence in medicine. *Minim Invasive Ther Allied Technology*, *28*, 73-81. https://doi.org/10.1080/13645706.2019.1575882

Mishra, A., Khan, S. y Das, A. (2023). Evolution of Diagnostic and Forensic Microbiology in the Era of Artificial Intelligence. *Cureus*, *15*(9), e45738. https://doi.org/10.7759/cureus.45738

National Research Council (2011). *Review or the Scientific Approaches Used During the FBI's Investigation of the 2001 Anthrax Letters*. https://doi.org/10.17226/13098

Oliveira, M., Mason-Buck, G., Ballard, D., Branicki, W. y Amorim, A. (2020). Biowarfare, bioterrorism and biocrime: A historical overview on

microbial harmful applications. *Forensic Sci Int.*, *314*, 110366. https://doi.org/10.1016/j.forsciint.2020.110366

Orden PCI/1381/2018, de 18 de diciembre, por la que se regula la Red de Laboratorios de Alerta Biológica "Re-Lab".

Real Decreto de 1882. Por el que se Aprueba la Ley de Enjuiciamiento Criminal, 14 de septiembre de 1882.

Real Decreto 664/1997, de 12 de mayo, sobre la protección de los trabajadores contra los riesgos relacionados con la exposición de agentes biológicos durante el trabajo.

Rhoads, D. D. (2021). Computer vision and artificial intelligence are emerging diagnostic tools for the clinical microbiologist. *J Clin Microbiol*, *58*. https://doi.org/10.1128/JCM.00511-20

Satam, H., Joshi, K., Mangrolia, U., Waghoo, S., Zaidi, G., Rawool, S., Thakare, R. P., Banday, S., Mishra, A. K., Das, G. y Malonia, S. K. (2023). Next-Generation Sequencing Technology: Current Trends and Advancements. *Biology*, *12*, 997. https://doi.org/10.3390/biology12070997

Schmedes, S. y Budowle, B. (2009). Microbial Forensics. En *Encyclopedia of Microbiology* (pp. 22-34). 4th edition. https://doi.org/10.1016/B978-0-12-801238-3.02483-1

Schmedes, S. E., Sajantila, A. y Budowle, B. (2016). Expansion of Microbial Forensics. *J. Clin Microbiol*., *54*(8), 1964-1974. https://doi.org/10.1128/JCM.00046-16

Zheng, Y., Qiu, X., Wang, T. y Zhang J. (2021). The Diagnostic Value of Metagenomic Next-Generation Sequencing in Lower Respiratory Tract Infection. *Front Cell Infect Microbiol*., *11*, 694756. https://doi.org/10.3389/fcimb.2021.694756

Habilidades prácticas de actuación policial en la atención a familiares y allegados de personas desaparecidas

Practical Skills in Police Action in the Dealing with Relatives of Missing Persons

Ana Isabel Álvarez-Aparicio
Grupo de Trabajo de Intervención Psicológica en Desapariciones del Colegio Oficial de la Psicología de Madrid (GIPD-COPM).
gipd@cop.es | https://orcid.org/0000-0003-2837-9211

José María Martínez Fernández
Grupo de Trabajo de Intervención Psicológica en Desapariciones del Colegio Oficial de la Psicología de Madrid (GIPD-COPM).
https://orcid.org/0009-0006-3925-2389

Elena Herráez-Collado
Grupo de Trabajo de Intervención Psicológica en Desapariciones del Colegio Oficial de la Psicología de Madrid (GIPD-COPM).
https://orcid.org/0000-0001-8207-7615

DOI: https://doi.org/10.14201/cp.31941
Recibido: 20-03-24 | Aceptado: 04-05-24

Resumen
La desaparición de una persona supone un gran impacto que no queda limitado a su entorno más cercano. También los profesionales pueden verse afectados por los elevados niveles de incertidumbre y sufrimiento que experimentan familiares y allegados. Dar un tratamiento prioritario a la problemática de las desapariciones resulta crucial. El desarrollo de unas óptimas habilidades prácticas, que promueva estrategias de intervención adecuadas en la atención al entorno de la persona desaparecida, se valora esencial. Del mismo modo, se considera necesaria la implementación de medidas de gestión del estrés y autocuidado del profesional para prevenir problemáticas asociadas, de manera directa o indirecta, a la exposición a este tipo de situaciones.

Palabras clave
Personas desaparecidas; Desapariciones; Habilidades; Intervención psicológica; Actuación policial; Intervinientes; Estrés laboral; Autocuidado.

Abstract
The disappearance of a person implies a great impact that is not limited to those closest to the person. Professionals can also be affected by the high levels of uncertainty and distress experienced by relatives and loved ones. Addressing the issue of disappearances as a priority is crucial. The development of optimal practical skills, promoting appropriate intervention strategies in the care of the missing person's environment, is considered essential. Similarly, the implementation of stress management and self-care measures for the professional is considered necessary to prevent problems associated, directly or indirectly, with exposure to this type of situation.

Keywords
Missing persons; Disappearances; Skills; Psychological intervention; Police action; Responders; Professional stress; Self-care.

1 La problemática de las desapariciones en España

La desaparición de personas es una problemática común a todas las sociedades y culturas (López *et al*., 2023). A lo largo de la historia de la humanidad son muchos los registros de personas que han desaparecido sin dejar rastro, sumiendo a sus seres queridos en la incertidumbre y el dolor.

Nadie escapa a la posibilidad de vivir una desaparición en su entorno, e incluso ser quien desaparece, pues esta condición no es exclusiva de sexo, raza, edad o nivel socioeconómico alguno (Ministerio del Interior, 2017).

Son muchas las motivaciones que pueden existir tras una desaparición, pudiéndose clasificar esta en nuestro país como

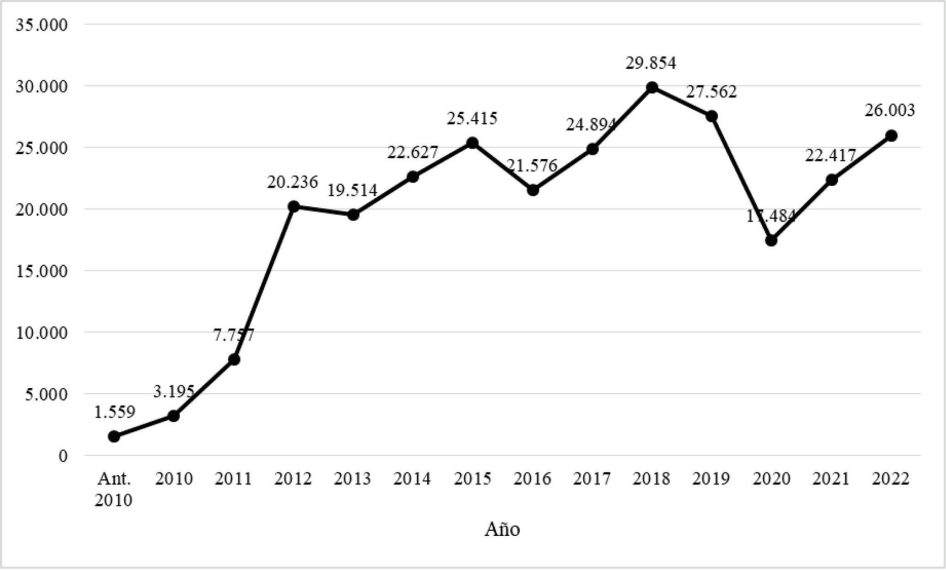
voluntaria, involuntaria o forzosa (Cereceda y Tourís, 2019), o de manera operativa y congruente con las investigaciones de García-Barceló *et al*. (2019), como voluntaria-escape, voluntaria-disfuncional, involuntaria-accidental e involuntaria-forzosa; propiciando tres posibles desenlaces en el caso de ser resuelta: aparición en buen estado de salud, aparición con lesiones de índole física y/o psicológica, aparición de la persona fallecida (López *et al*., 2023).

Pero con independencia de las causas motivadoras, si hay un elemento común a todas ellas, ese es la incertidumbre (De Puelles, 2018), así como el impacto psicológico y emocional que se produce a múltiples niveles (Álvarez-Aparicio, 2018). De este modo, y como señalan diversos autores (Boss, 2001; De Castro, 2019; De Puelles, 2018), la desaparición de un ser querido presenta particularidades en comparación con otros sucesos traumáticos que dificultan notablemente el proceso de adaptación a la situación, eliminándose ritos individuales y sociales que pueden facilitar el ajuste a una nueva realidad donde el ser querido ya no está.

Pero como ya se ha señalado, la sacudida que la desaparición de una persona provoca, no se limita a su entorno más cercano, sino que también incide sobre la comunidad de pertenencia del ausentado y sus familiares y allegados, la sociedad en sí misma, incapaz de dar respuesta a lo ocurrido pese a los recursos invertidos y los propios profesionales que buscan obtener resultados que permitan dar solución a la desaparición, poniendo fin al sufrimiento que su mantenimiento en el tiempo provoca (Álvarez-Aparicio, 2018).

Cada año, una media de 23.000 denuncias por desaparición de personas se interponen en nuestro país (figura 1), de ellas, desde que se tienen registros en el Sistema PDyRH, la mayor parte se resuelven satisfactoriamente en los primeros días, quedando alrededor de un 5 % sin cesarse (López *et al*., 2023). Debe tenerse en cuenta que el Sistema de Personas Desaparecidas y Restos Humanos sin Identificar (PDyRH) comenzó su funcionamiento en el año 2010, siendo plenamente operativo para todos los Cuerpos Policiales en el año 2012. Se trata pues, de un sistema dinámico

Figura 1: Evolución anual del número de denuncias interpuestas por desaparición de personas en España. *Nota.* Extraído y adaptado de «*Informe Anual Personas Desaparecidas durante el año 2022*» de López *et al*., 2023, p. 29. Puesto que el Sistema PDyRH comenzó a estar plenamente operativo en el año 2012, el incremento registrado entre los años 2010 y 2012 es especialmente elevado. Puede apreciarse igualmente el descenso registrado en el año 2020 (como consecuencia de la COVID).



que está en constante actualización, conforme la situación de las denuncias varía (López *et al*., 2022).

Cuando un ser querido desaparece, su entorno inicia una búsqueda incansable del mismo (Martel *et al*., 2021). En paralelo, la investigación se inicia y los profesionales se unen en pro de un mismo objetivo: dar con el paradero de la persona ausente de su residencia habitual de la que familiares y amigos carecen de información sobre su estado o situación.

Como señala Álvarez-Aparicio (2024, p. 39):

> Las desapariciones deben entenderse como procesos dinámicos que van a ir evolucionando en el tiempo conforme se modifican las circunstancias que las envuelven y su consiguiente investigación. Consecuentemente, las reacciones y necesidades que se van a observar en las personas afectadas, pueden también fluctuar, en ocasiones de forma rápida e imprevisible, siendo preciso que el profesional sea

capaz de adaptarse y emplear las habilidades, estrategias, técnicas y herramientas más adecuadas en cada caso.

Así, la inexistencia de dos situaciones iguales, dada la idiosincrasia de cada suceso, cada afectado y cada fase del proceso que supone una desaparición, hace que la flexibilidad y la perspectiva evolutiva, sean dos aspectos esenciales que los y las profesionales deben contemplar en cada intervención. Para ello resulta esencial que estos estén debidamente capacitados y especializados en el abordaje de esta problemática.

Con frecuencia, y como piden diferentes Asociaciones de Familiares de Personas Desaparecidas y otros profesionales, los recursos son insuficientes, sobre la base de que pese a la inquietud y alarma social que genera esta problemática, sigue sin ser considerada un problema de Estado, valoración que sí tienen otras casuísticas de similar calado (Beltrán, 2016).

La *Comisión Especial para el estudio de la problemática de las personas desaparecidas sin causa aparente* constituida en 2013 por acuerdo del Pleno del Senado, en su informe de conclusiones, fue clara en este sentido señalando la necesidad de abordar de manera prioritaria la problemática de las personas desaparecidas de manera global, abarcando tanto los aspectos técnicos y legislativos, como también los humanitarios. Diez años después, y pese a los avances logrados, aún existen grandes elementos de mejora.

Así, especialmente en los casos en que las ausencias se mantienen en el tiempo, en lo que ha venido a denominarse *desapariciones de larga duración,* su exigencia hace que sea preciso una preparación formativa e informativa específica y especializada de los profesionales que llevan la investigación, como así quedó también recogido en la *Comisión Especial para el estudio de la problemática de las personas desaparecidas sin causa aparente* (2013).

Como señalan algunos autores (Álvarez-Aparicio, 2015), con frecuencia, fruto de los estereotipos sociales, se atribuye al personal interviniente una invulnerabilidad psicológica

a las situaciones, por críticas que estas sean, más cercanas al mito. La realidad, de la mano de diferentes estudios, muestra que los profesionales también pueden verse afectados en mayor o menor medida, al constituir estas situaciones procesos tóxicos donde el sufrimiento humano está presente (Martín y Parada, 2008; Robles y Medina, 2002). Así, es justamente el contacto con el sufrimiento humano, lo que genera mayores niveles de ansiedad y estrés en los profesionales, como han avalado autores como Kroes, Margolis y Hurrell (1974), que apreciaron en sus investigaciones que la exposición al peligro físico podía desencadenar menores niveles de estrés que la atención directa a las víctimas o la comunicación de malas noticias a los familiares de estas.

Como se verá más adelante, cuando un ciudadano desaparece, a las exigencias externas que el investigador tiene que enfrentar, ya sean procedentes de familiares y allegados, la organización policial, la administración, los medios de comunicación, o la propia sociedad, se le unen con frecuencia las exigencias internas a las que el propio profesional se somete, producto de unas elevadas expectativas. La ausencia de avances en la investigación y con ello de respuestas a las demandas del entorno de la persona ausente, pueden ser un importante foco de malestar alimentado por el sentimiento de impotencia y falta de control, ante una realidad que se desconoce (Álvarez-Aparicio, 2015).

La deshumanización y el distanciamiento de las víctimas, como mecanismo de defensa por un lado, o la sobre-implicación en el caso por otro, puede tener serias consecuencias tanto para el entorno de la persona ausente como para los profesionales que llevan la investigación y la investigación misma (Álvarez-Aparicio, 2015). De ahí la importancia de desarrollar unas buenas prácticas en el marco policial (incluidas en ellas unas óptimas habilidades), en la atención al entorno de la persona desaparecida, como quedó de manifiesto en la Reunión de la Presidencia Española del Consejo de la Unión Europea en octubre de 2023 en Materia de Personas Desaparecidas (Álvarez *et al.*, 2023; Vinuesa, 2023), en consonancia con lo perseguido por el *I Plan Estratégico en materia de Personas Desaparecidas*, desarrollado por el Centro Nacional de Desaparecidos (Ministerio del Interior, 2022).

2 La importancia de unas buenas habilidades prácticas en la atención a familiares y allegados de personas desaparecidas

Si bien se ha visto que las consecuencias que una desaparición tiene se producen a muchos y diversos niveles, a continuación, nos centraremos en aquellos, objeto del presente escrito, sobre los que una adecuada atención puede suponer cambios relevantes.

Como se ha señalado, quizá uno de los ámbitos más duramente afectados por una desaparición, sea su entorno más cercano, pero no es el único. En ocasiones, son también los profesionales implicados en la búsqueda y localización de la persona, junto a otros intervinientes de la salud, seguridad y emergencias, quienes pueden verse perjudicados. Poseer unas buenas habilidades en la atención a familiares y allegados de la persona en paradero desconocido, no solo puede suponer un beneficio para estos sino también para los profesionales implicados y la investigación misma (Álvarez-Aparicio *et al*., 2023).

2.1 Beneficios para familiares y allegados

La desaparición de un ser querido supone, a su entorno más cercano, una situación difícil de gestionar. A los problemas de índole psicológico y emocional que puedan surgir, se unen otros de carácter económico, judicial o social (Álvarez-Aparicio, 2018).

Diferentes investigaciones coinciden en señalar el duelo prolongado, la depresión y el estrés postraumático, como las reacciones que con mayor frecuencia aparecen en familiares y allegados de la persona desaparecida (Pérez-Bambó, 2021), suponiendo mayor alteración y patología con respecto a otros sucesos en los que la persona resulta fallecida (Barakovic *et al*., 2013, 2014; Huang y Habermas, 2019; Isuru *et al*., 2019; Pérez-Bambó, 2021; Powell *et al*., 2010).

Los estudios analizados por Pérez-Bambó (2021) en la revisión sistemática efectuada sobre una muestra de 17 artículos publicados sobre el tema desde el año 2000[1], señalan concretamente como principales consecuencias de una desaparición: (a) sintomatología asociada al trauma (94 %); (b) alteraciones en el proceso de duelo, duelo patológico, traumático o prolongado (88 %) y (c) depresión (82 %). De forma más concreta algunos de los síntomas más frecuentes recogidos por los estudios revisados fueron (Pérez-Bambó, 2021, p. 18):

> Aislamiento social y sentimiento de soledad (71 %), pérdida de seguridad y de confianza en la vida y en las personas (65 %), ansiedad (59 %), pensamientos intrusivos (59 %), sentimiento de culpa (47 %), tristeza (47 %), problemas somáticos (41 %), miedo (35 %), insomnio y pesadillas (29 %), pérdida de sentido (29 %) e irritabilidad (24 %) y en menor medida desesperanza (18 %), pérdida de interés por las actividades personales (18 %), vergüenza (18 %), conflictos familiares (12 %) y problemas de concentración (12 %).

Un reciente estudio realizado en España por De Vicente y Santamaría (2022) mediante el Cuestionario del Impacto del Trauma (CIT) en una muestra de familiares de personas desaparecidas, arroja resultados similares, informando que:

> De los 29 indicadores de malestar psicológico e impacto psicosocial estudiados, las familias con personas desaparecidas presentan puntuaciones muy elevadas en 26 de ellos, siendo muy superiores a las puntuaciones de la población general en 20 de ellos. Los más significativos son: deterioro en el funcionamiento, intrusión, depresión, disociación, cambio vital, trastor-

1. Las muestras estudiadas en los artículos seleccionados representan una población heterogénea en cuanto a procedencia, causa de la desaparición y parentesco con la persona desaparecida. La mayoría de los estudios fueron hechos en países europeos, aunque la población europea estudiada representa solo un 38 % sobre la muestra total. Casi el 60 % de los artículos hacen referencia a países en conflicto o tras el mismo. La muestra global supuso un total de 4569 personas, de las cuales 3.381 fueron familiares de personas desaparecidas (74 %).

> nos de sueño, alteración cognitiva, alteración de la activación y reactividad, distanciamiento social, pánico, autosabotaje, desregulación emocional, ideación suicida, problemas somáticos, ansiedad, rumiación (p. 2).

Con base en los estudios realizados se puede observar sintomatología asociada a altos niveles de estrés y ansiedad consecuencia de las exigencias y auto-exigencias que de la situación se derivan. Las elevadas puntuaciones en disociación obtenidas por De Vicente y Santamaría (2022), muestran una sintomatología postraumática de especial gravedad, junto a alteraciones de carácter somático e internalizante, un elevado impacto en el ámbito interpersonal y una visión negativa del mundo, los demás y ellos mismos. En definitiva, los estudios muestran que la desaparición de un ser querido puede suponer una interferencia completa en todas las esferas de la persona.

En cuanto a aquellos elementos que pueden influir en mayor grado en el desarrollo de psicopatología destacan: la creencia ambivalente, la idea de que la persona desaparecida pueda seguir con vida, así como un estilo de afrontamiento evitativo. Del mismo modo, un pensamiento contrafáctico ascendente (consistente en pensar que las cosas podrían haber ido mejor de darse otras alternativas), cogniciones negativas, rumiación y atenuación (desvalorización, omisión o atenuación del aspecto positivo), aparecen asociados a una mayor morbilidad psicológica (Barakovic *et al*., 2013, 2014; Huang y Habermas, 2019; Isuru *et al*., 2019; Kennedy *et al*., 2020; Lenferink *et al*., 2017; Lenferink *et al*., 2018a, 2018b, 2019; Pérez-Bambó, 2021; Powell *et al*, 2010).

En contraposición, aquellos mecanismos que parecen estar presentes en mayor medida facilitando la integración de lo ocurrido y la reducción consecuente de sintomatología se basan en: el apoyo social (real y percibido); un afrontamiento activo centrado en el problema; la implicación en organizaciones comunitarias, asociaciones de familiares de personas desaparecidas o movimientos para preservar su memoria; la autocompasión y la autocomprensión; el apoyo profesional y, en menor medida, un pensamiento contrafáctico descendente (Andersen *et al*., 2020; Arenliu *et al*., 2019; Huang y Habermas, 2019; Kennedy

et al., 2020; Lenferink *et al*., 2017; Lenferink *et al*., 2018a, 2018b, 2019; Pérez-Bambó, 2021; Powell *et al*, 2010).

Partiendo de estos factores, diferentes investigadores han propuesto diversos tipos de intervenciones: (a) terapia grupal o grupos de apoyo mutuo (Andersen *et al*., 2020; Arenliu *et al*., 2019; Barakovic *et al*., 2014; Kennedy *et al*., 2020; Lenferink *et al*., 2018a, 2018b); (b) reactivación conductual (Andersen *et al*., 2020; Arenliu *et al*., 2019; Barakovic *et al*., 2014; Kennedy *et al*., 2020; Lenferink *et al*., 2018a, 2018b); (c) aceptación de emociones incómodas y tolerancia a la incertidumbre (Arenliu *et al*., 2019; Kennedy *et al*., 2020; Lenferink *et al*., 2017; Lenferink *et al*., 2018a, 2018b, 2019; Powell *et al*, 2010); (d) resignificación de la pérdida (Andersen *et al*., 2020; Arenliu *et al*., 2019; Huang y Habermas, 2019; Kennedy *et al*., 2020; Lenferink *et al*., 2017); (e) expresión emocional y el uso de técnicas narrativas (Andersen *et al*., 2020; Huang y Habermas, 2019; Lenferink *et al*., 2019); (f) desarrollo de la autocompasión y el entrenamiento en atención plena (Kennedy *et al*., 2020; Lenferink *et al*., 2017; Lenferink *et al*., 2018a, 2018b, 2019). En menor medida, algunos estudios proponen también el uso de: técnicas simbólicas, reestructuración cognitiva, psicoeducación exposición, en imaginación y técnicas de relajación (Pérez-Bambó, 2021, p. 21).

En cuanto a los enfoques terapéuticos recomendados, pese a la escasez de estudios existentes sobre eficacia de los tratamientos aplicados, la revisión efectuada por Pérez-Bambó (2021) sugiere la Terapia Cognitivo-Conductual, el Mindfulness, la Terapia de Aceptación y Compromiso y la Terapia Centrada en la Compasión, integradas en un marco psicosocial más amplio, como opciones de intervención óptimas. En estos casos, además, resulta especialmente indicado el formato grupal.

Unas buenas habilidades por parte de los profesionales que intervienen en casos de desaparición deben insertarse en las acciones a desarrollar en todo momento por cuanto se persigue amortiguar el impacto del suceso y favorecer una integración adaptativa del mismo, proporcionar recursos de afrontamiento y prevenir que la situación (y sus consecuencias derivadas), empeore.

Como se ha visto, facilitar y reforzar el apoyo social (real y percibido), asegurando que este se mantiene en el tiempo, proporcionar estrategias de control de la activación, manejo y gestión emocional o facilitar la integración de la experiencia mediante estrategias narrativas, simbólicas y de integración cognitiva, junto al desarrollo de técnicas y estrategias de autocuidado; son solo algunos de los aspectos donde unas buenas habilidades son esenciales y que se han mostrado eficaces en el afrontamiento de situaciones donde un ser querido desaparece. El profesional de las Fuerzas y Cuerpos de Seguridad (FCS) puede aquí marcar la diferencia.

El impacto que una situación supone para cada persona viene marcado, junto a variables de índole ambiental, situacional y personal, por la percepción del hecho y los recursos para hacerle frente (Robles y Medina, 2002). El profesional de las FCS no puede cambiar el suceso pero sí el modo en que es percibido y por tanto puede ser afrontado. En desapariciones, donde el manejo de la incertidumbre se revela complejo y esencial (De Puelles, 2018) y el dolor y sentimiento de vacío hacen mella en la unidad biopsicosocial que es la persona (Acinas, 2012), dotar de habilidades prácticas al profesional resulta vital. Una buena comunicación que ajuste expectativas y facilite el funcionamiento adaptativo de la persona, junto a un adecuado manejo de herramientas que doten de control y faciliten la gestión de la situación, puede resultar beneficioso para todas las partes implicadas.

2.2 Beneficios para los profesionales (FCS)

Como se ha señalado, con frecuencia se adjudican a los integrantes de las FCS unas cualidades poco realistas, de marcada superioridad, en su desempeño profesional y afrontamiento personal ante situaciones de elevada complejidad. No obstante, la realidad muestra que si bien los profesionales que se mueven en el ámbito de la seguridad y las emergencias pueden tener un umbral de resistencia mayor al de la población general, también se ven afectados por las situaciones que viven (Martín y Parada, 2008).

Cualquier situación adversa, estresante, crítica y/o traumática puede ser entendida como un proceso tóxico por la afectación que puede conllevar. Nadie es totalmente inmune. No obstante la mayor parte de las reacciones experimentadas suelen ser normales y de carácter transitorio. Más allá de esto, según algunos autores, todos tenemos un *punto crítico* a partir del cual pueden darse desajustes psicológicos. Factores de desarrollo personal, capacidad de expresión emocional, marcadores biológicos y esquemas cognitivos, serían determinantes (Robles y Medina, 2002).

El proceso de búsqueda y localización de una persona desaparecida es una situación altamente estresante y potencialmente traumática para muchas de las personas afectadas, también para los profesionales que trabajan para resolver el caso (Álvarez-Aparicio, 2018). Como señala Álvarez-Aparicio (2015, p. 16):

> En el caso de las desapariciones, máxime si estas tienen un carácter prolongado, las demandas por parte del entorno del desaparecido a las FCS para una rápida y eficaz resolución de la situación se convierten en una presencia constante y mantenida en un tiempo, cuyo fin es imposible de determinar. A las exigencias externas, ya sean procedentes de la familia, la organización policial, la administración, los medios de comunicación, o la propia sociedad, se le unen las exigencias internas, producto de unas elevadas expectativas.

Los riesgos psicosociales más específicos de los profesionales que se enfrentan a situaciones adversas con cierta frecuencia son el estrés traumático secundario y el desgaste profesional o *burnout* (Newell y MacNeil, 2011), no estando exentos de otros riesgos como el estrés o las agresiones (Pacheco *et al*., 2012). Tal es el caso de los integrantes de las FCS (Pérez-Serrano *et al*., 2023)

A las variables de índole personal, ambiental y situacional propias de las tareas a desarrollar, se le unen otras de carácter organizacional como los horarios, la cantidad de casos y per-

sonas a atender, la sobrecarga laboral, emocional y temporal, la falta de recursos humanos, materiales y de reconocimiento, etc., que son factores de riesgo de estrés traumático secundario y desgaste profesional (Garrosa, 2012a). Se reconoce además, que el personal policial a menudo está expuesto a diversos factores estresantes específicos de su trabajo, como son: peligros y riesgos inherentes al trabajo policial, eventos traumáticos, así como factores estresantes organizacionales, como desafíos relacionados con el aumento de las cargas de trabajo y la escasez de personal (Purba y Demou, 2019; Simonovska *et al*., 2023); si bien existen pocos estudios sobre factores estresantes crónicos, como el trabajo en áreas de alto riesgo o exposición prolongada a situaciones potencialmente traumáticas, pese a los efectos significativos que puede tener en la salud y el bienestar del profesional (Simonovska *et al*., 2023).

Tanto el estrés traumático secundario (que puede ocurrir súbitamente y supone que «el profesional adquiere los síntomas por la exposición o el contacto con la situación o con las personas que sufren directamente el trauma» [Newell y MacNeil, 2011]), como el desgaste profesional o *burnout* (que se caracteriza por «un estado de agotamiento físico, emocional y mental, como consecuencia de la excesiva implicación laboral y de las altas demandas del trabajo» [Garrosa, 2012a]), genera una serie de reacciones emocionales-cognitivas, motoras y somáticas que pueden afectar tanto al trabajador, en forma de enfermedad y pérdida de bienestar, como a la organización y a la calidad del servicio asistencial prestado (Puerto, 2007). En el caso del *burnout* además, se cree que los efectos acumulativos de lidiar con las experiencias negativas y los eventos traumáticos pueden incrementar el riesgo de sufrirlo (Kohan y Mazmanian, 2003).

Como se ha visto y señala Álvarez-Aparicio (2015), «lejos de lo que pueda pensarse, es precisamente el contacto con el sufrimiento humano, lo que genera mayores niveles de ansiedad y estrés». Las investigaciones realizadas por Kroes, Margolis y Hurrell (1974), mostraron cómo ante situaciones de crisis solía predominar en menor grado el peligro físico como factor de estrés, que la atención a las víctimas o la comunicación de malas noticias a los familiares de estas. En el ámbito policial, una revi-

sión de la literatura relacionada con el impacto de la investigación criminal en el bienestar de los profesionales (Cartwright y Roach, 2022), concluye que existen una serie de factores que impactan negativamente, principalmente aquellos que tienen que ver con casos en los que la víctima era una persona vulnerable (especialmente un menor).

En los casos de desaparición, familiares y allegados están ávidos de información y precisan respuestas para calmar la incertidumbre que experimentan. Los profesionales, carentes de estas, se sienten con frecuencia impotentes ante unas demandas a las que es difícil dar solución, pudiendo mostrar diversas reacciones, desde una sobreimplicación en la resolución de la situación, hasta la deshumanización y distanciamiento del entorno de la persona desaparecida (Álvarez-Aparicio, 2015). En ambos casos se resiente la relación con los familiares y allegados, el autoconcepto y autoestima del profesional y la calidad de la atención dispensada y la investigación realizada.

Así, a las altas demandas surgidas de agentes externos (entorno de la persona ausente, medios de comunicación, organización o institución de pertenencia...) e internos (las propias exigencias del profesional), se le añaden otros factores como la escasez de recursos (materiales y humanos) para encontrar y dar respuestas a lo ocurrido. Como señala Garrosa (2012a, p. 273), estos elementos, «la experiencia prolongada de escasos recursos y un alto nivel de demandas, conducen al agotamiento y a la pérdida de expectativas profesionales».

Pero las tareas en el ámbito de la seguridad y emergencias, como es el trabajo policial, también tiene consecuencias psicológicas positivas como: (a) una alta satisfacción laboral en los investigadores que trabajan por ejemplo en explotación sexual infantil (Holt y Blevins, 2011); (b) lo que ha venido a denominarse *resiliencia vicaria* en base a la observancia de la resiliencia que poseen las víctimas (Engstrom *et al*., 2008; Foley y Massey, 2021; Hernandez-Wolfe *et al*., 2015); (c) experimentación de sentimientos positivos ayudando a superar su trauma a la víctima (*satisfacción por compasión*), ya sea identificándolas, arrestando a los culpables (de haberlos) o protegiendo al resto de la población (Foley y Massey, 2021).

Son por tanto necesarias acciones a nivel personal, organizacional y relacional. Como señala Garrosa (2012a, p. 275), los profesionales en contacto con situaciones potencialmente traumáticas, como puede ser una desaparición, «necesitan tener unas adecuadas condiciones laborales, mejorar las competencias emocionales de resistencia y la formación en materia de autocuidado, ante las experiencias emocionales agudas y crónicas laborales. Para ello, se deben fomentar los recursos personales y organizacionales de una manera integrada».

En la misma línea, Álvarez-Aparicio (2015, p. 9) expone que:

> Medidas de prevención, como formación especializada en el área, que promueva estrategias de intervención apropiadas en la interacción con el entorno del desaparecido, así como en el automanejo emocional del estrés y variables asociadas, que un caso de este tipo suponen; se revelan como las más adecuadas para maximizar la calidad del trabajo desarrollado, y minimizar el impacto negativo que estas situaciones pueden tener sobre el interviniente, tanto en el ámbito personal como profesional.

En definitiva, como señala Benedito (1997), cualquier profesión que implique interacciones con otras personas, requiere además de los conocimientos técnicos, las habilidades psicológicas suficientes para llevarlas a cabo de forma eficaz. En este sentido, formación e información, no solo a las familias, sino a los profesionales como enlace con estas, resulta esencial para un buen desempeño laboral y personal (Álvarez-Aparicio, 2015).

Como se ha visto, el empleo de unas adecuadas habilidades en la atención a familiares y allegados de personas desaparecidas, no solo tiene beneficios para estas, que pueden ver facilitado el proceso de aceptación y adaptación a una nueva realidad donde su ser querido se encuentra en paradero desconocido, sino también para el profesional, que puede ver reducidos sus niveles de estrés como consecuencia de mayor sensación de control así como la probabilidad de aparición de problemáticas como el *burnout* o el estrés traumático secundario.

2.3 Beneficios para la investigación

Es una cuestión ampliamente estudiada que la *alianza terapéutica* que se establece entre el profesional y la persona que precisa de atenciones y respuestas, tiene un papel clave en el éxito de las intervenciones realizadas, tanto o más incluso, que las técnicas empleadas (Martín y Muñoz, 2009).

Como señala Galán (2018, p. 12), «cuando una persona desaparece la investigación debe centrarse en saber qué ocurrió. Por ausencia de pruebas directas, este tipo de investigaciones son las más difíciles de indagar». Como indica este mismo autor, en lo que ha definido como *escena fantasma*, «con frecuencia no hay escena del suceso, ni cuerpo, arma o testigos». Por ello, el entorno de la persona desaparecida puede proporcionarnos información clave en el proceso.

La entrevista policial es una técnica científica más al servicio de la investigación y que resulta fundamental en casos de desapariciones. Desde un punto de vista policial, todas aquellas personas con las que haya tenido contacto la persona desaparecida, constituyen una fuente esencial de información que facilita pistas, datos o referencias que enfocan o dirigen las demás actuaciones policiales. Así, como expone González (2013):

> En muchos casos, además, sólo se cuenta con esta información, por no existir otro tipo de indicios. Por tanto, una adecuada realización de la entrevista policial, resulta fundamental para la obtención de testimonios de aquellas personas que puedan aportar información o tengan conocimiento del hecho.

Con la entrevista «se persigue la obtención de información lo más exacta y completa posible, reduciendo el trauma a los entrevistados y protegiendo los derechos de los acusados (de haberlos)» (González, 2015, p. 188). Para ello, el profesional debe estar adecuadamente formado y entrenado tanto en una serie de técnicas como de habilidades (González, 2008).

Recordar supone esfuerzo. A ello, debe añadirse que niveles muy elevados de activación dificultan el procesamiento hipocampal lo que puede dar lugar a dificultades para recordar lo ocurrido con detalle, e incluso a lagunas de memoria (Álvarez-Aparicio, 2018). Es por ello esencial que, desde un primer momento se establezca una buena relación interpersonal que facilite la colaboración del entorno afectado por la desaparición. En ocasiones, las personas son remisas a colaborar en base a casuísticas y creencias poco ceñidas a la realidad que es fundamental ajustar y, en su caso, flexibilizar. Así, es posible que piensen que si colaboran, se les va a requerir constantemente con las consiguientes molestias, o que si aportan determinada información pueden dañar la imagen de la persona desaparecida o la suya propia, incluso sentirse juzgados, o lo que es peor, ser acusados.

No se debe perder de vista que el entrevistador eficaz ayuda al entrevistado a recordar, facilita la comunicación de lo recordado, y rastrea sistemáticamente, con orden y sin prisa, todos los aspectos del hecho, registrándolos de forma extensa y objetiva (González, 2008). Unas buenas habilidades en la atención a familiares y allegados pueden generar unos niveles importantes de confianza que faciliten este punto.

3 Habilidades requeridas para el adecuado desarrollo de la función policial durante la intervención en desapariciones

Hoy día la actuación policial está continuamente expuesta a valoración y crítica. Si bien, frecuentemente, este ejercicio recibe una estimación positiva, no es extraño escuchar o leer opiniones negativas por diferentes motivos, lo que lleva en muchos casos, a que se critique y se genere solo un estereotipo de las personas integrantes de los cuerpos policiales. A la visión desfavorable que en ocasiones reciben las FCS sobre la labor que realizan, se une la percepción de una escasa capacitación, actitudes y habilidades mostradas por sus integrantes ante diferentes problemáticas que por su naturaleza requieren cierta proximidad e

implicación. Además, ponen de manifiesto el inadecuado manejo de emociones, así como la carencia de habilidades necesarias para la resolución de muchos delitos (Alemán, 2022) y realización óptima de actuaciones policiales, entre las que podrían encajarse perfectamente las actividades necesarias a desarrollar en la desaparición de personas.

Diferentes estudios señalan la percepción de una respuesta ineficaz y la demanda de cambios en las intervenciones policiales por parte de la ciudadanía, principalmente en aquellas actuaciones relacionadas, tanto con el trato recibido, para evitar fenómenos de victimización secundaria, como con el incremento de la protección y de la seguridad (González y Garrido, 2015).

Teniendo en cuenta, (a) estos cambios sugeridos (en especial lo relativo a la victimización secundaria por las graves implicaciones que puede tener para las personas afectadas); (b) la gran cantidad de ocasiones en que esta victimización se puede generar a lo largo de una investigación policial y judicial y (c) la evolución llevada a cabo por las FCS para adaptarse a las nuevas realidades y necesidades sociales; se puede llegar a la siguiente conclusión: estas FCS, como instituciones de primera respuesta que intervienen desde los momentos iniciales en muchos episodios complicados de la vida de las personas, deberían tener la capacidad de proporcionar la ayuda necesaria a la ciudadanía sin afectar y/o menoscabar su salud mental cuando esta se enfrenta a situaciones inesperadas y altamente estresantes (Valencia y Trejos, 2013).

Se puede considerar, por tanto, que las FCS pueden y/o deben hacer uso de una suerte de estrategias y herramientas específicas que minimicen el impacto negativo para las personas de los sucesos altamente impactantes en los que intervienen a menudo, como son los casos de desaparición de personas. En términos genéricos, se plantean una serie de herramientas en consonancia con unos *primeros auxilios psicológicos*, que precisan ser adaptadas a la idiosincrasia de cada caso y situación. Por primeros auxilios psicológicos se entiende «un grupo de intervenciones psicológicas tempranas, breves y prácticas orientadas a paliar y prevenir

los efectos psicológicos de los sucesos traumáticos a corto, medio y largo plazo» (Muñoz *et al*., 2007, p. 13).

En este sentido, Valencia y Trejos (2013, p. 10) en relación a los *primeros auxilios psicológicos* en el servicio de atención al ciudadano desde un enfoque humanista, concluyen entre otras cuestiones, que:

> Los primeros auxilios psicológicos se convierten en la herramienta fundamental que los policías de la actualidad deberían aprender a manejar, para así contribuir con una prestación de servicio de atención al ciudadano en forma integral.
>
> Se hace necesario incluir dentro de la formación integral del policía los primeros auxilios psicológicos, ya que estos hacen parte del equipo de primera respuesta ante una necesidad de la comunidad.
>
> Es importante considerar que los primeros auxilios psicológicos no necesariamente deben ser aplicados por los profesionales de la salud mental, cualquier persona que esté debidamente capacitada y entrenada los puede aplicar.
>
> Cuando se le da el manejo de intervención inadecuado a una persona que ha experimentado una crisis circunstancial, puede generar trastornos mentales, intensidad de las manifestaciones físicas y emocionales, atentar o poner en riesgo la integridad de sí mismo y de las personas.

Por su parte Céspedes *et al*. (2020), sin nombrar específicamente esta técnica, sí hace referencia a una serie de habilidades necesarias para desarrollarla y llevar a cabo una actuación policial eficiente, concluyendo que la adecuada gestión de la emoción, la empatía y la comunicación asertiva son cuestiones fundamentales para prestar un buen servicio a la ciudadanía. Por ello, la inteligencia emocional ha cobrado especial interés en la formación de la Policía, para conseguir que el personal esté

preparado y tenga las herramientas suficientes para hacer frente a su día a día. Así mismo, formar en habilidades psicosociales a los y las integrantes de la Policía contribuye, en gran medida, a que estos actúen reconociendo las necesidades de la ciudadanía y cumplan con ellas, lo que sin duda también mejorará la buena imagen de la institución policial.

La Organización Mundial de la Salud (OMS) en 1999, define las habilidades para la vida o competencias psicosociales como «la habilidad de una persona para enfrentarse exitosamente a las exigencias y desafíos de la vida diaria». El quehacer diario de las FCS implica a menudo poner en práctica estas competencias en situaciones de alto impacto emocional para las personas; tanto para la ciudadanía que interactúa con los profesionales, como para los propios profesionales, por lo que se hace necesaria una adecuada capacitación y formación en estas cuestiones como indica Álvarez-Aparicio (2015).

La resolución de conflictos y el bienestar emocional son cruciales ante situaciones de estrés agudo que pueden darse en el trabajo policial (Antuña, 2022). Asimismo, considera este autor que la inteligencia emocional afecta a nuestra vida cotidiana en distintos ámbitos como la salud física y mental o la educación (Baudry *et al*., 2018; Li *et al*., 2021; Martins *et al*., 2010; Schutte *et al*., 2007; como se citó en Antuña, 2022).

En el estudio llevado a cabo por López et. al (2006), en el que examinaron la inteligencia emocional en una muestra de policías locales de Canarias, se comprueba por sus resultados que, si bien poseían habilidades adecuadas para conocer, comprender, regular y controlar sus emociones, la mayoría necesitaba mejorar sus competencias para percibir éstas. Dichos resultados, junto con otros expuestos anteriormente, ponen de manifiesto que unas adecuadas habilidades psicosociales e inteligencia emocional en las personas integrantes de las FCS mejora, no solo su bienestar psicológico, sino su salud mental en general. Esto, sin duda, repercutirá en un mejor desarrollo de las labores policiales que lleven a cabo, algo de suma importancia cuando se trata de campos de trabajo emocionalmente tan impactantes para la ciudadanía como son las desapariciones de personas.

3.1 Fases de la intervención policial y tareas a desarrollar en el ámbito de las desapariciones de personas

Atendiendo a las labores policiales a desarrollar en el ámbito de la desaparición de personas, se pueden establecer diferentes fases en la intervención policial considerando tanto los avances en la investigación como el tiempo transcurrido. Así, se puede hablar de fase de denuncia, fase de investigación y fase de cancelación o cese, siendo todas ellas importantes en lo que tiene que ver con la interacción del profesional de las FCS con el entorno de la persona desaparecida. Estas fases comparten muchas actuaciones y van a requerir la puesta en práctica de habilidades similares, aunque también será necesario emplear en mayor medida unas u otras de manera específica y diferencial en función de cada una de las fases.

Se sabe que, como en otro tipo de hechos que acercan la ciudadanía a las FCS, en el caso de la desaparición de personas el momento de la denuncia se muestra como un elemento clave. En el Protocolo *de Actuación de las Fuerzas y Cuerpos de Seguridad ante casos de personas desaparecidas* (Cereceda y Tourís, 2019, p. 23) se establece que:

> La denuncia es una declaración emitida, verbal o escrita, que permite la puesta en conocimiento del hecho de la desaparición de una persona, y en el ámbito de este protocolo de actuación, ante los miembros de las Fuerzas y Cuerpos de Seguridad, independientemente de si ese hecho reviste o no caracteres de delito.

Así mismo, tal denuncia es procedente en todos los supuestos en que tenga lugar la desaparición de una persona para la puesta en marcha de las actuaciones encaminadas a la localización de la misma, tal y como recoge el citado Protocolo (Cereceda y Tourís, 2019, p. 30).

Iniciado de este modo el procedimiento policial, a lo largo de todo el proceso será necesario ir recopilando información

para poder avanzar en el esclarecimiento de los hechos, lo que implica una serie de actuaciones profesionales, que precisan de habilidades específicas en cada caso. Estas pueden ser: la inspección ocular del domicilio de la persona desaparecida; el reconocimiento de los lugares que frecuentaba habitualmente; establecer contacto con familiares, amistades, compañeros de clase, de trabajo o de cualquier otra actividad que realizase; toma de declaración a testigos sobre el último momento en que se tuvo contacto con la persona desaparecida; recopilar el contenido de cámaras de video vigilancia; recoger medios tecnológicos que pudiera utilizar la persona desaparecida, así como posibles vehículos; realizar comprobaciones y verificaciones en centros hospitalarios y de otro tipo; establecer colaboración con otras organizacione; elaboración y ejecución de dispositivos de búsqueda, etc. (Cereceda y Tourís, 2019).

Del mismo modo, además de las labores propias de la investigación policial, los profesionales de las FCS deben observar una serie de actuaciones en cuanto a la atención, protección y orientación a los familiares de las personas desaparecidas, tal y como reflejan Cereceda y Tourís (2019, p. 125):

> Las Fuerzas y Cuerpos de Seguridad habilitarán canales de comunicación con las familias y personas allegadas al desaparecido, siempre procurando que ello no suponga un obstáculo para la investigación, búsqueda y localización de la persona desaparecida. Por consiguiente, se debe ser consciente de la angustia que genera la ausencia de una persona al entorno más cercano al que pertenece.

Como consecuencia, el Protocolo señala a continuación una serie de cuestiones a tener en cuenta en esas intervenciones, como son: (a) tratar de empatizar con los familiares y escucharlos sin reprimir las emociones y sentimientos que manifiesten, pudiendo ser habituales la agitación, la culpa, la ansiedad o la incertidumbre; (b) recomendar la posibilidad de requerir ayuda profesional; (c) ser cuidadoso con las respuestas para no generar mayor angustia de la que ya están padeciendo; (d) no gene-

rar ni dar falsas esperanzas, adecuando la información facilitada a la realidad de cada caso, pero siendo honestos y transmitiendo información real y veraz.

3.2 Habilidades a poner en práctica en la interacción con el entorno de la persona desaparecida

En relación a habilidades básicas para desarrollar un adecuado trabajo de los profesionales de las FCS en el ámbito de las desapariciones, a lo largo de este apartado se ha hecho referencia a diferentes conceptos que, con ánimo de operativizarlos y conseguir que sean útiles para el/la policía, se van a centrar y resumir en: habilidades relacionadas con la inteligencia emocional, la escucha activa y aquella clave en la gestión de la incertidumbre. Jugando un papel básico crucial, unas buenas habilidades de comunicación.

Respecto a la inteligencia emocional, puede definirse como un conjunto de habilidades que contribuyen a la evaluación y expresión, la regulación y el uso de los sentimientos (Salovey y Mayer, 1990, p. 189). Unos años más tarde, Goleman popularizó el término y enumeró tres componentes principales: la empatía, la asertividad y las relaciones prosociales (Goleman, 1997; Goleman y Cherniss, 2005; como se citó en Antuña, 2022).

Goleman (1997) considera que la empatía es la capacidad que tiene una persona para reconocer las emociones en los demás. Es decir, la habilidad de comprender los sentimientos de los otros y poder leer sus mensajes no verbales. Goleman (1997) señala que hay tres tipos de empatía, que funcionan de manera independiente en cada persona, a saber: empatía cognitiva, empatía emocional y preocupación empática.

Analizando cada tipo de empatía por separado, se puede considerar la empatía cognitiva como la capacidad de intentar comprender cómo se siente o qué debe estar pensando otra persona. Tener empatía cognitiva significa ver las cosas con la perspectiva de los demás, ponerse en los zapatos de otros. La empatía

emocional consiste en sentir físicamente con la otra persona, es la base de cualquier relación saludable y la razón por la que tenemos química con otras personas. En cuanto a la preocupación empática, a la que se conoce también como compasión, se trata del nivel más alto de empatía y no implica únicamente preocuparse por lo que piensa y siente la otra persona, sino hacer algo para mejorarlo.

En el ámbito policial, y en lo que al abordaje de las desapariciones respecta en relación a familiares y allegados, puede mostrarse dicha habilidad, por ejemplo, siendo sensible a las necesidades de las personas, entendiendo la dificultad del momento que pueden estar atravesando, adaptando tiempos y espacios a la misma y mostrando interés genuino por sus preocupaciones, entre otras.

Respecto al concepto de asertividad, según la Real Academia Española (2014) se define como «cualidad de asertivo», la cual, dicha de una persona, se refiere a que expresa su opinión de manera firme y con seguridad, respetando las ideas de los demás. Como señala Terroni (2009, p. 36), «juega un papel importante en las interacciones grupales, ya que constituye una habilidad o destreza a la hora de emitir opiniones y en los procesos de influencia grupal». Además, continúa Terroni (2009, p. 37) «posee relación directa con el saber decir, con el control emocional y con el lenguaje corporal. Por lo tanto, en la asertividad intervienen variables comunicacionales lingüísticas así como otros factores paralingüísticos (contacto visual, gestos, entonación, etc.)». En relación al objeto del presente artículo, en el ámbito de las desapariciones se puede conseguir esa asertividad utilizando un tono de voz relajado, un lenguaje sencillo y adaptado a la persona, escuchando lo que la otra persona tenga que transmitir, manteniendo contacto visual durante la interacción, explicando de forma sincera la información que en cada momento se pueda facilitar, poniendo el foco en los objetivos a lograr, manejando adecuadamente las objeciones y discrepancias que se puedan plantear, y siendo claro y honesto en las cuestiones a exponer, principalmente.

Por su parte, las relaciones prosociales mencionadas por Goleman (1997), pueden entenderse «como el conjunto de compor-

tamientos destinados a ayudar a otras personas y/o grupos». La mayoría de autores hace una conceptualización similar y considera que el fin de esos comportamientos es producir una mejora en el otro y/o en su situación (Auné *et al*., 2014). Entre los múltiples beneficios de estas relaciones y conductas prosociales está que pueden reforzar la autoestima de otros y la del que las realiza. Como señalan Auné *et al*. (2014, p.29) «es una competencia laboral relevante en muchas profesiones, como pueden ser las de ayuda humanitaria». En este sentido, en el ámbito de las desapariciones de personas, las/los integrantes de las FCS pueden contribuir a ponerlas en práctica mostrando disponibilidad para cuando la persona lo necesite, ofreciendo un teléfono directo para contactar, llamando de vez en cuando a las personas allegadas a la persona desaparecida, facilitando la información que se pueda transmitir, etc.

Por tanto, en resumen y de manera general, se puede demostrar la inteligencia emocional mediante diferentes estrategias de comunicación y habilidades que denotan que el profesional entiende la situación por la que la persona puede estar pasando y lo que puede estar experimentando. Es importante, por tanto, ser sensible a las necesidades de la persona, mostrarse disponibles y accesibles, no juzgar ni cuestionar lo que manifiesta la persona en relación a su experiencia, evitar minimizar sus sentimientos y/o quejas, no transmitir prisa o incomodidad entre otras, siempre mostrando interés genuino en la persona, así como siendo honesto y sincero en las apreciaciones que se efectúen.

En cuanto a la escucha activa, se puede entender como la habilidad de demostrar, con el comportamiento, que se está escuchando al que habla. No simplemente se está oyendo, sino que se está entendiendo, comprendiendo, dando sentido a lo que se oye. Al escuchar activamente se atiende a lo que la persona expresa directamente; y también, de manera muy importante, a los sentimientos, pensamientos y emociones que subyacen a lo que se está diciendo (Garrido, 2015). Se puede demostrar esta habilidad mediante técnicas como mantener contacto visual, una adecuada disposición psicológica de apertura, resumir algunos aspectos, realizar preguntas aclaratorias, observar el comportamiento no verbal, dejar hablar, respetar los silen-

cios, evitar distracciones o evitar discusiones y críticas, entre otras (De la Cruz, 2014; Garrido, 2015; como se citó en Herrera *et al*., 2020, p. 39).

Otras de las habilidades básicas para los profesionales de las FCS que trabajan en el ámbito de las desapariciones de personas, son aquellas relacionadas con la gestión de la incertidumbre y cómo facilitar su manejo a las personas afectadas. Aspecto crucial en muchas de estas situaciones, especialmente en los casos de desapariciones de larga duración. Si para los profesionales puede ser difícil trabajar en contextos de alta incertidumbre, mucho más difícil suele hacerse la situación para familiares y allegados de la persona desaparecida, de forma que, entre las habilidades a poner en práctica por los profesionales de las FCS en relación a este aspecto, se puede encontrar la habilidad para manejar diferentes estados de ánimo y/o reacciones de los familiares, derivando en su caso a otros profesionales cuando fuere necesario o gestionar de forma adecuada la información que se les puede facilitar, sin generar falsas esperanzas pero cumpliendo con su derecho a estar informados puntualmente.

Para poder llevar a cabo un adecuado desarrollo de estas habilidades, que abarcan tantos aspectos de la vida personal y profesional de quien integra las FCS, es necesaria sin duda una formación específica. Además, hay que tener en cuenta, como ya se ha expuesto, que las desapariciones deben entenderse como procesos activos que van a ir fluctuando en el tiempo conforme cambian las circunstancias que las envuelven en paralelo a su investigación, por lo que es esencial que el profesional sea capaz de seleccionar y adoptar aquellas habilidades, estrategias, técnicas y herramientas más adecuadas para cada caso y situación para una resolución eficiente y eficaz de la misma.

Estas características hacen necesario que los profesionales de las FCS, para poder desarrollar las citadas habilidades, sean capaces de poner en práctica otras, quizá de menor entidad a nivel conceptual, pero igual de necesarias para el desarrollo de una adecuada labor policial. Así, se hace impres-

cindible la práctica de cierta flexibilidad, no en el sentido de no cumplir los protocolos necesarios sino de poder adaptar algunas medidas cuando la persona lo necesite. Por ejemplo, facilitar el correo electrónico para el envío de documentos que el familiar no haya aportado en el primer momento, en vez de exigir que vaya físicamente de nuevo si eso es algo que le supone mayor estrés, incomodidad o desasosiego, o que simplemente no tiene medio de transporte fácil hasta la dependencia policial.

Relacionado con ello está una necesaria capacidad de adaptación a las características de cada persona, así como al momento en que ésta se encuentre, ya que, ni se va a encontrar igual en todos los momentos y circunstancias, ni consecuentemente va a necesitar lo mismo. En ocasiones puede requerir únicamente un espacio para desahogo emocional, en otras conocer nueva información sobre el avance de la investigación (aunque no vaya en la dirección que espera), en otras encontrar respuestas a la ausencia de resultados... y en todas ellas el profesional de las FCS tiene que ser capaz de detectar, al menos, lo básico de esa necesidad y aportar algo de lo requerido.

Estas cuestiones tienen que ver claramente con la relación que se establece entre profesional de las FCS y persona allegada a la persona desaparecida, aspecto crucial a la hora de obtener información. De forma reiterada se ha hecho referencia por profesionales del ámbito (Gonzalez, 2008, 2013) a esta cuestión, resultando claro que, cuanto mejor relación se establece con la persona entrevistada, mayor es la cantidad de información que se obtiene y más rica en detalles. Para poder conseguir una adecuada relación de confianza con la persona entrevistada es necesario poner en práctica ciertas cuestiones.

Así, revisadas algunas de las habilidades fundamentales para una intervención policial adecuada en el ámbito de las desapariciones de personas, es evidente que ninguna de ellas se puede desarrollar o poner en práctica sin un manejo adecuado de la comunicación. La palabra procede de la raíz latina *communis,* que significa poner en común algo con otro y la raíz expresa comunión, algo que se vive en común.

Como proceso, la comunicación interpersonal consiste en la interacción e intercambio de mensajes entre dos o más personas. Como apunta Agüero (2012, p.8) «es un dar y recibir mensajes incluyendo todos los signos, símbolos, claves, significados, datos, información, vivencias, experiencias y estados emocionales». Hay muchos tipos de comunicación y muchas maneras de acercarse al concepto. Si se pone el foco en el sistema utilizado, es decir, en el tipo de signos empleados, podemos considerar la distinción entre comunicación verbal y no verbal, entre *lo que* se dice y *cómo* se dice. En una comunicación eficaz, si el contenido, *lo que* se dice, es importante; más aún lo es el *cómo*, el sentido de lo que se dice. Influye por tanto en esto último la postura, los gestos, el tono de voz, la mirada...

La comunicación interpersonal cumple una serie de funciones: (a) informativa, consiste en compartir significados, intercambio de información; (b) afectiva, ya que no son mensajes asépticos, implica cierta información emocional y (c) reguladora, hace que se vayan adaptando los comportamientos a lo que requiere la situación.

Igualmente, en el proceso comunicativo influye de manera fundamental el contexto en que se produce la comunicación y, desafortunadamente, en la intervención de las FCS en el ámbito de las desapariciones muchas veces ni el contexto físico ni el emocional lo facilitan. No obstante, y a modo de resumen de las habilidades y cuestiones concretas que las personas integrantes de las FCS deben poner en marcha durante su intervención en el ámbito de personas desaparecidas, se pueden destacar las siguientes (tabla 1):

Se puede concluir, por tanto, que unas adecuadas habilidades de los profesionales de FCS que faciliten estas cuestiones, van a ser fundamentales para generar altos niveles de confianza con familiares y allegados de la persona desaparecida, lo que facilitará un mayor aporte de información de utilidad para la investigación, así como un mejor pronóstico de la evolución de estas personas en el manejo de lo ocurrido.

Tabla 1: Habilidades básicas a tener en cuenta en la interacción con familiares y allegados de personas desaparecidas.

Aspectos a considerar
- Buscar un lugar privado y tranquilo. - Mostrarse respetuoso con la persona, denotando explícitamente atención e interés sobre lo que tenga que informar. La escucha activa y la empatía aquí resultan claves. Ser puntuales. - Colocarse a la misma altura que la persona e inclinarse ligeramente hacia ella. Denota cercanía y sintonía. - Mantener un lenguaje corporal de aceptación. - Mantener contacto ocular y cuidar nuestra gesticulación. - Escuchar todo lo que tenga que decir (incluso aunque no guste). - Primero escuchar y luego escribir, explicando el motivo de recoger la información. - Respetar los silencios. - Utilizar un lenguaje sencillo y adaptado a la persona. - Hablar despacio y utilizar un tono de voz relajado. Cuidar el tono, volumen, velocidad y entonación en la comunicación. - Emplear adecuadamente recursos de la comunicación como la paráfrasis, el resumen, el reflejo, la repetición o la clarificación. Ante cualquier duda, preguntar. - Prestar atención a los mensajes no verbales de la persona. A veces dice más lo que no se dice, que lo que se dice. - Emplear adecuadamente los gestos emocionales (ej. sonreír) y de escucha (ej. asentir), así como las indicaciones paraverbales de escucha (ej. aham…). - Respetar tiempos y espacios de la persona. - Discutir lo que sea importante para la persona. - Mostrar comprensión hacia la situación de la persona afectada. - Ser auténtico. Reconocer que al profesional no le ha ocurrido, pero quiere entenderlo… sin comparar casos ni situaciones similares: no hay dos desapariciones iguales. - Facilitar la expresión emocional, así como el distanciamiento físico-emocional en aquellas situaciones que la persona lo precise por sentirse desbordada. Ayudarla a integrar lo ocurrido. - Normalizar sus reacciones y validar sus sentimientos. - Señalar la confidencialidad de lo que traslade al investigador. En ocasiones, habrá información que tema compartir por miedo a dañar su imagen, la del entorno o la de la persona desaparecida. Tranquilizar en este aspecto. - Tener una disposición mental de apertura. - Mantener la calma, aunque la otra persona se muestre alterada. - Reafirmar y dar seguridad en aquello que sabemos. - Preguntar qué necesita. Ser sensible a sus necesidades en la medida de las posibilidades del profesional.

(Continúa)

Tabla 1: Habilidades básicas a tener en cuenta en la interacción con familiares y allegados de personas desaparecidas. *(Continuación)*

Aspectos a considerar
- Informar de cómo va la investigación y dejar tiempo para responder preguntas. Acceder a aquellas peticiones que fueran factibles. - Informar de los siguientes pasos a seguir. - Reforzar el manejo adecuado de la situación por el familiar o allegado. - Facilitar la conexión (y mantenimiento) con la red social de la persona afectada. - Asegurarse de que ha comprendido lo que se ha tratado. - Ser congruentes en la comunicación verbal y no verbal
Aspectos a evitar
- Mentir, ni hacer promesas que el profesional no sabe si podrá cumplir. - Cuestionar sus sentimientos. - Juzgar, ni culpar. - Minimizar el hecho o las quejas. - Imponer las ideas del profesional. - Interrumpir. - Distraerse. - Mostrarse inseguro y dar informaciones contradictorias. - Tomarse la actitud de la persona afectada como algo personal. - Hablar de manera impersonal. - Elucubrar o hacer conjeturas que la persona pueda recibir como información correcta y fiable. - Precipitarse, la información ambigua o alarmista y las actitudes de indiferencia o rechazo. - Transmitir sensación de tener prisa.

Nota. Elaboración propia.

4 El impacto psicológico de las desapariciones en los profesionales de las FCS. La importancia del autocuidado del profesional

Los profesionales de las FCS deben afrontar múltiples riesgos y situaciones potencialmente traumáticas que implican la exposición a un elevado nivel de estrés, que puede afectar en su bienestar psicológico (Caballero y Sánchez, 2018). Estrés que, en un primer momento, va a resultar positivo y adaptativo ya que

facilitará la realización de sus funciones y orientación a las diferentes tareas, lo que conocemos como *eutrés*; pero que, de prolongarse en el tiempo o bien generarse con una intensidad desbordante, puede tener consecuencias en diversas áreas y afectar a su rendimiento, lo que conocemos como *distrés*.

Como se ha señalado, existe una tendencia de atribución de un rol de omnipotencia e invulnerabilidad psicológica hacia los profesionales de la intervención, independientemente de la dificultad o dureza de la situación que deban gestionar (Álvarez-Aparicio, 2015). Sin embargo, los estudios reflejan que los profesionales de la emergencia pueden verse expuestos en poco tiempo a más incidentes traumáticos que la población general en toda su vida, situando la actividad policial como una profesión de alto estrés (Caballero y Sánchez, 2018; Martín y Parada, 2008); lo que implica, si tenemos en cuenta únicamente las demandas externas, una mayor probabilidad de desarrollar *distrés*.

En esta línea, De Puelles (2009) destaca que la carga emocional que puede experimentar el profesional en el ámbito policial puede venir dada, en el curso de sus funciones, como consecuencia de la exposición a situaciones de alto impacto emocional, donde puede ser objeto de peligros y violencia, y/o en contacto (de manera presencial o no) con el sufrimiento ajeno al ser consciente del mismo.

Diferentes autores han estudiado las situaciones que pueden tener mayor impacto psicológico y emocional en la actuación policial, destacando, entre otras, el encuentro con víctimas de agresiones físicas o sexuales, la exposición a cadáveres, que los afectados sean niños, los incidentes con excesivo interés por parte de los medios de comunicación, la exposición a situaciones con alto nivel de incertidumbre, el haber vivido una situación previa con un desenlace trágico y que tras intensos esfuerzos para resolver la situación el resultado sea negativo (Álvarez-Aparicio, 2015; Caballero y Sánchez, 2018; Martín y Parada, 2008; Mc. Caslin *et al*., 2006); circunstancias que pueden ser inherentes al contexto de las desapariciones de personas, ya sea de manera independiente o incluso en su conjunto, y que tienen en común el contacto con el sufrimiento humano o *sufrimiento vicario*.

En relación a la exposición al sufrimiento humano, y de manera específica a las situaciones de desapariciones, Álvarez-Aparicio (2015) manifiesta que:

> El relato que, de modo angustioso, el entorno del desaparecido puede realizar al policía, sobre todo si se trata de un menor, puede llevarle a experimentar un elevado malestar, acentuado por el sentimiento de impotencia que la falta de control sobre la situación le puede generar. Con el tiempo, la ausencia de avances en la investigación hace que con frecuencia el profesional acabe rehuyendo el contacto con unos familiares que siguen demandando unas respuestas que no se tienen. El temor a no saber qué decir, se convierte así en una fuente muy importante de estrés que pueden llevar a la deshumanización y al distanciamiento de los deudos por parte del profesional, como estrategias de afrontamiento (p. 10).

Así, el autocuidado del profesional se desvela esencial, cuestión harta difícil según diversos autores (Birch *et al*., 2017; Foley y Massey, 2019; Foley y Massey, 2021; Hartley *et al*., 2013) ya que:

> (...) Por un lado, existe una creencia general aceptada entre los integrantes de FCS, por la cual se asume que la exposición al trauma es un riesgo laboral específico que no puede ser evitado y por otro lado, se necesita responsabilidad individual para reconocer los síntomas propios y hacer algo por mejorarlos; siendo complicado debido a que se desarrollan paulatinamente y, además, existen grandes estigmas en la sociedad asociados a recibir ayuda psicológica. (Pérez-Serrano *et al*., 2023, p. 109)

4.1 Factores que influyen en el malestar psicológico de los profesionales de las FCS en contextos de desapariciones

De acuerdo a lo que se ha manifestado anteriormente, y tal y como señala Álvarez-Aparicio (2015), en el caso de las desapari-

ciones, sobre todo si estas son de larga duración, el entorno de la persona desaparecida va a mantener de manera constante y sin una duración determinada unas demandas a las FCS, con el fin de que la resolución sea rápida y eficaz. Esas altas expectativas externas pueden dar lugar a sentimientos de frustración e inutilidad ante la sensación de ser incapaz de ayudar.

Además de las exigencias externas, esta autora hace también referencia a la importancia de las exigencias internas de los profesionales como consecuencia de unas elevadas expectativas sobre sí mismos. Esto puede derivar en lo que se conoce como *autoexigencia de rol*, lo que supone, a su vez, la tendencia a anteponer siempre las necesidades del otro frente a las propias, sin tener en cuenta que de esta manera la calidad en la asistencia al ciudadano va a disminuir (Álvarez-Aparicio, 2021).

Otro factor que puede influir en el malestar del profesional es la *sobreimplicación* en el caso, directamente relacionada con lo que se conoce como Fatiga por Compasión. El profesional asume la investigación como un reto personal, o como un fracaso ante la ausencia de progresos, que puede suponer problemas para adoptar una visión más amplia de la situación y repercutir en la eficacia percibida (Álvarez-Aparicio, 2015).

Finalmente, se debe destacar la *falta de habilidades de afrontamiento* para el adecuado desarrollo de la función policial, como un factor más que puede influir en el malestar psicológico del personal de las FCS (Uriarte y Parada, 2008).

4.2 Problemáticas asociadas al estrés profesional en situaciones de desapariciones

El malestar experimentado por profesionales involucrados en el manejo de situaciones altamente estresantes, emocionalmente demandantes y/o traumatizantes a nivel secundario puede identificarse con diferentes términos: Estrés Traumático Secundario (ETS), Fatiga por Compasión o Desgaste por Empatía (Uriarte y Parada, 2008) y, como consecuencia de la cronificación del estrés, el Desgaste Profesional o *Burnout*.

4.2.1 Estrés Traumático Secundario (ETS)

El estrés traumático secundario se define como la consecuencia natural que afecta al comportamiento y a las emociones de las personas, por conocimiento del trauma sufrido en otros o a través de la experiencia subsecuente (Figley, 1995). En el contexto que nos ocupa, los profesionales de las FCS que desarrollen esta problemática lo harán como consecuencia de la exposición a la situación de desaparición y/o el contacto con las personas afectadas por la misma en los diferentes niveles.

Diversos estudios señalan que los profesionales que trabajan en contacto con el sufrimiento humano, como los profesionales de las FCS, tienen mayor probabilidad de experimentar esta problemática y ponen el foco en la empatía y la exposición como piezas clave para ello (Garrosa, 2012a). Esta misma autora, a su vez, señala que hay otros factores que pueden influir en el desarrollo de estrés traumático secundario, como los aspectos organizacionales, la sobrecarga laboral y temporal, la falta de reconocimiento profesional y las exigencias del puesto y carga emocional.

Esta problemática puede ocurrir de manera súbita y se manifiesta a través de síntomas muy similares a los del Trastorno por Estrés Postraumático (TEPT), como el aumento de emociones desagradables, la reexperimentación de la experiencia traumática a través de pesadillas o imágenes intrusivas y la evitación de estímulos o situaciones relacionadas, entre otros (Garrosa, 2012a; Uriarte y Parada, 2008). Asimismo, puede afectar a la autoestima del profesional y la autoeficacia percibida, fundamental para su desempeño laboral.

4.2.2 Fatiga por compasión

La *Fatiga por Compasión*, también conocida como *Desgaste por Empatía*, se define como la experiencia de fatiga física y emocional que los profesionales pueden experimentar como consecuencia del uso frecuente de la empatía con personas que experimentan situaciones traumáticas (Garrosa, 2012a).

Puede ir asociada a la evitación de determinadas situaciones o problemáticas, al sentir que el coste emocional que pueden suponer a nivel personal, es muy importante (Uriarte y Parada, 2008). Estos autores también destacan que «esta problemática se manifiesta más en forma de fatiga física y mental que en términos de sintomatología postraumática» (p. 591).

4.2.3 Desgaste profesional o Burnout

El *burnout* es una respuesta al estrés laboral crónico, que surge como una problemática asociada a las profesiones que pueden requerir una excesiva implicación laboral y altas demandas emocionales propias de su puesto, y tiene mayor incidencia en los profesionales de la salud y la seguridad pública. Se caracteriza por: (a) el agotamiento físico y emocional, que lleva a una pérdida de motivación y sentimientos de fracaso; (b) la despersonalización, que supone actitudes y sentimientos negativos o insensibles hacia las personas con las que trabaja y (c) la falta de realización personal, implicando una valoración negativa del propio rol profesional y de sus logros (Álvarez-Aparicio, 2015; Caballero y Sánchez, 2018; Fidalgo, 2006; Garrosa, 2012a; Uriarte y Parada, 2008).

A diferencia del estrés traumático secundario, el *burnout* es progresivo y se produce cuando el profesional se siente desbordado y sin recursos para afrontar las demandas del puesto; pudiendo suponer que sus expectativas profesionales se vean frustradas. Las investigaciones al respecto muestran mayores niveles de Burnout en los profesionales de las FCS frente a la población general, posicionándoles como población de riesgo para experimentar este síndrome y sus consecuencias asociadas (de la Fuente-Solana *et al*., 2013).

La adopción de una personalidad resistente caracterizada por un gran sentido del compromiso, una buena sensación de control sobre los acontecimientos y asumir los cambios o experiencias estresantes como retos, puede conllevar una mejor protección frente al *burnout* (Uriarte y Parada, 2008).

4.3 Estrategias de autocuidado y afrontamiento del estrés en profesionales de las FCS

Para promover un equilibrio en la respuesta de estrés y, por tanto, reducir el posible impacto psicológico negativo, es fundamental no solo incidir en los aspectos organizacionales o de la situación, sino que los profesionales de la intervención en desapariciones desarrollen estrategias personales de autocuidado. Se entienden los autocuidados como comportamientos iniciados por uno mismo que se deciden incorporar para promover una buena salud y bienestar (Sherman, 2004, como se cita en Álvarez-Aparicio, 2021). Además, esta autora señala que «no solo se trata de que con estos autocuidados el profesional alcance una adecuada salud mental y un óptimo bienestar laboral, sino que gracias a ellos es posible que la calidad asistencial al ciudadano mejore».

Es frecuente que en muchos casos y de manera inconsciente, los profesionales de las FCS tiendan a actuar durante su intervención empleando estrategias de supresión emocional (lo que coloquialmente se conoce como *ponerse una coraza*) para protegerse y aminorar el impacto emocional de la situación, dando prioridad así a una adecuada actuación a nivel técnico (Caballero y Sánchez, 2018; Martín y Parada, 2008). Estas estrategias son útiles en un primer momento y están avaladas por la *Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad* en el ejercicio de sus funciones; pero empleadas de forma generalizada pueden tener un efecto perjudicial. Por ello, tras la intervención es fundamental un cambio de actitud que facilite la toma de conciencia de lo ocurrido, la apertura emocional y la puesta en marcha de estrategias de afrontamiento que permitan la autorregulación.

Las diferentes medidas a implementar se puede clasificar en: (a) medidas de intervención primarias o de prevención, aquellas que se deben realizar antes de que aparezcan los factores de riesgo y están dirigidas a eliminar o reducir la exposición a los mismos; (b) medidas de intervención secundarias, las que se realizan de manera preventiva durante la afectación de la situación o ante los primeros síntomas, con el fin de reducir el impacto de los riesgos que no se han podido evitar inicialmente y (c)

medidas de intervención terciarias o de protección, que permitirán minimizar los daños de un riesgo que ya se ha producido actuando una vez que la salud se ve afectada (Sánchez, 2020).

4.3.1 Estrategias preventivas

Con el fin de evitar los riesgos asociados al alto impacto emocional al que están expuestos los profesionales de las FCS en el contexto de desapariciones, se debe partir de la prevención como principal estrategia, a través de la preparación técnica, la información sobre la situación y una formación especializada en este ámbito que fomente estrategias de intervención adecuadas con los profesionales (Álvarez-Aparicio, 2015; Fernández-Millán, 2020; Martín y Parada, 2008). Asimismo, Martín y Parada (2008) señalan que la responsabilidad de prevención debe recaer tanto en la organización como en el propio profesional.

También es importante identificar los límites de la tarea que se está realizando (con el fin de establecer unas expectativas realistas) y conocer las estrategias para poder enfrentarse a distintas situaciones y sus consecuentes reacciones. Esto permitiría, a su vez, que el profesional pueda mejorar la percepción subjetiva que tiene de sí mismo y sus propias capacidades, aumentando su sensación de control.

Garrosa (2012b) propone que esta primera fase de actuación esté centrada en los aspectos teóricos en torno a esos riesgos para su comprensión mediante: el conocimiento de diferentes modelos explicativos, el análisis de los factores organizacionales y del propio puesto que puedan estar implicados y las variables de personalidad y recursos que pueden funcionar como factores de protección o resistencia.

El siguiente paso consistirá en aprender a observar e identificar las reacciones que puedan ser indicativas de un problema de estrés laboral. Garrosa (2012b, p.279) señala que «es importante que la persona conozca cómo responde ante las situaciones estresantes y traumáticas, estableciendo un perfil personal de sus respuestas fisiológicas, emocionales, cognitivas y conductuales». Así, mediante la autobservación, «se pretende que el profesional

sea consciente de cómo le afecta el estrés que está sufriendo y se pueden establecer indicadores de riesgos con las medidas de intervención en cada caso» (Garrosa, 2012b, p.280).

4.3.2 Estrategias para la promoción del autocuidado

Se clasifican en función de los cuatro niveles de respuesta de las personas: (A) nivel cognitivo, (B) nivel fisiológico, (C) nivel emocional y (D) nivel conductual (Martín-Daza, 1994).

A) Estrategias de autocuidado a nivel cognitivo. Tienen como objetivo cambiar la percepción, interpretación y evaluación de la situación y de los recursos propios (Martín-Daza, 1994). Se trata principalmente de ser conscientes del discurso mental y los pensamientos y creencias sobre uno mismo, el mundo y los demás, que pueden estar presentes al interpretar las distintas situaciones que se deben afrontar, con el fin de analizarlos y cambiarlos por otros que sean de utilidad y se ajusten más a la realidad. En la gestión de una desaparición pueden ser frecuentes pensamientos que denotan sentimientos de culpa y están relacionados con la autoexigencia de rol, como pensar que «no he hecho lo suficiente» o bien que «debería haber actuado de una manera diferente». También pueden aparecer pensamientos que cuestionen la propia capacidad y valía del profesional, sobre todo en desapariciones de larga duración, como «no valgo para nada, no soy un buen profesional».

Una vez identificados a través de un autorregistro, se pueden tener en cuenta las siguientes preguntas de ayuda para *modificar los pensamientos y creencias negativas* (tabla 2):

Tabla 2: Preguntas para modificar el discurso cognitivo.

Preguntas que cuestionan la objetividad de los pensamientos	*¿Qué pruebas tengo de que esto realmente es así? ¿Hay algo que me demuestra lo contrario?*
Preguntas que cuestionan la utilidad de los pensamientos	*¿Para qué me sirve pensar así? ¿Qué consecuencias negativas está teniendo en mí?*
Preguntas para identificar las emociones que generan	*¿Cómo me siento al pensar así?*
Preguntas para buscar pensamientos alternativos	*¿Qué otra cosa puedo pensar en su lugar? ¿Qué puedo pensar para sentirme mejor?*

Nota. Extraído y adaptado de «*La técnica de la reestructuración cognitiva*» de Bados y García, 2010.

Además, sobre todo en momentos de mayor estrés, se deben incorporar estrategias de *parada de pensamiento*, para frenar un diálogo negativo que puede interferir en la tarea a realizar; *distracción cognitiva*, prestando atención a otros elementos de la realidad para desconectar de aquello que genera malestar y *autoinstrucciones positivas*, o ideas que modulan los pensamientos negativos y, generalmente, motivan a la acción y la resolución de la situación.

(B) Estrategias de autocuidado a nivel fisiológico. El objetivo de estas herramientas es reducir la activación fisiológica que pueda influir en la adecuada ejecución de la tarea y/o en aquellas actividades propias del espacio personal del profesional. Para ello, se han desarrollado técnicas que inciden directamente en la activación del sistema nervioso parasimpático, el responsable de la relajación (Labrador, 2008). Entre ellas, se destacan las siguientes:

- *Técnicas de control de la respiración*: dentro de las técnicas de relajación, son las más extendidas por su facilidad de aprendizaje y la obtención de beneficios inmediatos (Blanco *et al*., 2014). Tal y como señala Labrador (2008, p. 206):

  > El desarrollo de un patrón respiratorio caracterizado por una inspiración lenta, regular y con volúmenes elevados de aire en cada inspiración facilitará una buena oxigenación pulmonar y de todos los tejidos, un menor trabajo cardiovascular, así como una reducción de la activación general del organismo.

  La técnica más frecuente es la respiración diafragmática, pero también existen otras estrategias alternativas que facilitan que la persona focalice más la atención en la tarea que está realizando, como la respiración contando o la respiración profunda.

- *Relajación diferencial*: también conocida como relajación muscular progresiva de Jacobson. Es una técnica que se centra en distinguir las sensaciones experimentadas al tensar o destensar los músculos de diferentes zonas del cuerpo de manera independiente, logrando una respuesta de

relajación subjetiva a nivel cognitivo y emocional (Labrador, 2008).

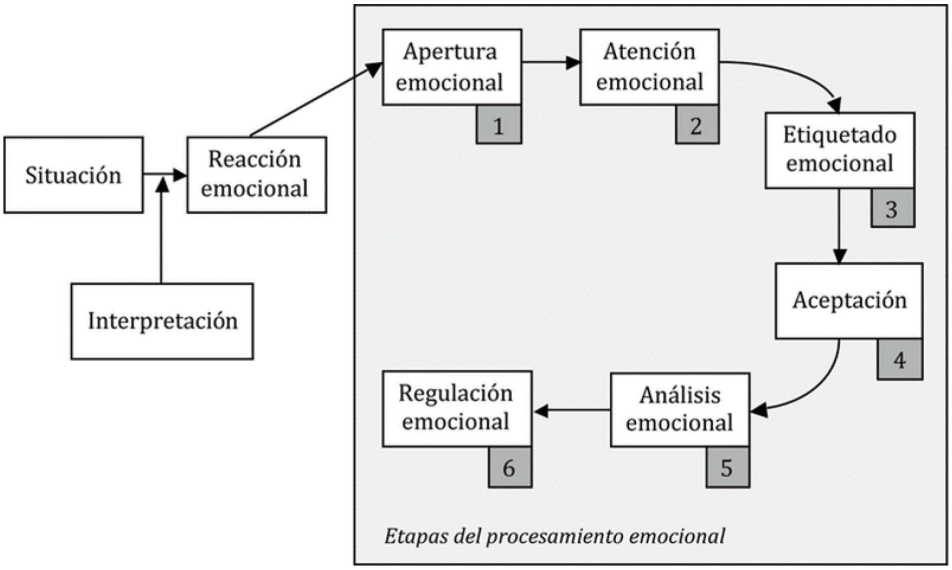
- *Relajación autógena de Schultz*: con esta técnica se trata de realizar un recorrido por el cuerpo centrando la atención en percibir diferentes sensaciones corporales para su posterior regulación.

(C) Estrategias de autocuidado a nivel emocional. Tal y como señala de Puelles (2009): «se ha comprobado que dotar a los policías de estrategias de manejo emocional ante las tareas con elevada exigencia incidirá en una mayor optimización de su actuación profesional, así como en la asimilación saludable de estas experiencias» (p. 193). Para ello, las principales estrategias a nivel emocional son las siguientes:

- *Ventilación o expresión emocional*: es una técnica que consiste en identificar las emociones reprimidas y expresarlas. Evita que las emociones que causan dolor se queden encerradas en el interior. Esta estrategia es especialmente importante en profesionales expuestos a situaciones de alto impacto emocional como las desapariciones, debido a que permiten procesar aquello que les está afectando, ante la posibilidad de sentirse sobrepasados.

- *Regulación emocional*: el procesamiento emocional permite canalizar las reacciones que pueden darse de manera muy intensa o persistente, pudiendo incluso interferir en la vida de las personas (Hervás, 2011). Este mismo autor propone un modelo de seis pasos (figura 2) para llevar a cabo esta tarea y destaca la importancia y eficacia de incluir las variables emocionales en la intervención y gestión de las reacciones postraumáticas. Tras la reacción emocional, a través de la apertura, la persona puede acceder a lo que siente con el fin de poder prestar atención a diferentes aspectos de la emoción y etiquetarla o identificarla. Seguidamente se trata de llevar a cabo la aceptación, evitando juicios negativos de la propia experiencia; y proceder a entender el significado desde su origen, mensaje, validez y aprendizaje, es decir, llevar a cabo el análisis emocional. Finalmente, se realiza la regulación emocional cuando la persona es capaz de modular sus emociones.

Figura 2: Modelo de regulación emocional basado en el procesamiento emocional.



Nota. Extraído de «*Psicopatología de la regulación emocional: el papel de los déficits emocionales en los trastornos clínicos*» de Hervás, 2011, p. 352.

(D) Estrategias de autocuidado a nivel conductual. Este tipo de estrategias buscan el desarrollo y mantenimiento de hábitos saludables, con el fin de promover sensaciones de bienestar y recuperación del estrés profesional. Se destacan las siguientes:

- *Mantener una alimentación saludable*: una dieta equilibrada influye positivamente en la gestión del estrés, al aportar más energía para responder a las demandas externas (Martín-Daza, 1994) y mejorar el estado de ánimo. Asimismo, favorece el estado de alerta para reaccionar ante imprevistos y situaciones que requieren una rápida actuación, facilitando la toma de decisiones. En situaciones de estrés y ansiedad se liberan adrenalina y cortisol, y el organismo demanda energía rápida para reponer el gasto energético lo antes posible. Generalmente, se tiende a cubrir esa necesidad a través de alimentos ricos en azúcares simples, lo que supone una satisfacción inmediata al aumentar el nivel de glucosa en sangre neutralizando el cortisol, pero de corta duración y sin beneficios a medio y largo plazo (Cortés *et al*., 2018). Se trata, por tanto, de introducir en la dieta alimentos que aumenten el estado de

ánimo y mitiguen el cansancio y la fatiga, como los alimentos ricos en triptófano y magnesio.

- *Mantener un adecuado descanso físico y psicológico*: existe una relación bidireccional entre la privación de sueño y el estrés, es decir, cualquiera de las dos variables puede influir en que se produzca la otra (del Río, 2006). Por ello, es fundamental tener unas buenas pautas de *higiene del sueño* que aseguren el descanso y, en consecuencia, la reparación del organismo para conseguir la energía necesaria. Además, sobre todo si debido a los turnos y horarios no se pueden tener periodos de sueño en una cantidad adecuada, es importante garantizar momentos de desconexión emocional que promuevan el descanso a nivel psicológico.

- *Realizar ejercicio físico*: la práctica cotidiana de ejercicio no solo va a tener beneficios a nivel físico, sino también a nivel psicológico. Los estudios señalan que con el deporte se reducen las consecuencias del estrés y mejora el estado de ánimo y la eficiencia en el trabajo (Márquez, 1995; Martín-Daza, 1994).

- *Realizar actividades agradables*: suponen una mejora en el estado de ánimo, permiten desconectar de las fuentes de estrés y fortalecen los vínculos sociales. En esta línea, se debe destacar también la importancia del apoyo social en el trabajo, directamente relacionado con la realización personal y la disminución del agotamiento emocional y las conductas y actitudes negativas de la persona hacia los demás (Santana y Farkas, 2007).

- *Mantener unas rutinas ordenadas*: conlleva beneficios para llevar a cabo las actividades cotidianas y responder ante posibles imprevistos. Además, generan sensación de control, mejoran la autodeterminación, constancia y perseverancia; frente al caos generado por la desorganización que puede repercutir directamente en un aumento de la sensación de estrés.

En resumen, la promoción de unas adecuadas estrategias de autocuidado por parte de la organización, y su puesta en práctica por parte del profesional de las FCS especializado en desa-

pariciones, va a ser esencial para el buen manejo del estrés en situaciones potencialmente traumáticas. Para su aprendizaje, tanto las propias entidades como las personas implicadas, deben contar con profesionales de la psicología especializados en el ámbito, que puedan implementar programas de gestión del estrés específicos de acuerdo a sus necesidades.

5 Conclusiones

La desaparición de personas es una circunstancia que supone un alto impacto emocional y psicológico y afecta a diferentes niveles, no solo a las familias y personas allegadas sino también a los profesionales de las FCS encargados de su investigación, entre otros.

Lejos de lo que se suele pensar, atribuyendo la cualidad de invulnerabilidad, el personal de las FCS está expuesto a numerosos riesgos y eventos potencialmente traumáticos, que hacen que su profesión esté considerada de alto estrés. Así, situaciones como el contacto con víctimas de agresiones, la exposición a cadáveres o que los afectados sean menores, no son infrecuentes en su devenir profesional. Todas ellas, sumado al alto nivel de incertidumbre tan representativo en las desapariciones, pueden darse en este contexto laboral, y tienen en común la exposición al sufrimiento humano.

La adquisición y mejora de unas buenas habilidades prácticas en la atención a familiares y allegados de personas desaparecidas por parte del personal de las FCS va a conllevar beneficios para el entorno de la persona desaparecida, para los propios intervinientes y también para la investigación. En primer lugar, se trata de desarrollar acciones que amortigüen el impacto del suceso, proporcionen recursos de afrontamiento, refuercen el apoyo social y favorezcan una mejora de la situación para promover un adecuado manejo de la incertidumbre al entorno afectado. Respecto a los profesionales, la puesta en marcha de habilidades tendrá beneficios al reducir sus niveles de estrés,

como consecuencia de mayor sensación de control, así como disminuir la probabilidad de aparición de diferentes problemáticas asociadas al estrés. En relación a la investigación, unas buenas habilidades permitirán el establecimiento de una óptima relación interpersonal que facilite la colaboración con las FCS del entorno afectado por la desaparición.

Las habilidades que se requieren para el adecuado desarrollo de la actuación policial en el contexto de la desaparición de personas deben llevarse a cabo a lo largo de toda la intervención. De manera que, partiendo de que nos encontramos ante un proceso dinámico, los profesionales deben tener flexibilidad y capacidad de adaptación. Además, es fundamental el uso de la escucha activa y de las diferentes habilidades relacionadas con la inteligencia emocional, como la empatía. Por otra parte, es también importante que los profesionales conozcan estrategias para la gestión de la incertidumbre, que puedan trasladar a las personas afectadas, y dispongan de unas adecuadas habilidades de comunicación.

Ante la desaparición de una persona, los profesionales deben afrontar las altas expectativas externas que el entorno va a colocar sobre ellos para su rápida y eficiente resolución; además de las expectativas internas derivadas de la autoexigencia de rol. Una mala gestión de estos factores, sumada a la sobreimplicación que se puede dar en algunas circunstancias y la falta de habilidades de afrontamiento, puede ser clave para el desarrollo del estrés negativo o *distrés*. Además, de no abordarse adecuadamente, ese estrés puede derivar en diferentes problemáticas asociadas a los profesionales de la intervención, como el Estrés Traumático Secundario, el Desgaste por Empatía o el *Burnout*.

Para lograr una buena gestión del estrés laboral, será fundamental la implementación de diferentes estrategias por parte de la organización, el entorno y de los propios profesionales. Estrategias que deben aplicarse de manera preventiva antes de que aparezca el malestar, y también cuando se den las primeras reacciones como consecuencia de la situación estresante. Se debe destacar tener una adecuada formación y capacitación, disponer de información de la situación y de las posibles reac-

ciones relacionadas con el estrés; además de conocer y practicar estrategias de autocuidado en todos los niveles, desde la autorregulación emocional hasta la promoción de hábitos saludables.

En definitiva, se puede señalar que las características que definen la compleja problemática de las personas desaparecidas, especialmente cuando estas se mantienen en el tiempo, hacen su abordaje especialmente exigente para los profesionales; requiriendo, para su eficaz desarrollo, tanto de unas buenas habilidades en la interacción y gestión, como de un adecuado manejo de pautas básicas de actuación. Es por ello necesario una formación especializada en el área, como ya se concluyó en la *Comisión Especial para el estudio de la problemática de las personas desaparecidas sin causa aparente* celebrada en 2013.

Financiación

El presente trabajo no recibió financiación específica de agencias del sector público, comercial o de organismos no gubernamentales.

Conflicto de intereses

Los autores declaran que no existen conflictos de intereses.

Referencias

Acinas, P. (2012). Duelo en situaciones especiales: suicidio, desaparecidos, muerte traumática. *Revista Digital de Medicina Psicosomática y Psicoterapia*, *2*(1), 1-17. http://www.psicociencias.com/pdf_noticias/Duelo_en_situaciones_especiales.pdf

Agüero, P. M. Z. (2012). *La comunicación interpersonal*. EUMED-Universidad de Málaga. https://biblioteca.utec.edu.sv/siab/virtual/elibros_internet/55772.pdf

Alemán Méndez, L. S. (2022) *Estudio de caso. Desarrollo de habilidades sociales en la formación policial y su relación con el desarrollo humano* [Tesis de Maestría Universidad Iberoamericana Puebla]. https://hdl.handle.net/20.500.11777/5363 http://repositorio.iberopuebla.mx/licencia.pdf

Álvarez-Aparicio, A. I. (2015). El efecto de las desapariciones en los profesionales de la intervención. Su efecto en los profesionales de las FFCCSSEE. *Revista Ciencia Policial. Revista Técnica del Cuerpo Nacional de Policía, 128*, 9-24.

Álvarez-Aparicio, A. I. (2018). Intervención psicológica en desapariciones, pautas básicas de actuación policial. *Revista Ciencia Policial. Revista Técnica del Cuerpo Nacional de Policía, 150,* 7-27.

Álvarez-Aparicio, A. I. (2021). *Importancia del autocuidado en quienes ejercen la mediación policial* [Conferencia]. II congreso internacional de mediación policial y policía de proximidad. Instituto de Educación Superior de Formación Policial y Seguridad Pública del Chaco-Argentina.

Álvarez-Aparicio, A. I. (2024). Situación actual de la problemática de las desapariciones en posibles contextos de violencia de género en España. La importancia de profesionales de la psicología en su abordaje. *Cuadernos de Crisis*, *23*(1), 31-49. https://www.cuadernosdecrisis.com/docs/2024/_Article_D_24_1_23.pdf

Álvarez-Aparicio, A. I., Martínez Fernández, J. M. y Acinas Acinas. (25-26 de octubre de 2023). *Buenas prácticas en la atención a familiares y allegados en casos de desaparición de personas por parte de las Fuerzas y Cuerpos de Seguridad* [Conferencia]. Reunión Presidencia Española del Consejo de la Unión Europea 2023 en Materia de Personas Desaparecidas, Madrid, España.

Andersen, I., Poudyal, B., Abeypala, A., Uriarte, C., y Rossi, R. (2020). Mental health and psychosocial support for families of missing per-

sons in Sri Lanka: A retrospective cohort study. *Conflict and Health*, *14*(1), 1-15. https://doi.org/10.1186/s13031-020-00266-0

Antuña, C. (2022). Bienestar psicológico, inteligencia emocional y resolución de conflictos en miembros de los cuerpos y fuerzas de seguridad del estado español: un estudio correlacional. *MLS Psychology Research, 5*(2), 123-134. https://dialnet.unirioja.es/servlet/articulo?codigo=8752943

Arenliu, A., Shala-Kastrati, F., Berisha Avdiu, V., y Landsman, M. (2019). Posttraumatic Growth Among Family Members with Missing Persons From War in Kosovo: Association With Social Support and Community Involvement. *Omega (United States)*, *80*(1), 35–48. https://doi.org/10.1177/0030222817725679

Auné, S. E., Blum, D., Abal-Facundo, J. P, Lozzia, G. S., y Horacio, F. A. (2014). La conducta prosocial: Estado actual de la investigación. Perspectivas en Psicología: *Revista de Psicología y Ciencias Afines, 11*(2), 21-33. https://www.redalyc.org/articulo.oa?id=483547666003

Bados, A. y García Grau, E. (2010). *La técnica de la reestructuración cognitiva.* Universitat de Barcelona. https://diposit.ub.edu/dspace/bitstream/2445/12302/1/Reestructuraci%C3 %B3n.pdf

Barakovic, D., Avdibegovic, E., y Sinanovic, O. (2013). Depression, Anxiety and Somatization in Women with War Missing Family Members. *Materia Socio Medica*, *25*(3), 199. https://pubmed.ncbi.nlm.nih.gov/24167436/

Barakovic, D., Avdibegović, E., y Sinanović, O. (2014). Posttraumatic stress disorder in women with war missing family members. *Psychiatria Danubina*, *26*(4), 340–346. https://www.psychiatria-danubina.com/UserDocsImages/pdf/dnb_vol26_no4/dnb_vol26_no4_340.pdf

Beltrán, J. C. (2016). *Personas Desaparecidas y Cadáveres: Evaluación y Análisis Criminológico* [Trabajo Fin de Máster, Universidad de Alcalá]. https://iuicp.uah.es/export/sites/iuicp/es/titulaciones/.galleries/Documentos/trabajo-de-investigacion-jose-carlos-beltran-martin.pdf

Benedito, M. (1997). La comunicación y el enfermo terminal. *Cuadernos de Medicina Psicosomática, 42-43*, 85-92.

Birch, P., Vickers, M. H., Kennedy, M., y Galovic, S. (2017). Wellbeing, occupational justice and police practice: an 'affirming environment'? *Police Practice and Research, 18*(1), 26-36. https://doi.org/10.1080/15614263.2016.1205985

Blanco, C., Estupiñá, F. J., Labrador, F. J., Fernández-Arias, I., Bernardo-de-Quirós, M., y Gómez, L. (2014). Uso de técnicas de relajación en una clínica de psicología. *Anales de Psicología*, *30*(2), 403-411. https://doi.org/10.6018/analesps.30.2.158451

Boss, P. (2001). *La pérdida ambigua. Cómo aprender a vivir con un duelo no terminado.* Gedisa.

Caballero Peláez, C. y Sánchez Reales, S. (2018). Salud mental en las Fuerzas y Cuerpos de Seguridad del Estado: modelo vulnerabilidad y estrés. *Ciencia Policial. Revista Técnica del CNP, 150*, 27-49.

Cartwright, A. y Roach, J. (2022). A price paid? A review of the research on the impact of investigating serious crime on the wellbeing of police staff. *The Police Journal, 95*(1), 109-126. https://doi.org/10.1177/0032258X211049335

Cereceda, J. y Tourís, R. M. (2019). *Protocolo de actuación de las Fuerzas y Cuerpos de Seguridad ante casos de personas desaparecidas.* España: Gabinete de Coordinación y Estudios. Secretaría de Estado de Seguridad. Ministerio del Interior. https://servicios.mpr.es/VisorPublicaciones/visordocumentosicopo.aspx?NIPO=126190173&SUBNIPO=&IDPUBLICACION=021912619

Céspedes, N. E., Pabón, L. M., Tafur, D. C., Palomino, N. L., Cervantes, L. C. y Fajardo, E. (2020). Fortalecimiento de las habilidades psicosociales para mejorar el servicio de policía y aumentar la confianza social. *Redipe, 9(5),* 88-112. https://doi.org/10.36260/rbr.v9i5.977

Comisión Especial para el estudio de la problemática de las personas desaparecidas sin causa aparente, en su sesión celebrada el día 18 de diciembre de 2013. *Boletín Oficial de las Cortes Generales, Senado, 290*, de 23 de diciembre de 2013. https://www.senado.es/legis10/publicaciones/pdf/senado/bocg/BOCG_D_10_290_2172.PDF

Cortés Romero, C. E., Escobar Noriega, A., Cebada Ruiz, J., Soto Rodríguez, G., Bilbao Reboredo, T., y Vélez Pliego, M. (2018). Estrés y cortisol: implicaciones en la ingesta de alimento. *Revista Cubana de Investigaciones Biomédicas, 37*(3), 1-15. http://scielo.sld.cu/pdf/ibi/v37n3/ibi13318.pdf

De Castro, S. (2019). Un imposible duelo. *Affectio Societatis (Medellín), 16*(30), 208-221. https://doi.org/10.17533/udea.affs.v16n30a11

De la Fuente-Solana, E. I, Aguayo-Extremera, R., Vargas-Pecino, C. y Cañadas de la Fuente, G. R. (2013). Prevalence and risk factors of burnout syndrome among Spanish police officers. *Psycothema, 25*(4), 488-493. https://doi.org/10.7334/psicothema2013.81

De Puelles, M. C. (2009). Exigencia y carga emocional del trabajo policial: la intervención policial ante catástrofes y emergencias masivas. *Psicopatología Clínica Legal y Forense, 9*(1), 171-196. https://dialnet.unirioja.es/servlet/articulo?codigo=3238806

De Puelles, M. C. (2018). Afrontamiento resiliente de la desaparición de un ser querido. *Psicopatología Clínica Legal y Forense, 18*(1), 151-175. https://dialnet.unirioja.es/servlet/articulo?codigo=7165691

De Vicente, A. y Santamaría, P. (2022). *Evaluación de Sintomatología Postraumática. Familiares de personas desaparecidas*. TEA Ediciones.

Del Río Portilla, I. Y. (2006). Estrés y sueño. *Rev Mex Neuroci, 7*(1), 15-20. https://www.medigraphic.com/pdfs/revmexneu/rmn-2006/rmn061d.pdf

Engstrom, D., Hernández, P. y Gangsei, D. (2008). Vicarious resilience: A qualitative investigation into its description. *Traumatology, 14*(3), 13-21. https://doi.org/10.1177/1534765608319323

Fernández-Millán, J. M. (2020). *Psicología aplicada a la ayuda en situaciones de emergencia y catástrofe*. Pirámide.

Fidalgo M. (2006). NTP 704: *Síndrome de estar quemado por el trabajo o «Burnout» (I): definición y proceso de generación.* Centro Nacional de Condiciones de Trabajo. Instituto Nacional de Seguridad e Higiene en el Trabajo. https://www.insst.es/documents/94886/326775/ntp_704.pdf

Figley, C. (1995). Compassion fatigue as secondary traumatic stress disorder: An overview. En C. R. Figley (ed.), *Compassion fatigue: Coping with secondary traumatic stress disorder in those who treat the traumatized* (pp. 1-20). Brunner/Mazel.

Foley, J. y Massey, K. (2019). Police officers and post-traumatic stress disorder: discussing the deficit in research, identification and prevention in England and Wales. *The Police Journal, 92*(1), 23-34. https://doi.org/10.1177/0032258X18761284

Foley, J. y Massey, K. L. D. (2021). The 'cost' of caring in policing: From burnout to PTSD in police officers in England and Wales. *The police journal, 94*(3), 298-315. https://doi.org/10.1177/0032258X20917442

Galán, A. (2018). *Introducción a la investigación de desaparecidos*. Galán.

García-Barceló, N., Tourís, R. M. y González, J. L. (2019). Personas desaparecidas: conveniencia de fomentar la investigación científica en España. *Boletín Criminológico, 183*. https://doi.org/10.24310/boletin-criminologico.2019.v25i2019.6833

Garrido, E. (2015). UF0346-Comunicación efectiva y trabajo en equipo. Editorial Elearning, SL. https://www.editorialelearning.com/catalogo/media/iverve/uploadpdf/1525963226_UF0346_demo.pdf

Garrosa, E. (2012a). Principales riesgos psicosociales en los intervinientes. En Pacheco, T. (ed.), *Atención Psicosocial en emergencias* (pp. 263-274). Síntesis.

Garrosa, E. (2012b). Prevención de riesgos psicosociales con intervinientes: buenas prácticas para el autocuidado. En T. Pacheco (ed.), *Atención Psicosocial en emergencias* (pp. 275-300). Síntesis.

Goleman, D. (1997). *Inteligencia Emocional*. Paidós.

González, J. L. (2008). La entrevista policial. *Revista Ciencia Policial. Revista Técnica del Cuerpo Nacional de Policía, 88*, 15-33.

González, J. L. (2013). La entrevista policial. *Técnicas de entrevista policial*. Universidad Autónoma de Madrid.

González, J. L. (2015). La entrevista y el interrogatorio de sospechosos. En A. Giménez-Salinas y J. L. González Álvarez (ed.), *Investigación criminal. Principios, técnicas y aplicaciones* (pp. 183-196). LID Editorial.

González, J. L. y Garrido, M. J. (2015). Satisfacción de las víctimas de violencia de género con la actuación policial en España. Validación del Sistema VioGen. *Anuario de Psicología Jurídica, 25*(1), 29-38. https://doi.org/10.1016/j.apj.2015.02.003

Hartley, T. A., Sarkisian, K., Violanti, J. M., Andrew, M. E. y Burchfiel, C. M. (2013). PTSD symptoms among police officers: associations with frequency, recency, and types of traumatic events. *International journal of emergency mental health, 15*(4), 241. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4734407/

Hernandez-Wolfe, P., Killian, K., Engstrom, D. y Gangsei, D. (2015). Vicarious resilience, vicarious trauma, and awareness of equity in trauma work. *Journal of humanistic psychology, 55*(2), 153-172. https://doi.org/10.1177/0022167814534322

Herrera, D. D., Méndez, J. M. y Lemus, D. M. (2020). Análisis de la incidencia de la escucha activa como técnica de comunicación efectiva en oficiales de la Policía Nacional en el 2020. *Ocronos, 3*(5), 493.

https://revistamedica.com/incidencia-escucha-activa-comunicacion-oficiales-policia-nacional-en-el-2020/

Hervás, G. (2011). Psicopatología de la regulación emocional: el papel de los déficit emocionales en los trastornos clínicos. *Psicología Conductual,19*(2) 347-372. https://extension.uned.es/archivos_publicos/webex_actividades/5413/psicopatologiadelaregulacionemocionalelpapeldelosdeficitemocionales.pdf

Holt, T. J., y Blevins, K. R. (2011) Examining job stress and satisfaction among digital forensic examiners. *Journal of Contemporary Criminal Justice, 27*(2), 230-245. https://doi.org/10.1177/1043986211405899

Huang, M., y Habermas, T. (2019). The ambiguity of loss affects some, but not all autobiographical memories: redemption and contamination, agency and communion. *Memory*, *27*(10), 1352-1361. https://doi.org/10.1080/09658211.2019.1655579

Isuru, A., Hewage, S. N., Bandumithra, P., y Williams, S. S. (2019). Unconfirmed death as a predictor of psychological morbidity in family members of disappeared persons. *Psychological Medicine*, *49*(16), 2764-2771. https://doi.org/10.1017/S0033291718003793

Kennedy, C., Deane, F. P., y Chan, A. Y. C. (2020). "What Might Have Been…": Counterfactual Thinking, Psychological Symptoms and Posttraumatic Growth When a Loved One is Missing. *Cognitive Therapy and Research*, *45*, 322-332. https://doi.org/10.1007/s10608-020-10156-7

Kohan, A. y Mazmanian, D. (2003). Police work, burnout, and pro-organizational behavior: A consideration of daily work experiences. *Criminal Justice and Behavior, 30*(5), 559-583. https://doi.org/10.1177/0093854803254432

Kroes, W. H., Margolis, B. L. y Hurrell, J. J. (1974). Job stress in policemen. *Journal of Police Science and Administration, 2*(2), 145-155. https://psycnet.apa.org/record/1975-10622-001

Labrador, F. J. (2008). Técnicas de control de la activación. En F. J. Labrador (ed.), *Técnicas de modificación de conducta* (pp.199-223). Pirámide.

Lenferink, L., Eisma, M. C., de Keijser, J., y Boelen, P. A. (2017). Grief rumination mediates the association between self-compassion and psychopathology in relatives of missing persons. *European Journal of Psychotraumatology*, *8*(6). https://doi.org/10.1080/20008198.2017.1378052

Lenferink, L., de Keijser, J., Wessel, I., y Boelen, P. A. (2018a). Cognitive-Behavioral Correlates of Psychological Symptoms Among Relatives of Missing Persons. *International Journal of Cognitive Therapy*, *11*(3), 311-324. https://doi.org/10.1007/s41811-018-0024-y

Lenferink, L., Wessel, I., y Boelen, P. A. (2018b). Exploration of the Associations between Responses to Affective States and Psychopathology in Two Samples of People Confronted with the Loss of a Loved One. *Journal of Nervous and Mental Disease*, *206*(2), 108-115. https://doi.org/10.1097/NMD.0000000000000781

Lenferink, L. I. M., De Keijser, J., Wessel, I., y Boelen, P. A. (2019). Cognitive behavioural therapy and mindfulness for relatives of missing persons: A pilot study. *Pilot and Feasibility Studies*, *5*(1), 1-17. https://doi.org/10.1186/s40814-019-0472-z

Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad. *Boletín Oficial del Estado, 63,* de 14 de marzo de 1986. https://www.boe.es/eli/es/lo/1986/03/13/2/con

López, J., Bravo, M., Martín, M., Pavón, J., Gómez, F., Carrasco, T., Rodríguez, F., Prieto, I. y Guisado, A. (2022). *Informe Anual Personas Desaparecidas durante el año 2021.* España: Centro Nacional de Desaparecidos (CNDES), Ministerio del Interior. https://www.interior.gob.es/opencms/pdf/prensa/balances-e-informes/2022/Informe-Personas-Desaparecidas-en-Espana-2022.pdf

López, J., Bravo, M., Vinuesa, N., Pavón, J., Romero, L. J., Gómez, F., Carrasco, T., Rodríguez, F., Prieto, I., García, M. y Guisado, A. (2023). *Informe Anual Personas Desaparecidas durante el año 2022.* Es-

paña: Centro Nacional de Desaparecidos (CNDES), Ministerio del Interior. https://www.interior.gob.es/opencms/export/sites/default/.galleries/galeria-de-prensa/documentos-y-multimedia/balances-e-informes/2023/Informe-anual-personas-desaparecidas-2023.pdf

López, M., Acosta, I., García, L. A. y Fumero, A. A. (2006). Inteligencia Emocional en policías locales. *Ansiedad y estrés, 12*(2-3), 463-477. https://dialnet.unirioja.es/servlet/articulo?codigo=2244346

Márquez, S. (1995). Beneficios psicológicos de la actividad física. *Rev. De Psicol. Gral. Y Aplic., 48*(1), 185-206. https://dialnet.unirioja.es/servlet/articulo?codigo=2378944

Martel, E., Fillol, A., Quiroz, A. M., Baca, C., Salas, C. R., Custodio, E. E., Fuertes, E., Estebes, G., Vásquez, J. I., Bautista, M. I., Calderón, R. H., Revilla, S. y Soto, Y. (2021). *Protocolo de Acompañamiento Psicosocial para la Búsqueda de Personas Desaparecidas con Enfoque Humanitario*. Ministro de Justicia y Derechos Humanos de Perú. Comité Internacional de la Cruz Roja. https://cdn.www.gob.pe/uploads/document/file/1823752/PROTOCOLO%20DE%20ACOMPA%C3 %91AMIENTO%20-%20Versi%C3 %B3n%20final.pdf.pdf?v=1619564476

Martín, L. y Muñoz, M. (2009). *Primeros auxilios psicológicos*. Síntesis.

Martín, J. y Parada, E. (2008). Estrés y Ansiedad en salvamentos, rescates y auxilios. En E. Parada (ed.), *Psicología y Emergencia. Habilidades psicológicas en las profesiones de socorro y emergencia* (pp. 69-92). Descleè De Brouwer.

Martín-Daza, F. (1994). NTP 349: *Prevención del estrés: intervención sobre el individuo.* Centro Nacional de Condiciones de Trabajo. Instituto Nacional de Seguridad e Higiene en el Trabajo. https://www.insst.es/documents/94886/326853/ntp_349.pdf

Mc. Caslin, S.E., Metzler, T.J., Best, R.S., Weiss, D.S., Fagan, J., Liberman, A. y Marmar, C.R. (2006). The impact of personal threat on police officers' responses to critical incident stressors. *The Jour-*

nal of Nervous and Mental Disease, *194*(8), 591-7. https://doi.org/10.1097/01.nmd.0000230641.43013.68

Ministerio del Interior (2017). *Informe sobre Personas Desaparecidas en España.* Gobierno de España. https://www.interior.gob.es/opencms/pdf/prensa/balances-e-informes/2017/Informe_Desaparecidos_Espana_2017.pdf

Ministerio del Interior (2022). *I Plan Estratégico en Materia de Personas Desaparecidas 2022-2024*. Gobierno de España. https://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/interior/Documents/2022/090322_I_Plan_Estrategico_Personas_Desaparecidas_22-24.pdf

Muñoz, M., Ausín, E., y Pérez-Santos, E. (2007). Primeros auxilios psicológicos: protocolo ACERCARSE. *Psicología Conductual, 15*(3), 479-505. https://www.behavioralpsycho.com/wp-content/uploads/2020/04/10.Mu%C3 %B1oz_15-3oa.pdf

Newell, J. y MacNeil, G. (2011). A comparative analysis of burnout and professional quality of life in clinical mental health providers and health care administrators. *Journal of Workplace Behavioral Health*, *26*, 25-43. https://doi.org/10.1080/15555240.2011.540978

Pacheco, T. (coord.), (2012). *Atención psicosocial en emergencias*. Síntesis.

Pérez-Bambó, I. (2021). *Efectos Psicológicos de la Pérdida de un ser Querido por Desaparición: Recomendaciones para el Tratamiento de los Familiares* [Trabajo Fin de Máster, Universidad a Distancia de Madrid]. https://udimundus.udima.es/bitstream/handle/20.500.12226/1178/TFM_Isabel%20Pe%cc%81rez%20Bambo%cc%81.pdf?sequence=1&isAllowed=y

Pérez-Serrano, M., Moral-Aguilera, A. M. y González-Álvarez, J. L. (2023). Bienestar psicosocial de investigadores de explotación sexual infantil de la Guardia Civil. *Behavior & Law Journal*, *9*(1). https://doi.org/10.47442/blj.2023.104

Powell, S., Butollo, W., y Hagl, M. (2010). Missing or Killed. The Differential Effect on Mental Health in Women in Bosnia and Herzegovina of

the Confirmed or Unconfirmed Loss of their Husbands. *European Psychologist*, *15*(3), 185-192. https://doi.org/10.1027/1016-9040/a000018

Puerto, A. (2007). Estrés laboral y estrés postraumático. Control de estrés en profesionales de la emergencia. *XV Curso de Postgrado Psicología de Urgencias y Emergencias*. Colegio Oficial de la Psicología de Madrid.

Purba, A. y Demou, E. (2019). The relationship between organisational stressors and mental wellbeing within police officers: a systematic review. *BMC Public Health, 19*, 1-21. https://doi.org/10.1186/s12889-019-7609-0

Real Academia Española (2014). Diccionario de la lengua española (23a ed.).

Robles, J. I. y Medina, J. L. (2002). *Intervención Psicológica en las catástrofes*. Síntesis.

Salovey, P., y Mayer, J. D. (1990). Emotional Intelligence. *Imagination, Cognition and Personality, 9*(3), 185-211. https://doi.org/10.2190/DUGG-P24E-52WK-6CDG

Sánchez, E. (2020). *Intervención sobre el Estrés Laboral: Medidas Preventivas*. Colegio Oficial de la Psicología de Madrid. https://www.copmadrid.org/web/files/comunicacion/Guia4Prevencion.pdf

Santana, A.I. y Farkas, C. (2007). Estrategias de autocuidado en equipos profesionales que trabajan en maltrato infantil. *Psykhe, 16*(1), 77-89. http://dx.doi.org/10.4067/S0718-22282007000100007

Simonovska, T., Sinclair, R. y Duval, K. (2023). International health and wellness of online child sexual exploitation police personnel: individual, management, and organizational realms of responsibility. *Frontiers in Psychology, 14*. https://doi.org/10.3389/fpsyg.2023.1155733

Terroni, N. N. (2009). La comunicación y la asertividad del discurso durante las interacciones grupales presenciales y por computadora. *Psico-USF*, *14*(1), 35-46. https://doi.org/10.1590/S1413-82712009000100005

Uriarte, C. y Parada, E. (2008). Trabajar en profesiones de emergencia: afrontar el estrés por incidente crítico y prevenir el desgaste psíquico y el desgaste por empatía. En E. Parada (ed.), *Psicología y Emergencia. Habilidades psicológicas en los profesionales de socorro y emergencia* (2.ª ed., pp. 573-599). Desclée De Brouwer.

Valencia, A. y Trejos, J. (2013). Los primeros auxilios psicológicos en el servicio de atención al ciudadano desde un enfoque humanista. *Revista Logos Ciencia & Tecnología, 4*(2), 42-52. https://doi.org/10.22335/rlct.v4i2.189

Vinuesa, N. (25-26 de octubre de 2023). *Prevención y Sensibilización del fenómeno y tercer sector social* [Conferencia]. Reunión Presidencia Española del Consejo de la Unión Europea 2023 en Materia de Personas Desaparecidas, Madrid, España.

Pasado y presente de las armas químicas: consecuencias para la vida y el medio ambiente

Past and Present of Chemical Weapons: Consequences for Life, and the Environment

Manuel Damián Cantero Berlanga
Universidad Católica de Murcia UCAM.
damiancb952@gmail.com | https://orcid.org/0000-0002-3095-3510

María Méndez Rocasolano
Universidad Católica San Antonio de Murcia UCAM.
mmrocasolano@ucam.edu | https://orcid.org/0000-0002-5345-8352

DOI: https://doi.org/10.14201/cp.31811
Recibido: 14-11-23 | Aceptado: 16-01-24

Resumen
Las armas químicas han sido utilizadas a lo largo de la Historia con devastadores efectos en la población civil y el medio ambiente. Esta investigación abordará el tratamiento que reciben las armas químicas, su origen, clasificación y regulación en la Convención sobre Armas Químicas (CWC), así como sus efectos en la población y en el medioambiente. Este sistema busca así establecer un régimen de control con la finalidad de prevenir la proliferación de este tipo de sustancias, así como regular su comercio entre los Estados Parte. A continuación, se explorarán los métodos utilizados para la destrucción de las armas químicas y su eliminación segura. Por último, se advertirá sobre el impacto ambiental de las armas químicas y sus efectos devastadores, tales como la contaminación del suelo y de las aguas subterráneas o en la flora y la fauna de la zona.

Palabras clave
Armas químicas; Convención sobre armas Químicas de 1993; Destrucción de las armas químicas; Medio Ambiente; Seguridad; TEDAX.

Abstract
Chemical weapons have been used throughout history with devastating effects on the civilian population and the environment. This research will address the treatment of chemical weapons, their origin, classification and regulation in the CWC, as well as their effects on the population and the environment. This system thus seeks to establish a control regime with the aim of preventing the proliferation of this type of substances, as well as to regulate their trade among the States Parties. The methods used for the destruction of chemical weapons and their safe disposal will then be explored. Finally, the environmental impact of chemical weapons and their devastating effects, such as contamination of soil and groundwater or on the flora and fauna of the area, will be discussed.

Keywords
Chemical weapons; Chemical Weapons Convention of 1993; Destruction of chemical weapons; Environment; Security; TEDAX.

1 Introducción

Desde los anales de la Historia se tiene constancia del uso de sustancias químicas con fines bélicos, lo que ha desembocado, por otra parte, en un importante desarrollo de la investigación y que ha contribuido, inevitablemente, al avance de la Ciencia y, por ende, el de la humanidad, aunque, como veremos más adelante, con efectos no siempre positivos.

En este sentido, la génesis y naturaleza de las armas químicas radica en su uso para causar daño, bien sea a personas, animales, plantas o ecosistemas en su conjunto. Es por ello por lo que el uso de armas químicas en las contiendas ha sido habitual desde la antigüedad y, como consecuencia del desarrollo tecnológico, ha ido incrementando sus efectos adversos y la extensión territorial de sus efectos.

Al mismo tiempo, el uso de químicos no es inherente al ámbito militar, sino que también es ampliamente utilizado por la indus-

tria, pero, a diferencia de los primeros, el principal perjudicado en este caso es el ecosistema.

De esta manera, las armas químicas pueden tener diversas formas de atacar al cuerpo humano (causando daños en los tejidos biológicos, afectando al sistema nervioso o a órganos vitales, entre otros) y al medioambiente (contaminación de los ecosistemas marinos, deforestación o extinción de especies animales), lo que pone de manifiesto su peligrosidad.

Debido a ello la Comunidad Internacional ha realizado denodados esfuerzos por su erradicación dando origen a una prolífica legislación internacional, siendo necesario centrar el foco en su destrucción o neutralización, estableciendo procedimientos que eliminen la letalidad de éstas en complejos adecuados y por métodos que aseguren o minimicen los daños a las personas y al medio ambiente.

En este sentido, los Estados han destinado numerosos recursos para minimizar los daños ocasionados y evitar en el futuro que tales situaciones se puedan volver a producir, al regularizar su uso y producción.

En España, concretamente cabe resaltar la labor de los TEDAX cuya función, al intervenir y actuar ante la presencia de estos agentes nocivos, permite salvaguardar la integridad de los ciudadanos y desarrollar las tecnologías que minimicen sus efectos en el medio ambiente, fruto del análisis e investigación de sus mecanismos, elementos y restos.

2 Las armas químicas en la antigüedad

Las armas químicas, como señalan Prokop, Opluštil, DeFrank y Damborský (2006) se han utilizado durante milenios y, como consecuencia de aquello, se han hallado pruebas de su existencia en la antigüedad y en la época clásica, destacando el uso de venenos de origen animal o de vegetal.

Tal es así que se han documentado numerosos casos de uso de armas químicas en diferentes culturas y civilizaciones. Si bien, aunque estos primeros intentos no eran tan sofisticados como las armas químicas modernas, demuestran el conocimiento temprano de los efectos destructivos de ciertas sustancias químicas como, por ejemplo, el curare amazónico, cuyos efectos dañinos afectaban tanto a las personas como al entorno natural.

Así, como señala Mayor (2020) atendiendo a los estudios realizados por el arqueólogo británico Simon James de la Universidad de Leicester, encontró una de las primeras evidencias (siglo III a.C.) de armas químicas usadas por las tropas del Imperio persa que utilizaron gases venenosos durante el sitio de *Dura* (situada al este de Siria). En esta contienda los persas prendieron betún y cristales de azufre en los túneles de los enemigos y los gases originados durante la ignición fueron aspirados por los sitiados, que perecían en escasos minutos.

En la antigua China, el filósofo Mo Zi ya recomendaba lanzar un tipo de antorchas (a las que incorporaban arsénico, azufre o betún para producir mezclas incendiarias o explosivas) en las minas que el enemigo cavaba donde los hostiles perdían la vida como consecuencia de los gases emanados, erigiéndose como una práctica común hasta casi el año 1000 de nuestra era. De esta manera, los distintos emperadores de China –al evidenciar el éxito de estas nuevas maneras de hacer la guerra– ordenaron el desarrollo de técnicas con el objeto de producir humo tóxico y desorientar o asfixiar a los enemigos durante las batallas. Todas estas tácticas se ponen de manifiesto en el aclamado libro *El arte de la guerra* de Sun Tzu conforme a la investigación llevada a cabo por Shua (2019). En este Tratado militar se ejemplifica, por primera vez, el uso, de forma masiva, de armas químicas contra población civil con la intención de mostrar que, para ganar una guerra, no hace falta destruir al enemigo, sino atacar su cadena de suministros o bases de abastecimiento, ya que en ello radica el valor intrínseco de las armas químicas y que, actualmente, hemos podido observar en la Guerra de Ucrania conforme al relato de Hernández (2023).

Igualmente, Spanevello y Suárez (2011) describieron que ya en la India se empleó el veneno de origen animal para la creación de armamento bélico. De ello ha quedado constancia en tra-

tados militares como el *Arthashastra* escrito en el siglo IV a. C por el estratega y gobernante Chanakya, dónde se describen diversas técnicas para el envenenamiento de pozos de agua.

En Occidente, señala Pons (2006) que durante el periodo de la Grecia Clásica se utilizaron diferentes sustancias venenosas en conflictos militares (como, por ejemplo, flechas y lanzas envenenadas con veneno de serpiente o humos tóxicos para operaciones de asedio) y que fueron adoptadas y perfeccionadas por estadistas militares romanos. Por su parte, destaca Trigo (2023) que un hito remarcable fue el llevado a cabo por el mal llamado Imperio Bizantino, dónde se valieron de la innovación y desarrollo tecnológico para la creación de armas químicas que, especialmente el uso del fuego griego (cuya fórmula ha sido perdida), jugaron un rol decisivo en las batallas navales dónde los barcos sucumbían ante la imposibilidad de extinguir las llamas.

Más adelante, durante el Renacimiento, se redescubrió el uso de las armas químicas. Así Leonardo da Vinci propuso el uso de polvo de sulfuro de arsénico y verdín en el siglo XVI durante los combates. Concretamente, como expone Otero (2022) proponía arrojar el veneno (compuesto por yeso, polvo de sulfuro de arsénico y verdín molido) en forma de polvo sobre las galeras, dónde los soldados lo inhalaban y resultaban asfixiados.

Finalmente, no podemos olvidar que el conocimiento y el uso de armas químicas en la antigüedad eran limitados en comparación con las armas químicas modernas. De modo que, como defiende González-Hernández (2021), la eficacia y la sofisticación de estas armas se fueron desarrollando con el tiempo, especialmente a partir de la Revolución Industrial en el siglo XIX.

3 Sobre la prohibición del desarrollo, la producción, el almacenamiento y el empleo de armas químicas y su destrucción

Tal y como enuncia Barberis (2017) y De Fortuny (2015) la Convención sobre Armas Químicas (en adelante, CWC) es am-

pliamente reconocida como uno de los tratados más exhaustivos en materia de control de armamento y su alcance abarca la no proliferación, el desarme y medidas de fomento de la confianza y seguridad.

Esto se evidencia en las obligaciones generales establecidas en su Artículo I[1], dónde Estado Parte se compromete a abstenerse en el desarrollo, adquisición o almacenaje de armas químicas o a su utilización para fines bélicos. Al mismo tiempo, Pita (2011) indica que se impone la obligación de su destrucción y de la eliminación de las instalaciones creadas para tales fines. En consecuencia y como se venía analizando, la CWC se perfila como un texto integral que prohíbe el desarrollo, producción, almacenamiento, transferencia y empleo de armas químicas, lo cual lo convierte en un tratado de no proliferación. Además, impone a los Estados Parte que poseen armas químicas la obligación de destruirlas, lo que también lo convierte en un Tratado de desarme.

Sin embargo, no podemos olvidar que algunas de estas sustancias químicas proporcionan una gran función a la comunidad científica y por ende a la sociedad. Ya que no solo se utilizan para elaborar armas potencialmente mortales, sino que además pueden usarse en experimentación contribuyendo al desarrollo y avance del conocimiento. Es por ello por lo que la CWC únicamente prohíbe su uso con fines bélicos, permitiendo su utilización con fines científicos (atendiendo en todo caso a criterios estrictamente restrictivos en cuanto a su uso, cantidades máximas permitidas y prohibiciones de exportación). Dichos límites se encuentran divididos en relación con el régimen de peligrosidad de los compuestos, estableciendo la lista de clasificación tripartita.

A su vez, como apunta De Salazar Serantes (2013), la CWC cuenta con un Anexo en el que se incluyen diversas listas de sustancias químicas tóxicas sujetas a medidas de verificación que, en origen, fueron utilizadas o producidas como armas.

1. Vid. Art. I CWC.

3.1 Lista 1

En su análisis, Riba (2005) advierte que la primera lista destaca por su controversia ya que en ésta se recogen las sustancias químicas tóxicas (incluidos sus precursores) que se han desarrollado, producido, almacenado o empleado como armas químicas planteando un peligro grave para el objetivo o propósito de la CWC al tener escasa o nula utilidad para los fines no prohibidos por la CWC.

En cuanto a la transferencia, se advierte que los Estados parte solo pueden transferir sustancias químicas de la Lista 1 a otro Estado Parte para fines de investigación, médicos, farmacéuticos o de protección, estando prohibida la transferencia de estas sustancias a un tercer Estado. En caso de que dicha transferencia se efectuase y quebrantase lo estipulado por la convención, la Secretaría Técnica será notificada por ambas partes 30 días antes de la transferencia (excepto si se trata de menos de 5 miligramos de saxitoxina para fines médicos o diagnósticos).

De este modo, cada Estado Parte debe presentar cada año una declaración pormenorizada sobre las transferencias realizadas el año anterior, en la cual se ha de incluir información sobre el nombre químico (fórmula estructural y número de registro del *Chemical Abstracts Service*), la cantidad adquirida de otros Estados o transferida a otros Estados Parte y el destinatario, la cantidad y la finalidad de cada transferencia.

Sin perjuicio de lo anterior, es importante señalar que serán las normas nacionales las que deberán establecer la seguridad, producción y emisión debiendo priorizar la salud de la población y la protección del medio ambiente mediante el establecimiento de mecanismos limitadores (como la prohibición de una operación continua de las líneas de producción o limitando la producción en recipientes de reacción y sus volúmenes, pudiendo producirse solo en instalaciones únicas de pequeña escala).

En definitiva, tal y como se ha venido advirtiendo la normativa internacional aplicable permite la producción de sustan-

cias químicas de la Lista 1 pero limita sus fines y volumen de producción e impone severas prohibiciones a laboratorios que tienen restricciones adicionales en cuanto a la cantidad total permitida.

3.2 Lista 2

En la segunda Lista, como enuncia Cervell (2003) se alude a todas aquellas sustancias químicas producidas con fines comerciales no prohibidos por la CWC al establecer un mecanismo de control basado en la solicitud de información que se hace en relación con el año anterior (es decir, no requiere autorización, sino notificaciones correspondientes al año anterior acerca de las cantidades de cada sustancia química de la Lista 2) sobre las sustancias producidas, elaboradas, consumidas, importadas y exportadas, así como una especificación cuantitativa de las importaciones y exportaciones respecto de cada país interesado.

En contraposición con la notificación anteriormente mencionada para la Lista 1, la Lista 2 impone a los Estados Parte la obligación de presentar declaraciones anuales correspondientes al año anterior que incluyan datos nacionales sobre la producción, elaboración, consumo, importación y exportación de cada sustancia química de la Lista 2[2].

Al mismo tiempo, se imponen obligaciones[3] a los complejos industriales en los cuales se hayan producido, elaborado o con-

2. Toda esta información, en un primer momento, será proporcionada por medio de declaraciones sobre las cantidades importadas y exportadas con cada país interesado, que serán elaboradas 30 días después de la entrada en vigor de la Convención, y posteriormente se deberán elaborar declaraciones anuales 90 días tras la finalización del año anterior.

3. Los requisitos de Declaración para aquellas actividades relacionadas con las sustancias de la Lista 2 son mucho más permisivo, solicitando que las actividades previstas sean a más tardar declaradas 60 días antes del comienzo del calendario del año siguiente (pudiendo ser presentada con 5 días de antelación si ya se hubiese presentado la declaración anual). De igual manera, no es necesario presentar la declaración de conformidad de las mezclas con baja concentración de una sustancia química de la

sumido dichas sustancias durante cualquiera de los tres años del calendario anterior o se prevea que vayan a producir, elaborar o consumir cantidades específicas de sustancias químicas de la Lista 2 y que se concretan en presentación de declaraciones iniciales y anuales[4].

Además, y de manera opuesta a la primera casuística relatada que prohibía la automatización de los procesos de extracción de las sustancias químicas, el punto 6º de la parte VII, se permite una vía para las declaraciones de un complejo industrial[5] (que deben incluir su nombre y el de su propietario, la ubicación y el número de plantas declaradas de acuerdo con lo dispuesto en la Parte VIII del anexo de la CWC, así como toda la información relativa a la capacidad de producción, almacenamiento, ubicación, actividades principales, etc.) dotando al sistema de una información completa sobre la fabricación de los productos manufacturados de la Lista 2.

Por otra parte, otra de las obligaciones establece que cuando se declare un complejo industrial se deberá incluir la información de cada sustancia química de la Lista 2 siempre y cuando rebase el umbral de declaración con mención al nombre químico y para el caso de tener que elaborar la declaración anual sobre actividades anteriores, se deberá prever las cantidades que fuera a elaborar o consumir el complejo industrial durante el calendario siguiente, así como sus finalidades.

Al mismo tiempo, cada Estado Parte tiene la obligación de declarar todos los complejos industriales que hayan producido,

Lista 2 (excepto cuando se considera que la facilidad de recuperación o atendiendo a su peso pueda ser peligroso). Cfr. Art. VIII, párrafo 21, apartado i).

4. Atendiendo a los límites para la presentación de declaraciones varían según las cantidades de sustancias químicas producidas, elaboradas o consumidas en los años anteriores o previstas para el próximo año calendario de: a) 1 kg de una sustancia química designada "*" en la parte A de la Lista 2; b) 100 kg de cualquier otra sustancia química enumerada en la parte A de la Lista 2; o c) 1 tonelada de una sustancia química enumerada en la parte B de la Lista 2.

5. Se entiende por complejo industrial (factoría, explotación) la integración local de una o más plantas, con cualquier nivel administrativo intermedio, bajo un solo control operacional y con una infraestructura común.

en cualquier momento desde el 1 de enero de 1946, una sustancia química de la Lista 2 para fines bélicos, proporcionando la Secretaría técnica a los Estado Parte una lista que contenga toda la información relativa a los complejos industriales declarados, en caso de solicitud.

Todos estos requisitos garantizan la transparencia y el intercambio de información sobre las actividades relacionadas con dichas sustancias químicas y garantizan que solo serán transferidas a los Estado Parte o recibidas de éstos.

No obstante, cabe resaltar que, a nuestro juicio es una limitación muy vaga, ya que 193 de los 195 Estados reconocidos por las Naciones Unidas son parte de esta convención y deja a cantidad de Estados al margen de estas obligaciones.

Finalmente, respecto de las transferencias a Estados no parte de la convención, se insta a que cada Estado adopte las medidas necesarias para que las sustancias químicas transferidas se destinen únicamente a fines no prohibidos por la Convención[6].

3.3 Lista 3

Concluyendo esta parte de la investigación, observamos que la Lista 3 recoge las sustancias químicas que se producen en grandes cantidades para fines no prohibidos, lo que obliga como defiende Gómez (2016) a los Estados parte a hacer declaraciones anuales sobre sus actividades relacionadas con la defensa química y con la producción, consumo y transferencia de estas sustancias.

Con relación a esta lista, se presenta la obligación de comunicar los datos nacionales del año anterior, pero dicho control es aún más laxo que el enunciado en la Lista 2 (sin embargo, los

6. Lo que se llevará a cabo por medio de un certificado en el que se haga constar, respecto de las sustancias químicas transferidas: a) La prohibición de su uso para fines prohibidos por la Convención; b) Que no serán transferidas de nuevo; c) Los tipos y cantidades de esas sustancias químicas; d) Certificado de conocimiento del uso o usos de las sustancias y e) El nombre y la dirección de aquellos usuarios que sean los destinatarios del producto.

complejos industriales que pretendan la producción o vayan a producir sustancias de la Lista 3 deben ser declarados cuando inicien su actividad y, en todo caso, anualmente). Asimismo, y por su baja peligrosidad, no se incluye la obligación de declaraciones de conformidad para aquellas sustancias químicas que presenten una baja concentración. Si bien deberán presentarse dichas declaraciones cuando puedan suponer un peligro según su cantidad o por su facilidad de recuperación.

Cabe mencionar que entre las obligaciones a la hora de declarar un complejo industrial (haciéndose extensible a todos aquellos originados a partir del 1 de enero de 1946) respecto a la Lista 3, se debe incluir cierta información, como la cantidad de sustancia producida en el año anterior (expresando las cuantías en ciertos tramos cuyo mínimo es de 30 toneladas y cuyo tramo máximo es más de 100.000 toneladas).

Por otra parte, la CWC establece que se deben establecer ciertas medidas con la transferencia de sustancias químicas de la Lista 3 a Estados no Parte en la convención. De modo que cada Estado Parte debe tomar medidas para garantizar que dichas sustancias se utilicen exclusivamente para fines permitidos y, para asegurarse de esto, el Estado Parte que realiza la transferencia exigirá al Estado receptor un certificado[7].

Todas estas medidas tienen como objetivo garantizar la trazabilidad, previniendo la transferencia inadecuada o el uso indebido de sustancias químicas de la Lista 3, y que resultan similares a aquellas de la Lista 2, aunque de menor entidad (por ejemplo, la convención establece que cinco años tras la entrada en vigor de la convención se podrán aplicar otras medidas para estas sustancias químicas).

En cierre, podemos aseverar que las principales diferencias entre la Lista 1, la Lista 2 y la Lista 3 se refieren a la clasificación de las sustancias químicas y su régimen de control. Las sustancias de la Lista 1 son sustancias químicas tóxicas que tienen

7. Dicho certificado deberá incluir, al menos, los siguientes aspectos y finalidades: a) que se utilizarán solo para fines permitidos por la convención; b) la prohibición de transferirlas nuevamente; c) los tipos y cantidades de las sustancias químicas; d) el uso final de las mismas; y e) el nombre y dirección del usuario final.

propiedades de guerra química y que tienen poco o ningún uso industrial legítimo (y, por ello, estas sustancias están prohibidas absolutamente, así como su producción, posesión y uso). Tras ello, la Lista 2 contiene sustancias químicas tóxicas que tienen un uso industrial legítimo, pero que también pueden utilizarse con fines de guerra química (y, por ello, están sujetas a medidas de control y verificación). Y por último la Lista 3 que comprende sustancias químicas que no tienen una utilización común para fines de guerra química, pero que podrían ser utilizadas para la producción de agentes químicos tóxicos (y que, como las anteriores, estarán sujetas a medidas de control y verificación, aunque en menor grado que las de la Lista 2).

4 Clasificación de las armas químicas y sus efectos nocivos

Al contrario de lo que ocurre con las armas convencionales, el uso de las armas químicas ha provocado un rechazo unánime de la comunidad política a nivel internacional. Es por ello por lo que la CWC define las armas químicas como aquellas que, conjunta o separadamente, se puedan encuadrar en los apartados que, a continuación, se analizarán conforme al estudio realizado previamente por Muñoz-Canales y Rodríguez-López (2021).

El primero de ellos está dedicado a las sustancias químicas tóxicas o sus precursores (salvo cuando se destinen a fines no prohibidos por la presente convención, siempre que los tipos y cantidades de que se trate sean compatibles con esos fines). Seguidamente, el relativo a las municiones o dispositivos destinados de modo expreso a causar la muerte o lesiones mediante las propiedades tóxicas derivadas de las sustancias especificadas anteriormente. Y, en último lugar, aquel apartado dedicado a cualquier equipo destinado de modo expreso a ser utilizado directamente en relación con el empleo de las municiones o dispositivos especificados en el apartado.

Por su interés en la investigación, en los próximos apartados se procederá a realizar una clasificación de las citadas armas, describiendo sus tipos, riesgos y posibles efectos.

4.1 Agentes neurotóxicos

Los agentes neurotóxicos (que son utilizados como agente o componente principal en las llamadas armas químicas botulínicas), como define Velasco (2014), son sustancias químicas que afectan al sistema nervioso, interfiriendo en la transmisión de señales entre las células nerviosas. Estos agentes pueden tener efectos perjudiciales en la salud humana tanto a corto como a largo plazo, ejemplo de ello pueden ser los gases nerviosos (como el gas sarín y el gas VX).

El principal componente de estos agentes son los compuestos organofosforados que se utilizan en pesticidas y en otros usos industriales. Estas sustancias actúan inhibiendo la enzima llamada acetilcolinesterasa, que es esencial para la función normal del sistema nervioso. De modo que, al inhibir esta enzima, los compuestos organofosforados causan una acumulación de la acetilcolina (un neurotransmisor), lo que lleva a una sobreestimulación de los receptores nerviosos y puede provocar síntomas como debilidad muscular, dificultad respiratoria, mareos, convulsiones e incluso la muerte (si bien, para ciertos compuestos organofosforados existen antídotos que tienen efectos contrarios como la atropina o las oximas que actúan desplazando el órgano fosforado), tal y como recoge en su estudio Manrique (2002).

Por último, atendiendo al origen de estos agentes neurotóxicos, Quinto (1999) señala que su uso es esencialmente militar ya que poseen la capacidad de interferir con la función del sistema nervioso, pese a que en la actualidad sean usados para fines agrícolas y sanitarios debido a sus propiedades insecticidas y fitosanitarias.

4.2 Agentes vesicantes

Los agentes vesicantes (también llamados agentes *blister*) actúan a nivel macroscópico y tienen la capacidad de provocar ampollas o vesículas en la piel, así como en las membranas mucosas y los ojos, cuando entran en contacto con ellos.

Uno de los principales agentes vesicantes es el gas mostaza (*iperita,* cuyo término alude a la región de Yprès dónde fue utilizada por el Ejército Alemán en 1915), estudiado ampliamente por Zúñiga (2015). Este agente se presenta en estado líquido, aceitoso e incoloro (dependiendo su color y olor de las impurezas), volatilizándose fácilmente, con un olor similar al ajo o a mostaza, de ahí su nombre. El gas mostaza fue ampliamente utilizado durante la Primera Guerra Mundial a raíz de la cual fue considerado una sustancia prohibida y ampliamente condenada por la Comunidad Internacional –aunque no por ello ha cesado su utilización, como se ha puesto de manifiesto en el escenario bélico de la región de Siria–. Su efecto visible más notorio es su capacidad de causar graves quemaduras químicas en la piel produciendo ampollas, afectando a los pulmones y provocando lesiones oculares.

Otro agente vesicante son las llamadas *lewisitas*, las cuales fueron sintetizadas por el Capitán Lewis (militar de Estados Unidos durante los años 1917 y 1918) usando arsénico y cloro y cuyas consecuencias acarrean ampollas y quemaduras en la piel, así como daños internos si se inhalan o se ingieren.

En tercer lugar, Jiménez (2005) sitúa los agentes nitrogenados como aquellos compuestos químicos que contienen nitrógeno (siendo los más destacados HN_1, HN_2 y HN_3) y que causan ampollas y quemaduras en la piel, así como efectos sistémicos si se inhalan o se absorben.

No obstante, como dijimos al comienzo estas sustancias pueden tener efectos beneficiosos para el ser humano, incluso en el ámbito sanitario. Tal es así que el gas mostaza contribuyó al desarrollo de la quimioterapia, al descubrirse los notables efectos que tenía sobre la médula ósea, causando la supresión del sistema inmunológico y dañando las células que se dividen rápidamente, como las cancerosas. Esta investigación, tal y como recoge Camacho (2020) condujo al desarrollo de la primera clase de medicamentos quimioterapéuticos conocidos como agentes alquilantes (como la ciclofosfamida y el clorambucilo) y que supusieron un punto de partida para los tratamientos contra el cáncer, la cual ha ido evolucionando y desarrollando múltiples clases de procedimientos con diferentes mecanismos de acción.

4.3 Agentes sanguíneos

Schecter y Fry (2005) señalan que estos agentes, como su propio nombre indica, afectan directamente al sistema circulatorio y a la sangre, ya que están diseñados o bien para causar daño y disfunción en el sistema sanguíneo del organismo afectado, o bien para impedir el transporte de oxígeno produciendo finalmente la asfixia.

Éstos se clasifican en dos grupos, los simples (que físicamente desplazan al oxígeno, como el metano o el nitrógeno) y los químicos (los cuales interfieren con el transporte de oxígeno a nivel celular, causando hipoxia tisular[8]).

Los compuestos químicos más utilizados son los derivados del cianuro (como el cianuro de hidrógeno o el cianuro de potasio) que bloquean el transporte de oxígeno en el cuerpo. En concreto, el cianuro inhibe la enzima citocromo oxidasa, necesaria para el proceso de respiración celular promoviendo la anoxia tisular y en consecuencia, la muerte celular; la exposición al cianuro puede provocar asfixia y la muerte rápidamente. Cabe mencionar que Chauhan, D'cruz, Faruqi, Singh, Varma, Singh y Karthik (2008) afirman que el cianuro de hidrógeno se utiliza como precursor en la síntesis de muchos compuestos químicos, que van desde polímeros hasta plásticos, empleándose también en la industria farmacéutica y para la fumigación de barcos y edificios.

Un segundo ejemplo lo encontramos en el arsénico que afecta al sistema circulatorio y provoca daño en los glóbulos rojos y en los vasos sanguíneos, causando anemia, problemas cardiovasculares y daño en órganos vitales.

8. La hipoxia tisular se refiere a una insuficiencia de oxígeno en los tejidos del cuerpo que resulta en una disminución de la oxigenación celular puede desencadenar respuestas celulares y moleculares adversas que comprometen el funcionamiento normal de los tejidos y órganos, lo que puede llevar a un daño tisular considerable afectando a la salud en general.

Otro elemento utilizado en estos agentes es el fosgeno que, aunque se clasifica principalmente como un agente asfixiante, también puede causar daño en los tejidos pulmonares y provocar edema pulmonar, lo que puede llevar a una insuficiencia respiratoria grave.

Por último, Domingo y Pita (2014) incluyen el cloro. En su forma gaseosa es irritante para los pulmones y las vías respiratorias, provocando dificultad para respirar, tos, dolor en el pecho y edema pulmonar y finalmente asfixia.

4.4 Agentes incapacitantes

Atendiendo a los agentes incapacitantes, García (2019) los define, en concordancia con lo establecido en la CWC, como cualquier sustancia química que no figure en una lista y que pueda producir rápidamente efectos sensoriales en los seres humanos, irritación o efectos físicos incapacitantes temporales y que tienen como objetivo principal incapacitar o deshabilitar temporalmente a las personas expuestas a ellas.

A diferencia de los agentes letales (que causan la muerte) los agentes incapacitantes buscan afectar el funcionamiento normal del sistema nervioso central o periférico, generando una variedad de efectos fisiológicos y neurológicos que limitan la capacidad de la persona para llevar a cabo acciones y tareas básicas. Un ejemplo de ello son los agentes lacrimógenos (como el gas pimienta) que provocan irritación en ojos, piel y garganta acarreando problemas respiratorios y náuseas y que suelen ser utilizados por las fuerzas policiales y antidisturbios en el cumplimento de la ley para hacer frente a problemas de orden público y para la protección personal, tal y como especifica García (2019).

5 Destrucción de las armas químicas y de sus instalaciones: efectos y consecuencias

Se entiende por destrucción de armas químicas conforme al artículo IV de la CWC, el proceso en virtud del cual las sustan-

cias químicas se convierten de forma irreversible en una materia inapropiada para la producción de armas químicas y que hace que las municiones y demás dispositivos sean inutilizables en cuanto tales de modo irreversible[9].

De acuerdo con la CWC, se impone la obligación a cada Estado de determinar qué procedimiento se ha de seguir para conseguir la destrucción de las armas químicas (pero nunca con procedimientos como el vertido en una masa de agua, enterramiento o incineración a cielo abierto por considerar que no son adecuados para el fin que buscan y pueden provocar desastres para la salud humana y de los ecosistemas). Dicha obligación implica, como sostiene Bernachi (2022), que deben destruirse en instalaciones designadas y debidamente equipadas.

Para organizar la destrucción de las armas químicas, el CWC no sigue el criterio de lista tripartita que se ha analizado durante la realización de la presente investigación (Listas 1, 2 y 3), sino que crea 3 nuevas categorías. La Categoría 1 relativa a armas químicas basadas en sustancias químicas de la Lista 1 (la más peligrosa) así como sus piezas y componentes. A continuación. La Categoría 2, destinada a armas químicas basadas en todas las demás sustancias químicas y sus piezas y componentes. Y, finalmente la Categoría 3, que abarca todo tipo de municiones y dispositivos no cargados y equipo concebido específicamente para su utilización directa en relación con el empleo de armas químicas.

Dicho lo cual, la CWC marca distintos espacios temporales (ya que los plazos son marcados desde la entrada en vigor del CWC en el respectivo Estado Parte) para la eliminación de las armas químicas de acuerdo con la categoría de éstas, comenzando la destrucción de las armas químicas de la Categoría 1 dos años después a más tardar de la entrada en vigor del CWC, completándose la destrucción total de estas armas en los próximos diez años. En cuanto a la destrucción de las armas químicas de la Categoría 2 comenzará un año después, y se completará la destrucción cinco años después e incrementándose las cantidades de sustancias químicas que se destruyen anualmente en rela-

9. Vid. Art. IV CWC.

ción con el peso de éstas. Por último, en cuanto a las armas de la Categoría 3, comenzarán su destrucción un año después y se completará la destrucción cinco años después.

A este respecto, la CWC tiene una sección específica para la destrucción[10] de aquellas armas químicas que consideran antiguas, es decir aquellas producidas antes de 1925 (independientemente de su estado de conservación) y aquellas elaboradas entre 1925 y 1946 (las cuales se encuentran previsiblemente en tal estado que ya no pueden emplearse como armas químicas). Como consecuencia de tal estado de conservación y de su antigüedad, estas armas químicas pueden suponer un peligro potencial para la salud de los seres humanos y, bien sea directa o indirectamente, han de ser tratadas y destruidas con especial cuidado.

Otra categorización que se ha de tener en cuenta son las llamadas armas "abandonadas" que son aquellas armas químicas que hayan sido abandonadas por un Estado, después del 1 de enero de 1925 en el territorio de otro Estado, sin el consentimiento de este último (no estando incluidas en este apartado aquellas que fueron vertidas o hundidas en aguas internacionales).

En lo que concierne a las armas abandonadas (siendo aplicable también a las armas químicas antiguas) el Estado Parte en cuyo territorio se encuentren presentará a la Secretaría técnica, treinta días después de la entrada en vigor de la CWC, toda la información pertinente disponible acerca de ellas incluyendo el tipo, la cantidad y la condición actual de esas armas químicas con obligación adyacente de informar a la Secretaría Técnica si encontrase nuevas armas químicas (ciento ochenta días máximo) y de tomar medidas para su destrucción y eliminación, incluyendo los residuos tóxicos que se desencadenen como consecuencia de tal actividad de destrucción.

Sin embargo, las actuaciones difieren a la hora de hablar sobre las armas químicas abandonadas, ya que el Estado Parte (donde se encuentren las armas químicas) celebrará consultas

10. A este respecto, la parte IV (b): antiguas armas químicas y armas químicas abandonadas (disposiciones generales del CWC).

a los efectos de destruir las armas químicas abandonadas en colaboración[11].

Si bien, es importante destacar que, en este ámbito, existe una gran cooperación internacional ya que el Estado Parte que haya abandonado los elementos químicos en suelo de otro Estado Parte proporcionará todos los recursos financieros, técnicos, expertos, de instalación y de otra índole que sean necesarios (colaborando así el Estado donde se hallen dichos elementos químicos).

Tal es así que, de acuerdo con la Organización para la Prohibición de las Armas Químicas (en adelante, OPWC), la destrucción de reservas mundiales de arsenales de armas químicas asciende al 99 %. Sin embargo, estos datos solo se centran en aquellos países que forman parte de la CWC, quedado al margen de las inspecciones y verificaciones antes mencionadas países como Corea del Norte (que no han ratificado la CWC).

A este respecto cabe señalar que, a partir de 1989, el programa químico de Corea del Norte se consideró como avanzado, y desde ese momento no ha cesado en la producción de manera significativa de gases nerviosos, vesicantes, neurotóxicos, entre otros, además de una diversidad de sistemas de proyección. De esta manera, se estima que Corea del Norte posee un considerable arsenal de agentes químicos, con potencial uso en una eventual ofensiva contra Corea del Sur, al mismo tiempo que ha desarrollado medidas de protección para su población civil con el objetivo de mitigar los efectos de dichos agentes. Concretamente, como informa Pulido (2003), en 1999, el gobierno de Corea del Sur informó la existencia de ocho instalaciones químicas, cuatro centros de investigación y seis sitios de almacenamiento de agentes químicos que el gobierno norcoreano había establecido. Se tiene conocimiento, de acuerdo con informes estadounidenses, que en estas instalaciones se produce gas sarín, tabún, fosgeno, ácido prúsico, gas mostaza, entre otros.

11. Dichas consultas comenzaran 30 días después de que haya sido informada la Secretaría General Técnica y ambos Estados elaboraran un plan para la eliminación de dichas armas químicas.

Asimismo, no podemos dejar de mencionar la proliferación de nuevos agentes no contemplados, en ese momento, por la CWC como, entre muchos otros, el llamado *novichok* (en ruso "novato" o "nuevo veneno", son una serie de agentes químicos nerviosos y altamente tóxicos que fueron desarrollados en la Unión Soviética durante la Guerra Fría) –utilizado en dos ciudades de Reino Unido–, y que son considerados mucho más potentes que los agentes nerviosos tradicionales (caracterizados por su estructura química única y su alta letalidad incluso una pequeña cantidad), viéndose la necesidad, por parte de todos los miembros del CWC, de actualizar la lista de sustancias (concretamente, en noviembre de 2019 el *novichok* fue añadido a la Lista 1), tal y como advierten Constanzi y Koblentz (2020).

5.1 Métodos de descontaminación de productos tóxicos

Desde el momento de la producción de las armas químicas se observó la necesidad, y posteriormente obligación, de elaborar métodos eficaces para la descontaminación de esos productos tóxicos y sus derivados, con el objetivo de eliminar o neutralizar las sustancias venenosas tanto en el personal como en los equipos.

De esta manera, las tecnologías de destrucción dependen de las características del arma que se pretenda destruir (armas químicas unitarias, ensambladas, agentes de armas químicas a granel, municiones de armas químicas recuperadas y municiones binarias[12]) y, en consecuencia, los procedimientos de destrucción se pueden dividir en dos grupos. El primero engloba un conjunto de tecnologías que implican, bien procesos de destrucción a alta temperatura (pirolisis de plasma, incineración y las cámaras de explosión), o bien, sistemas de tratamiento de gases de escape asociado. El segundo se corresponde con la destrucción a

12. Destaca este último caso por su complejidad, ya que se trata de armas químicas en que el agente tóxico no se encuentra activo en el arma, sino que se encuentra en forma de precursores físicamente separados. El objetivo que se busca con estas últimas armas es el de tener dos o más precursores menos tóxicos que la mezcla final resultante y poder ser transportados de manera más segura o en algunas ocasiones, con el objeto de ser menos detectados por separado.

baja temperatura tal como la neutralización (es decir, el uso de agentes neutralizantes o una solución de descontaminación) y la hidrólisis seguida de tratamientos secundarios de los subproductos resultantes como biodegradación u oxidación con agua supercrítica.

La descontaminación, por su parte, abarca no solo los tejidos biológicos, sino también aquellas superficies que puedan entrar en contacto directo con la piel. En el contexto militar, dicha lista incluiría ropa, equipo electrónico (computadoras), camiones, barcos, aviones, helicópteros e incluso tierra.

Sin embargo, como defiende LeJeune (1998), la incineración no es compatible con la descontaminación; después de todo, descontaminar un objeto útil mediante la incineración no tiene mucho sentido especialmente cuando ese objeto es una persona viva. Por ello, muchas veces el costo de descontaminación de un elemento es mayor al del valor del objeto, lo que desemboca en su abandono[13].

Asimismo, afirma Cervell (2017) que el uso de agentes químicos sobre la población (civiles o no) se realiza con el único objetivo de colapsar los hospitales –y de herir asimismo a aquellos que entran en contacto con las víctimas–, como fue el caso de varios de los ataques sufridos en Siria en 2017. La descontaminación en estos casos es muy compleja ya que requiere de equipo especializado de protección, no estando preparados para atender en caso de una gran afluencia de víctimas.

5.1.1 La neutralización química e hidrólisis

Esta técnica consiste en el empleo de sustancias químicas o reactivos específicos para neutralizar o descomponer dichas armas. Los descontaminantes químicos más activos son probablemente la mezcla formada por dietilentriamina; éter monometílico de etilenglicol e hidróxido de sodio, que se conoce

13. La misma táctica se sigue con ciertas zonas geográficas en tiempo de guerra, procediéndose a abandonar el área en lugar de proceder a su descontaminación.

como agente descontaminante DS2[14] y cuyo componente activo es 1-metoxietanol.

Este sistema, aunque es un descontaminante efectivo de amplio espectro, es altamente corrosivo para muchos materiales, no siendo adecuado para uso general y está siendo reemplazado por sistemas oxidativos. El objetivo en la descontaminación oxidativa es típicamente lograr la conversión a elementos de baja toxicidad. Por su parte, la descomposición hidrolítica deriva en materiales menos tóxicos, como el sulfóxido de vinilo y/o la sulfona de vinilo, que son compuestos inofensivos según Popiel y Nawała (2013). Con la hidrólisis, se consigue que las armas químicas se descompongan mediante la reacción con el agua. Una de las desventajas de la hidrólisis es la gran cantidad de residuo generado, que puede ser hasta 5 o 6 veces el agente destruido, siendo la toxicidad relativamente baja conforme a los estudios llevados a cabo por Locatelli (2014).

5.1.2 La descontaminación enzimática

Barletta (2020) sostiene que esta técnica puede traer un amplio campo de mejora y desarrollo, se trata del uso de preparaciones que consisten en catalizadores enzimáticos que aumentan la velocidad de las reacciones. En este sentido, las enzimas son catalizadores biológicos ambientalmente benignos y altamente eficientes capaces de desintoxicar muchas veces su propio peso de agente químico. Asimismo, las enzimas son capaces de aumentar las velocidades de reacción hasta 10 veces en comparación con las reacciones no catalizadas.

El uso de enzimas catalíticas también podría desempeñar un importante papel en la destrucción de los arsenales de agentes químicos, tal como lo requiere la CWC. Sin embargo, hasta ahora, no ha habido esfuerzos significativos en esta área. La principal razón de esta falta de uso ha sido el tiempo y, en menor medida, el costo y que las instalaciones construidas y autorizadas para la destrucción de agentes químicos requerirían demoras significativas para recibir la autorización para

14. Se trata de un líquido polar no acuoso, compuesto por un porcentaje en peso de 70 % dietilentriamina, 28 % etilenglicol monometil éter y 2 % de hidróxido sódico.

utilizar diferentes tecnologías. Además, Prokop *et al.* (2006) advierten que, hasta hace poco, no existía una producción a escala industrial de las enzimas, lo que conllevaba costes muy altos.

Además, las enzimas no son tóxicas, no son corrosivas ni inflamables y su principal ventaja es que cuando se liberan al medio ambiente son fácilmente biodegradables. En contra, según Popiel y Nawała (2013) tenemos que mencionar la baja estabilidad y alta especificidad de este método. Siendo uno de los métodos más interesantes para la detoxificación de la mostaza azufrada la oxidación catalizada por enzimas.

5.1.3 Detonación controlada

Algunas armas químicas, como las municiones químicas, pueden ser destruidas mediante la detonación controlada en instalaciones seguras. Este método involucra la explosión controlada de las municiones para desactivar y destruir los agentes químicos, así como hacerse cargo de los gases, que deben ser tratados para completar la destrucción. Además, la detonación puede cambiar la estructura química del agente, volviéndolo más estable y menos propenso a fugas o degradación con el tiempo.

5.1.4 La destrucción térmica

Es una tecnología que utiliza el calor generado mediante un proceso de calentamiento eléctrico en un contenedor especial denominado cámara de detonación estática. Dicha cámara confina y dirige la explosión dentro de la cámara, minimizando el riesgo de fugas o dispersión no controlada de los agentes químicos evitando la liberación de gases y residuos al medio ambiente, logrando así la destrucción completa del agente químico y la carga explosiva asociada. De esta forma, la descontaminación de agentes químicos depende de las características específicas de los mismos, siendo un proceso de eliminación o neutralización de estas sustancias tóxicas de manera segura y efectiva para proteger a las personas y al medio ambiente. En la mayoría de las ocasiones, para la eliminación de las armas químicas, se utiliza más de un solo proceso de neutralización.

5.2 Destrucción de las instalaciones de armas químicas

Para promover un mejor planeta para todos, la humanidad se debe deshacer de las armas químicas que antaño provocaron tanto sufrimiento, pero también debe desmantelar o transformar esas plantas donde se generaron las armas. Para ello, el CWC tiene previsto un sistema por el cual se ha de detallar minuciosamente cada uno de los centros donde se produjeron armas químicas para proceder a su destrucción o conversión.

En lo que respecta a la destrucción, cada Estado Parte decidirá los métodos que ha de aplicar para la destrucción de las instalaciones de producción de armas químicas, con objeto de desactivar éstas, sin que se pueda producir en la misma ningún tipo de sustancias químicas pudiendo ser convertidas temporalmente en instalaciones de destrucción de armas químicas. Todo el proceso será notificado a la Secretaría técnica ciento cincuenta días antes de realizar cualquier actividad de conversión y los planes sobre la destrucción de la instalación deberán ser comunicados a la Secretaría Técnica con ciento ochenta días de antelación al comienzo de la destrucción.

Para vigilar que se cumplan dichos protocolos y como consecuencia de las obligaciones contraídas por la CWC, se ha de hacer una verificación de la destrucción de instalaciones de producción de armas químicas y de cada uno de los elementos del inventario declarado de conformidad con el plan detallado convenido para la destrucción.

Por último, Prokop (2006) resaltan la necesidad de hablar de la conversión de instalaciones de producción de armas químicas para fines no prohibidos en la CWC, independientemente de que puede ser que ya se esté utilizando con esos fines o se proponga (en un futuro) su utilización para éstos, dirigiéndose la solicitud al director general de la CWC. Cabe destacar que, en caso de que se quiera convertir la instalación, se ha de destruir todo el equipo especializado que conste en la misma y, además, deben eliminarse todas las características especiales de los edificios y estructuras que distingan estos edificios, estableciendo una limitación temporal de seis años para su completa transformación.

6 Impacto medioambiental de las armas químicas

Las armas químicas representan una grave amenaza para el medio ambiente debido a su capacidad de causar daños devastadores. Estas armas, diseñadas para liberar sustancias químicas tóxicas con el objetivo de infligir daño tanto en los seres humanos como en su entorno, tienen efectos perjudiciales a largo plazo en los ecosistemas y los recursos naturales.

La exposición a agentes químicos letales puede contaminar el suelo, el agua y el aire, afectando a la flora y a la fauna, así como poner en peligro la salud de las comunidades cercanas. De esta manera, el impacto ambiental de las armas químicas es una preocupación global que requiere una atención urgente y medidas efectivas para prevenir su uso y promover la descontaminación y restauración de las áreas afectadas, tal y como señala Mazo (2023).

Su mayor impacto se ha constatado durante los periodos bélicos ya que dichas tácticas de guerra, por su crueldad, ocasionan un daño incalculable a la biodiversidad de los lugares donde actúan estos químicos.

Un claro ejemplo de ello fue la Segunda Guerra Mundial, donde se utilizaron gran cantidad de productos químicos tóxicos, como los fosgenos y los agentes vesicantes, en ataques contra instalaciones portuarias que contaminaron grandes masas de agua y que, al ser liberados al mar, contaminaron los ecosistemas costeros dañando la vida marina (incluyendo peces, moluscos y crustáceos).

Seguidamente, durante la guerra de Vietnam (concretamente en el Valle A Luoi) Uesugi (2019) narra cómo se utilizaron herbicidas como el Agente Naranja, que contenía dioxina. La aplicación de este químico (utilizado para la deshojar las selvas donde se ocultaban los vietnamitas durante la guerra) contaminó los ríos y cuerpos de agua, afectando la vida acuática y causando daños a largo plazo en los ecosistemas. Además, causó la des-

trucción de vastas áreas de selva, alterando drásticamente los ecosistemas acuáticos y terrestres.

Por su parte, Cánovas (2013) apunta que la contaminación de suelos y aguas subterráneas también se ve afectada por estas armas, como ocurrió durante la guerra de Siria desde 2011, al informarse de ataques con armas químicas que han provocado la liberación de sustancias químicas tóxicas en el aire y el suelo, contaminando los recursos hídricos y los suelos agrícolas.

Igualmente, durante el conflicto en Irán e Irak (que tuvo lugar entre 1980 y 1988), se informó que ambos bandos vertieron residuos químicos en ríos y cuerpos de agua como una táctica de guerra, así como del uso de armas químicas, incluido el gas mostaza y el gas sarín. Estos químicos causaron daños significativos a la flora y fauna en las áreas afectadas, provocando la muerte masiva de animales y afectando la diversidad biológica de la región tal y como sostienen numerosas fuentes como Pita (2008) o Peláez (2020).

Más recientemente, estos químicos han sido utilizados como instrumento de presión política por grupos paramilitares, como las FARC, que, a pesar de que sus objetivos eran tanto la población civil como las fuerzas policiales, terminaron afectando al entorno (Hernández, 2018). Un ejemplo de esta situación se observa en la utilización de agentes químicos y biológicos que, con el propósito de neutralizar a los miembros de las Fuerzas Militares, ocasionaron un daño irreparable a los territorios amazónicos al traficar con uranio enriquecido y posiblemente con otras armas químicas, causando una importante deforestación en el territorio como advirtieron Torrijos (2009), Sarmiento (2020) o Molina-Orjuela (2022).

Por último, alejándonos de las causas de origen bélico o motivaciones políticas, consideramos que una de las mayores irresponsabilidades de la Historia ha sido el vertido de enormes cantidades de armas químicas en los océanos de todo el mundo a lo largo de los últimos años como consecuencia del desarrollo tecnológico y el abandono o destrucción de dichas armas[15]. Así,

15. Así, la Comisión de Protección del Medio Ambiente del Mar Báltico (organización

en vista del creciente uso del lecho marino para fines económicos (como parques eólicos marinos, cables submarinos y oleoductos), el riesgo de encontrarse con municiones arrojadas al mar está en aumento. Si bien, como señalan Dos Santos, Shem, França, Perera y Correia (2023) no se conocen las ubicaciones exactas, las identidades químicas y las cantidades de armas químicas vertidas, no cabe duda de que la vida marina, en las áreas de vertido, se ha visto afectada al estar expuesta accidentalmente a las armas químicas, lo que ha tenido graves consecuencias para la salud.

En este sentido, a juicio de Domingo y Pita (2013), la CWC cometió un gran error ya que no obliga a los Estados parte a recuperar y destruir los vertidos de armas químicas que fueron arrojados al mar antes de 1985. Esto fue porque hasta la década de los cincuenta, se consideraba como una técnica de destrucción ambientalmente adecuada. No obstante, es importante destacar que solo con la destrucción de las armas químicas no se acaba el problema de la contaminación *per se*, ya que los productos descontaminantes químicos suelen generar subproductos tóxicos, que pueden afectar negativamente al medio ambiente y pueden dañar al usuario, y su descomposición química da como resultado determinados subproductos no deseados que, en caso de llegar a fuentes de agua o al suelo, pueden poner en peligro el medio ambiente.

Estos ejemplos ilustran algunos de los impactos perjudiciales que las armas químicas han tenido en el medio ambiente. Es importante destacar que la lista de efectos negativos es extensa y varía según los tipos de armas químicas utilizadas, la cantidad liberada, la duración de la exposición y la ubicación geográfica. Además, es fundamental tomar medidas para prevenir y mitigar estos efectos, así como para asegurar la destrucción segura de las armas químicas y prevenir su uso en el futuro.

---

internacional intergubernamental que se dedica a la protección y conservación del medio ambiente marino del Mar Báltico establecida en 1974) estima que unas 40 000 toneladas de municiones químicas fueron arrojadas al Mar Báltico después de la Segunda Guerra Mundial. Aún en la actualidad, existe la posibilidad de que las personas se encuentren con armas químicas mientras trabajan en el entorno marino del Mar Báltico meridional y occidental.

7 La neutralización, desactivación e intervención de las armas químicas en España: especial referencia a la Policía Nacional como garantes de la seguridad

Como advierte Llorente (2022), en la lucha contra el terrorismo y la radicalización violenta los Fuerzas y Cuerpos de Seguridad juegan un papel principal para afrontar la amenaza terrorista con materiales nucleares y radiactivos, tal y como ha quedado reflejado en la Estrategia Nacional contra el Terrorismo de 2019.

Como comentan Machín (2014), Herráiz, Berbel, Landáburu, Martínez, Rivero y Val (2021), en España (concretamente en el ámbito de la Policía Nacional)[16] la especialidad TEDAX-NRBQ (Dirección General de la Policía [DGP], 2023) cuyos orígenes se remontan a 1975 y que forma parte de la política de defensa nacional orientada a la prevención de ataques bioterroristas– tiene como misión principal intervenir y actuar ante la presencia y la detección de supuestos artefactos explosivos y todo tipo de agentes NRBQ, así como la recogida, el transporte, análisis e investigación de los mecanismos, elementos y restos de dichos artefactos y de las sustancias o agentes (incluyendo elementos nucleares, radiológicos, biológicos o químicos).

Para el cumplimiento de tal misión, como señala Valverde (2022), sus agentes se despliegan por todo el territorio nacional con grupos distribuidos de forma estratégica (lo que permite dar respuesta a los riesgos de artefactos explosivos y agentes NRBQ de forma rápida y eficaz), realizando, esencialmente, tres tipos de funciones: técnico-operativas, de investigación y desarrollo y, finalmente, de cooperación docente.

Así las funciones técnico-operativas suponen la intervención de los agentes ante la presencia de artefactos explosivos o agentes NRBQ, así como el apoyo técnico en las investigaciones de hechos en los que éstos hayan sido utilizados. Por su parte,

16. Ya que en la Guardia Civil dicha función recae en TEDAX-NRBQ (en el ámbito rural).

las funciones de investigación y desarrollo están destinadas al diseño y actualización de medios materiales de desactivación e intervención de dichas armas lo que implica, necesariamente, una evaluación permanente y un continuo perfeccionamiento de los procedimientos. Finalmente, estos agentes de la policía nacional serán los encargados de la formación, actualización y especialización permanente, así como del intercambio de conocimientos y técnicas utilizadas tanto en el ámbito nacional como internacional.

Para el cumplimiento de estas funciones, estas unidades se sirven de una serie de Protocolos que serán activados en caso de ataque o accidente, o su mera posibilidad, con el objeto de eliminar o reducir la amenaza. En dichos Protocolos se prevé, en primer lugar, establecer una zona de aislamiento y acceso a la zona de riesgo sectorizando la zona, de conformidad con lo estipulado en sus Instrucciones o Circulares de trabajo, en tres áreas: una de máximo riesgo o caliente, una intermedia o templada y una fría. A continuación, se realizará una evaluación inicial de los riesgos y se darán instrucciones a los servicios de emergencia que hayan sido comisionados para, posteriormente, llevar a cabo la comunicación y envío de muestras del incidente a la Unidad de Gestión de la Red de Laboratorios de Alerta Biológica y la descontaminación de las personas que hayan sido expuestas ante dichos agentes o sustancias peligrosas y del lugar.

Por todo ello, la labor de estos técnicos especialistas en desactivación de artefactos explosivos es esencial para el mantenimiento de la seguridad ciudadana en todos aquellos sucesos en los que se vea implicada un arma química o biológica que ponga en peligro la integridad de las personas y del medio ambiente.

8 Conclusiones

Las armas químicas han causado horrores inimaginables en la Historia de la humanidad; su capacidad para generar sufrimiento extremo y un daño irreparable a las personas y al medio ambiente es irreversible. Estos terribles instrumentos de guerra

han dejado un legado de devastación y dolor, recordándonos la urgencia de su prohibición y eliminación definitiva. Ello se va consiguiendo paulatinamente gracias a instrumentos como la CWC (que ha posibilitado que cada vez haya menos armas químicas en el mundo).

Sin embargo, es importante destacar que, pese a que la CWC ha logrado avances significativos en la prohibición y eliminación de armas químicas, no está exenta de críticas y, por ello, han de exigirse mejoras potenciales para fortalecer aún más su implementación, efectividad y combatir los desafíos que acechan actualmente a nuestra sociedad como consecuencia del desarrollo tecnológico y el uso de armas cada vez más invasivas y dañinas para el medioambiente.

Una de las críticas más comunes es que la verificación efectiva y exhaustiva de las actividades declaradas puede ser un desafío logístico y técnico y, a pesar de que muchas veces se cuenta con la buena voluntad de los Estados Parte, el Tratado dispone de pocos recursos para vigilar su cumplimiento. En consecuencia, el ordenamiento previsto, además de no estar actualizado a los avances de la tecnología, carece de un verdadero instrumento sancionador que motive a los Estado firmantes para abordar con firmeza el problema. Al mismo tiempo, como hemos venido diciendo, la CWC únicamente es de aplicación para los Estados Parte, dejando al margen de regulación, y, especialmente, sanciones, a países como Corea del Norte cuya carrera armamentística supone una grave amenaza para la vida y para los ecosistemas terrestres y marinos.

Otra de las críticas más notables es, con el avance de la Ciencia y la tecnología, la posibilidad de que se desarrollen nuevas sustancias químicas y métodos de producción de armas químicas que no estén específicamente incluidos en las listas del CWC (como sucedió con el *novichok*). Esto plantea desafíos para mantener actualizado el Convenio y asegurar que abarque todas las posibles amenazas emergentes. Sin embargo, pese a que sea una crítica adecuada lo cierto es que el desarrollo tecnológico siempre irá un paso por delante del legislador. Como consecuencia de lo antedicho, la única solución a esta situación no es otra que

agilizar los procedimientos para que la actualización de los catálogos no se dilate en el tiempo en exceso.

Al mismo tiempo, preocupa el uso de armas químicas en conflictos armados al suponer una violación flagrante del CWC. Sin embargo, su aplicación y cumplimiento efectivo en situaciones de conflicto puede ser difícil debido a las circunstancias operativas y la falta de acceso a las zonas afectadas (en suma, cuando la mayoría de los Estados en los que existe un conflicto armado quedan al margen de la CWC).

Otro punto importante y que, lamentablemente, no ha sido tratado con esmero por la Comunidad Internacional es el vertido de dichas armas al mar, planteando importantes desafíos en términos de impacto ambiental, riesgos para la salud y dificultades técnicas. Ello es consecuencia de que la identificación precisa y la recuperación de las armas químicas sumergidas en el mar puede ser extremadamente difícil debido a la falta de información precisa sobre su ubicación y estado. Pero no cabe duda alguna de que la presencia de armas químicas en el mar plantea un riesgo para la salud humana, especialmente para las comunidades costeras, las personas que dependen de los recursos marinos y los humanos que los consumen. Además de la contaminación de los espacios marinos (la más común), no se ha de olvidar los efectos nocivos sobre la superficie terrestre, como la deforestación, la pérdida de fertilidad en el suelo y la extinción de especies y sus entornos.

Por otro lado, el desarrollo tecnológico también nos ofrece esperanzas, ya que las últimas tecnologías plantean el uso de enzimas para la destrucción de armas químicas, pudiendo producirse a gran escala (lo que permite una mayor disponibilidad y aplicabilidad en diferentes situaciones). Estas tecnologías presentan ventajas significativas, como ofrecer un método más específico y eficiente para descomponer y desactivar los agentes químicos reduciendo el riesgo de contaminación y minimizando el impacto en el medio ambiente (facilitando al mismo tiempo el proceso de descontaminación y evitando daños innecesarios). De modo que, a medida que se continúa investigando y desarrollando enzimas específicas para diferentes agentes químicos, el uso de enzimas se perfila como una opción prometedora y efectiva para la descontaminación y elimina-

ción segura de armas químicas, vislumbrándose en el horizonte un futuro sin presencia de estas armas. Por todo ello, los Estados Parte deberían promocionar e invertir en estos procesos de descontaminación para conseguir así remediar los daños ocasionados como consecuencia de la creación de armas químicas y sus componentes.

Cabe destacar que en España la misión de neutralizar estas armas recae en las Fuerzas y Cuerpos de Seguridad (especialmente en los miembros de la Policía Nacional y la Guardia Civil) y en las Fuerzas Armadas que, encargadas de mantener la seguridad en el territorio nacional frente a estas amenazas, han propiciado un notable incremento en el desarrollo tecnológico para reducir los efectos adversos que desencadenan la utilización de estas armas.

Por último y para concluir, se hace necesario, en los tiempos cambiantes en los que nos encontramos con varios conflictos bélicos activos en pleno año 2024, hacer una especial referencia a la insustituible labor que los miembros de las Fuerzas y Cuerpos de Seguridad del Estado realizan en España y en otras partes del mundo para garantizar la seguridad y la libertad de los ciudadanos.

Más concretamente centraremos esta parte de las conclusiones en enfatizar la actividad de la Policía Nacional, al ser el cuerpo policial competente, según la Ley Orgánica 2/1986, de Fuerzas y Cuerpos de Seguridad, en las zonas urbanas que más población concentran en España. Los miembros de las instituciones policiales y también la sociedad, han venido haciendo frente a distintas amenazas cometidas a través de métodos comunes como las armas de fuego y los explosivos. Sin embargo, al igual que avanza la sociedad, avanzan los medios de ataque, motivo por el cual se precisa, cada vez más, una policía formada y actualizada con los distintos modos de delincuencia. La Policía Nacional, a través de la creación de la especialidad NRBQ (Nuclear, Radiológico, Biológico y Químico), se ha anticipado a las nuevas formas de delincuencia y modos de terrorismo, buscando de esta forma la especialización para combatir, de manera eficaz y eficiente, el ataque a través de las armas que se han venido describiendo durante la presente investigación.

Además, la Dirección General de la Policía también cuenta con la Unidad de Subsuelo y Protección Ambiental, dependiente de la

Comisaría General de Seguridad Ciudadana, teniendo entre sus misiones la inspección y control de vertidos industriales en medio urbano, elemento necesario y fundamental contra los ataques que podrían llevarse a cabo mediante el uso de este tipo de armas.

De esta forma, no debe caerse en el error de pensar que la incidencia que las armas químicas pueden tener sobre la vida o el medio ambiente es un problema de carácter militar, pues son las unidades que se encuentran en los núcleos urbanos quienes se encargan de neutralizar, en primera instancia, la amenaza o, en su caso, paliar los daños.

Glosario

CWC: Convención sobre armas químicas de 1993.

DGP: Dirección General de la Policía.

FARC: Fuerzas Armadas Revolucionarias de Colombia.

NRBQ: Nuclear, radiológica, biológica y química.

OPWC: Organización para la prohibición de las armas químicas.

TEDAX: Técnico especialista en desactivación de artefactos explosivos.

Referencias

Barberis, M. B. (2017). Los veinte años desde la creación de la Organización para la Prohibición de Armas Químicas. *Afese*, *65*.

Barletta, A. F. (2020). Armas de destrucción masiva-armas químicas: una vieja amenaza que no pierde vigencia. *Boletín Científico Tecnológico*, *24*(1), 55-72.

Bernachi, A. (2022). Armas químicas y el marco internacional. En Universidad de la Defensa Nacional (Ed.), *Desarme y no proliferación: un enfoque multidisciplinario* (pp. 11-27). UNDEF Libros.

Camacho, L. H. (2020). Nacimiento de la quimioterapia. *Medicina*, *42*(4), 599-601. https://doi.org/10.56050/01205498.1562

Cánovas Sánchez, B. (2013). Siria, otra vez a vueltas con las armas químicas. *Instituto Español de Estudios Estratégicos*, *46*, 1-13.

Cervell Hortal, M. J. (2003). La Supervivencia de la Convención Sobre Armas Químicas. *REDI*, *55*, 849. https://doi.org/10.15581/010.33.169-203

Cervell Hortal, M. J (2017). El ataque de Estados Unidos contra Siria por el empleo de armas químicas: ¿acto 'contra regem' o contramedida por violación del 'ius cogens'? *Anuario Español de Derecho Internacional*, *33*, 169-203.

Chauhan, S., D'Cruz, R., Faruqi, S., Singh, K. K., Varma, S., Singh, M. y Karthik, V. (2008). Chemical warfare agents. *Environmental Toxicology and Pharmacology, 26*(2), 113-122. https://doi.org/10.1016/j.etap.2008.03.003

Costanzi, S. y Koblentz, G. D. (2020). Updating the CWC. *Arms Control Today*, *50*(3), 16-20.

De Fortuny, T. (2015). *Convención sobre armas químicas. Diccionario de la guerra, la paz y el desarme.* Icaria.

De Salazar Serantes, G. (2013). La III Conferencia de examen de la Convención para la prohibición de las armas químicas: búsqueda del equilibrio entre desarme, no proliferación y cooperación internacional. *Pre-bie3*, *3*, 27.

Dirección General de la Policía. (1 de diciembre de 2023). *TEDAX-NRBQ*. https://www.policia.es/_es/tupolicia_conocenos_estructura_dao_cginformacion_especialidades_tedax.php

Domingo, J. y Pita, R. P. (2013). La destrucción según la convención de armas químicas y su aplicación en Siria. *Pre-bie3*, *6*, 21.

Domingo, J. y Pita, R. P. (2014). El cloro como arma: De la primera guerra mundial al conflicto sirio. *Pre-bie3*, *3*, 31.

Dos Santos, M. C., Shem, P. M., França, T. C. C., Perera, R. P. y Correia, V. B. (2023). Assessment of the impact of chemical weapons disposal in the ocean according to international conventions. En *Sensing of Deadly Toxic Chemical Warfare Agents, Nerve Agent Simulants, and their Toxicological Aspects* (pp. 407-422). Elsevier. https://doi.org/10.1016/B978-0-323-90553-4.00018-4

García Vázquez, B. (2019). La ambigüedad del concepto de algunas armas incapacitantes menos letales en la Ley Nacional sobre el uso de la fuerza. *Revista de la Facultad de Derecho de México*, *69*(275-1), 596-600. https://doi.org/10.22201/fder.24488933e.2019.275-1.71840

Gómez Sainz de Aja, N. (2016). La actividad de la Autoridad Nacional Española en el marco de la Convención para la Prohibición de las Armas Químicas. *Anales de Química de la RSEQ*, *112*(4), 225-230.

González-Hernández, I. J. (2021). El desarrollo tecnológico en las revoluciones industriales. *Ingenio y Conciencia. Boletín Científico de la Escuela Superior Ciudad Sahagún*, *8*(16), 41-52. https://doi.org/10.29057/escs.v8i16.7118

Hernández, O. (16 de febrero de 2023). Armas químicas en Ucrania: ¿por qué el Kremlin necesita que te creas este mensaje? *El Confidencial*. https://www.elconfidencial.com/mundo/2023-02-16/armas-quimicas-la-mosca-rusa-detras-de-la-oreja-de-ucrania-zumba-otra-vez-su-propaganda_3573039/

Hernández Méndez, J. A. (2018). Amenazas nucleares, biológicas y químicas, una estrategia de manejo. *Revista Científica General José María Córdova*, *16*(21), 17-31. https://doi.org/10.21830/19006586.299

Herráiz España, J., Berbel Bueno, C., Landáburu Jiménez, E., Martínez Ruiz, M., Rivero Segalàs, M. T. y Val Vidal, J. C. (2021). Bioseguridad y defensa. ¿El nuevo reto global? *IEEE*, *21*, 899-925.

Jiménez Gómez, S. (2005). Agresivos químicos. *Monografías de la Real Academia de Farmacia. Monografía* 26.

LeJeune, K. E. (1998). *Employing enzymes in the detoxification of nerve agent chemical weapons* (Doctoral dissertation, Carnegie Mellon University).

Llorente Aguilera, C. (2022). La Estrategia de Seguridad Nacional de España 2021 y el terrorismo nuclear. *Revista del Instituto Español de Estudios Estratégicos*, *19*, 197-244.

Locatelli, O. A. (2014). La destrucción de las armas químicas en Siria. *Visión conjunta*, *11*, 18-25.

Machín, N. (2014). Las armas biológicas. Perspectivas de futuro. *UNISCI Discussion Papers*, *35*, 205-221. https://doi.org/10.5209/rev_UNIS.2014.n35.46428

Manrique, J. M. (2002). La Fabricación y uso de Gases de Guerra en España. *Revista Defensa*, *296*, 63-68.

Mayor, A. (2020). *Fuego griego, flechas envenenadas y escorpiones: Guerra química y bacteriológica en la Antigüedad*. Desperta Ferro Ediciones.

Mazo, A. F. (2023). La protección de los animales como integrantes del medio ambiente en el derecho de los conflictos armados. *Actualidad Jurídica Ambiental*, *132*, 64-108.

Molina-Orjuela, D. E. (2022). Impactos del conflicto armado colombiano sobre el medio ambiente y acciones para su efectiva reparación. *Revista Científica General José María Córdova*, *20*(40), 1087-1103. https://doi.org/10.5209/rev_UNIS.2014.n35.46428

Muñoz-Canales, V. y Rodríguez-López, J. (2021). Armas químicas: descripción general de tipos, riesgos y tratamientos. *Revista de Química*, *35*(2), 4-18. Recuperado a partir de https://revistas.pucp.edu.pe/index.php/quimica/article/view/23527

Otero Solana, V. (2022). El arma química, el arma de destrucción masiva más versátil y aterradora. *Revista Española de Derecho Militar*, *118*, 55-114.

Peláez, D. A. (2020). La estrategia del expansionismo hegemónico iraní en Siria y Afganistán. *Revista Científica General José María Córdova*, *18*(32), 749-767. https://doi.org/10.21830/19006586.639

Pita, R. P. (2008). *Armas químicas: la ciencia en manos del mal*. Plaza y Valdés, S. L. https://doi.org/10.5211/9788496780606

Pita, R. P. (2011). Proliferación de armas químicas. *Cuadernos de Estrategia*, *153*, 81-86.

Pons, J. A. M. (2006). Armas químicas: qué son y cómo actúan. *Anales de Química de la RSEQ*, *1*, 55-64.

Popiel, S. y Nawała, J. (2013). Detoxification of sulfur mustard by enzyme-catalyzed oxidation using chloroperoxidase. *Enzyme and Microbial Technology*, *53*(5), 295-301. https://doi.org/10.1016/j.enzmictec.2013.06.002

Prokop, Z., Opluštil, F., DeFrank, J. y Damborský, J. (2006). Enzymes fight chemical weapons. *Biotechnology Journal: Healthcare Nutrition Technology*, *1*(12), 1370-1380. https://doi.org/10.1002/biot.200600166

Pulido Gragera, J. (2003). Agentes químicos y biológicos versus capacidad nuclear. La otra punta de lanza de Corea del Norte. *UNISCI Discussion Papers*, *2*, 1-8.

Quinto, J. O. (1999). NTP 512: Plaguicidas organofosforados (I): aspectos generales y toxicocinética. *Centro Nacional de Condiciones de Trabajo*, *1*(7).

Riba, P. M (2005). La aplicación de la Convención sobre las Armas Químicas. *Revista Mexicana de Política Exterior*, *75*, 55-70.

Sarmiento, E. (2020). Incidencia del proceso de paz con las FARC en la política antidrogas de Colombia. *Revista Científica*

General José María Córdova, *18*(32), 817-837. https://doi.org/10.21830/19006586.632

Schecter, W. P. y Fry, D. E. (2005). The surgeon and acts of civilian terrorism: chemical agents. *Journal of the American College of Surgeons, 200*(1), 128-135. https://doi.org/10.1016/j.jamcollsurg.2004.09.002

Shua, A. M. (2019). *La guerra*. Editorial Páginas de Espuma.

Spanevello, R. y Suárez, A. (2011). Los pecados de la química. En *Química y civilización* (pp. 303-310). Argentina: Asociación Química Argentina.

Torrijos, V. (2009). Los argumentos para alejarse de la paz en Colombia: ideas para alejarse de la guerra. En Torrijos, V. (Dir.), *Asuntos estratégicos, seguridad y defensa* (pp. 59-65). Universidad del Rosario.

Trigo Alonso, A. M. (2023). Ciencia perdida. *Revista Digital de Acta, 143*.

Uesugi, T. (2019). Aproximación dialógica a los desastres tóxicos: El Agente Naranja en el valle A Luoi (Vietnam). *AIBR: Revista de Antropología Iberoamericana, 14*(1), 40-41. https://doi.org/10.11156/aibr.v14i1.70845

Valverde Ogallar, R. (2022). Seguridad nacional frente a la amenaza/riesgo biológico. *Cuadernos de Estrategia, 217*, 281-314.

Velasco, M. J. S. (2014). Descubrimiento y destrucción humana: armas químicas, el agente nervioso Sarín. *MoleQla: Revista de Ciencias de la Universidad Pablo de Olavide, 14*(5-3).

Zúñiga, R. C. (2015). El uso de armas químicas en Siria, un desafío para el derecho internacional. *Anuario Colombiano de Derecho Internacional, 8*, 17-40. https://doi.org/10.12804/acdi8.1.2015.01

MISCELÁNEA

Explorando las huellas digitales de los criptoactivos mediante fuentes abiertas

Exploring Cryptoasset Fingerprinting through Open Sourcing

Ana Díaz Bernardos[1]
Policía Nacional.
ana.diaz.bernardos@gmail.com

DOI: https://doi.org/10.14201/cp.31816
Recibido: 21-02-23 | Aceptado: 10-04-24

Resumen

El uso de los criptoactivos ha experimentado un notorio aumento en los últimos años, introduciendo consigo una serie de conceptos novedosos en la economía española. Este fenómeno ha permitido a los usuarios operar de nuevas formas, lo que entraña una serie de ventajas y riesgos inherentes que deberían conocer. Las ventajas asociadas a estos activos financieros han supuesto un reclamo que ha hecho que cada vez más individuos hagan uso de los mismos. Esta atracción se ha traducido en una mayor presencia de los criptoactivos en las investigaciones policiales, utilizados como medio de pago, promocionados como inversiones con rendimientos rápidos e incluso utilizados en operativas de blanqueo de capitales procedentes de todo tipo de delitos. La versatilidad en su utilización y su cada vez más marcada presencia en la sociedad plantea desafíos significativos para las autoridades, que deben, sin limitar las oportunidades legítimas que los criptoactivos pueden ofrecer, adaptar su legislación para salvaguardar a la población frente a los posibles riesgos asociados a los criptoactivos y fomentar su uso responsable y seguro. En este sentido, las Fuerzas y Cuerpos de Seguridad están en la obligación de proteger a los ciudadanos en este nuevo ámbito virtual que se presenta.

---

1. Graduada en Derecho y máster en Justicia Criminal. Policía investigadora en la Brigada Central de Delincuencia Económica y Fiscal, de la Unidad Central de Delincuencia Económica y Fiscal, Comisaría General de Policía Judicial de la Policía Nacional.

Palabras clave
Criptoactivos; Trazabilidad; Blockchain; Bitcoin; Cluster; Ethereum; Token; Herramientas; Billetera; Exchange.

Abstract
The use of cryptoassets has experienced a notable increase in recent years, introducing a series of new concepts into the Spanish economy. This phenomenon has allowed users to operate in new ways, which comes with a number of inherent advantages and risks that they should be aware of. The advantages associated with these financial assets have created a demand that has caused more and more individuals to make use of them. This attraction has translated into a greater presence of cryptoassets in police investigations as they are increasingly used as a means of payment, promoted as investments with quick returns and even used in money laundering operations from all types of crimes. The versatility in their use and their increasingly marked presence in society poses significant challenges for authorities, who must, without limiting the legitimate opportunities that cryptoassets can offer, adapt their legislation to safeguard the population against the possible associated risks and promote their responsible and safe use. In this sense, the Security Forces are obliged to protect citizens in this new virtual environment presented to us.

Keywords
Cryptoassets; Traceability; Blockchain; Bitcoin; Cluster; Ethereum; Token; Tools; Wallet; Exchange.

1 Interés por los criptoactivos

La Comisión Nacional del Mercado de Valores (CNMV), organismo nacional competente para la supervisión de los mercados, afirmó en el año 2021 que «los criptoactivos, incluyendo las criptomonedas y la tecnología que les da soporte, pueden ser elementos que dinamicen y modernicen el sistema financiero en los próximos años» (Comunicado conjunto de la CNMV y

del Banco de España sobre el riesgo de las criptomonedas como inversión, 2021, p. 1). Finalizando el año 2023, podríamos afirmar que es una realidad que estos elementos están en vías de hacerlo.

Si esto sucede es fundamental dotar a los ciudadanos de información válida y veraz sobre las ventajas y los riesgos que presenta operar con ellos, así como dotar a las Fuerzas y Cuerpos de Seguridad de los conocimientos necesarios para enfrentarse al uso indebido que los delincuentes puedan hacer de los mismos. En este sentido, el presente artículo pretende aportar ciertos conocimientos básicos al lector que le permitan dar respuesta a la realidad actual e intentar eliminar, o al menos disipar, la creencia de que la operativa con criptoactivos llevada a cabo por los delincuentes es demasiado compleja para enfrentarla.

Han sido varias instituciones, y no solo nacionales, las que han advertido desde hace algunos años de los riesgos de operar con criptoactivos, hecho que se ha visto incentivado por el interés, cada vez más creciente, de la sociedad mundial por estos activos financieros. Son dos los motivos principales que convierten a los criptoactivos en un producto de alto riesgo para el inversor minorista y que coinciden en destacar muchas de las entidades e instituciones financieras: su extrema volatilidad y la complejidad para el inversor minorista.

En este sentido, las autoridades europeas supervisoras (ESA), entre las que se encuentra la Autoridad Europea de Valores y Mercados (ESMA), advierten a los inversores minoristas de que muchos criptoactivos no son adecuados como inversión ni medio de pago o intercambio, ya que revisten un marcado carácter especulativo. Así mismo, les instan a preguntarse si podrían permitirse perder todo el dinero invertido, asumir un alto riesgo debido al alta volatilidad de estos activos, si han consultado si los bróker o empresas con las que operan están advertidas por los organismos nacionales competentes para ello o si disponen de medidas adecuadas para proteger los dispositivos que utilizan para operar con criptoactivos, ya que todos ellos son riesgos específicos asociados a estos activos financieros.

En el caso de España, el organismo nacional competente para la supervisión de los mercados es la CNMV; en el año 2018 informó en un comunicado conjunto con el Banco de España de los riesgos asociados a estos activos de la siguiente manera:

> La CNMV y el Banco de España tienen entre sus prioridades ofrecer información al público para que los inversores y usuarios de servicios financieros estén en condiciones de afrontar con confianza la creciente complejidad del entorno financiero. En consecuencia, ambas autoridades creen oportuno publicar este comunicado, dirigido a inversores y en general a usuarios financieros minoristas. Es esencial que quien decida comprar este tipo de activos digitales o invertir en productos relacionados con ellos considere todos los riesgos asociados y valore si tiene la información suficiente para entender lo que se le está ofreciendo. En este tipo de inversiones existe un alto riesgo de pérdida o fraude. (Comunicado conjunto de la CNMV y del Banco de España sobre «criptomonedas» y «de ofertas iniciales de criptomonedas» [ICO], 2018, pp. 2 y 3)

Aunque los criptoactivos llevan más de una década en el panorama mundial, fue en el año 2021 cuando varios criptoactivos, principalmente el *bitcoin* y el e*ther*, experimentaron una elevada volatilidad en sus precios, lo que llevó a que aumentase de manera muy significativa su publicidad, encaminada a atraer inversores, lo que impulsó a más personas a operar con ellos. Como consecuencia ha llevado aparejado un aumento de los delitos relacionados con las inversiones en criptoactivos, también favorecido por la escasa cultura de inversión.

Este hecho habría sido uno de los motivos que ha generado la necesidad de muchos países de ponerse al día en materia de criptoactivos, colocándolos en una posición preferente en la agenda normativa de esos. En España, en el año 2022, la institución supervisora de los mercados dispuso la Circular 1/2022, de 10 de enero, de la Comisión Nacional del Mercado de Valores, relativa a la publicidad sobre criptoactivos presentados

como objeto de inversión, que tiene por objeto desarrollar las normas, principios y criterios a los que debe estar sujeta la actividad publicitaria de los criptoactivos. Además, en su informe anual publicado recientemente, informó que, en aplicación de esta cCircular, gestionó más de cien expedientes informativos y analizó casi mil piezas publicitarias.

Más recientemente, y en el mismo sentido, la Unión Europea ha aprobado el Reglamento de Mercados de Criptoactivos (MICA) [Reglamento (UE) 2023/1114 del Parlamento Europeo y del Consejo, de 31 de mayo de 2023, relativo a los mercados de criptoactivos], que se ha convertido en el primer instrumento regulador de estos activos, pero que no será de aplicación hasta el 30 de diciembre de 2024, como dice su artículo 149. Esta norma ha dado cobertura jurídica a los criptoactivos y establecido unas reglas comunes a todos los operadores en la Unión Europea, pero por el momento ha dejado fuera de esta cobertura a los llamados NFT (*tokens* no fungibles) y las DeFi (operadores descentralizados).

Para dar por finalizado este apartado, que, entre los riesgos descritos y la carrera de las instituciones financieras por dotar de un marco jurídico y de protección al inversor de criptoactivos, puede generar en el lector una alarma social que quedaría bastante lejos de la realidad. Cabe decir que la tecnología *Blockchain* y los criptoactivos no tienen por qué constituir un problema para la sociedad española ni mundial. Estos elementos tienen el potencial de optimizar las transacciones que todo ciudadano realiza regularmente, otorgándoles mayor transparencia y seguridad al estar respaldadas por una base de datos compartida y descentralizada.

Así, adquirir conocimientos sobre trazabilidad resulta de gran utilidad no solo desde la perspectiva policial, sino también como ciudadano inmerso en una sociedad donde la tecnología *Blockchain* y los criptoactivos ganan cada vez más terreno. De esta manera, las Fuerzas y Cuerpos de Seguridad pueden rastrear fondos fraudulentos y localizar a los criminales que abusan de estos elementos y, al mismo tiempo, los ciudadanos pueden verificar el estado de sus transacciones mediante esta tecnología, que ha llegado para quedarse.

2 Aproximación conceptual

Los siguientes conceptos tienen como objetivo proporcionar al lector las capacidades básicas para comprender la operativa con criptoactivos. Estos conceptos esenciales se presentan de manera sucinta, ya que la intención del presente artículo no es formar expertos en inversión de criptoactivos, sino brindar al lector de unas nociones básicas e introducirlo en este interesante mundo digital.

2.1 ¿Qué es una criptomoneda?

Las criptomonedas son monedas virtuales, intercambiables y descentralizadas, basadas en la criptografía, lo que les permite garantizar su titularidad y asegurar la integridad de las transacciones.

No existen de forma física y tampoco están identificadas físicamente con una cifra o código, queda constatada su existencia a través de un registro de transacciones, contenido dentro de la llamada cadena de bloqueos o *blockchain*.

En la actualidad existen multitud de criptomonedas; las más populares son *bitcoin* y *ether*.

2.2 ¿Qué es un *token*?

Al igual que las criptomonedas, los *tokens* son activos digitales criptográficos, que pueden ser creados por cualquier usuario privado, intercambiados y también funcionan usando la tecnología *Blockchain*.

Los *tokens* necesitan una *blockchain* y una criptomoneda que permita su desarrollo, es decir, los *tokens* no tienen su propia *blockchain* o cadena de bloques, sino que circulan por aquellas que permitan su registro; también necesitan un contrato que los defina.

2.3 ¿Qué es la *blockchain* o cadena de bloques?

La *blockchain* o cadena de bloques es un tipo de base de datos descentralizada, en la que los datos se registran, comparten y sincronizan a través de una red distribuida de ordenadores llamados nodos. Estos nodos interactúan entre sí, sin necesidad de un servidor central, lo que permite el mantenimiento de la *blockchain* sin necesidad de intermediación de terceros.

Existen diferentes tipos de *blockchain* o cadenas de bloques:

- Pública: son aquellas que son accesibles desde Internet. Un ejemplo serían la *Blockchain* de *Bitcoin*, *Ethereum* o *Tron*.

  El funcionamiento de esta red es abierto, esto significa que todos los datos registrados en la *blockchain* pública están disponibles y cualquier usuario puede revisarlos.

- Privada o permisionada: con la evolución de la tecnología *blockchain* se crearon las redes privadas o permisionadas, cuya principal diferencia con las públicas es que las *blockchain* privadas o permisionadas dependen de un servidor central que controla todas las acciones y no son accesibles a todas las personas.

2.4 ¿Qué es un monedero de criptoactivos, billetera o *wallet*?

Un monedero de criptoactivos, también llamado billetera o *wallet* en inglés, es una herramienta que permite al usuario almacenar las claves públicas y privadas, que son las que controlan el acceso a sus criptoactivos y le permiten enviar y recibir pagos.

Es importante señalar que los monederos o *wallet* no contienen criptoactivos. Los monederos lo que contienen son las claves privadas que permiten al usuario operar con sus activos y que están asociadas a la clave pública correspondiente y esta a la dirección.

Para una mejor comprensión se explican los siguientes conceptos:

- Clave privada: es una clave de dominio privado, a la que solo debe tener acceso el propietario de los criptoactivos. La clave privada le va a otorgar la propiedad al usuario y el acceso a sus activos. Funciona como un pin o una contraseña.

- Clave pública: asegura la propiedad de la dirección, que no del monedero, y se puede compartir sin riesgo a que accedan a los fondos del usuario. Esta se deriva de la clave privada y sirve para verificar la autenticidad de las transacciones.

- Dirección o *address* en inglés: es un código compuesto por números y letras, que presentará un formato según el criptoactivo con el que se opere, por lo que no es posible enviar *ether* (ETH) a una dirección *bitcoin* (BTC) y viceversa.

  La dirección indica el origen o destino de un pago del criptoactivo en el que se esté operando y es el código visible en la *blockchain*.

  Desde un monedero se pueden crear varias direcciones a las que enviar y recibir fondos.

  Si el usuario opera con el criptoactivo *bitcoin* (BTC) las direcciones presentarían el siguiente formato comenzando por bc1, 1 o 3. Los siguientes ejemplos se han obtenido aleatoriamente de fuentes abiertas; ejemplos:

  - bc1qc026d7ght3cdjd0ugwvc23mfqsag0q2hvw0l3x
  - 1AdFdaGhGmNQiobrvdnKHPyN9yMuGgfHiF
  - 3EuMyVyv9M1yShgsUscPqT6MZmFZiFN2LGQ

  Si opera con la criptomoneda *ether* (ETH) o los *tokens* que operan en la Red *Ethereum*, el inicio de las direcciones sería siempre 0x, por ejemplo:

  - 0xAe6aEEbfC0E060F992010D596F4A7276f182D444

Si lo hace con la criptomoneda *tron* (TRX) se vería así:

- TYnNCewqZXmsVB6t8NMtYdGYtC38Sc250N

Y así, según el criptoactivo con el que se opere.

- Frase semilla o *seed* en inglés: en la actualidad muchos monederos de criptoactivos derivan sus claves de una única, conocida como frase semilla o *seed*. El propietario de la frase semilla puede reconstruir las claves privadas, desde las que se derivan las claves públicas y de estas las direcciones, y así disponer de los fondos.

  La frase semilla está formada por una lista de palabras en inglés, de 12 a 36 palabras en inglés, que incluye toda la información necesaria para recuperar un monedero o *wallet* de criptoactivos.

2.5 Formas de depósito de los criptoactivos

Pueden ser un dispositivo físico de *hardware*, un programa informático o un servicio que alberga las claves. La principal diferencia es la forma de custodiar la clave privada del monedero de criptoactivos.

- *Exchanges*: las claves privadas están en manos de un tercero que es una institución financiera o una plataforma de intercambio de criptoactivos llamada *exchange*. Las exchanges no son monederos, sino que el usuario posee una cuenta que les brinda una descripción general de sus transacciones y tiene la capacidad para recibir y enviar fondos. Algunos ejemplos de Exchange son *Kraken*, *Binance*, *Coinbase* o *Huobi*.

- Monederos con custodia: al igual que ocurre con las exchanges, en los monederos con custodia también la clave privada está en manos de un tercero. Algunos ejemplos son los llamados monederos *online* o en línea que serían calificados como monederos calientes o *hot wallet* porque están conectados a Internet, y que son páginas web que se asimilan al banco online. Por ejemplo, *Xapo, Bitpay* o *Blockchain.com*.

- Monedero sin custodia o con custodia propia: permite a los usuarios conservar y utilizar sus criptoactivos ya que son ellos mismos quienes custodian sus claves privadas. Algunos ejemplos serían:

    - Los monederos fríos: son monederos que no están conectados a Internet. Son los monederos de papel, en el que el propietario escribe sus claves privadas en un papel y las custodia. El principal problema de este tipo de monederos es que, si se pierde el apunte, el propietario perdería el acceso y el control de sus criptoactivos.

    - Los monederos mixtos: son los monederos *hardware* como *Trezor, Ledger* o *Keepkey*, entre otros; estos dispositivos físicos albergan las claves del monedero del usuario, pero es este quien custodia el dispositivo. Hablamos de monederos mixtos y no fríos porque para realizar una transacción es necesario conectarlos a Internet.

    - Los monederos calientes o *hot wallet*: son aquellos que están conectados a Internet de manera continua. Por ejemplo, *Electrum, Jaxx, Bitcoin Core* o *Atomic*, que son aplicaciones que el usuario instala en su dispositivo móvil, *tablet* u ordenador y puede operar con sus criptoactivos a través de ellos.

2.6 ¿Qué es una transacción de criptoactivos?

Una transacción es la transferencia de fondos entre usuarios en el ecosistema de los criptoactivos, que queda registrado en la cadena de bloques o *blockchain*.

Una transacción incluye:

- La identificación (*ID*) de la transacción o *hash*, como se puede observar en la Figura 1.

Figura 1: Identificación de la transacción o *hash*, término informático que se refiere a la huella digital. El *hash* permite verificar el contenido de una transacción.

Nota. Recorte aleatorio de un *hash* tomando del buscador público *Blockchair* (*Blockchair* 2023).

- El número de criptoactivos enviados; un ejemplo sería el recogido en la Figura 2.

Figura 2: Cantidad de criptoactivos enviados y su equivalencia en dólares.

Nota. Recorte aleatorio del valor de los activos enviados del buscador público *Etherscan* (*Etherscan*, 2023a).

- La comisión pagada por la transacción (*fee* en inglés), como se observa en la Figura 3.

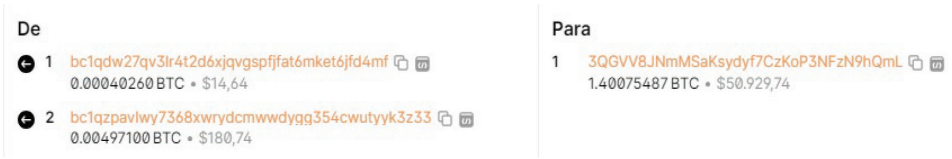
Figura 3: Comisión o *fee* cobrado por la transacción operada.

Nota. Recorte aleatorio de la comisión de la transacción del buscador público *Etherscan* (*Etherscan*, 2023a).

- Entradas o dirección de remitente.

  En el caso de las transacciones operadas con *Bitcoin* puede haber más de una entrada o dirección de remitente, como se observa en la Figura 4.

Figura 4: Direcciones de *Bitcoin* que indican el origen (las que se encuentran a la derecha de la imagen) y destino (las que se encuentran a la izquierda de la imagen) de un pago de *bitcoin*, y son el código visible en la *blockchain*.



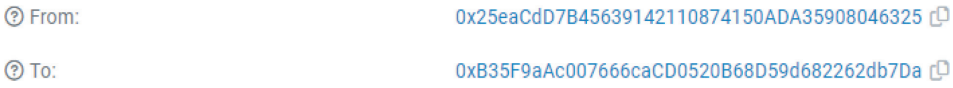
Nota. Recorte aleatorio de una transacción del buscador público *Blockchain Explorer* (*Blockchain Explorer*, 2023).

Esto se debe a que la cantidad de fondos no es suficiente para enviar el pago o a que el remitente ha decidido usar varias

direcciones para enviar el pago. Se explica más detenidamente en el apartado de trazabilidad de *Bitcoin*.

En las transacciones operadas en la Red *Ethereum* solo figura una dirección de entrada o de remitente por transacción *(From)*, como se observa en la Figura 5:

Figura 5: Dirección remitente y dirección de destino de la transacción.



Nota. Recorte aleatorio de una transacción tomado del buscador público *Etherscan* (*Etherscan*, 2023a).

- Salidas o dirección del destinatario.

  En el caso de las transacciones operadas con *Bitcoin* puede haber más de una salida o dirección de destinatario, como se puede observar en la Figura 6.

Figura 6: Direcciones de *Bitcoin*.

Nota. Recorte aleatorio de una transacción del buscador *Blockchain Explorer* (*Blockchain Explorer*, 2023).

Podría tratarse de dos envíos o pagos, o que una salida se correspondiese al pago y otra al cambio (sobrante).

Bitcoin utiliza una tercera dirección llamada dirección de cambio, que se genera porque no se envía la cantidad exacta de *bitcoin* al destinatario, dando lugar a un sobrante que se envía a la dirección de cambio, que también pertenece al remitente. Se explica detenidamente más adelante.

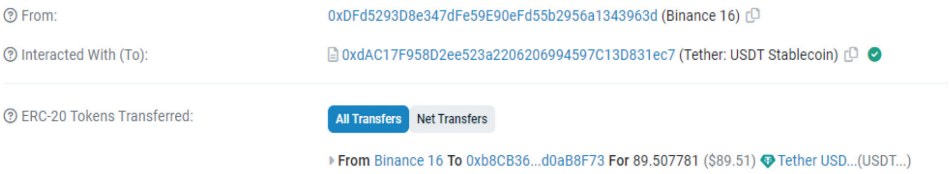
En las transacciones operadas en la Red *Ethereum* solo hay una dirección de salida o de destinatario *(To)* por transacción, como se observa en la Figura 7.

Figura 7: Dirección remitente y dirección de destino de la transacción.

Nota. Recorte aleatorio de una transacción tomado del buscador público *Etherscan* (*Etherscan*, 2023a).

Caso especial es cuando las transacciones se realizan con el activo *tether* (USDT) ya que va a figurar la dirección del contrato o *smart contract* de *Tether* (*tether:* USDT *Stablecoin*). En este caso la dirección de destino es la que se contiene en el apartado *ERC-20 Tokens Transferred*, señalada en la Figura 8.

Figura 8: Transacción operada en la Red *Ethereum* con el activo *tether* (USDT).



Nota. Recorte aleatorio de una transacción con USDT tomado del buscador público *Etherscan* (*Etherscan*, 2023b).

3 Trazabilidad por fuentes abiertas

A continuación, se presentan algunas herramientas de código abierto que permiten al usuario rastrear criptoactivos, junto con algunos trucos que facilitarán esta tarea. Además, se explican qué son los *exchanges*, elementos importantes para obtener información.

3.1 Propuesta de herramientas

Existen diferentes herramientas o buscadores de código abierto, accesibles a través de Internet, que sirven para realizar la trazabilidad de transacciones con criptoactivos. Algunas de ellas son las siguientes:

- *Blockchain Explorer*. Esta herramienta sirve para trazar las transacciones de varios criptoactivos como *bitcoin* (BTC) o *ether* (ETH). También permite ver la capitalización de estos activos, entre otras funcionalidades.

- *Blockchair*. Este buscador permite trazar transacciones de la Red *Bitcoin* de manera muy similar a *Blockchain Explorer*.

- *Wallet Explorer*. Esta herramienta permite descubrir los flujos en la Red *Bitcoin* e indica si la dirección que se ha introducido pertenece a un *cluster*, el resto de direcciones asociadas al mismo y si se trata de una cartera dentro de algún servicio identificado como una exchange o proveedor de criptoactivos.

  Esta herramienta resulta de utilidad para conocer a qué exchange se debe dirigir el investigador para solicitar más información sobre las transacciones de interés, pero se ha de tener en cuenta que está desactualizada por lo que no listará algunas direcciones pertenecientes a proveedores de servicios de criptoactivos.

- *Etherscan*. Esta herramienta permite trazar todas las transacciones dentro de la Red *Ethereum*, entre las que están las operadas con el activo *ether* (ETH) y los *tokens* ERC-20, como *tether* (USDT).

- *Tronscan*. Esta herramienta permite trazar las transacciones operadas en la Red *Tron*, entre las que están las operadas con la criptomoneda *tron* (TRX) y también las operadas con *tokens* que utilicen esta red. Este buscador permite trazar transacciones de la Red *Tron* de manera muy similar a *Etherscan*.

3.2 Las *exchanges*

Las *exchanges* o casas de cambio son proveedores de servicios de criptoactivos que permiten operar con estos activos de forma sencilla, por este motivo son muchos los usuarios que hacen uso de ellos. «Estos exchanges son necesarios en el mundo electrónico, ya que son la manera más sencilla de cambiar criptomonedas

y hacer trading con ellas, o lo que es lo mismo, comprar y vender estos activos cotizados» (Callejo y Ronco, 2020, p. 89).

Existen varios tipos de *exchange*. Los e*xchanges* centralizados son entidades que ofrecen servicios financieros con criptoactivos y se establecen como intermediarios entre los usuarios que operan con ellos ya que facilitan la compra de criptoactivos con dinero fiat a través de una simple transferencia o pago con tarjeta de crédito. Además, disponen de liquidez y un alto número de paridades entre criptoactivos y dinero fiat. Algunos de ellos son *Binance*, *Kraken*, *Houbi, OKX* o *Coinbase*.

Una alternativa a este tipo de *exchanges* son los llamados *exchanges* descentralizados o DEX, que son plataformas de código abierto que únicamente ofrecen el espacio digital donde se produce el intercambio de criptoactivos sin intermediarios, es decir, no hacen de intermediarios entre los usuarios. De esta manera los criptoactivos no se depositan en estas entidades en ningún momento, como sí sucede en los centralizados. Son menos los usuarios que hacen uso de este tipo de *exchanges* debido a que su planteamiento resulta más complejo que el de los *exchanges* centralizados. Algunos de ellos son *SusiSwap*, *PancakeSwap* o *Uniswap*.

3.3 Bitcoin y la Red *Ethereum*

A continuación, se explica cómo rastrear por fuentes abiertas las redes *Bitcoin* y *Ethereum*.

3.3.1 Bitcoin

Bitcoin es un activo, un protocolo, un *software* de código y una red entre pares (P2P) creada en 2009. Su *White paper*, o documento técnico que explica el funcionamiento de esta red, se puede consultar a través de Internet. Como ya se ha indicado, una herramienta de consulta de las transacciones operadas con esta criptomoneda es *Blockchain Explorer*.

Cabe introducir aquí el concepto de *altcoins* o monedas alternativas, que son todas aquellas que no son *bitcoin*; existen

multitud de ellas y se pueden consultar en sitios web como *CoinMarketCap*, que también aporta información sobre el valor de cotización de los criptoactivos.

Bitcoin para validar las transacciones en su *Blockchain* o cadena de bloques utiliza el sistema llamado *Proof of Work*, en el cual los usuarios, llamados mineros, a través de sus ordenadores, validan las transacciones y obtienen una recompensa por ello.

Para empezar a trazar los investigadores deben conocer los diferentes formatos que puede presentar una dirección de *Bitcoin*. Estas comienzan con el número 1 o 3 y tiene entre 26 y 35 caracteres. También son válidos el llamado formato de dirección *bech32*, que comienza con bc1q y tiene más caracteres, y el formato *Taproot*, que comienza con bc1p, ambos introducidos más recientemente.

Ejemplos de direcciones *Bitcoin* obtenidas aleatoriamente del buscador *Blockchain Explorer*:

- bc1qv8HySZ9aPq1xw51GmGQhp4fnydj201AFdt
- bc1qc026d7ght3cdjd0ugwvc23mfqsag0q2hvw0l3x
- 1AdFdaGhGmNQiobrvdnKHPyN9yMuGgfHiF
- 3EuMyVyv9M1yShgsUscPqT6MZmFZiFN2LGQ

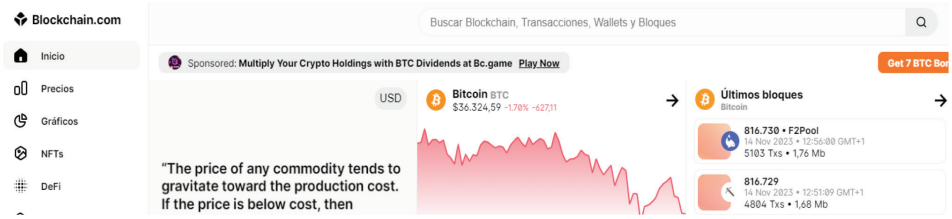
También se deben conocer los formatos de las claves privadas ya que será indispensable para realizar la incautación de los fondos depositados en los monederos. En *Bitcoin* la clave privada tiene entre 51 o 52 dígitos y empieza por 5, 6, K o L.

A continuación, se propone cómo realizar la trazabilidad de transacciones *Bitcoin*:

Si se utiliza la herramienta *Blockchain Explorer*, los pasos a seguir serían los siguientes:

1) Introducir el *hash*, la dirección o el bloque que se quiere trazar en el buscador que se puede observar en la Figura 9.

Figura 9: Imagen del buscador *Blockchain Explorer*, donde introducir el *hash*, dirección o bloque para obtener información del mismo.



Nota. Recorte del buscador público *Blockchain Explorer* (*Blockchain Explorer*, 2023).

Si, al introducir una dirección o *hash*, la herramienta indica que no se han encontrado resultados, puede ser que se trate de una dirección *Bitcoin* o *hash* con un formato incorrecto y pueda pertenecer a otra criptomoneda o se haya escrito incorrectamente.

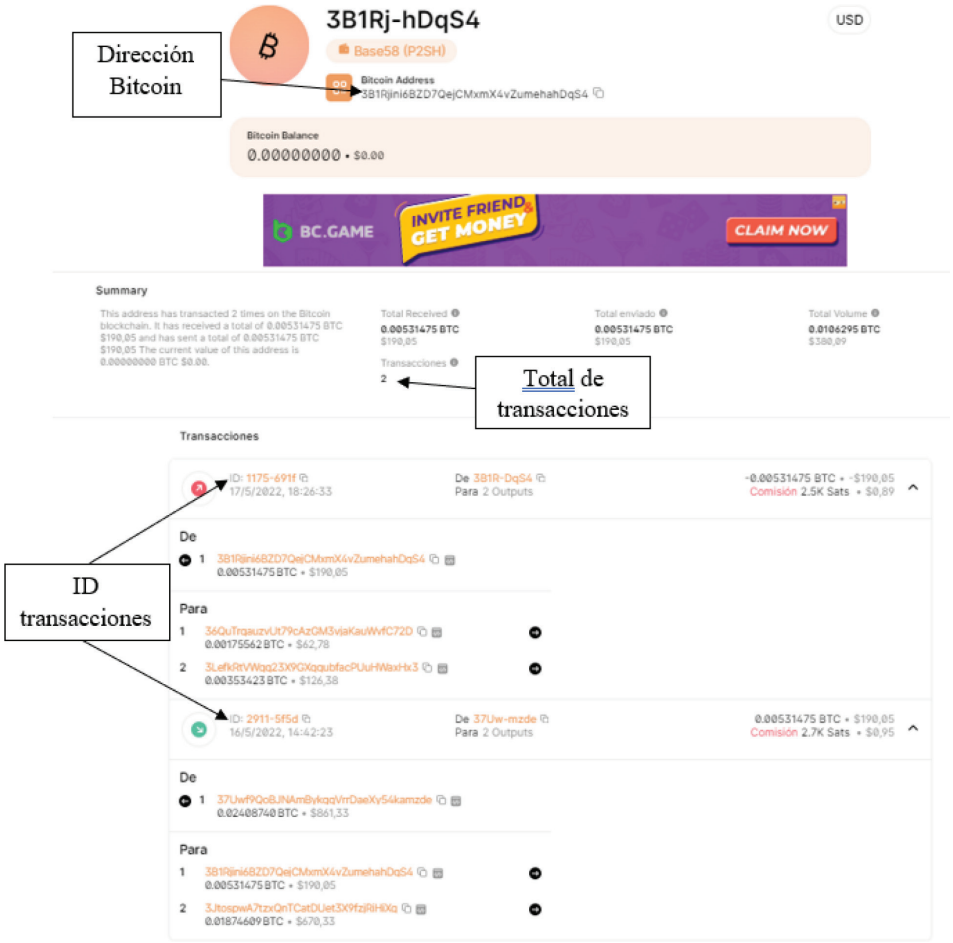
2) Si se introduce una dirección, aparecerá la imagen que se muestra más abajo como Figura 10.

   En el siguiente ejemplo se observan varios elementos que se han de tener en cuenta a la hora de trazar una dirección *Bitcoin*.

   La dirección que se ha introducido en el buscador figura completa en la parte superior de la imagen, el resto de direcciones, así como los *hash* (ID) de las transacciones, se muestran como enlaces y se pueden consultar clicando encima de ellas.

   Las transacciones de entrada van acompañadas de un símbolo de color verde. Por el contrario, las de salida van seguidas de un símbolo rojo. Estas últimas llevan aparejada una comisión, calculada, en el caso de *Bitcoin*, en una unidad llamada *satoshi*, que es la representación mínima en la que se puede operar en el sistema *Bitcoin*.

Figura 10: Información sobre una dirección de *Bitcoin*.



Nota. Recorte editado del buscador público *Blockchain Explorer*.

Por último, señalar que este buscador muestra la fecha y la hora en formato europeo y la zona horaria es la hora local, pero otras herramientas utilizan formatos distintos como UTC, que habrían de tenerse en cuenta.

3) La dirección de cambio:

Un supuesto que se puede dar en las transacciones con *bitcoin* es que una transacción de salida presente varias direcciones de destino, y que una de ellas pertenezca también al propio

remitente. Es la llamada dirección de cambio, donde se envía el saldo sobrante de la transacción.

Esto sucede porque no se envía la cantidad exacta de *bitcoin*, sino que existe un sobrante que retorna a la dirección de cambio que también pertenece al remitente.

En ocasiones es posible deducir qué dirección es la dirección de cambio, bien por los saldos o utilizando la herramienta *Wallet Explorer*, pero en otros casos resulta difícil saberlo. Existen algunos trucos para hacer esta averiguación:

- El primero es que exista una coincidencia entre las direcciones de remitente y destinatario, figurando la misma dirección en el apartado del remitente *(From)* y del destinatario *(To)*.

- Que la propia herramienta utilizada marque que se trata de la dirección de cambio como se recoge en la Figura 11. En este ejemplo se ha utilizado la herramienta *Blockchair*:

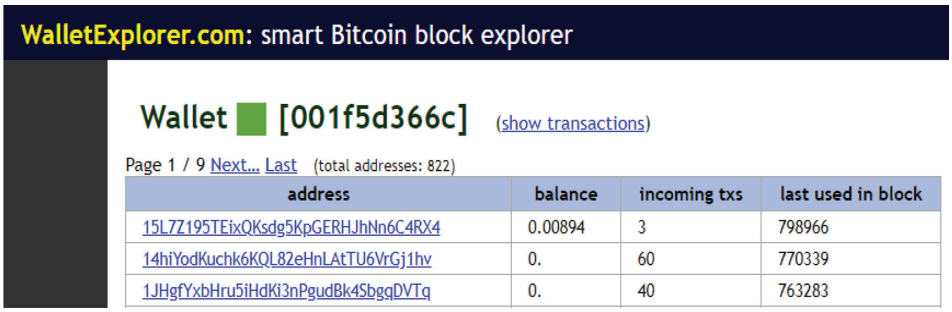
Figura 11: Dirección de cambio en el sistema *Bitcoin*.

Nota. Recorte aleatorio editado de una transacción del buscador público *Blockchair*.

- Que la dirección de remitente y la de cambio pertenezcan al mismo *cluster*.

Se utilizaría la herramienta *Wallet Explorer*, introduciendo la dirección del remitente en el buscador y clicar en «*show wallet addresses*». Todas las direcciones que figuren en el listado pertenecen al mismo remitente. Un ejemplo visual se observa en la Figura 12.

Figura 12: Direcciones incluidas en un *cluster* por la herramienta *Wallet Explorer*.



Nota. Recorte aleatorio de un *cluster* del buscador público *Wallet Explorer* (*Wallet Explorer*, 2023).

Este es un buen momento para introducir el concepto de *cluster*.

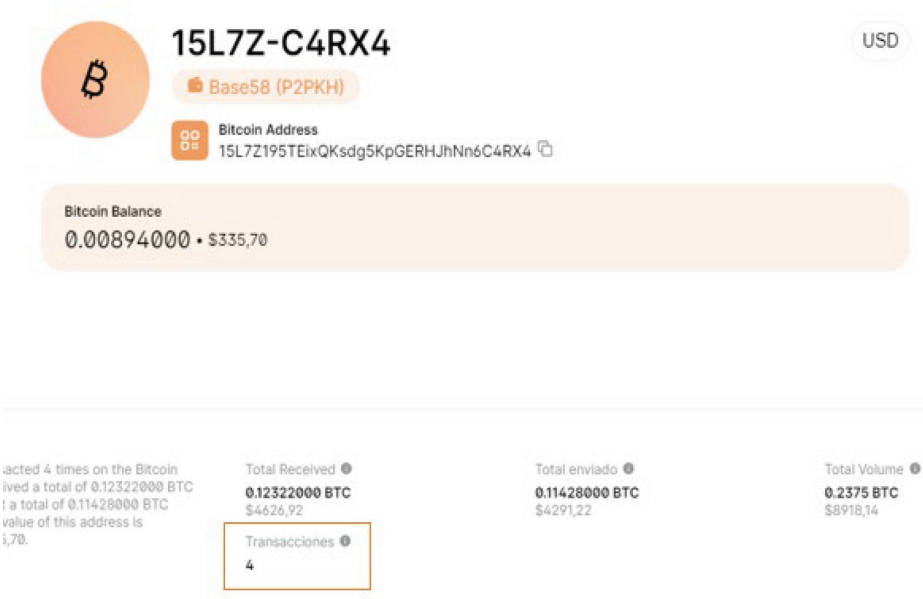
Un *cluster* es la agrupación de direcciones dentro de un monedero de criptoactivos, billetera o *wallet*. A efectos operativos, esto significa que gracias a un *cluster* se pueden saber las direcciones controladas por un mismo monedero, pero existe una diferencia entre *cluster* y monedero, ya que el *cluster* es la agrupación de direcciones, pero un monedero puede verse como un solo *cluster* o como varios.

Para saber cuántas direcciones tiene un *cluster* se puede acudir a la herramienta *Wallet Explorer*.

A continuación, se explica en un ejemplo práctico:

Se utiliza la dirección *Bitcoin* 15L7Z195TEixQKsdg5KpGERHJhNn6C4RX4, que según *Blockchain Explorer* presenta 4 transacciones como se observa en la Figura 13.

Figura 13: Información sobre la dirección 15L7Z195TEixQKsdg5KpGERHJhNn6C4RX4.



Nota. Recorte editado de una dirección del buscador público *Blockchain Explorer*.

Esta misma dirección se introduce en el buscador *Wallet Explorer*, que la relaciona con un monedero o *wallet*, en este caso es el número 001f5d366c (este nombre de monedero es un identificador que utiliza la propia herramienta).

La herramienta indica que desde este monedero se han realizado más de 2000 transacciones, por lo que existen más direcciones de *Bitcoin* asociadas a este monedero, ya que la que se ha consultado solo presentaba 4 transacciones. Para conocer el resto, basta con clicar en el enlace «*show wallet addresses*», que aparece resaltado en la Figura 14.

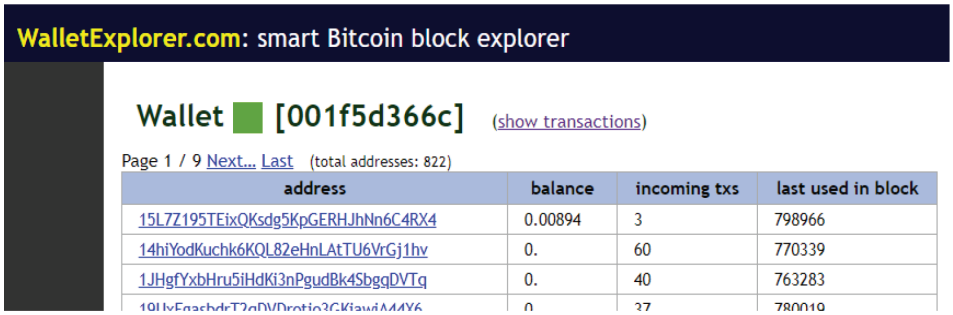
Hay que tener en cuenta que se están utilizando herramientas de rastreo que a menudo no logran identificar todas las direcciones de un monedero, por ello resulta interesante usar varias herramientas por si alguna aporta más información.

Figura 14: Información sobre un *cluster* a través de la herramienta *Wallet Explorer*.

Nota. Recorte editado de un *cluster* del buscador público *Wallet Explorer*.

En este caso, la herramienta indica que el monedero controla 822 direcciones, el balance de cada una de ellas y las transacciones que han operado, como se puede ver en la Figura 15.

Figura 15: Información sobre un *cluster* a través de la herramienta *Wallet Explorer*.



Nota. Recorte de un *cluster* del buscador público *Wallet Explorer* (*Wallet Explorer*, 2023).

Esta herramienta no siempre identifica si el monedero pertenece a un servicio de criptoactivos como, por ejemplo, a una *exchange*, en estos casos existen indicadores que permiten pensar que la dirección que se está trazando pertenece a un monedero de un servicio de criptoactivos identificado. Uno de los indicadores de que la dirección trazada pertenece a un servicio de criptoactivos es que figuren cientos o miles de transacciones y cientos de direcciones asociadas al mismo.

Si la herramienta sí identifica el monedero de un servicio de criptoactivos identificado como, por ejemplo, una *exchange*

o proveedor de criptoactivos, lo que hace es titular junto al número de *wallet* el nombre del servicio; un ejemplo visual es el recogido en la Figura 16.

Figura 16: Identificación de un monedero.

Nota. Recorte del buscador público *Wallet Explorer* (*Wallet Explorer*, 2023).

- Otro truco para identificar una dirección de cambio es que las cantidades sean redondas ya que es un indicador de que esa transacción se corresponde al envío efectivo y la otra al cambio. Un ejemplo es el recogido en la Figura 17.

Figura 17: Identificación de dirección de cambio por cantidades redondas.

Nota. Recorte aleatorio de una transacción del buscador público *Blockchair* (*Blockchair*, 2023).

Es más probable que el remitente envíe una cantidad exacta al destinatario, es decir, 2,5 *bitcoin* y no 0,419232 *bitcoin*, que seguramente se corresponderían con el excedente y, por lo tanto, la dirección bc1qjh-

0j25ng7525544uzjy8q8pxavekhefcaumj5 sería la dirección de cambio en esta operación.

- Por último, que la cantidad al cambio en dólares sea redonda es un indicador de que esa transacción es la correspondiente al envío y la restante al excedente. Para ello habría que consultar *CoinMarketCap* para conocer el valor de la criptomoneda enviada en el día de su envío y realizar el cálculo.

4) Varias direcciones de envío o remitente:

También se puede dar el caso de que una transacción salida presente varias direcciones de remitente, en este caso las direcciones que aparezcan en el apartado de *from* o de pertenecen a la misma persona. Es el caso de la transacción que aparece en la Figura 18.

Figura 18: Direcciones del remitente.

Nota. Recorte aleatorio de una transacción del buscador público *Blockchain Explorer* (*Blockchain Explorer*, 2023).

Esta transacción presenta 4 direcciones, que envían un total de 0,5 *bitcoin* a la dirección bc1qwq4qlw2h0920vyjwv9sca499tl2km9fkv8ylq7. Como se puede observar, la suma de las cantidades de las 4 direcciones permite alcanzar la cantidad enviada y el pago de la *fee*. Cabe señalar que la cantidad sobrante de la transacción (0,78 *bitcoin*) es enviada a la dirección bc1qgtsgwf905d2raq4ukt9fhj86daupzrtf7mcysh (dirección de cambio y también del remitente, que es posible

deducir al ser la misma que las dos últimas que figuran en el apartado del remitente [De]). Es decir, la cantidad de fondos no es suficiente para enviar el pago por lo que se envía desde varias direcciones con fondos, fusionándose para realizarlo. Las direcciones pertenecen al mismo remitente.

Asimismo, como sucede en este caso con la dirección bc1qgtsgwf905d2raq4ukt9fhj86daupzrtf7mcysh, se observa la misma en varias ocasiones en el apartado del remitente. Esto es posible ya que los fondos de *bitcoin* no se fusionan, es decir, son dos entradas diferentes a esa dirección o dos fragmentos de *bitcoin* generados por separado que se están gastando en la misma transacción.

A modo resumen, los pasos a seguir para realizar una trazabilidad de *Bitcoin* serían:

1) Introducir en el buscador *Blockchain Explorer* u otra herramienta la dirección *Bitcoin* que se quiere trazar.

2) Introducir la misma dirección en la herramienta *Wallet Explorer* para saber a qué monedero está asociada y el resto de direcciones, para ello habrá que clicar en «*show wallet addresses*». Se pueden dar dos situaciones:

   La primera que no liste la *wallet* como perteneciente a ningún proveedor de criptoactivos, figuraría un código alfanumérico como se puede observar en la Figura 19.

Figura 19: Información sobre un *cluster*.

Wallet [156b7c55c2] (show transactions)

Page 1 / 1 (total addresses: 3)

address	balance	incoming txs	last used in block
1JgnPM5WyhSktkskrGGE9D2AvzQvTpzydW	0.	2	447866
1K2WJRiLXU3bcWZ8Y4ifuxagdALPzsN1dM	0.	1	447866
1Mx8facDozfFzo9oLtY36PZf2qmfkZntkr	0.	1	447866

Page 1 / 1 (total addresses: 3)

Nota. Recorte del buscador público *Wallet Explorer* (*Wallet Explorer*, 2023).

En este ejemplo se observan tres direcciones en el mismo *cluster*, que pertenecen al mismo monedero. Al no identificar ningún proveedor de criptoactivos, interesará seguir trazando.

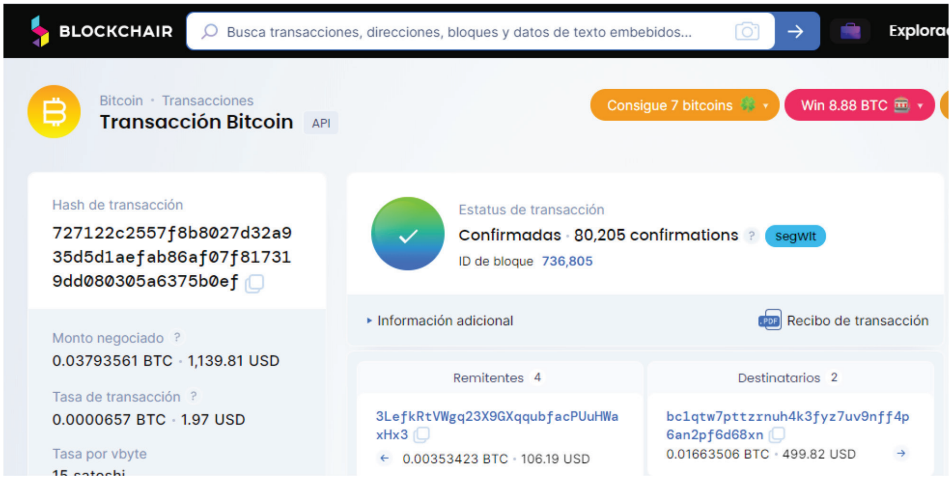
Y la segunda situación es que la herramienta *Wallet Explorer* indique que la dirección introducida sí pertenece a un proveedor de criptoactivos; en este caso en vez de un código alfanumérico aparecería la denominación del servicio, como se puede observar en la Figura 20.

Figura 20: Información sobre un *cluster* identificado.

Nota. Recorte del buscador público Wallet Explorer (Wallet Explorer, 2023).

3) Por otro lado, si en vez de una dirección se introduce un *hash*, aparecerá la imagen que se muestra en la Figura 21. En este ejemplo se ha utilizado el buscador *Blockchair*.

Figura 21: Información relativa a un *hash*.



Nota. Recorte aleatorio de una transacción del buscador público *Blockchair* (*Blockchair*, 2023).

Otra forma de trazar transacciones de *Bitcoin* es mediante el *hash* de la operación. Esta forma es útil cuando se trata de direcciones que presentan numerosas transacciones, al centrarse en la operación objeto de análisis.

Además, introduciendo el *hash*, a través de los buscadores *Blockchain Explorer* o *Blockchair*, clicando en el símbolo de flecha, es posible seguir los fondos hacia delante y hacia atrás entre direcciones *Bitcoin*.

3.3.2 Red *Ethereum*

La Red *Ethereum* fue creada en 2013 y su cadena de bloques o *Blockchain* comenzó a funcionar en 2015. Se trata de una plataforma descentralizada creada para almacenar códigos y programas informáticos que pueden ejecutarse en cualquier lugar.

Es de código abierto y en ella se pueden utilizar *ether* (ETH) y otros muchos *tokens* y NFT como medio de pago o como elemento integral de un contrato inteligente. Una herramienta de consulta es *Etherscan*.

La Red *Ethereum* usa un sistema llamado *Proof of Stake* (prueba de participación) para la validación y creación de los bloques que contienen las transacciones operadas en esta red. En este sistema, los usuarios con *ether* se eligen al azar para validar la red, ordenando transacciones y creando nuevos bloques. Se requiere menos energía y *hardware* para este tipo de consenso.

El *ether* es la criptomoneda nativa de *Ethereum*. En esta red también se puede operar con diversos *tokens* a través de la norma ERC-20, que es un estándar técnico utilizado para la creación e implementación de contratos inteligentes *(smart contract)* en la *blockchain* de *Ethereum*. Este estándar define las reglas que los *tokens* deben seguir dentro de la Red *Ethereum*. La lista completa de todos los *tokens* ERC-20 puede consultarse en *Etherscan*.

Para poder enviar esos *tokens*, es necesario tener un pequeño saldo de *ether* en el monedero.

Los más usados por los investigados son las llamadas *stablecoin* o monedas estables, que son aquellos *tokens* diseñados para minimizar la volatilidad del precio de los criptoactivos. *Tether* (USDT), *USD Coin* (USDC), *Binance* USD (BUSD) y DAI son los más utilizados y están colaterizados con el dólar (paridad 1:1 con el dólar). Es común ver como los investigados cambian sus criptoactivos *bitcoin* (BTC) o *ether* (ETH) por *stablecoin* para mantener el valor de los criptoactivos.

Mención especial para el *token tether* (USDT) por ser uno de los principales *tokens* que se encuentran en las investigaciones. Este *token* se ejecuta sobre la Red *Ethereum*, aunque también existe implementación sobre *Bitcoin* y *Tron*.

Los *tokens* deben ejecutarse a través de un contrato inteligente o *smart contract*, que son contratos inteligentes de ejecución automática que residen en una dirección de la Red *Ethereum*.

En la herramienta de *Etherscan*, junto a la dirección, figura un símbolo de documento que indica que es un contrato.

Tanto los *tokens* como los contratos inteligentes o *smart contract* no tienen requisitos para su creación y cualquiera puede crearlos, lo que ha llevado a que muchos resulten proyectos fraudulentos.

Otra forma de operar en la Red *Ethereum* es a través de plataformas descentralizadas o DeFi, que son servicios que facilitan la interacción directa entre usuarios sin intermediarios. Permite a los usuarios de la plataforma que conecten o vinculen directamente sus monederos para comprar, vender o intercambiar criptomonedas o *tokens*. Las más famosas son *SushiSwap* y *Uniswap*.

Además, este ecosistema DeFi permite a los usuarios suministrar liquidez de criptomonedas o *tokens* a través de contratos inteligentes o *smart contract*, por una pequeña recompensa.

Estas funcionalidades hacen más complejo el trabajo de rastreo ya que los servicios descentralizados no reportan información de las transacciones debido a que los intercambios se

realizan de forma anónima, sin registro, identificación o reglas KYC/AML.

Para empezar a trazar en la Red *Ethereum* se debe conocer el formato que presenta una dirección de esta red; las direcciones comienzan por 0x.

Algunos ejemplos obtenidos de manera aleatoria del buscador *Etherscan* serían los siguientes:

- 0x974CaA59e49682CdA0AD2bbe82983419A2ECC400

- 0x0829190D34F282c780A92f7b0ae739d859f6aecf

- 0x503828976D22510aad0201ac7EC88293211D23Da

Las direcciones de *Ethereum* se pueden compartir públicamente para recibir *ether*, *tokens* y NFT, y para ver un saldo en relación a la dirección. Se utilizan para almacenar *ether*, *tokens* y contratos, entre otros.

También hay que conocer los formatos de las claves privadas; en *Ethereum* la clave privada contiene 64 caracteres hexadecimales.

A continuación, se explica cómo trazar en la Red *Ethereum* ya que presenta algunas particularidades y diferencias con la Red *Bitcoin*.

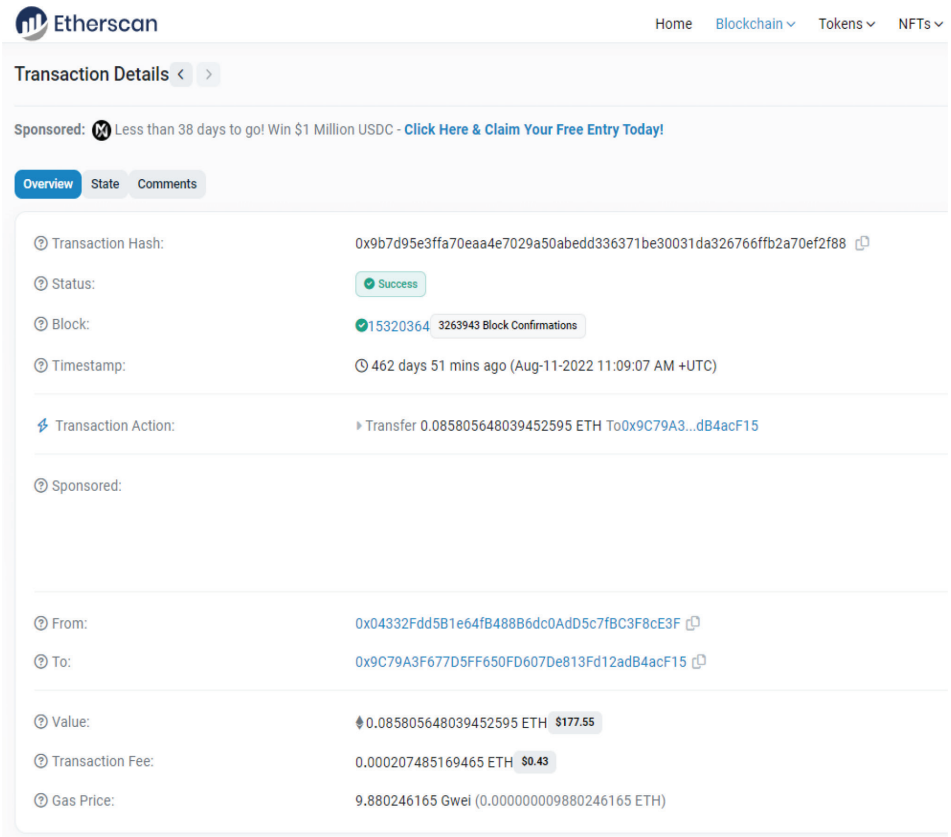
Si se utiliza la herramienta *Etherscan* los pasos a seguir serían los siguientes:

1) Introducir en el buscador el *hash*, la dirección o el bloque que se desee trazar.

   Este buscador permite explorar bloques, transacciones, contratos inteligentes o *smart contract*, transferencias de *tokens* y transacciones internas, entre otros.

2) Si se introduce un *hash* en el buscador aparecerá la siguiente imagen recogida en la Figura 22.

Figura 22: Información relativa a un hash a través de la herramienta *Etherscan*.



Nota. Recorte aleatorio de una transacción del buscador público *Etherscan* (*Etherscan*, 2023b).

Este tipo de búsqueda puede aportar diferente información, como cuándo tuvo lugar una transacción en concreto, cuándo fue verificada, las direcciones de origen o remitente y de destino, qué tarifa de transacción o *fee* se pagó. A diferencia de si se introduce en el buscador una dirección, que figurarán todas las transacciones operadas por esta.

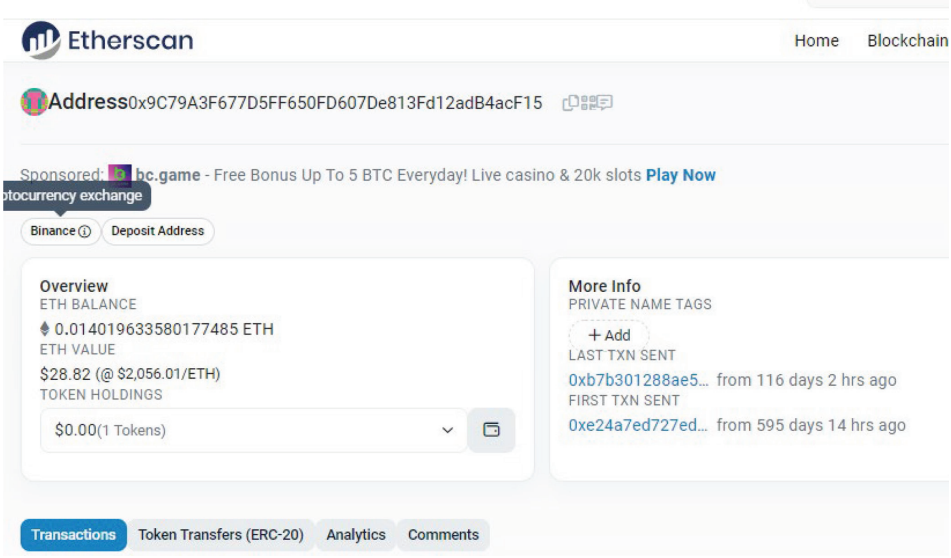
Etherscan, a diferencia de *Wallet Explorer*, no reconoce las direcciones como parte de un *cluster*, por lo que se debe trazar siempre en un contexto y si es posible listar las direcciones.

Si se quiere seguir los fondos, en este ejemplo se trazarán los 0,08 ETH en la dirección de destino *(to)* 0x9C79A3F677D-5FF650FD607De813Fd12adB4acF15.

3) Si se introduce una dirección de la Red *Ethereum* aparecerá la imagen que se recoge en la Figura 23.

   En el caso de que este buscador arroje un resultado negativo, se pueden consultar otras cadenas de bloques para verificar esta dirección en ellas.

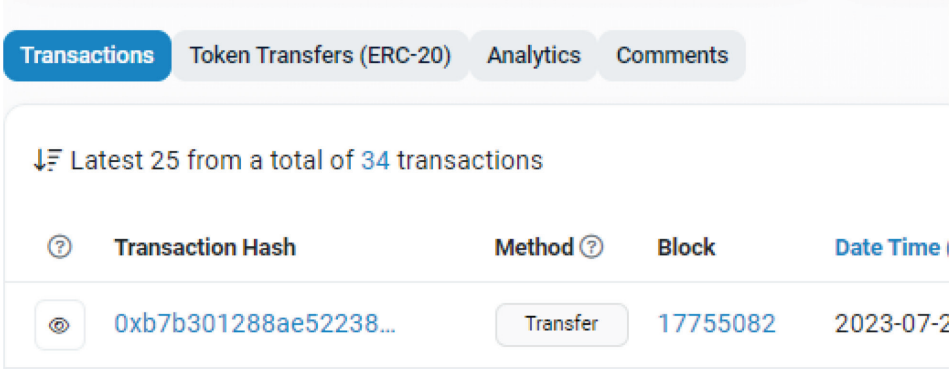
Figura 23: Información sobre una dirección en la Red *Ethereum*.



Nota. Recorte aleatorio de una dirección del buscador público *Etherscan* (*Etherscan*, 2023b).

El primer apartado que figura con respecto a una dirección, «*Transactions*», es el referente a todas las transacciones operadas en *ether* con esa dirección tanto de entrada como de salida; un ejemplo visual es el que se recoge en la Figura 24.

Figura 24: Información sobre las transacciones asociadas a una dirección de la Red *Ethereum*.



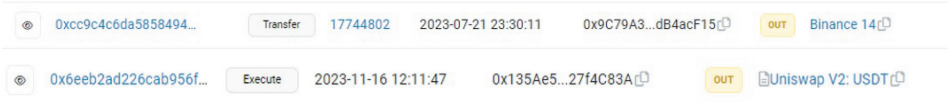
Nota. Recorte aleatorio del apartado *Transactions* del buscador público *Etherscan* (*Etherscan*, 2023a).

A diferencia de *Bitcoin*, la Red *Ethereum* no utiliza direcciones de cambio. Esto hace más fácil conocer dónde terminan los fondos, ya que las transacciones en la Red *Ethereum* van de una dirección a otra dirección. Esto puede resultar similar a transacciones entre cuentas bancarias.

En la imagen anterior se ven todas las transacciones que ha operado la dirección que se ha introducido en el buscador; en este caso figuran treinta y cuatro. Si fuese de interés filtrar por transacciones de entrada o de salida, en la parte superior derecha figuran tres puntos que al clicar sobre ellos se despliegan varias opciones de filtrado.

Otra ventaja de este buscador es que algunos servicios ya están etiquetados, por ejemplo, se pueden ver varias direcciones con etiquetas de *exchange*, como *Binance*, *Kraken*, *Bitfinex*, *Huobi*, *Gemini*, etc. También se pueden encontrar contratos de *tokens* y plataformas de NFT. A continuación, se muestran dos ejemplos en la Figura 25.

Figura 25: Identificación de direcciones asociadas a *exchanges*.



Nota. Recorte aleatorio editado del apartado *Transactions* del buscador público *Etherscan*.

En este apartado también se puede ver el tipo de transacción que tuvo lugar en la pestaña «*Method*». Son varias las operativas que pueden figurar como, por ejemplo, «*Approve*», «*Multicall*», «*Transfer*» o «*Swap*».

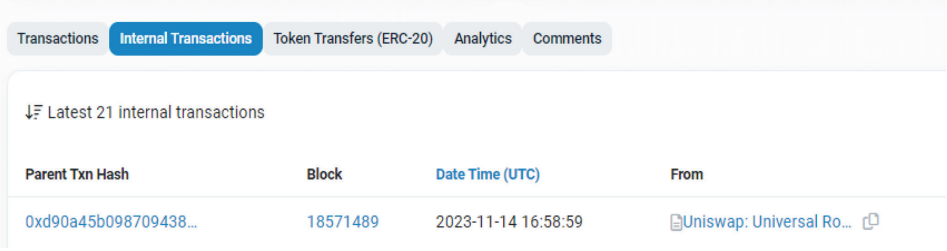
Esto puede dar al investigador que está trazando una idea del tipo de transacción que se está realizando, y si se clica en la transacción de interés y se observa el apartado «*logs*» se obtendrá toda la información sobre el método utilizado.

A continuación de «*Transactions*», figura el apartado «*Internal txns*», relativo a las transacciones internas que están relacionadas con las transacciones que interactúan con un contrato inteligente o *smart contract*.

Esta pestaña muestra, por ejemplo, el uso de servicios descentralizados como *SushiSwap* o *Uniswap*, y también entradas de mezcladores o *mixer*.

Esta pestaña no siempre estará visible, solo si la dirección ejecutó transacciones internas. Si fuese visible aparecería tal y como se observa en la Figura 26.

Figura 26: Información relativa a transacciones a través de *smart contract*.

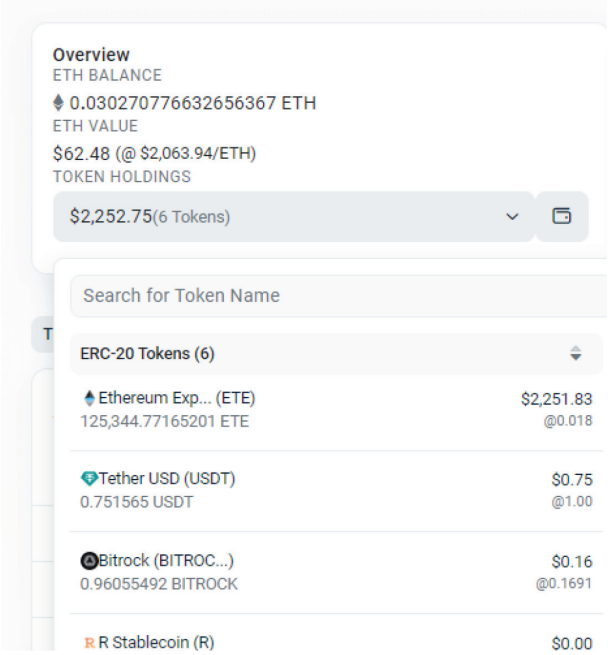


Nota. Recorte aleatorio del apartado *Internal Transactions* del buscador público *Etherscan* (*Etherscan*, 2023b).

La siguiente pestaña que figura es «*ERC20 Token Txns*», relativa a las transacciones operadas con *tokens* ERC20 de la Red *Ethereum*. El sistema *Ethereum* permite a los usuarios mantener o almacenar la moneda nativa de *Ethereum*, *ether* (ETH), y uno o más de estos *tokens* en una dirección de *Ethereum*. *Etherscan* indica los *tokens* depositados en esa dirección y su valor a día de la consulta.

Cuando se introduce la dirección a trazar en el buscador, uno de los apartados que figura es «*Token*»; si figura alguno como es el caso del siguiente ejemplo, en la pestaña «*ERC20 Token Txns*» se podrán consultar las transacciones operadas con los mismos de la misma manera que en el apartado de «*Transactions*» ya explicado. El apartado referido puede observarse en la Figura 27.

Figura 27: Información sobre los *tokens* de una dirección de la Red *Ethereum*.



Nota. Recorte aleatorio de una dirección del buscador público *Etherscan* (*Etherscan*, 2023b).

Esta dirección presenta un valor de *ether* 0,03 y otras cantidades de 6 tokens diferentes, que se corresponden al día de la consulta con un valor de más de 2.000 dólares. En la pestaña «*ERC20 Token Txns*» se puede obtener más información al respecto.

4 Conclusiones

A continuación, se realiza una síntesis de los puntos que se consideran más relevantes:

- El uso de los criptoactivos ha experimentado un notorio aumento en los últimos años, introduciendo consigo una serie de conceptos novedosos en la economía española. Este fenómeno ha permitido a los usuarios operar de nuevas formas, lo que entraña una serie de ventajas y riesgos inherentes que deberían conocer.

- Por ello, adquirir conocimientos sobre trazabilidad resulta de gran utilidad no solo desde la perspectiva policial, sino también como ciudadano inmerso en una sociedad donde la tecnología *Blockchain* y los criptoactivos ganan cada vez más terreno. De esta manera, las Fuerzas y Cuerpos de Seguridad pueden rastrear fondos fraudulentos y localizar a los criminales que abusan de estos elementos y, al mismo tiempo, los ciudadanos pueden verificar el estado de sus transacciones mediante esta tecnología, que ha llegado para quedarse.

- Debido al incremento en el uso de los criptoactivos, su presencia en las investigaciones policiales también ha crecido, presentándose de diferentes formas: utilizados como método de pago, en operativas de blanqueos de capitales procedentes de diferentes tipologías delictivas y también como productos de inversión que sirven de reclamo en estafas. Son varios los elementos que dificultan su seguimiento e incautación y que resultan de interés para los delincuentes, como son la rapidez que presentan las transacciones con estos activos, su carácter internacional y, en cierta medida, su anonimato.

- Este panorama social ha generado la necesidad de muchos países de ponerse al día en materia de criptoactivos, colocándolos en una posición preferente en su agenda normativa. Un ejemplo es el Reglamento de Mercados de Criptoactivos (MICA) [Reglamento (UE) 2023/1114 del Parlamento Europeo y del Consejo, de 31 de mayo de 2023, relativo a los mercados de criptoactivos], que se ha convertido en el primer instrumento regulador de estos activos, pero que no será de aplicación hasta el 30 de diciembre de 2024 como dice su artículo 149. Esta norma ha dado cobertura jurídica a los criptoactivos y establecido unas reglas comunes a todos los operadores en la Unión Europea.

- Existen multitud de criptoactivos en la actualidad, si bien son varios los que se encuentran con mayor frecuencia en las investigaciones policiales, como *bitcoin*, *ether*, *monero*, *tether* y otras *stablecoins*.

- Debido al diseño de algunos de los criptoactivos existentes es posible trazarlos a través de fuentes abiertas, si bien, en ocasiones, sería conveniente la utilización de herramientas comerciales específicas de trazabilidad que ayudarán en esta tarea al investigador. Hay que tener en cuenta que el análisis de las transacciones con herramientas de código abierto debe estar basado siempre en el contexto de la investigación. El análisis de las transacciones, junto con el análisis de la información obtenida de otras fuentes, resulta de gran importancia para detectar la actividad delictiva e identificar a los responsables.

- Los puntos de compromiso en investigaciones con criptoactivos, y donde se deben centrar los esfuerzos del investigador, es en el momento en que son intercambiados por otros criptoactivos o por dinero *fiat*, ya que permiten una mayor trazabilidad y es posible que se puedan identificar a las personas que podrían estar detrás de la operativa investigada.

Glosario

BILLETERA: monedero o *wallet* en inglés, cartera digital que contiene las claves necesarias para acceder a los criptoactivos del usuario.

BITCOIN: con mayúscula, presenta un significado más amplio que *bitcoin*, y corresponde a la red, la tecnología, el protocolo o la *blockchain*.

BITCOIN (BTC): en minúscula, es cada unidad de criptoactivo, divisible en unidades *satoshis* (1 BTC equivale a 100.000.000 *satoshis*).

BLOCKCHAIN O CADENA DE BLOQUES: es la tecnología que da soporte a los criptoactivos, es descentralizada y está distribuida en redes de usuarios, en ella se almacenan las transacciones y se graban los paquetes de datos.

CAPITALIZACIÓN DEL MERCADO: sirve para estimar el tamaño o magnitud de un criptoactivo o proyecto respecto de otro. Se calcula al multiplicar el precio de un criptoactivo por la cantidad de unidades que están en circulación.

CLUSTER: grupo de direcciones de criptoactivos que están vinculadas o asociadas de alguna manera. Las direcciones pueden pertenecer a un usuario o entidad. Estas agrupaciones pueden ser utilizadas para el análisis de transacciones y seguimiento de fondos en la *blockchain*, resultando útil para detectar patrones de gasto, comportamientos y relaciones entre diferentes partes en el ecosistema de los criptoactivos.

CNMV: abreviatura de Comisión Nacional del Mercado de Valores. Es el organismo encargado de la supervisión e inspección de los mercados de valores españoles y de la actividad de cuantos intervienen en los mismos.

CÓDIGO ABIERTO: forma de distribuir el contenido digital que permite a los usuarios disponer y en ocasiones modificar el contenido.

CONSENSO: acuerdo unánime de los miembros de una red de *blockchain* sobre las transacciones, lo que permite crear un bloque. Es una de las principales características de la tecnología *blockchain*.

CONTRATO INTELIGENTE: o *smart contract* en inglés.

CRIPTOACTIVO: activo digital que utiliza la criptografía para garantizar la seguridad de las transacciones. Las criptomonedas *bitcoin* y *ether* son ejemplos de criptoactivos.

DEFI: abreviatura de *Decentralized Finance* en inglés. Se trata de un conjunto de servicios financieros que operan en una red *blockchain*, basados en contratos inteligentes o *smart contract* en inglés, que buscan descentralizar el acceso a esos servicios sin depender de intermediarios.

DESCENTRALIZACIÓN: distribución de tareas entre más de una institución para evitar una única institución central que monopolice las funciones, procesos o poderes. Es una de las principales características de la tecnología *blockchain*.

DEX: abreviatura de *exchange* descentralizado. Su principal característica es que opera sin que medie intermediario centralizado, es decir, las transacciones se realizan directamente entre los usuarios a través de contratos inteligentes en *blockchain*. Un ejemplo es Uniswap, que opera en la Red *Ethereum* y permite el intercambio de *tokens* ERC-20 de manera descentralizada.

DINERO FIAT: o dinero fiduciario, es cualquier moneda emitida de forma convencional por un gobierno y declarada como medio legal de intercambio, por ejemplo, el euro o el dólar.

ERC-20: estándar de *tokens* que utilizan la Red *Ethereum*. Es el más utilizado.

ESA: abreviatura de autoridades europeas supervisoras en inglés.

ESMA: abreviatura de Autoridad Europea de Valores y Mercados en inglés. Forma parte del Sistema Europeo de Supervisión Financiera y su objetivo es garantizar una supervisión financiera adecuada en toda la Unión Europea.

ETHER (ETH): activo nativo de la Red *Ethereum*.

ETHEREUM: red distribuida de código abierto basada en *blockchain*. Esta red ofrece el desarrollo de aplicaciones descentralizadas.

EXCHANGE: plataforma o servicio de intercambios de criptoactivos, también permite el cambio de dinero fiat por criptoactivos y viceversa, además de otros servicios como la custodia de fondos. Existen varios tipos: centralizados (CEX), descentralizados (DEX) o híbridos. Algunos de estos proveedores de servicios con criptoactivos son *Kraken*, *Binance*, *Coinbase* o *Huobi*.

FEE: comisión por la prestación de un servicio.

HASH: término informático que se refiere a la huella digital, formado por una combinación de números y letras, que permite saber si el documento original ha sido modificado. El *hash* permite verificar el contenido de una transacción.

LIQUIDEZ: capacidad de un criptoactivo para ser comprado o vendido en el mercado sin afectar significativamente a su valor. Una alta liquidez significa que hay suficientes usuarios dispuestos a comprar o vender el criptoactivo, lo que facilita las transacciones con ese activo digital.

NODO: ordenador conectado a una red *blockchain* que guarde las copias de registro de las transacciones. Cuantos más nodos haya en una red, más descentralizada y segura será.

NTF: o *token* no fungible, es un tipo de activo que representa la propiedad o autenticidad de un elemento específico a través de la tecnología *blockchain*.

STABLECOIN: su traducción en español sería moneda estable, que hace referencia a que su valor está ligado al de otro activo o divisa, como por ejemplo el dólar.

TOKEN: representación digital de un activo o servicio. La mayoría utilizan la Red *Ethereum*.

TRADING: se refiere a la compraventa de criptoactivos con el fin de obtener un beneficio.

VOLATILIDAD: es la variación de un activo en un periodo de tiempo determinado. En el caso de los criptoactivos se dice que presentan una alta volatilidad debido a que su precio puede variar significativamente en un corto periodo de tiempo.

Referencias

Blockchair (2023). Buscador público de cadena de bloques o *blockchain*. https://blockchair.com/es

Blockchain Explorer (2023). Buscador público de cadena de bloques o *blockchain*. https://www.blockchain.com/es/explorer

Callejo, C. y Ronco, V. (2020). *Criptomonedas para dummies*. Grupo Planeta.

Comisión Nacional del Mercado de Valores (2018). *Comunicado conjunto de la CNMV y del Banco de España sobre «criptomonedas» y «ofertas iniciales de criptomonedas» (ICO)*.

Comisión Nacional del Mercado de Valores (2021). *Comunicado conjunto de la CNMV y del Banco de España sobre el riesgo de las criptomonedas como inversión*.

Comisión Nacional del Mercado de Valores (2022). *Estudio sobre las criptomonedas y la efectividad de las medidas impulsadas por la CNMV. Informe de Resultados mayo-junio de 2022*.

Etherscan (2023a). Buscador público de cadena de bloques o *blockchain*. https://etherscan.io/

Etherscan (2023b). Listado completo de *tokens* ERC-20. https://etherscan.io/tokens

Parlamento Europeo y Consejo. *Reglamento de Mercados de Criptoactivos (MICA) (REGLAMENTO (UE) 2023/1114 DEL, de 31 de mayo de 2023, relativo a los mercados de criptoactivos).*

Tronscan (2023). Buscador público de cadena de bloques o *blockchain*. https://tronscan.org/#/

Wallet Explorer (2023). Buscador público de cadena de bloques o *blockchain*. https://www.walletexplorer.com/