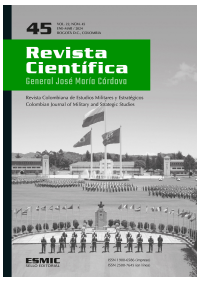

Revista Científica General José María Córdova
(Revista Colombiana de Estudios Militares y Estratégicos)
Bogotá D.C., Colombia
ISSN 1900-6586 (impreso), 2500-7645 (en línea)
Web oficial: www.revistacientificaesmic.com

Seguridad y legislación frente a amenazas al sistema de agua potable en España

Security and legislation against threats to the drinking water system in Spain

Adrián Nicolás Marchal González
Universidad Nebrija, Madrid, España
amarchal@nebrija.es

Citación APA: Marchal González, A. N. (2024). Seguridad y legislación frente a amenazas al sistema de agua potable en España.*Revista Científica General José María Córdova, 22(45)*, 199-218. https://doi.org/10.21830/19006586.1229

Publicado en línea: 5 de febrero de 2024

Enviar un artículo a la Revista

Revista Científica General José María Córdova
(Revista Colombiana de Estudios Militares y Estratégicos)
Bogotá D.C., Colombia

Volumen 22, número 45, enero-marzo 2024, pp. 199-218
https://doi.org/10.21830/19006586.1229

Seguridad y legislación frente a amenazas al sistema de agua potable en España

Security and legislation against threats to the drinking water system in Spain

Adrián Nicolás Marchal González
Universidad Nebrija, Madrid, España

Resumen. Este artículo analiza la importancia estratégica de la seguridad en la infraestructura crítica del agua, como recurso fundamental para la vida humana. En particular, explora el sistema de seguridad de esta infraestructura en España, así como la legislación existente frente a las amenazas a las infraestructuras críticas, en particular la del abastecimiento de agua potable. Se describen los tipos de ataques que pueden presentarse, la preparación de los sistemas de seguridad pasiva y activa ante estos y el desarrollo legislativo para sancionarlos. Pese a ser un tema cada vez más crucial, debido a que esta infraestructura puede ser un objetivo terrorista con impactos incalculables sobre la vida, la salud, la economía y la sociedad, se concluye que hay vacíos en la tipificación y definición de sanciones contra este tipo de ataques en España.

Palabras clave: abastecimiento de agua; derecho penal; seguridad hídrica; seguridad humana; terrorismo

Abstract. This article examines the strategic significance of security in critical water infrastructure, an essential resource for human life. Focusing on Spain, it explores the security system of this infrastructure and the existing legislation against threats to critical infrastructures, particularly drinking water supply. The study describes potential types of attacks, the preparedness of passive and active security systems against these threats, and the legislative developments to penalize them. Despite the increasing importance of this issue, as water infrastructure can be a target for terrorism with unimaginable impacts on life, health, economy, and society, the paper concludes that there are gaps in the classification and definition of sanctions against such attacks in Spain.

Keywords: criminal law; human security; terrorism; water security; water supply

Sección: Dosier • Artículo de investigación científica y tecnológica
Recibido: 15 de mayo de 2023 • Aceptado: 15 de enero de 2024

Contacto: Adrián Nicolás Marchal González ✉ amarchal@nebrija.es

Introducción

El presente artículo de investigación se centra en la crucial importancia de mantener la seguridad en las infraestructuras críticas (IC), especialmente aquellas dedicadas al suministro de agua, un recurso esencial para la vida, la industria y el comercio. Este análisis busca destacar la relevancia del agua como un elemento vital y explora las implicaciones de asegurar su disponibilidad continua y segura. Tal es la importancia del agua que el derecho internacional humanitario (DIH) le brinda una protección especial en el Protocolo Adicional I a los Convenios de Ginebra de 1949 (Comité Internacional de la Cruz Roja [CICR], 1977):

> Se prohíbe atacar, destruir, sustraer o inutilizar los bienes indispensables para la supervivencia de la población civil, tales como los artículos alimenticios y las zonas agrícolas que los producen, las cosechas, el ganado, las instalaciones y reservas de agua potable y las obras de riego, con la intención deliberada de privar de esos bienes, por su valor como medios para asegurar la subsistencia, a la población civil o a la Parte adversa, sea cual fuere el motivo, ya sea para hacer padecer hambre a las personas civiles, para provocar su desplazamiento, o con cualquier otro propósito. (art. 54, párr. 2)

Pero no solo las leyes que recogen este tipo de protección al agua. Religiones como el Islam condenan el uso de este bien como medio de guerra. Así, el Corán estipula que no puede ser envenenada durante la guerra y que incluso al enemigo se le debe permitir el acceso a ella. Esto se fundamenta en la *safa* (del árabe, *Ley del derecho al agua*), que considera al agua como un recurso de todos y que, por ende, debe distribuirse equitativamente.

A pesar de estas normas y creencias, a lo largo de la historia y en tiempos más recientes, han sucedido constantes ataques a fuentes de agua potable en conflictos bélicos. Si nos remontamos al año 1000 a.C., encontramos a guerreros chinos envenenando reservas de agua enemigas. En 1462, esta táctica se empleó contra los turcos otomanos por el Empalador de Valaquia, en Rumanía (Patrón, 2018), y fue igualmente utilizada por los finlandeses contra los soviéticos durante la Guerra de Invierno (Trotter, 2013). En el siglo actual, se han registrado varios ataques terroristas dirigidos a infraestructuras y reservas hídricas. Estos ataques, de diversa índole, comparten el objetivo de sembrar el terror en la sociedad y desestabilizar gobiernos. Un ejemplo notable ocurrió en 2002, cuando cuatro miembros de un grupo salafista fueron detenidos intentando contaminar con productos químicos el sistema de abastecimiento de agua de la embajada estadounidense en Roma.

En ese mismo año, en Denver, Estados Unidos, dos miembros de Al Qaeda fueron arrestados por conspirar para envenenar el agua de la ciudad (Melendo, 2019). En 2006, en Inglaterra, un tanque de agua fue envenenado con herbicidas (Pantusa & Maiolo, 2018), y en Dinamarca, un lago fue intencionalmente contaminado (Martínez, s.f.). En 2007, se registró un incidente similar en China (Xinhua, 2007), seguido en 2008 por otros en Virginia, Estados Unidos y en Tailandia (Pedersen, 2001). En 2009, Filipinas enfrentó un envenenamiento de sus aguas por parte del Frente Moro de Liberación Islámica (Acosta, 2009). Finalmente, en

2010, se reportaron incidentes en India (TNN, 10 de noviembre de 2010) y en Inglaterra (*BBC News*, 14 de mayo de 2010) que involucraban a rebeldes maoístas y a dos individuos neonazis, respectivamente.

En 2011, en España, se desactivó una célula islamista que planeaba envenenar el agua en respuesta a la muerte de Osama Bin Laden (Efe, 2011). Luego, en 2012, Australia (Hoffman, 2011) y Afganistán (Faiez & Vogt, 2012) experimentaron ataques similares. Entre 2015 y 2016, Inglaterra fue de nuevo blanco de un ataque, esta vez mediante el hackeo de una depuradora para contaminar el agua (Zuloaga, 2018). En 2018, la policía italiana arrestó a un refugiado que intentaba envenenar el agua de una localidad y una base militar (Mic, 2018). Finalmente, a principios de 2021, un intento de hackeo en una planta potabilizadora en Florida, EE. UU., activó las alarmas de seguridad.

El agua es un recurso esencial continuamente utilizado por la ciudadanía. Dependemos de ella para beber, asearnos, y en múltiples contextos como hospitales, centros de salud e industrias. Su vital importancia en nuestra vida diaria la convierte en un potencial objetivo terrorista. Un ataque a este recurso podría alterar significativamente el funcionamiento normal de la sociedad, no solo a través del envenenamiento del agua, sino también mediante la interrupción de su suministro. Estas acciones terroristas pueden manifestarse de diversas maneras, desde el envenenamiento directo hasta el corte del suministro, que podría ocurrir a consecuencia de un ataque convencional contra las estaciones de tratamiento de aguas potables (ETAP) o mediante ataques cibernéticos.

Pero ¿hasta qué punto es real la posibilidad de producirse este tipo de ataque? En España actualmente nos encontramos en el nivel 4 de alerta antiterrorista, siendo el nivel 5 el más elevado. Este se decreta ante la previsión de un ataque inminente, permitiendo la movilización de las fuerzas armadas, lo que a la postre representa la mayor diferencia con las medidas adoptadas en el nivel actual. En el nivel 4 conlleva reforzar los mecanismos de seguridad en sectores estratégicos, incluyendo fronteras y aeropuertos.

A esto se añade que, a menudo, los terroristas buscan infundir miedo en la sociedad y obtener repercusión mediática. La historia ha demostrado que, tras un atentado, la ciudadanía suele temer el uso del medio en el que se llevó a cabo el ataque. Por ejemplo, los atentados del 11 de septiembre en EE. UU. (Pleterski, 2010), los del 11 de marzo en Madrid (Exceltur) o los del 17 de agosto en Barcelona (Salvatierra, 2017) resultaron en una disminución del uso del transporte público y la visita a lugares emblemáticos concurridos por un tiempo. Un ataque al agua tendría un impacto directo en nuestros hogares, un espacio considerado inviolable, donde solemos bajar nuestros niveles de alerta al sentirnos seguros.

Tipos de ataques

Desde los albores de la historia, han ocurrido innumerables ataques entre países, organizaciones y tribus con el objetivo de desestabilizar al enemigo, reducir sus resistencias o invadir sus territorios. Una táctica comúnmente empleada por las hordas enemigas era el

envenenamiento de ríos y pozos para privar a los habitantes de las zonas en conflicto de un recurso vital como el agua. Esto tenía el propósito de forzarlos a abandonar su lugar o a consumir alimentos y agua insalubres. Adrienne Mayor (2003) detalla este tipo de tácticas en su libro *Greek fire, poison arrows & scorpion bombs: Biological and chemical warfare in the ancient world*. Un ejemplo histórico presentado en este libro es el asedio de la ciudad griega de Cirra por los guerreros de Delfos durante la guerra entre la Liga Anfictiónica de Delfos y Cirra (595-585 a.C.), donde se envenenó el agua que llegaba a la ciudad con elébora, una planta angiosperma venenosa de la familia de las ranunculáceas.

Aunque pueda parecer una táctica bélica del pasado, el uso del envenenamiento como estrategia de guerra no ha desaparecido. Existen normativas que prohíben estas maniobras, reflejadas en el artículo 23 del reglamento de La Haya, que establece: "queda particularmente prohibido: a) Emplear veneno o armas envenenadas" (Convención II de La Haya, 1899, art. 23). Igualmente, en el DIH consuetudinario "se especifica que la prohibición de emplear veneno abarca, asimismo, el envenenamiento de pozos y otras redes de abastecimiento de agua" (Henckaerts & Doswald-Beck, 2007).

Hoy en día, esta práctica aún se observa en conflictos armados. Un ejemplo reciente es el ataque sufrido por Israel, donde una de sus plantas potabilizadoras fue objeto de una intrusión cibernética. El objetivo era modificar las cantidades de cloro en el agua, un ataque que Israel atribuye a Irán (Cembrero, 2020). Así, la posibilidad de un ataque a una ETAP por parte de un grupo terrorista es real y se puede dar en diversas formas y desde diferentes enfoques, como se ha evidenciado en los ejemplos anteriores, todos altamente peligrosos. Estos diversos tipos de ataques serán analizados en detalle a continuación.

Ataques físicos

Un ataque físico se define en esta investigación como una acción violenta y repentina contra las instalaciones de una ETAP. Este tipo de ataque tiene como objetivo interrumpir la prestación del servicio, en casos de menor gravedad, o causar la destrucción de las barreras de contención del agua. Esto último podría resultar en una gran inundación, provocando extensos daños materiales y humanos en las ciudades afectadas. Dentro de los posibles ataques físicos se debe distinguir entre:

> Aquellos cuyo fin pueda ser para hacerse con determinados productos, que, por su utilización en la potabilización del agua, se puedan encontrar en una ETAP y que posteriormente podrían ser usados en otros atentados de gran envergadura (como podría ser el caso de una bombona de gas cloro, que, en caso de ser manipulada de manera malintencionada, ocasionaría una nube tóxica que provocaría afecciones en las vías respiratorias de las personas que lo inoculasen o incluso la muerte), o de elementos precursores, que son aquellas sustancias que pueden ser usadas para la creación de explosivos y drogas, y que están regulados en el Reglamento (CE) nº 273/2004 del Parlamento Europeo y del Consejo, de 11 de febrero de 2004, sobre precursores de drogas (Boletin Oficial del Estado, 2004) y en el Reglamento (CE) nº 1277/2005 de la Comisión de 27 de julio de 2005, por el que se establecen normas

de aplicación para el Reglamento (CE) nº 273/2004 del Parlamento Europeo y del Consejo, sobre precursores de drogas, y para el Reglamento (CE) nº 111/2005 del Consejo, por el que se establecen normas para la vigilancia del comercio de precursores de drogas entre la Comunidad y terceros países.

Por otro lado, están los ataques dirigidos específicamente contra una ETAP con el objetivo de provocar una denegación de servicio a la ciudadanía o causar una alteración mediante el vertido de contaminantes en las piscinas de agua en diferentes etapas de tratamiento. El fin de estos ataques es convertir el agua en un producto no apto para el consumo o peligroso para la salud humana.

Entre los posibles ataques físicos se incluyen lo que usan vehículos, bien sea para superar las medidas de seguridad perimetrales o contra la barrera de control de acceso, lo que implica un riesgo de atropello para el personal de vigilancia y trabajadores de la ETAP. Finalmente, no se puede descartar el uso de explosivos en un ataque a una ETAP. Las posibilidades para perpetrar un atentado de este tipo son variadas, incluyendo desde el lanzamiento remoto de un misil teledirigido, ataques con drones, coches bomba, hasta el uso de chalecos bomba, como se ha mencionado antes.

En cualquier caso, un ataque de este tipo tendría una amplia repercusión mediática, algo que los terroristas buscan activamente. Como se ha dicho, la explosión de un artefacto, dependiendo del volumen y tipo de explosivo utilizado, podría causar daños incalculables, interrumpir el suministro de agua o, en el caso de un ataque al muro de contención de una presa, provocar su ruptura y una consiguiente inundación.

Otro aspecto relevante es el bajo costo y la facilidad de adquisición de los componentes para fabricar explosivos. Estos pueden elaborarse con acetona (comercializada como removedor de esmalte de uñas), peróxido de hidrógeno (conocido también como agua oxigenada), ácido clorhídrico (disponible en internet por poco más de cinco euros) y ácido sulfúrico (vendido en tiendas como desatascador de tuberías)

El principal desafío en la fabricación de este explosivo es su alta volatilidad. Es extremadamente sensible a las altas temperaturas, a los golpes y a la fricción, cualquiera de los cuales podría desencadenar una explosión no deseada. Además, este tipo de explosivo comienza a descomponerse aproximadamente a los diez días de su creación.

Es importante destacar que este tipo de reacción química no es detectable por los sistemas actuales de detección de explosivos en los aeropuertos, que se basan en la identificación de compuestos nitrogenados. Esto representa un desafío para las Fuerzas y Cuerpos de Seguridad del Estado (FFCCSS), ya que dificulta detectar la presencia de este material en caso de que se introduzca ilegalmente en el país.

Ataques químicos/biológicos

Estos son los ataques más peligrosos, ya que, de no detectarse, podrían envenenar o causar enfermedades a un gran número de habitantes de una ciudad. Por ejemplo, en la Comunidad Autónoma de Madrid, una sola ETAP da servicio a más de tres millones de personas. Si el

agua contaminada llegase a los hogares, estaríamos hablando de cientos de miles de personas que podrían sufrir envenenamiento inmediato o desarrollar enfermedades futuras. El agua se convierte, así, en un vehículo ideal para la propagación de estos ataques, dado que todos consumimos y dependemos de este recurso esencial en mayor o menor medida.

Esta situación generaría una sensación de inseguridad en la sociedad y podría colapsar otros servicios públicos, como el sanitario, que enfrentaría dificultades para atender al número tan elevado de personas que requerirían asistencia médica, lo que podría resultar en un número de defunciones inimaginable para la sociedad.

Los ataques químicos o biológicos, al igual que el uso de venenos, están prohibidos por los Convenios Internacionales. Sin embargo, esto no significa que todos los países hayan cesado la investigación o el uso de armas biológicas y químicas en ataques contra la sociedad. Un ejemplo de esto es el ataque ocurrido en mayo de 2019 en la provincia de Latakia, Siria, donde se utilizó gas cloro (EFE, 2019). Un ataque de este tipo se caracteriza por el uso de agentes químicos o biológicos que pueden causar infecciones, reacciones adversas, lesiones orgánicas, incapacidad temporal o incluso la muerte.

El Programa Internacional de Seguridad de las Sustancias Químicas, publicado por la Organización Mundial de la Salud (OMS), indica cuáles son las sustancias más peligrosas para la salud de los seres vivos. Estos componentes, presentes tanto en materia viva como inorgánica que forma parte de la vida diaria, pueden ser beneficiosos en cantidades adecuadas, mejorando las condiciones de vida. Sin embargo, en dosis elevadas, se vuelven altamente perjudiciales.

Entre los químicos que la OMS destaca está el *arsénico*, un compuesto extremadamente tóxico que puede causar intoxicaciones crónicas; el *benceno*, asociado a diversas enfermedades crónicas, incluyendo ciertos tumores cancerígenos; el *cadmio*, perjudicial para los sistemas renal, óseo y respiratorio; las *dioxinas*, con una durabilidad permanente; el *flúor*, que en exceso es dañino para el sistema óseo; el *plomo*, un metal pesado muy tóxico con amplios efectos nocivos en la salud global; y el *mercurio*, que representa una amenaza para los fetos humanos y en las primeras etapas de la vida (OMS, 2021).

Un lugar aparte ocupan los disruptores endocrinos, sustancias químicas externas que causan graves problemas de salud al alterar los niveles hormonales y afectar su equilibrio y funcionalidad. Sus efectos son especialmente peligrosos porque no son inmediatos y no presentan síntomas clínicos identificables. Estas sustancias se encuentran en detergentes, cosméticos, perfumes y en los ya mencionados pesticidas o plaguicidas.

Ataques cibernéticos

Con el auge de internet y las tecnologías de información y comunicaciones (TIC), así como la creciente digitalización de procesos, se ha generado una nueva vulnerabilidad en la seguridad que las IC de los Estados deben considerar. La implementación de la tecnología 5G ha incrementado aún más el riesgo de ataques cibernéticos, puesto que ofrece a los atacantes mayor anonimato y una capacidad de ataque más rápida y difícil de prever.

Un ataque cibernético se define como cualquier intento de acceso remoto no autorizado a un ordenador o dispositivo conectado a la red. El propósito de estos ataques puede ser controlar el sistema para extraer información, destruir datos o alterar el funcionamiento normal del dispositivo. Esto puede ser con fines de lucro, exploración de vulnerabilidades de seguridad, o para interrumpir un suministro. Estos ataques se ejecutan mediante algoritmos lógicos y códigos maliciosos que se insertan en los archivos del ordenador, corrompiendo tanto el dispositivo como sus comunicaciones y comprometiendo la seguridad de toda la red a la que pertenece.

Las intrusiones cibernéticas pueden ocurrir de diversas maneras. Una es la interceptación de comunicaciones que el objetivo realiza con otros dispositivos a través de la red. Otra manera es la infestación del equipo al conectarle físicamente un dispositivo externo que contenga *malware*. Este *software* malicioso está diseñado para infiltrarse en un dispositivo sin autorización del propietario con el fin de robar, manipular, eliminar o secuestrar la información almacenada.

Es importante destacar que no todos los ataques cibernéticos deben considerarse maliciosos. Dentro de la comunidad *hacker* existen quienes utilizan sus habilidades informáticas y conocimiento de redes para acceder a sistemas burlando las medidas de seguridad. Sin embargo, su objetivo es informar a las empresas sobre estas brechas de seguridad, en lugar de explotarlas para fines ilícitos. Son conocidos como *hackers* éticos o de sombrero blanco (Jaimovich, 2018).

El verdadero problema surge con los *hackers* de sombrero negro, que buscan beneficios personales. Estos actúan extorsionando directamente a la empresa afectada o vendiendo información robada en el mercado negro, comúnmente a través de la DeepWeb o la DarkWeb, donde los terroristas podrían acceder a dicha información y utilizarla para perpetrar ciberataques. Cuando el objetivo de estos ataques es infundir miedo en la sociedad o desestabilizar el funcionamiento de infraestructuras críticas, como una ETAP, se consideran actos de ciberterrorismo.

Entre los diferentes tipos de ataque cibernético se encuentran los siguientes (AyudaLey, 2018):

- *Troyanos:* Nombrados así por el caballo de Troya de la mitología, se camuflan como *software* legítimo. Requieren que el usuario los ejecute o instale en el dispositivo para infectarlo. Son peligrosos porque pueden instalarse involuntariamente, por ejemplo, a través de un pendrive conectado a la CPU de un ordenador. Una vez en el sistema, pueden servir como puerta de acceso a otros *malwares*, robar información o tomar el control remoto del dispositivo infectado.
- *Virus:* Son programas o códigos diseñados para autorreplicarse e infectar otros dispositivos a través de la red, con el objetivo de controlar las operaciones del equipo infectado. Comúnmente, estos virus destruyen la información contenida en el dispositivo.

- *Spyware:* Este tipo de *malware* suele ocultarse dentro de otro *software* o archivo, aunque también puede activarse remotamente mediante *plugins* o extensiones para navegadores de internet. Su función principal es espiar las actividades realizadas en el dispositivo afectado para obtener información relevante.
- *Phishing:* Este método es ampliamente utilizado para engañar y robar datos a las víctimas. Consiste en enviar correos electrónicos que aparentan ser de organismos estatales o entidades bancarias. Estos correos informan sobre una supuesta incidencia que requiere solución a través de un enlace, donde se solicitan datos personales de la víctima.
- *Ransomware:* En este tipo de ataque, el ordenador queda "secuestrado" por los atacantes. La pantalla muestra un mensaje informando sobre el secuestro y las instrucciones para la liberación del dispositivo, generalmente el pago de un rescate en bitcoins u otra moneda digital.
- *Gusano:* Este *malware* se autorreplica y crea copias de sí mismo en diferentes ubicaciones. Se propaga a través de listas de contactos y otros medios.
- *Denegación de servicio (DoS o DDoS):* Este ataque implica el envío masivo de solicitudes a un servidor con el objetivo de sobrecargarlo y provocar su colapso. Esto resulta en la caída del servidor y la inoperatividad de cualquier sitio web alojado en él. Puede presentarse como DoS, donde las solicitudes provienen de un solo ordenador, o DDoS, donde se utilizan múltiples ordenadores o redes, a menudo controlados sin el conocimiento de sus propietarios (una Botnet), para lanzar el ataque.

El Incibe-Cert (s.f.), canal específico de comunicación entre los Equipos de Respuesta a Incidentes Nacionales de Referencia (CSIRT) y la Secretaria de Estado de Seguridad (SES), y que opera junto al Centro Nacional de Protección de Infraestructuras Críticas (CNPIC) cuando se trata de la gestión de incidentes referentes a operadores críticos, registró en 2019 un aumento de las gestiones por incidentes en infraestructuras críticas del 13,29% respecto del año anterior, hasta llegar a la cifra de 818 incidentes, de los cuales el 20,29% de estas acciones tuvieron que ver con la intromisión de *malware*. Entre los sectores estratégicos que gestiona el CSIRT, el 7,8% tuvieron que ver con el sector del agua, según información del Gobierno de España a través del "Estudio sobre la cibercriminalidad en España", que elabora el Ministerio del Interior (Cereceda Fernández-Oruña et al., 2019).

Análisis de los sistemas de seguridad

Los sistemas de seguridad son dispositivos, ya sean físicos, lógicos o personales, fijos o móviles, destinados a preservar la integridad de bienes muebles e inmuebles, y la de las personas que se encuentran bajo su protección. Están diseñados para prevenir la acción delictiva de un adversario que pretenda atacar la instalación asegurada. En caso de que la prevención

falle, su operatividad se orienta hacia la detección del intruso, el retraso del asalto, o su interrupción y neutralización.

Los sistemas de seguridad se clasifican en pasivos y activos. Los sistemas de seguridad pasivos no evitan que la intromisión se produzca, pero facilitan la detección de la misma o la retrasan, como es el caso de los muros, vallas, cámaras. Por otro lado, los sistemas de seguridad activos se caracterizan por su proactividad, e incluyen sistemas lógicos de seguridad como las contraseñas y el control de accesos.

A continuación se analiza el caso del sistema de seguridad de la infraestructura de suministro de agua en la Comunidad Autónoma de Madrid. En la actualidad, gracias a la instalación de más de 900 cámaras de seguridad, se cuenta con vigilancia en el 45 % de las instalaciones, entendidas como tal aquellas en las que hay algún tipo de construcción edificada. En lo que se refiere a la ETAP, está ubicada en un enclave geográfico junto a la presa que le suministra el agua, con una orografía montañosa que dificulta su acceso. Su seguridad está compuesta por vallas perimétricas que delimitan la instalación, con malla electrosoldada de más de tres metros de altura y coronadas con concertinas (alambre de espino en espiral), lo que impide que sean saltadas.

Igualmente, el perímetro se encuentra protegido mediante avisadores acústicos, altavoces IP, que advierten a los intrusos de su acceso a una zona restringida y ofrecen mensajes de voz que facilitan instrucciones en caso de emergencia. Estos altavoces están dotados de una memoria que permite grabar mensajes preestablecidos que pueden alternarse con los mensajes en directo que requieran enviar los operarios. Además, su sistema de comunicación IP es compatible con los sistemas de análisis de video, por lo que estos pueden activarse mediante los procesadores si es detectada una intromisión.

La estación se encuentra dotada de cámaras de seguridad bispectral por IP, lo que permite que, en caso de avería del terminal, no se vea comprometido el resto de la instalación; solo se necesita sustituir dicho elemento mientras el resto de componentes siguen operativos. Además, cuentan con un sistema de inteligencia artificial (AI) capaz de analizar las imágenes de video y detectar e identificar el contorno del objeto, por lo cual se puede distinguir entre animales, vehículos, camiones o personas. Esto facilita programar diferentes alertas en función del objeto detectado y seguirlo durante su desplazamiento.

La conexión mediante IP de los sistemas de seguridad permite la intercomunicación entre las diferentes cámaras y sensores. Así, si una de estas cámaras detecta una intrusión, puede activar de forma autónoma al resto de cámaras para que se enfoquen en la amenaza identificada. Además, el *software* instalado en estas cámaras, junto con su AI, permite al operador establecer distintas zonas de alerta. Si estas zonas son transitadas, se activarán las alarmas correspondientes.

En lo que respecta a la seguridad a través de cámaras de vigilancia, la protección exterior de la planta se ve reforzada por la incorporación de cámaras con sensor térmico. Estas cámaras son eficaces para advertir sobre intrusos a mayor distancia y en condiciones visua-

les adversas donde otros sistemas de vigilancia podrían fallar. Utilizan la radiación de calor emitida por los objetos, en función de su temperatura, para detectar accesos no autorizados, operando independientemente de la luminosidad exterior y manteniendo la privacidad de las personas. Además, estas cámaras pueden detectar incendios, fugas de gas o cambios de temperatura en maquinarias, emitiendo alertas correspondientes.

La seguridad perimetral de la estación también se fortalece con radares inteligentes de 180º de cobertura. Gracias a su avanzada AI, que se perfecciona con cada escaneo, estos radares son capaces de detectar y rastrear cuerpos móviles de forma precisa y con un bajo margen de error. El interior de las instalaciones se encuentra protegido con cámaras domo 360º, dotadas de cuatro sensores con una calidad de 5 MP para brindar una imagen continua de gran calidad. Los objetivos que monta esta cámara son autoenfocables y su calibración de posición no es fija, lo cual facilita una configuración muy precisa a la hora de su visualización.

Todas estas cámaras funcionan de manera autónoma, con analíticas integradas. Sin necesidad de un grabador en la instalación, pueden activar, según su configuración, cualquiera de las salidas del módulo IP, ubicado junto a la Central de Intrusión. De esta forma, conforme al reglamento de seguridad privada, envían al Centro de Control (CRA) la información de la zona activada. Paralelamente, la información de video puede ser transmitida al CRA para que el operador verifique la causa de la incidencia. El control de acceso al recinto está a cargo de vigilantes de seguridad, quienes cuentan con el apoyo de cámaras en su puesto operativo y lectores de tarjetas para identificar a las personas que intentan acceder.

La seguridad física está supervisada desde un puesto de control central ubicado en las oficinas centrales de la compañía. Desde allí, se tiene acceso a todas las imágenes y comunicación directa con el personal. Este sistema implementado es inverso al que existía antes para mejorar la eficiencia: ahora es el puesto de control quien inicia la comunicación con los vigilantes o el equipo en campo, lo que permite un intercambio de información directo y rápido mediante un código de respuestas. Esto soluciona el problema previo, donde los vigilantes debían esperar en "cola" para comunicarse con el control.

En este puesto de control también se cuenta con geolocalización de todos los vehículos disponibles, lo que permite comisionar al más cercano a una incidencia y así reducir los tiempos de respuesta. La sala de control está protegida por un sistema conocido como "operador muerto", que analiza el movimiento de los operarios en su interior y emite una alarma si no detecta movimiento.

En cuanto a la seguridad del agua, se fundamenta en el uso de autómatas distribuidos a lo largo de todo el proceso de potabilización, para supervisar sus diferentes etapas: preoxidación, precoloración, preozonización, coagulación, floculación y sedimentación; decantación; filtración rápida sobre lecho de arena; neutralización (ajuste de pH), y desinfección (Canal de Isabel II). Controlan y analizan continuamente los parámetros del agua (cloro residual, amonio, pH, aluminio y turbidez), asegurándose de que se mantengan dentro de

los estándares establecidos por las directivas de la Unión Europea. Para asegurar la calidad del agua, se utilizan diversos reactivos en el proceso de potabilización. Si estos parámetros no se corresponden con los óptimos establecidos, se genera una alarma en la Sala de Control para que el operador gestione la situación.

De manera paralela al control ejercido por estos dispositivos automáticos, se llevan a cabo controles de calidad y análisis de parámetros químicos y bacteriológicos en el laboratorio de la propia planta. Estos análisis se realizan siguiendo las recomendaciones de la Comisión Europea mediante tecnologías avanzadas, incluyendo métodos para determinar la toxicidad, medir los niveles de ATP (trifosfato de adenosina), inmunoensayos, cromatografías de gases, PCR para la reacción en cadena de la polimerasa, y tecnologías de secuenciación (Coelho, Batlle Ribas, & Coimbra, 2020). Estos procedimientos aseguran un seguimiento exhaustivo y preciso de la calidad del agua, complementando la vigilancia automatizada.

Los autómatas están conectados con la Sala de Control, donde se encuentra un cuadro sinóptico general que permite monitorear el proceso en cada una de sus fases y el estado de los equipos. Este sistema está integrado por un ordenador que actúa como receptor de información y emisor de órdenes para los autómatas. El núcleo de este sistema es un *software* SCADA (Supervisory Control and Data Acquisition), diseñado para analizar y supervisar las operaciones de los autómatas. Proporciona datos telemétricos de manera remota y cuenta con controladores lógicos que gestionan los procesos de forma autónoma o mediante intervención humana cuando es necesario. Este sistema también es capaz de generar informes a partir de los datos recopilados.

Además de los sistemas de seguridad ya mencionados, la empresa implementó un sistema de canalización para el agua depurada, diseñado como dos anillos controlados por válvulas de apertura remota, que permiten cortar o habilitar el paso del agua. Así, en caso de detectar que un ataque ha tenido éxito y el agua está contaminada, es posible cerrar la entrada de agua a uno de los anillos, manteniendo el suministro a la población desde otra ETAP.

Al margen de los sistemas de seguridad descritos anteriormente, gestionados por la empresa privada como operadores críticos, el CNPIC, como órgano estatal, es responsable de las políticas y actividades de seguridad de estos servicios esenciales. El CNPIC, por supuesto, colabora estrechamente con las empresas para garantizar la integridad de estas instalaciones.

Para ello, el CNPIC ha elaborado directrices que sirven como base para los planes de seguridad que las IC deben desarrollar, conforme a la Ley 8/2011. Estos planes se enmarcan dentro del Plan de Seguridad de Infraestructuras Críticas, desarrollado en mayo de 2007, y que ha sido declarado como documento clasificado.

Los responsables de la empresa deben elaborar dos instrumentos de planificación para proteger la infraestructura, cumpliendo así con lo establecido en el Real Decreto 704/2011 sobre la protección de infraestructuras críticas:

1. El *Plan de Seguridad del Operador*, que establece la estrategia general que seguirá el operador para garantizar la seguridad de la instalación, junto con el *Plan de Protección Específico*, que detalla las medidas concretas que el operador debe implementar para abordar diferentes escenarios de riesgo y amenazas específicas a la infraestructura.
2. El *Plan de Emergencia*, en cumplimiento de la Directriz Básica de Planificación ante Riesgos de Inundaciones. Este plan define las actuaciones que deben llevarse a cabo por todos los activos implicados (empresa, Protección Civil, FFCCSS, Cuerpo de Bomberos, Personal Sanitario de Urgencias) en caso de una incidencia en la presa o en las instalaciones de la ETAP.

Marco jurídico de aplicación

La legislación actual, tanto europea como española, establece criterios claros sobre la protección de las IC. No obstante, existe una carencia en cuanto a la responsabilidad penal específica para delitos contra estas infraestructuras en los textos normativos. La Directiva Europea 2008/114/CE del 8 de diciembre de 2008 define la importancia de estas infraestructuras así:

> El elemento, sistema o parte de este situado en los Estados miembros que es esencial para el mantenimiento de funciones sociales vitales, la salud, la integridad física, la seguridad, y el bienestar social y económico de la población, cuya perturbación o destrucción afectaría gravemente a un Estado miembro al no poder mantener esas funciones.

A pesar de esto, los ataques a estas infraestructuras deben ser encajados dentro de otros delitos ya tipificados a los que puedan asemejarse. Esta falta de especificidad legal podría hacer que las organizaciones criminales consideren atentar contra estas instalaciones, ya que las violaciones a la seguridad de las IC podrían acarrear penas menores en comparación con otros delitos.

No fue hasta el año 2004, tras los atentados del 11 de marzo en Madrid, cuando el Consejo Europeo instó a la Comisión Europea a desarrollar una estrategia global para la protección de las IC, lo cual condujo a la creación de la "Comunicación sobre protección de las infraestructuras críticas en la lucha contra el terrorismo". Esta comunicación presentaba una serie de propuestas enfocadas en mejorar la prevención, preparación y respuesta de Europa ante acciones terroristas que afectaran a estos servicios esenciales.

En 2005, se publicó el *Libro verde sobre el Programa Europeo para la Protección de Infraestructuras Críticas* (PEPIC), que marcó el inicio de este programa y la creación de la Red de Información sobre Alertas en Infraestructuras Críticas (CIWIN, por sus siglas en inglés). Este documento subrayó la necesidad de fortalecer la seguridad de las IC y de reducir sus vulnerabilidades, así como de establecer canales de comunicación efectivos entre todos los actores implicados en la seguridad de estas instalaciones.

El programa PEPIC identificaba todas las amenazas a las que estas infraestructuras están expuestas, incluyendo tanto las de origen natural como las causadas por el hombre, con especial énfasis en las amenazas terroristas. El PEPIC estableció que la responsabilidad de la protección de estas infraestructuras recae tanto en los Estados dentro de sus fronteras como en los operadores críticos, delineando un marco de responsabilidad compartida y cooperación.

En 2008, para reforzar la estrategia de protección de las IC, se promulgó la Directiva 2008/114/CE del Consejo, del 8 de diciembre, sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección. Esta directiva definió conceptos clave en la protección de las IC, como el propio término de *infraestructura crítica*, el análisis de riesgo, el significado de protección en este contexto y la identificación de propietarios u operadores de IC europeas, entre otros.

En su primera versión, la directiva no incluyó las estaciones hídricas en la lista de IC. Centraba su atención en los sectores de energía (electricidad, petróleo y gas) y transportes en todas sus modalidades. Fue con la publicación de la "Directiva NIS" que se reconoció finalmente la importancia del sector hídrico dentro de la sostenibilidad de los Estados, lo que amplió así el alcance y la cobertura de la directiva para incluir un sector vital para la vida diaria y la seguridad de la población.

Conviene recordar que una IC se refiere a los sistemas, redes, activos y servicios físicos y de información cuyo funcionamiento ininterrumpido es esencial para garantizar la seguridad nacional, la salud, la economía y la seguridad pública de una nación. Estas infraestructuras pueden incluir, entre otras cosas, servicios de energía, telecomunicaciones, transporte, agua y saneamiento, servicios de salud y sistemas financieros. La interrupción o destrucción de estas infraestructuras puede tener un impacto significativo en la salud, la seguridad, la economía o el bienestar social de la nación.

En la cúspide de la legislación nacional existente se encuentra la Constitución Española (CE), que, si bien no desarrolla articulado alguno sobre la protección de las IC, sí otorga garantías jurídicas a la acción del Estado en materia de seguridad pública. Por ello, tanto la LPIC como el reglamento que la desarrolla, el Real Decreto 704/2011, han emanado de esa competencia atribuida por la CE al Estado. De igual manera, la CE atribuye en su artículo 104 a las FFCCSS la responsabilidad de "garantizar la seguridad ciudadana" (Constitución Española, 1978).

Dentro del marco constitucional español, existe un conjunto de leyes que regulan la responsabilidad en la seguridad de las infraestructuras, que abarcan aspectos físicos, cibernéticos y de protección de datos. Entre estas leyes se incluye la Ley 9/68, de 5 de abril, Reguladora de los Secretos Oficiales, a la cual se acogen los Planes de Seguridad de las IC.

Asimismo, está la Ley Orgánica 10/1995 de 23 de noviembre, del Código Penal (CP), que, aunque no se refiere específicamente a las IC, contempla delitos relacionados con ciberataques y ciberterrorismo, como el acceso indebido e ilegítimo a sistemas informáticos con la intención de borrar, dañar o interrumpir su funcionamiento (CP, arts. 264 y ss.). Allí también se contemplan modalidades delictivas relacionadas con el "descubrimiento y revelación de secretos e informaciones relativas a la Defensa Nacional" (CP, cap. III, Título XXIII, arts. 598 y 603).

También se encuentra la LO 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal, cuyo objeto es garantizar y proteger los datos personales de las personas, así como el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el reglamento para su desarrollo.

También está la Ley 8/2011, de 28 de abril, establecida para proteger las IC. Esta legislación responde a la necesidad de cumplir con la Directiva Europea, no solo en términos de protección de las IC, sino también en la descripción de un sistema organizativo para la salvaguarda de los servicios esenciales e involucrar a todos los actores relevantes. A raíz de esta ley, se creó el CNPIC, dependiente de la Secretaría de Estado de Seguridad. Su promulgación tuvo la clara intención de establecer las medidas necesarias para asegurar la seguridad en las IC, especialmente ante actos violentos y, más específicamente, ante amenazas de carácter terrorista.

El desarrollo de esta ley se realizó a través del Real Decreto 704/2011, de 20 de mayo, que aprobó el Reglamento de Protección de las Infraestructuras Críticas, con el propósito de detallar y expandir los aspectos cubiertos por la LPIC, y, en concordancia con la transposición obligatoria de la Directiva 2008/114/CE, establecer los planes que deben elaborar las instituciones afectadas para proteger las IC.

Además, la Ley 5/2014, de 4 de abril de 2014, de Seguridad Privada, aún en fase de desarrollo reglamentario, regula la prestación de servicios de seguridad por parte de entidades privadas, tanto personas físicas como jurídicas. Esta ley se enfoca en la protección de bienes materiales y humanos, y establece el modelo para la coordinación entre empresas y personal de seguridad privada con las FFCCSS.

Por su parte, la LO 4/2015, de 30 de marzo, de Protección de la Seguridad Ciudadana (LOPSC), confiere la protección de las infraestructuras e instalaciones en las que se prestan servicios básicos para la comunidad, entendiendo por tales los "Servicios de suministro y distribución de agua, gas y electricidad". Sin embargo, la protección de estas instalaciones es llevada a cabo por empresas privadas de seguridad, eso sí, bajo una estrecha colaboración con las FFCCSS. En cuanto a su función sancionadora, esta ley solo prevé sanciones administrativas, no penales, tal y como se refleja en su sección 3.ª (art. 45), donde se establece que no se pueden imponer sanciones administrativas por hechos que ya hayan sido sancionados penalmente. En los casos en que las acciones puedan considerarse delitos, se deben transferir a la autoridad penal competente; mientras se resuelve

el proceso penal, ya sea con una sentencia firme o con la decisión de no proceder por delito, se interrumpe el plazo para la prescripción de la sanción administrativa.

La Ley 17/2015, del Sistema Nacional de Protección Civil, es fundamental para la protección de personas y bienes frente a emergencias y catástrofes, tanto de origen humano como natural. Esta ley establece los conceptos clave en el ámbito de la protección civil y la gestión de emergencias. Su desarrollo legislativo (RD 407/1992, de 24 de abril; RD 393/2007, de 23 de marzo) proporciona un marco para la elaboración de los Planes de Protección Civil y Autoprotección, incluyendo la creación de registros y la definición de las funciones de la Comisión Nacional de Protección Civil.

La Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, está organizada en cinco títulos: uno preliminar y cuatro adicionales. El primer título se centra en los Órganos competentes de la Seguridad Nacional. El segundo título aborda los Sistemas de Seguridad Nacional. El tercer título trata sobre la Gestión de crisis en el marco del Sistema de la Seguridad Nacional. Finalmente, el cuarto título se dedica a la Contribución de recursos a la Seguridad Nacional (Boletín Oficial del Estado, 2015). Otra legislación española que afecta al sector del agua, tal y como se recoge en el sitio web del CNPIC, son las que presenta Vidal Delgado (2017).

Las IC del sector hídrico están protegidas en el marco del Plan Nacional de Protección de Infraestructuras Críticas, diseñado con el propósito de definir los criterios y directrices esenciales para mantener la seguridad de las IC y ha sido declarado como documento clasificado. Su objetivo se persigue a través de la implementación y articulación de programas y medidas preparadas para activarse en caso de ataque; el fomento de una cultura de colaboración entre las distintas instituciones partícipes en el catálogo de IC, gracias al intercambio de información relevante y un marco para mitigar las consecuencias derivadas de una crisis.

Asimismo, están cobijadas por la Estrategia de Seguridad Nacional de 2017, donde se destaca su importancia y se señalan como principal amenaza los actos terroristas yihadistas. La estrategia establece como objetivo "asegurar la correcta provisión de los servicios esenciales para la sociedad, haciendo más robusto y resiliente el sistema de infraestructuras críticas sobre el que se sustenta" (Presidencia del Gobierno, 2017). Para alcanzar este fin, determina líneas de acción orientadas a cumplir la legislación de protección de las IC y fortalecer su seguridad mediante la planificación, prevención, reacción, mitigación y restauración de servicios. Además, promueve la cooperación entre los sectores público y privado, fomentando el intercambio de información entre entidades y velando por la innovación en seguridad y la colaboración internacional (Presidencia del Gobierno, 2017).

Igualmente, la Estrategia Española de Ciberseguridad 2019, siguiendo las bases de sus versiones anteriores de 2013 y 2017, enfoca sus acciones en la protección de las IC contra ciberataques. Esto se lleva a cabo mediante la implementación del Esquema

Nacional de Seguridad y asegurando el cumplimiento de las normativas relacionadas con la seguridad de las IC, en vista de los riesgos cibernéticos a los que están expuestas.

Como se observa, el conjunto de normativas existentes relativas a las IC, especialmente en lo concerniente al agua, consiste meramente en leyes que buscan proteger los sectores estratégicos, mas no contemplan sanciones ante las acciones punitivas. Esta responsabilidad, por ende, recae en el Estado, pero para ejercerla debe cumplir con una doble garantía, tal como se establece en la CE: "Nadie puede ser condenado o sancionado por acciones u omisiones que en el momento de producirse no constituyan delito, falta o infracción administrativa, según la legislación vigente en aquel momento" (art. 25.1). Esto implica que no se puede sancionar ninguna acción que no esté previamente definida como punible (garantía formal) y que tal acción debe estar claramente descrita en una ley (garantía material).

Resulta llamativo que en las leyes descritas, dedicadas a la protección de las IC, no se especifiquen las sanciones para acciones que atenten contra la seguridad de estas instalaciones. Esto es especialmente relevante dado que el propósito de estas leyes es asegurar la seguridad de infraestructuras que proveen servicios esenciales para la sociedad, de modo que la ausencia de un marco sancionador específico las deja expuestas a cualquier ataque, incluyendo los de naturaleza terrorista.

Entre las leyes discutidas, solo las normativas supletorias, como la LOPSC, contemplan la posibilidad de imponer sanciones. En su disposición adicional segunda, se establece: "La protección de las infraestructuras críticas se regirá por su normativa específica y supletoriamente por esta Ley". Ante la falta de sanciones en la Ley 8/2011, la responsabilidad de sancionar recae en la LOPSC, a través de los artículos 35.1 y 36.9, como se ha dicho. Las sanciones, al ser administrativas, deben ser impuestas por la autoridad administrativa competente. Su cuantía puede oscilar entre 30001 y 600000 euros, considerando que la mayoría de acciones contra una IC podrían clasificarse como infracciones muy graves.

Por otro lado, la Ley 5/2014, de 4 de abril, de Seguridad Privada, establece un marco sancionador para las entidades, el personal y los usuarios de la seguridad privada, tal como se menciona en su preámbulo. Resulta curioso que, siendo las IC usuarios de la seguridad privada, esta ley también contemple sanciones para ellas. Por ejemplo, una ETAP podría ser sancionada en caso de sufrir un ataque malicioso si se considerase que ha incumplido con el art. 59.1., que se refiere a "La falta de adopción o instalación de las medidas de seguridad que resulten obligatorias". Esto se clasifica como una infracción muy grave para los usuarios de la seguridad privada, según dicha ley.

En efecto, para acciones punibles dirigidas contra las ETAP o sus servicios, la única opción para buscar sanciones privativas de libertad reside en el CP. Aunque no hay una tipificación específica para delitos contra las IC, en el CP es posible encajar estos ataques dentro de preceptos ya existentes. Un ejemplo es el artículo 325, que protege los recursos naturales y el medio ambiente. Este artículo sanciona a quien provoque o realice emisiones, vertidos, radiaciones, extracciones, entre otros, que causen o puedan causar daños sustanciales a la

calidad del aire, del suelo, de las aguas, o a la fauna y flora. Por lo tanto, un ataque que resulte en la contaminación de los recursos hídricos podría ser considerado bajo este artículo, aplicando penas de prisión, multas y la inhabilitación para ejercer ciertas profesiones u oficios. Encontramos también mención a delitos llevados a cabo contra las aguas en el Título XVII del CP (art. 343).

Visto lo anterior, cabría preguntarse cómo se han castigado los ataques a las aguas en el territorio nacional español. En el caso de Abdellatif Aoulad, quien en 2011 planeó envenenar las aguas potables de un complejo turístico en el sur de España, la condena fue de dos años de prisión según la sentencia de 12 de julio de 2013 de la Sección 2.ª de la Sala de lo Penal (SAN 3593/2013 y STS 474/2014). En este caso, la condena se debió a la difusión de videos de ideología terrorista, ya que el delito planeado de envenenamiento no se llegó a realizar.

En casos consumados de acciones contra el agua, existen varias sentencias condenatorias en España. Por ejemplo, la STS 875/2006 de 06 de septiembre de 2006 condenó a un hombre a tres años y seis meses de prisión por vertidos incontrolados de residuos que contaminaron agua subterránea y pozos. En la STS 411/2012 de 18 de mayo de 2012, se confirmó la sentencia de la Audiencia Provincial de Barcelona imponiendo dos años de prisión por vertidos incontrolados de sustancias contaminantes en un río. Además, una sentencia del Juzgado de Instrucción n.º 2 de Guadalajara condenó a seis meses de prisión a un conductor de camión cisterna por un delito contra el medio ambiente, al verter combustible por error en la red general de agua (EDCM/EP, 2019).

En la legislación española, se observa una notable diferencia en la responsabilidad penal de los ataques a las IC, si se la compara con la descripción en el CP de aquellas acciones que deben considerarse como actos terroristas en sus diferentes figuras y la punibilidad que acarrean. Mientras que los artículos del 573 al 580 bis del CP establecen penas por la comisión de este tipo de ilícito penal que pueden llegar hasta la prisión permanente revisable "si se causara la muerte de una persona" (CP, art. 573) o hasta los quince años en casos en que "se causara cualquier otra lesión" (CP, art. 574).

Así se han dictado condenas por pertenencia o apoyo a bandas terroristas. Por ejemplo, la sentencia SAN 1845/2021, de 4 de mayo, condenó a dos personas a dos años y un día de prisión por un delito de autoadoctrinamiento terrorista, por su actividad en apoyo a la organización terrorista Daesh. Asimismo, la STS 608/2013, de 17 de julio, confirmó penas de seis años de prisión a dos individuos por su pertenencia activa a una banda terrorista. En casos de asesinato terrorista, la sentencia AN 75/2010 de la Audiencia Nacional impuso treinta años de prisión por este comisión y otros catorce intentos de asesinato.

Frente a esta gravedad, no existe una tipificación similarmente rigurosa para los ataques contra las IC. Esto resulta significativo, considerando que los ataques a las IC pueden tener un impacto grave y podrían, en ciertos casos, equipararse a actos de terrorismo. La disparidad en la legislación resalta la necesidad de revisar y posiblemente fortalecer las

sanciones aplicables a los ataques contra las IC, especialmente cuando estos actos pueden representar una amenaza seria a la seguridad y el bienestar de la sociedad.

Conclusiones

La seguridad en las IC, especialmente en el sector hídrico, cobra cada vez mayor importancia. La concienciación y acción tanto de los Estados como de los operadores son cruciales para legislar y planificar en aras de la seguridad de un recurso cada vez más escaso y esencial para la vida. Una acción aparentemente simple, como disolver una sustancia en el agua durante su tratamiento y distribución a la población, puede tener consecuencias catastróficas. Un ataque a un recurso tan vital puede provocar envenenamientos o enfermedades. Además, los efectos no siempre son inmediatos; pueden manifestarse tardíamente, lo que complica la detección del origen del problema. Para cuando se identifique, servicios esenciales como la sanidad podrían verse abrumados y, posiblemente, colapsados.

Aunque hasta ahora la mayoría de los países no han experimentado ataques directos contra ETAP, la historia y el análisis presentado en este trabajo muestran tentativas de ataques a diversas plantas potabilizadoras, como las vinculadas a la organización terrorista Al-Qaeda. Además, los servicios de inteligencia han identificado a las ETAP como posibles objetivos críticos para atacar a la población a través del suministro de agua. El hecho de que un ataque parezca poco probable no significa que no pueda suceder. Es lo que se conoce en inteligencia como el sesgo del cisne negro; ignorar una amenaza potencial, aunque parezca improbable, puede tener consecuencias catastróficas si finalmente se materializa.

Por lo tanto, a pesar de las medidas de seguridad implementadas en las ETAP, resulta fundamental trabajar la inteligencia en todos los niveles, desde la empresa de seguridad hasta las FFCCSS y los responsables civiles, fomentando la colaboración entre ellos. La cooperación no solo debe ser nacional entre la seguridad pública y privada, sino también internacional, conforme lo establece la Directiva 2008/114/CE, para mitigar o minimizar las consecuencias de un posible ataque terrorista.

Además, se destaca la importancia de modificar la normativa para promover una prevención general y especial en este ámbito. Para prevenir, detectar y erradicar este tipo de amenazas, es crucial establecer una protección jurídica penal adecuada, elevando el nivel de seguridad legal en torno a las IC y sus posibles vulnerabilidades.

Agradecimientos

El autor desea agradecer a la Universidad Nebrija y a la Escuela Superior de Guerra “General Rafael Reyes Prieto” por su apoyo en la realización de este artículo.

Declaración de divulgación

El autor declara que no existe ningún potencial conflicto de interés relacionado con el artículo.

Financiamiento

El autor no declara fuente de financiamiento para la realización de este artículo.

Sobre el autor

Adrián Nicolás Marchal González es doctor en derecho, Universidad de Castilla-La Mancha, Ciudad Real, España; licenciado en criminología, Universidad Camilo José Cela, Madrid, España; licenciado en derecho, Universidad Carlos III de Madrid, España, y abogado en ejercicio. Es director del Departamento de Seguridad y Defensa de la Universidad Nebrija y director del Máster en Análisis de Inteligencia y Ciberinteligencia de la Universidad Nebrija, Madrid.

https://orcid.org/0000-0001-8647-1214 - Contacto: amarchal@nebrija.es

Referencias

Acosta, R. (2009, 9 de junio). Rogue MILF rebels poison water source of soldiers, local residents. *Business Mirror*. http://tinyurl.com/2ctcmcty

AyudaLey. (2018, 8 de octubre). Qué es un ciberataque y qué tipos existen. http://ayudaleyproteccionu datos.es/2018/10/08/ciberataque/

BBC News. (2010, 14 de mayo). County Durham terror plot father and son are jailed. http://tinyurl.com/m3uyz4bb

Cereceda Fernández-Oruña, J *Informe de la evolución de los delitos de odio en España 2019*. (2019). . Oficina Nacional de Lucha Contra los Delitos de Odio : Ministerio del Interior Secretaria de Estado de Seguridad Gabinete de Coordinación y Estudios.

Coelho M. R. Batlle Ribas M. Coimbra M. F. & European Commission Joint Research Centre. (2020). *Review of technologies for the rapid detection of chemical and biological contaminants in drinking water : erncip chemical and biological risks to drinking water thematic group*. Publications Office of the European Union. January

Comité Internacional de la Cruz Roja (CICR). (1977). *Protocolo I adicional a los Convenios de Ginebra de 1949 relativo a la protección de las víctimas de los conflictos armados internacionales*. https://goo.gl/51FWdS

Convención II de La Haya. (1899). *Relativa a las leyes y usos de la guerra terrestre y reglamento anexo*. http://tinyurl.com/msaxyfzp

Faiez, R., & Vogt, H. (2012, 7 de enero). Afghan officials say Taliban poisoned schoolgirls. *The Seattle Times*. http://tinyurl.com/yp9wzjy6

Forest, J., Howard, R., & Sheehan, A. (2013). *Weapons of mass destruction and terrorism*. McGraw-Hill.

Henckaerts, J.-M., & Doswald-Beck, L. (2007). *El derecho internacional humanitario consuetudinario Volumen I: Normas* (1.ª ed.). Comité Internacional de la Cruz Roja.

Incibe-Cert. (s.f.). Qué es Incibe-Cert. https://www.incibe-cert.es/sobre-incibe-cert/que-es-incibe-cert

Mayor, A. (2003). *Greek fire, poison arrows & scorpion bombs: Biological and chemical warfare in the ancient world*. Princeton.

Melendo, J. d. (2019). Amenazas sobre el sector de distribución. En Cátedra Miguel de Cervantes (Dir.), *Amenaza híbrida. La guerra imprevisible* (pp. 310-315). Academia General Militar; Universidad de Zaragoza. http://tinyurl.com/y9fccbce

Mic, M. (2018, 1.º de diciembre). Detienen a un refugiado que planeaba envenenar el suministro de agua de un pueblo de 10.000 habitantes. *Caso Aislado*. http://tinyurl.com/3ubp9xmz

Organización Mundial de la Salud (OMS). (2021). Diez sustancias químicas que constituyen una preocupación para la salud pública.

Pantusa, D., & Maiolo, M. (2018, 20 de marzo). Infrastructure vulnerability index of drinking water systems to terrorist attacks. *Taylor & Francis Online*. https://doi.org/10.1080/23311916.2018.1456710

Patrón Sánchez, B. (2018, 13 de febrero). Envenenamiento de pozos. *Vavel*.

Pedersen, D. (2001). Poison found in refugee camp water supply. *Mizzima*.

Pleterski, T. (2010). *El impacto del terrorismo sobre el turismo* [trabajo de grado, Universidad de Palermo, Universidad Politécnica de Valencia, Buenos Aires]. http://tinyurl.com/48pm5bej

Presidencia del Gobierno. (2017). *Estrategia de Seguridad Nacional*. Gobierno de España. http://tinyurl.com/mnw7h6nj

Salvatierra, J. (2017, 19 de agosto). El atentado en Barcelona golpea al sector turístico en pleno debate sobre sus límites. *El País*. http://tinyurl.com/bdhphw9h

TNN. (2010, 10 de noviembre). Maoists poison pond close to CRPF camp. *The Times of India*. http://tinyurl.com/2kmky35h

Trotter, W. R. (2013). *Winter war: The russo-finnish war of 1939-40*. Aurum Press.

Vidal Delgado, R. (2017). *Legislación actual y proyección, en el ciclo del agua en cuanto a seguridad de las infraestructuras*. Universidad de Málaga. http://tinyurl.com/bp7khr26

Xinhua. (2007, 12 de abril). One dead after mass food poisoning in China's Habrin.

Zuloaga, J. M. (2018, 12 de octubre). El Estado Islámico intentó "hackear" una depuradora y envenenar el agua de miles de personas en Inglaterra. *La Razón*. http://tinyurl.com/564kkhpz