Universidad Internacional de La Rioja
Facultad de Derecho

Máster Universitario en Derecho Digital

PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS. ANÁLISIS DE DERECHO COMPARADO ESPAÑOL - ARGENTINO

Trabajo fin de estudio presentado por:	Leonardo Germán Brond
Tipo de trabajo:	Trabajo Fin de Máster (T.F.M.)
Utilizar si se necesita alguna tipología más:	
Director/a:	Oriol Troyano Talavera
Fecha:	26 de julio de 2023 - Depósito

Resumen

El autor investiga la protección de las infraestructuras críticas en España y Argentina con especial énfasis en el derecho penal y procesal penal respecto de tres cuestiones concretas: el alcance de la tutela penal; la racionalidad de la escala penal; las posibilidades de una investigación exitosa contra los hackers. Analiza las figuras previstas en los artículos 264, 264 bis, 264 ter y 573 del código penal español. Se ocupa de si la escala penal es suficiente o si es necesaria una pena mayor. También averigua cuál es la medida más idónea para investigar un ciberataque contra las infraestructuras críticas.

El autor luego investiga la protección de las infraestructuras críticas en Argentina. Concluye que es necesario incorporar las infraestructuras críticas al código penal argentino con una escala penal adecuada. También afirma que es menester actualizar el código procesal penal argentino para incluir medidas de investigación tecnológica.

Palabras clave: (De 3 a 5 palabras)

ciberataque – daño informático – infraestructuras críticas – escala penal - investigación tecnológica

Abstract

The author investigates the protection of critical infrastructure in Spain and Argentina in focus on criminal law and criminal procedure law with regards to three specific issues: the scope of criminal protection of critical infrastructures; the rationality of the scale of punishment; the possibility of a successful investigation against hackers. He analyses the elements regulated in articles 264, 264 bis, 264 ter and 573 of spanish criminal code. He works with the question of the scale of punishment is adequate or if it needs to be increased. He inquires too which is the most appropriate measure to investigate a cyberattack against the critical infrastructures.

The author then investigates the protection of the critical infrastructures in argentine criminal code. He concludes that it is necessary to incorporate the critical infrastructures in the argentine code with an appropriate scale of punishment. He also affirms that it is necessary to update the argentine criminal procedure code to include technological investigation measures.

Keywords:

cyberattack - computer sabotaje - critical infrastructure – scale of punishment - technological investigation

Índice de contenidos

1. Introducción

"Protección de Infraestructuras Críticas" se define como "el conjunto de actividades destinadas a asegurar la funcionalidad, continuidad e integridad de las infraestructuras críticas con el fin de prevenir, paliar y neutralizar el daño causado por un ataque deliberado contra dichas infraestructuras y garantizar la integración de estas actuaciones con las demás que procedan de otros sujetos responsables dentro del ámbito de su respectiva competencia". Esta definición alude a protección en cuanto a medidas técnicas y de derecho administrativo, pero ninguna referencia hace a la tutela jurídico penal, ni a medidas de investigación tecnológica dentro de un proceso criminal. En efecto, resulta escasa la literatura existente sobre la protección de infraestructuras críticas y, más aún, desde la óptica jurídico-penal.

Por ello, esta investigación es un estudio de derecho comparado español - argentino acerca de la protección de las infraestructuras críticas con especial atención a los aspectos de derecho penal y procesal penal.

El primer capítulo, titulado "conceptos básicos de infraestructuras críticas", está elaborado sobre trabajos doctrinaros provenientes de distintas partes del mundo; ha detectado algunas problemáticas comunes y, por ello, pretende ser un pequeño aporte a una teoría general de las infraestructuras críticas, de modo de servir como información previa al análisis de cualquier legislación. Aquí se trabaja una definición de infraestructuras críticas, sus características, importancia y se elabora un concepto fundamental en la materia: el de "causas de criticidad". Se investigan casos históricos y casos prácticos llevados a sus últimas consecuencias.

El segundo capítulo está dedicado al análisis de la protección de las infraestructuras críticas en España. Aquí se trabaja la "normativa PIC", compuesta por la Ley 8/2011, el Decreto 704/2011 y el Reglamento de protección de las infraestructuras críticas. Se estudian también otras normas. Se desarrolla la definición de infraestructuras críticas, los sectores estratégicos y las "causas de criticidad" según la legislación española. Se investigan los componentes del Sistema de Protección de Infraestructuras Críticas y los instrumentos de planificación. Luego se pasa revista a las posibles sanciones frente a los ataques físicos y cibernéticos contra las infraestructuras críticas. Interesan aquí no solo las sanciones

previstas en el código penal, sino también las medidas de investigación tecnológica que puedan llevar a los ciberatacantes a juicio oral.

El análisis de la legislación argentina tiene lugar en el capítulo tercero. Aquí entran en consideración las principales resoluciones que regulan la materia. Se analiza la definición, las "causas de criticidad" y los sectores identificados según la legislación argentina. También se investiga la situación en el código penal y el código procesal penal argentino.

La tercera parte del presente trabajo contiene las conclusiones con respecto a la legislación española y la legislación argentina.

1.1. Justificación del tema elegido

La protección de las infraestructuras críticas representa un tema de máximo interés para los Estados en el marco de la Cuarta Revolución Industrial, en donde el ciberespacio se ha convertido en el quinto elemento. El efecto devastador que generan los ciberataques al sistema informático de una infraestructura crítica dentro de una sociedad hiperconectada tiene que ser castigado con una pena que resulte proporcional al daño causado. Y previo a ello, debe ser posible llevar a los hackers a juicio oral. Este último aspecto no resulta sencillo.

Estamos ante un tema de palpitante actualidad, puesto que los ciberataques se producen muy a menudo y generan ganancias económicas fabulosas para los ciberatacantes, que no son aprendices, ni cometen estos delitos para comer, sino que son hackers de sombrero negro -"*black hat kackers*"-, y acceden a una vida de lujo patrimonial haciendo "click", bloqueando datos y exigiendo el pago de rescates millonarios en criptomonedas.

Estas razones justifican el tema elegido.

1.2. Problema y finalidad del trabajo

A pesar de que el ciberataque a las infraestructuras críticas representa un problema de extrema gravedad, gran actualidad y de frecuente ocurrencia, no está debidamente regulado en España y, menos aún, en Argentina. En nuestra opinión, Argentina no tiene tipificado el ciberataque a las infraestructuras críticas, por más que la ley 26.388 haya incorporado los delitos informáticos al código penal argentino. Sin embargo, existen voces discordantes.

Por ello, este trabajo tiene por finalidad examinar la legislación penal española y analizar sus puntos objetables, para explicitar las razones a tener en cuenta con miras a una reforma penal.

También es finalidad del presente trabajo evaluar si es necesario incluir las infraestructuras críticas en el código penal argentino y, en su caso, esbozar los principales aspectos de la escala penal.

Por otra parte, la investigación tiene por finalidad evaluar cuál sería la medida de investigación tecnológica más apropiada con vistas a que la regulación penal no sea meramente derecho penal simbólico, sino que tenga posibilidades reales de concreción en sentido procesal.

1.3. Objetivos

El trabajo aquí desarrollado se propone, por ende, los siguientes objetivos:

Por un lado, conocer las ideas generales aplicables a todas las infraestructuras críticas.

Un segundo objetivo reside en comprender cómo se protegen las infraestructuras críticas en España.

Un tercer objetivo consiste en saber cómo están protegidas las infraestructuras críticas en Argentina.

El cuarto objetivo es averiguar qué relaciones pueden establecerse entre los sistemas español y argentino, sobre todo, en lo que respecta al derecho penal y procesal penal.

2. Marco teórico y desarrollo

2.1. CONCEPTOS BÁSICOS DE INFRAESTRUCTURAS CRÍTICAS

2.1.1. Definición de infraestructuras críticas

El término "infraestructura crítica", también conocido como "*Critical infrastructure*" en inglés, "*Kritische Infrastrukturen*" en alemán e "*Infraestruturas Críticas*" en portugués, surgió en la primera década del siglo XXI. Por ello, es un concepto relativamente joven. Cada vez que prendemos la luz, abrimos la canilla para obtener agua, utilizamos el transporte público, realizamos pagos a través de internet, entre otros ejemplos, están involucradas actividades esenciales que dependen de infraestructuras críticas.

Como primera aproximación, las infraestructuras críticas son "aquellas cuyo funcionamiento es indispensable para la normal operación de la sociedad" (BELTRÁN y SEVILLANO, 2021, 47).

La Directiva (UE) 2022/2557 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a la resiliencia de las entidades críticas y por la que se deroga la Directiva 2008/114/CE del Consejo, define "infraestructura crítica" como "un elemento, instalación, equipo, red o sistema, o parte de un elemento, instalación, equipo, red o sistema, que es necesario para la prestación de un servicio esencial" (art. 2, inc. 4, Directiva citada).

El concepto de "servicio esencial" también es definido por el legislador europeo: "un servicio que es crucial para el mantenimiento de funciones sociales vitales, las actividades económicas, la salud pública y la seguridad, o el medio ambiente" (art. 2, inc. 5, Directiva citada).

2.1.2. Características de las infraestructuras críticas

La doctrina considera que las infraestructuras críticas presentan tres características. Sin embargo, teniendo en cuenta el funcionamiento en la práctica, en nuestra opinión los rasgos esenciales son cuatro. Veamos.

2.1.2.1. Alto nivel de automatización

La primera de las características es que las infraestructuras críticas adoptan un alto nivel de automatización para su operatividad. Gran parte de las infraestructuras críticas de información son soportadas por proveedores de telecomunicaciones comerciales, lo cual requiere colaboración internacional, del sector público y privado (BELTRÁN y SEVILLANO, 2021, 47).

2.1.2.2. Interdependencia

El segundo rasgo reside en que existe una interdependencia entre todas las infraestructuras críticas, la cual impide considerarlas de manera aislada. El análisis debe ser global y la consideración debe abarcar a todas las infraestructuras críticas interconectadas. Lo que ocurre en una infraestructura repercute en las demás, produciendo problemas de seguridad en cascada. Así, por ejemplo, una afectación en el servicio de provisión de agua y de electricidad repercute en el servicio de atención médica (ECKE, 2020, 2; GUTERRES, 2016, 123).

2.1.2.3. Distribución en diferentes zonas geográficas

La tercera característica radica en que las infraestructuras críticas, en la generalidad de los casos, están distribuidas en distintas zonas geográficas, lo cual hace más compleja la protección en lo que atañe a su seguridad física.

Ello requiere del diseño de procedimientos de seguridad específicos, tales como control de accesos, planes de contingencia ante catástrofes, planes de evacuación, etc. (BELTRÁN y SEVILLANO, 2021, 48).

2.1.2.4. Causas de criticidad

Las tres características antes mencionadas no resultan suficientes para que una infraestructura sea calificable de crítica, ni para que una vez así calificada, permanezca luego en el catálogo de infraestructuras críticas. Pues, toda infraestructura crítica ha de cumplir, al menos, con una "causa de criticidad". Ello nos obliga a reconocer una cuarta característica. La "causa de criticidad" es un concepto casi "puro" en términos kelsenianos. Según Kelsen, la teoría pura del derecho "quiere liberar a la ciencia jurídica de todos los elementos que le son extraños" (KELSEN, 1993, 15). En este sentido, el concepto de "causa de criticidad" permite ser llenado con el contenido que resulte necesario para que una infraestructura resulte

calificable de "crítica" en cualquier país del mundo. Las causas de criticidad son –en parte- comunes a todos los países, y -en parte- relativas de país a país.

Por ello, sin perjuicio de lo establecido por la legislación de cada país, es posible reconocer las siguientes "causas de criticidad": a) El número de personas afectadas; b) El impacto económico; c) El impacto medioambiental; d) El impacto público y social.

2.1.3. Importancia de las infraestructuras críticas

Las definiciones y características analizadas coinciden en el carácter esencial de los servicios brindados por las infraestructuras críticas y los graves efectos que implicarían la interrupción de su funcionamiento para el país. Las infraestructuras críticas constituyen, por ello, "el sistema nervioso central de la economía de una nación" (CORREA-HENAO, y YUSTA-LOYO, 2013, 93). El mal funcionamiento o destrucción de tales infraestructuras críticas tendría un grave impacto sobre los servicios esenciales que ellas prestan (BELTRÁN y SEVILLANO, 2021, 47).

2.1.4. Amenazas a las infraestructuras críticas

Las infraestructuras críticas de los países están expuestas a múltiples amenazas en razón de su vulnerabilidad. Las amenazas pueden clasificarse en tres categorías: "causas naturales", "error humano/técnico" y "guerra/criminalidad/terrorismo" (ECKE, 2020, 2).

La amenaza de "causa natural" por excelencia es el cambio climático científicamente reconocido (ECKE, 2020, 2).

La amenaza mediante "guerra/criminalidad/terrorismo" se ha hecho patente con los atentados terroristas del 11 de septiembre de 2001 en Estados Unidos (CORREA-HENAO y YUSTA-LOYO, 2013, 94). España no ha sido ajena esta problemática, ya que el 11 de marzo de 2004 tuvieron lugar los atentados en cuatro trenes de Madrid.

Un peligro importante para las infraestructuras críticas proviene de amenazas híbridas. Se trata de combinaciones provenientes de operaciones militares realizadas en forma abierta y encubierta, presión diplomática y económica, desinformación y ataques en el ciberespacio.

El ciberespacio se ha transformado en una especie de quinto elemento. El filósofo griego Empédocles (484 a.C. - 424 a.C.) sostenía que nuestro universo estaba formado por una combinación de cuatro elementos inalterables y eternos: tierra, aire, agua y fuego. Cada

uno de los elementos tradicionales implica un campo de batalla. Los Estados tuvieron que desarrollar componentes específicos para cada uno de estos elementos: el Ejército para la tierra, la Fuerza Aérea para el aire, la Armada para el agua y los Bomberos para el fuego (RAMONET, 2016, 16).

Quien primero utilizó tecnología digital como herramienta de sabotaje fue Estados Unidos contra la Unión Soviética durante la guerra fría de los años ochenta. Los norteamericanos colocaron chips destinados a controlar los sistemas de un gasoducto ruso. Provocaron una de las mayores explosiones no termonucleares de la historia.

Pero el impulso decisivo a la protección de las infraestructuras críticas surgió cuando Rusia invadió a Estonia en 2007 por la retirada de la estatua del soldado soviético de un parque de Tallín, la capital de Estonia. El Soldado de Bronce había sido inaugurado por las autoridades soviéticas en 1947, que en aquel entonces se llamaba "Monumento a los libertadores de Tallín"; se encontraba en la capital. Los rusos parlantes de Estonia creen que el monumento representa el triunfo de la URSS sobre el nazismo. Sin embargo, muchos estonios étnicos consideran que los soldados rusos no fueron liberadores sino ocupantes, y ello era el recordatorio de la estatua. En 2007 el gobierno trasladó el Soldado de Bronce desde Tallín hacia un cementerio militar ubicado en las afueras de la ciudad. Los medios de comunicación rusos afirmaron falsamente que la estatua y las tumbas de guerra soviéticas eran destruidas por el gobierno de Estonia. Ello generó protestas con 150 heridos y un muerto. Un día después, Estonia sufrió ciberataques que duraron un mes. El ciberespacio quedó inutilizado; bancos, organismos gubernamentales y medios de comunicación dejaron de funcionar. Los ataques procedían de IP rusas. Expertos han calificado este ataque como la Primera Guerra de la Red. Ello ha generado conciencia de los riesgos en torno a los ciberataques y la ciberseguridad ("Estonia: proteger el ciberespacio frente a las intenciones rusas", https://es.euronews.com/next/2022/05/27/estonia-proteger-el-ciberespacio-frente-a-las-intenciones-rusas).

En 2008 Rusia atacó a Georgia, a consecuencia del conflicto por la región del Cáucaso por el control del enclave de Osetia del Sur, produciendo denegación de servicios (DDOS) que fueron la antesala de un desplazamiento militar en el territorio de Georgia ("La guerra de Rusia contra Georgia, también cibernética", https://www.ccn-cert.cni.es/gl/gestion-de-incidentes/lucia/23-noticias/725-la-guerra-de-rusia-contra-georgia-tambien-cibernetica.html).

En 2010 Israel infectó con el virus Stuxnet los sistemas informáticos de las Centrales Nucleares de Irán. De este modo, Israel ha saboteado las centrifugadoras del programa nuclear y ralentizando su capacidad de desarrollar armamento atómico ("Israel diseña un virus informático para boicotear el programa nuclear iraní", https://elpais.com/internacional/2011/01/16/actualidad/1295132408_850215.html).

El 27 de junio 2017, la víspera del Día de la Constitución ucraniana, Ucrania sufrió el ciberataque conocido como NotPetya, que infectó a más de 80 empresas de ese país y luego se expandió por Europa, Estados Unidos y la India, haciendo estragos en miles de organizaciones del mundo (https://cso.computerworld.es/cibercrimen/cinco-anos-despues-de-notpetya-lecciones-aprendidas). Londres acusó a Moscú por el ataque NotPetya (https://elpais.com/internacional/2018/02/15/actualidad/1518685885_628921.html).

Por ello, los Estados que pretendan proteger los datos de su población frente a ataques en el ciberespacio tendrán que realizar un esfuerzo similar al que otrora hicieron con sus fuerzas armadas para dominar la tierra, el aire, el agua y el fuego. En esta dirección, se destaca el esfuerzo de Ucrania, quien, tras la invasión de Rusia en febrero de 2022, usó herramientas de Amazon Web Services (AWS) -la división de computación en la nube de Amazon, para backupear más de 15 petabytes (15 millones de gigabytes) de datos esenciales de 50 autoridades gubernamentales ucranianas, 24 universidades y empresas del sector privado, y llevar toda esta información a la nube. La operación fue realizada en 24 horas y con un equipo de menos de cuatro personas. El apoyo a los equipos técnicos ucranianos estuvo a cargo de Liam Maxwell, director de Transformación Gubernamental en Amazon Web Services. De este modo, Ucrania usó una infraestructura de un tercero –servidores, programas y aplicaciones AWS- para poner a salvo todo el sistema en línea del Estado ("Así respaldó Ucrania todos sus datos públicos en la nube: 15 mil terabytes a salvo de la invasión rusa", 10/06/2023, https:www.clarin.com/tecnologia/respaldo-ucrania-datos-publicos-nube-15-mil-terabytes-salvo-invasion-rusa_0_oc8sA59NwK.html).

2.1.5. Casos prácticos

Para tener una imagen más nítida de lo que es un ciberataque a los sistemas informáticos de las infraestructuras críticas es conveniente analizar dos casos ocurridos en la práctica. Uno de ellos ocurrió en el Hospital Universitario de Düsseldorf, Alemania. El otro, en el Hospital Springhill de Alabama, Estados Unidos. Nos ocuparemos a continuación.

2.1.5.1. Uniklinik, Düsseldorf, Alemania

En 2020 se conoció en Alemania la primera víctima mortal vinculada a un ataque de ransomware. Era una paciente de urgencia que falleció durante el traslado en ambulancia desde el hospital universitario de Düsseldorf, afectado por un ransomware, hacia otro nosocomio en Wuppertal, en donde sería atendida. El hospital de Düsseldorf había sido víctima de un ciberataque realizado por autores desconocidos que bloquearon 30 servers: no era posible realizar operaciones a los pacientes; el servicio de urgencias tuvo que cerrar. El traslado desde Düsseldorf hacia Wuppertal –ubicada a 32 kilómetros de distancia- duró media hora y la paciente murió inmediatamente al ser enviada a Wuppertal.

Según manifestó el fiscal general a la prensa, si se pudiera demostrar la co-culpabilidad del hacker en el caso, sería condenado por homicidio culposo o, lisa y llanamente, por asesinato.

El gobierno alemán cree que los responsables posiblemente estén ubicados en Rusia, dado que el ransomware "Doppelpaymer" ya había sido utilizado por un grupo de hackers de Rusia contra empresas e instituciones (Cyberkriminalität, "Todesfall nach Hackerangriff auf Uni-Klinik Düsseldorf", 18/09/2020, por Christof Kerkmann y Lars-Marten Nagel, amp2. Hadelsblatt.com; "Der Hackerangriff auf die Uniklinik Düsseldorf und die Folgen", 18/09/20, www.deutschlandfunk.de; "Uniklinik Düsseldorf: Ramsonware "DoppelPaymer" soll hinter dem Angriff stecken", 22/09/20, www.heise.de; "Tod nach Systemausfall. Spur der Uniklinik-Hacker soll nach Russland führen", 22/09/20, www.spiegel.de).

2.1.5.2. Springhill Medical Center, Alabama, Estados Unidos

En 2021 se conoció en el Springhill Medical Center de Alabama, Estados Unidos, la muerte de un bebé por un ataque de ransomware. Al momento del ciberataque, se encontraban en el hospital Teiranni Kidd y su bebé. El ataque ransomware ocasionó que el bebé no obtuviera una atención debida. Pues, al momento del ciberataque, los médicos y enfermeras hicieron caso omiso a muchos pasos que hay que seguir en tales procedimientos. En ese contexto de ciberataque, los médicos pasaron por alto que el cordón umbilical estaba enrollado en el cuello del bebé. Esta situación desencadena señales de alerta en el monitor cardíaco cuando el cordón apretado corta el suministro de sangre y

oxígeno al feto. Sin embargo, el no funcionamiento del monitor provocó que al bebé se le diagnosticara un daño cerebral grave. 9 meses después, falleció.

En la demanda figura Katelyn Parnell, obstetra. Parece que los médicos sabían que no tenían gráficos desde hace tiempo. Imprimían los análisis en el laboratorio y los enviaban en papel. Katelyn le dijo a la jefa de las enfermeras que la muerte del bebé era evitable y que, de haber visto la lectura del monitor, habría hecho nacer al bebé por cesárea, según figura en la conversación en las capturas de pantalla que se ofrecieron como prueba.

No se descarta que la banda Ryuk, con sede en Rusia y que ya ha atacado a 235 hospitales y centros psiquiátricos, esté detrás del suceso. Ryuk recaudó al menos 100 millones de dólares por pagos de pedidos de rescate en 2020 ("Un bebé muere después de que unos hackers atacaran un hospital", 1/10/21, www.elespañol.com; "el hackeo en un hospital de Estados Unidos provoca la primera muerte de un bebé por ransomware", 1/10/2021, www.larazon.es).

2.1.6. Concepto de ransomware

Tal como hemos visto, los hospitales de Düsseldorf y Alabama fueron víctimas de un ataque de ransomware. El ransomware (del inglés "ransom" -rescate- y "ware" -acortamiento de software-) es una modalidad extorsiva que restringe el acceso al sistema de la víctima y exige el pago de un rescate para eliminar la traba (BARRIO ANDRÉS, 2020, 78).

En caso de pagar, el atacante restaura el acceso a los datos y contenidos. Por lo general, los black hat hackers (BLANCO, 2020, 14) exigen que el pago sea en bitcoin, porque es más difícil de rastrear y el receptor del dinero se mantiene en anonimato.

2.2. PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS EN ESPAÑA

2.2.1. Infraestructuras críticas en España

En España la información concerniente a las infraestructuras críticas, su ubicación, titularidad y administración, servicios que prestan, medios de contacto, nivel de seguridad que precisan en función de los riesgos evaluados, está clasificada como secreta debido a la alta sensibilidad para la seguridad nacional (art. 4.3, del Real Decreto 704/2011). Rige al respecto la legislación sobre secretos oficiales.

El art. 2.l, de la ley 8/2011 define "información sensible sobre protección de infraestructuras estratégicas" como "los datos específicos sobre infraestructuras estratégicas que, de revelarse, podrían utilizarse para planear y llevar a cabo acciones cuyo objetivo sea provocar la perturbación o la destrucción de éstas".

Las autoridades públicas tienen obligación de velar por la confidencialidad de los datos sobre infraestructuras críticas a los que tengan acceso (art. 15.2, ley 8/2011), es decir, que únicamente es posible acceder a la información con autorización.

Los sistemas, las comunicaciones y la información referida a la protección de las infraestructuras críticas deben contar con medidas de seguridad que garanticen la confidencialidad, integridad y disponibilidad de los datos (art. 15.2, ley 8/2011).

A pesar del carácter secreto de la información, existen en España más de 3.500 infraestructuras críticas reconocidas (LISA Institute).

La ley 8/2011 se aplica a las infraestructuras críticas ubicadas en territorio español vinculadas a los 12 sectores estratégicos contenidos en el anexo de la ley citada, cuales son: 1) Energía -producción y distribución-; 2) Tecnologías de la Información y las Comunicaciones –ya sean infraestructuras críticas en sí mismas, como redes de telecomunicaciones, o brinden servicio de información y comunicación a otras infraestructuras críticas-; 3) Transporte –aeropuertos, puertos, instalaciones multimodales, ferrocarriles y redes de transporte público, sistemas de control del tráfico-; 4) Agua –embalses, almacenamiento, tratamiento y redes-; 5) Salud –sector e infraestructura sanitaria-; 6) Alimentación -producción, almacenamiento y distribución-; 7) Sistema financiero y tributario –entidades bancarias, información, valores e inversiones-; 8) Industria nuclear -producción, almacenamiento y transporte de mercaderías peligrosas, materiales nucleares y radiológicos-; 9) Industria química -producción, almacenamiento y transporte de mercancías peligrosas y materiales químicos; 10) Instalaciones de investigación -laboratorios que por su idiosincrasia dispongan o produzcan materiales, sustancias o elementos críticos o peligrosos; 11) Espacio; 12) Administración -servicios básicos, instalaciones, redes de información, principales activos y monumentos del patrimonio nacional- (LISA Institute).

En 2014 España registró 63 incidentes contra centros críticos; en 2016 hubo 479; únicamente entre enero y julio de 2017 hubo 489. En enero y febrero de 2018 hubo más incidentes de ciberseguridad en infraestructuras críticas que en todo 2014 (VELASCO NÚÑEZ y SANCHIS CRESPO, 2019, 255).

El Instituto Nacional de Ciberseguridad (Incibe), en su Balance de Ciberseguridad 2020, reportó 1.190 ciberataques que tuvieron por destinatarios a operadores críticos y esenciales estratégicos (FERNÁNDEZ GARCÍA, 2022, 116).

En el balance de seguridad de 2022, Incibe reportó 118.820 incidentes gestionados; esto significa un 8,8 % más que en 2021. De tales incidentes, 546 tuvieron por destinatarios a operadores críticos y esenciales, en las siguientes proporciones: 37,36 % corresponde al sector "Energía"; 21,98 % pertenece a "Transporte"; 17,77 % corresponde a "Sistema financiero y tributario"; 8, 42 % corresponde a "Agua" (file:///balance_ciberseguridad_2022_incibe.pdf).

2.2.2. Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de infraestructuras críticas

La ley 8/2011 tiene por objeto establecer medidas de protección para las infraestructuras críticas mediante la transposición de la -hoy derogada- Directiva 2008/114/CE. Es una ley administrativa (JIMÉNEZ DÍAZ, 2017, 9). Está considerara "el principal hito normativo español" (FERNÁNDEZ GARCÍA, 2022, 122).

Es la primera ley que regula de manera integral las infraestructuras críticas, unificando protección que antes se encontraba dispersa (FERNÁNDEZ GARCÍA, 2022, 123). Ejemplos: la ley 16/1987, de 30 de julio, de Ordenación de los Transportes Terrestres, y la ley 21/2003, de 7 de julio, de Seguridad Aérea (GALINDO SIERRA, 2016, 10).

Sin embargo, en cuanto a su coercibilidad, observa Fernández Fernández que la ley 8/2011 "se trata de una de las pocas leyes sin régimen sancionador" (FERNÁNDEZ FERNÁNDEZ, 33).

2.2.2.1. Definición de infraestructuras críticas

El art. 2.e, ley 8/2011, define las infraestructuras críticas como las "infraestructuras cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales".

2.2.2.2. Causas de criticidad

Las "causas de criticidad" se denominan en la legislación española "criterios horizontales de criticidad". Están previstos en el art. 2.h, ley 8/2011. Tales pautas son:

2.2.2.2.a) Número de personas afectadas

Esta cifra se aprecia "en función del número potencial de víctimas mortales o heridos con lesiones graves y las consecuencias para la salud pública";

2.2.2.2.b) Impacto económico

Este impacto se calcula "en función de la magnitud de las pérdidas económicas y el deterioro de productos y servicios";

2.2.2.2.c) Impacto medioambiental, degradación en el lugar y sus alrededores;

Esta enumeración resulta excesiva. Pues, la referencia al "impacto medioambiental" abarca la degradación en el lugar y sus alrededores.

2.2.2.2.d) Impacto público y social

Este impacto se deduce de "la incidencia en la confianza de la población en la capacidad de las Administraciones Públicas, el sufrimiento físico y la alteración de la vida cotidiana, incluida la pérdida y el grave deterioro de servicios esenciales".

2.2.2.3. Concepto de protección de infraestructuras críticas

Otro concepto relevante es el de "protección de infraestructuras críticas", el cual es definido como "el conjunto de actividades destinadas a asegurar la funcionalidad, continuidad e integridad de las infraestructuras críticas con el fin de prevenir, paliar y neutralizar el daño causado por un ataque deliberado contra dichas infraestructuras y garantizar la integración de estas actuaciones con las demás que procedan de otros sujetos responsables dentro del ámbito de su respectiva competencia" (art. 2.k, Ley 8/2011).

2.2.2.4. Objetivos estratégicos de la protección de las infraestructuras críticas

La protección de las infraestructuras críticas se lleva a cabo mediante numerosos agentes del sector público y privado, sobre la base de la idea de "prevención", "preparación" y "respuesta" del Estado español a los atentados terroristas u otras amenazas que afecten las infraestructuras críticas (art. 1, ley 8/2011).

La ley 8/2011 va más allá de la mera protección material de las infraestructuras críticas. Apunta a una protección contra ataques deliberados de todo tipo, tanto de carácter físico como cibernético.

2.2.2.5. Ámbito de aplicación de la ley 8/2011

La ley 8/2011 se aplica a las infraestructuras críticas ubicadas en territorio español vinculadas a los 12 sectores estratégicos definidos en su anexo (art. 3.1). Existen excepciones y supuestos de aplicación concurrente de leyes.

Las excepciones se presentan en los supuestos de las infraestructuras dependientes del Ministerio de Defensa y de las Fuerzas y Cuerpos de Seguridad. Tales infraestructuras se rigen, a los fines de su control administrativo, por su propia normativa (art. 3.2).

La aplicación concurrente de leyes se verifica en los supuestos que conciernen al Centro Nacional de Inteligencia, la energía nuclear, al Consejo de Seguridad Nuclear y al Programa Nacional de Seguridad de la Aviación Civil. En estos casos la ley 8/2011 resulta aplicable sin perjuicio de lo previsto en las leyes específicas (art. 3.3, incisos “a”, “b” y “c”).

La ley 8/2011 obliga al Ministerio del Interior, a través de la Secretaría de Estado de Seguridad, a llevar el Catálogo Nacional de Infraestructuras Estratégicas, un instrumento que contiene la información de las infraestructuras estratégicas de España, entre ellas, las clasificadas como Críticas o Críticas Europeas (art. 4).

2.2.2.6. Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas

El Real Decreto 704/2011 contiene un artículo único, y es el que aprueba el Reglamento de Protección de las infraestructuras críticas, que tiene por objetivo desarrollar el marco previsto en la ley 8/2011.

2.2.2.7. Componentes del Sistema de Protección de Infraestructuras Críticas

El art. 5 de la ley 8/2011 establece los componentes del Sistema de Protección de Infraestructuras Críticas. Es relevante conocer estos componentes porque los hackers tienen que vencer las barreras de seguridad previstas. Se trata de instituciones, órganos y empresas tanto del sector público como del privado, con responsabilidades en el correcto

funcionamiento de los servicios esenciales o en la seguridad de los ciudadanos. A continuación, veremos las funciones de cada uno de los agentes.

2.2.2.7.a) la Secretaría de Estado de Seguridad del Ministerio del Interior

La Secretaría de Estado de Seguridad del Ministerio del Interior es el máximo responsable del Sistema de Protección de las infraestructuras críticas españolas (art. 6, Ley 8/2011). Es quien diseña y dirige la estrategia nacional de protección de infraestructuras críticas; aprueba los principales instrumentos de planificación: el Plan Nacional de Protección de Infraestructuras Críticas, los Planes de Seguridad de los Operadores, los Planes de Protección Específicos y los Planes de Apoyo Operativo; aprueba la declaración de una zona como crítica; identifica los diferentes ámbitos de responsabilidad en la protección de infraestructuras críticas; emite instrucciones y protocolos dirigidos al personal y los operadores de las infraestructuras críticas; supervisa los proyectos de interés y coordina programas financieros y subvenciones provenientes de la Unión Europea; colabora con los Ministerios y organismos del Sistema en la elaboración de normas sectoriales; en situaciones de crisis, asume las funciones que le sean acordadas por la Comisión Delegada del Gobierno (art. 6, del Real Decreto 704/2011).

2.2.2.7.b) el Centro Nacional para la Protección de las Infraestructuras Críticas

El Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC) es el órgano ministerial responsable del impulso, coordinación y supervisión de todas las actividades relacionadas con la protección de las infraestructuras críticas españolas. Fue creado en 2007. Depende de la Secretaría de Estado de Seguridad (art. 7, Ley 8/2011).

El CNPIC asiste al Secretario de Estado de Seguridad en la ejecución de sus tereas, actuando como contacto y coordinación con los agentes del Sistema.

Las funciones del CNPIC son ejecutar y actualizar el Plan Nacional de Protección de las Infraestructuras Críticas; determinar la criticidad de las estructuras; actualizar el catálogo español de infraestructuras críticas, en virtud de las causas de criticidad y la interdependencia sectorial a partir de la información proveniente de los agentes; intervenir en los instrumentos de planificación; dirigir análisis de riesgos en los Planes Estratégicos Sectoriales; establecer los contenidos mínimos de los Planes de Seguridad de los Operadores, de los Planes de Protección Específicos y de los Planes de Apoyo Operativo; evaluar Planes de Seguridad del Operador; analizar Planes de Protección Específicos; validar

los Planes de Apoyo Operativo; elevar al Secretario de Estado de Seguridad las propuestas para la declaración de una zona como crítica; implantar mecanismos permanentes de información, alerta y comunicación con todos los agentes del Sistema; analizar información sobre infraestructuras críticas; participar en simulacros de protección de infraestructuras críticas; coordinar reuniones sobre protección de infraestructuras críticas; elevar a la Comisión Europa informes sobre evaluación de amenazas, vulnerabilidades y riesgos encontrados en cada uno de los sectores en que se hayan designado infraestructuras críticas europeas (art. 7, del Real Decreto 704/2011).

2.2.2.7.c) los Ministerios y organismos integrados en el Sistema incluidos en el anexo de la ley 8/2011

Los Ministerios y organismos integrados participan en la elaboración de los Planes Estratégicos Sectoriales; verifican el cumplimiento de los Planes Estratégicos Sectoriales y de las actuaciones derivadas de éstos, excepto las que se correspondan con medidas de seguridad concretas establecidas en infraestructuras específicas, o las que deban ser realizadas por otros órganos de la Administración General del Estado; colaboran en la designación de operadores críticos y en la elaboración de la normativa sectorial; asesoran a la Secretaría de Estado de Seguridad en la catalogación de las infraestructuras ofreciendo al CNPIC la información para determinar su criticidad, inclusión, exclusión o modificación en el catálogo (art. 8, del Real Decreto 704/2011).

2.2.2.7.d) las Delegaciones del Gobierno en las Comunidades Autónomas y en las Ciudades con Estatuto de Autonomía

Las Delegaciones del Gobierno en las Comunidades Autónomas y en las Ciudades Autónomas tienen a su cargo coordinar las Fuerzas y Cuerpos de Seguridad del Estado en la aplicación del Plan Nacional de Protección de Infraestructuras Críticas en caso de activación de éste; participar en la implantación de los Planes de Protección Específicos y de los Planes de Apoyo Operativo en su territorio; proponer la declaración de una zona crítica (art. 9, del Real Decreto 704/2011).

2.2.2.7.e) las Comunidades Autónomas y las Ciudades con Estatuto de Autonomía

Las Comunidades Autónomas y las Ciudades con Estatuto de Autonomía tienen facultades para intervenir en la implantación de los Planes de Protección Específicos y de los

Planes de Apoyo Operativo en su territorio; también para proponer la declaración de una zona crítica (art. 10, del Real Decreto 704/2011).

2.2.2.7.f) las Corporaciones Locales, a través de la asociación de Entidades Locales de mayor implantación a nivel nacional

La regulación de estos agentes ha quedado inconclusa. Pues, si bien las "Corporaciones Locales" están mencionadas en el art. 5.f, de la ley 8/2011, lo cierto es que la ley citada prescinde luego de su tratamiento (cfr. arts. 6/13, ley 8/2011). Tampoco existe tratamiento en el Real Decreto 704/2011.

2.2.2.7.g) la Comisión Nacional para la Protección de las Infraestructuras Críticas

La Comisión Nacional para la Protección de las Infraestructuras Críticas es un órgano colegiado adscripto a la Secretaría de Estado de Seguridad. Tiene por función la aprobación de los Planes Estratégicos Sectoriales y la designación de los operadores críticos, a propuesta del Grupo de Trabajo Interdepartamental (art. 11, ley 8/2011).

Debe promover una cultura de seguridad de las infraestructuras críticas; promueve la aplicación efectiva de la ley 8/2011; aprueba la creación, modificación o supresión de grupos de trabajo sectoriales o de carácter técnico.

La Comisión es presidida por el Secretario de Estado de Seguridad y tiene una integración variada con representantes del Ministerio del Interior, del Ministerio de Defensa, del Centro Nacional de Inteligencia, del Departamento de Infraestructura y Seguimiento para Situaciones de Crisis, del Consejo de Seguridad Nuclear y de cada uno de los ministerios integrados en el sistema. La Comisión se reúne una vez al año con carácter ordinario, y con carácter extraordinario cuando así lo convoque el presidente (art. 11, del Real Decreto 704/2011).

2.2.2.7.h) el Grupo de Trabajo Interdepartamental para la Protección de las Infraestructuras Críticas

El Grupo de Trabajo Interdepartamental tiene a su cargo elaborar los diferentes Planes Estratégicos Sectoriales y proponer a la Comisión el nombramiento de operadores críticos por cada uno de los sectores estratégicos definidos (art. 12, ley 8/2011). También le corresponde proponer la creación de grupos de trabajo, informando los resultados; y

efectuar los estudios que le encomiende la Comisión. El Grupo de Trabajo es presidido por el director del CNPIC; tiene una composición variada con representantes de cada uno de los ministerios del sistema, de la Dirección Adjunta Operativa del Cuerpo Nacional de Policía, de la Dirección Adjunta Operativa de la Guardia Civil, de la Dirección General de Protección Civil y Emergencias del Ministerio del Interior, del Estado Mayor Conjunto de la Defensa, del Centro Nacional de Inteligencia, del Departamento de Infraestructura y Seguimiento para Situaciones de Crisis, del Consejo de Seguridad Nuclear y del CNPIC. Ese grupo se reúne dos veces al año con carácter ordinario, y con carácter extraordinario cuando así lo convoque el presidente (art. 12, del Real Decreto 704/2011).

2.2.2.7.i) los operadores críticos del sector público y privado

Los operadores críticos son agentes que integran el sistema, designados por la Comisión. Elaboran el Plan de Seguridad del Operador, debiendo acreditar la implementación de las medidas exigidas por la autoridad a través de una certificación; elaboran un Plan de Protección Específico por cada una de las infraestructuras Críticas, con la misma exigencia de certificación; asesoran a la Secretaría de Estado de Seguridad, mediante el CNPIC, en la valoración de las infraestructuras propias, actualizando los datos en forma anual; colaboran con el Grupo de Trabajo en la elaboración de los Planes Estratégicos Sectoriales y en la realización de los análisis de riesgos; designan un Responsable de Seguridad y Enlace; nombran un Delegado de Seguridad por cada una de sus infraestructuras críticas; facilitan las inspecciones a los fines de acreditar el cumplimiento de la normativa sectorial y adoptan las medidas necesarias en cada plan (art. 13, ley 8/2011).

Para la designación de operador crítico se requiere que al menos una de las infraestructuras por él gestionadas reúna la consideración de infraestructura crítica, según las casusas de criticidad previstas en el art. 2.h, ley 8/2011 (art. 14 del Real Decreto 704/2011).

2.2.2.8. Instrumentos de planificación

El sistema en análisis contiene cinco instrumentos para proteger las infraestructuras críticas: a) Plan Nacional de Protección de las Infraestructuras Críticas; b) Planes Estratégicos Sectoriales; c) Planes de Seguridad del Operador; d) Planes de Protección Específicos, e) Planes de Apoyo Operativo (art. 14, ley 8/2011). Los veremos a continuación.

2.2.2.8.1. Plan Nacional de Protección de las Infraestructuras Críticas

El Plan Nacional de Protección de las Infraestructuras Críticas es el instrumento de programación del Estado, elaborado por la Secretaría de Estado de Seguridad, que permite dirigir las actuaciones para proteger las infraestructuras críticas contra el terrorismo (art. 14, ley 8/2011). Su meta principal es conservar seguras las infraestructuras críticas españolas que prestan servicios esenciales (CORREA-HENAO y YUSTA-LOYO, 2013, 101). Con tal objetivo, este instrumento agrupa una serie de medidas para prevenir y proteger a las infraestructuras críticas de todas las amenazas que puedan afectarlas.

Este plan prevé distintos niveles de seguridad, en función de los niveles de amenazas. Los distintos niveles de seguridad contienen la adopción gradual de medidas de protección y requieren del uso de las Fuerzas y Cuerpos de Seguridad, las Fuerzas Armadas y los responsables de las infraestructuras críticas a proteger.

Está clasificado como secreto oficial. Se revisa cada cinco años (art. 18, del Real Decreto 704/2011). Este instrumento obliga a que todas las infraestructuras críticas tengan un responsable de seguridad que sirva de enlace con el CNPIC en caso de ser necesario; fomenta el intercambio de información entre las diferentes empresas e instituciones que se encuentran en el catálogo; define las medidas que deben ser adoptadas por las infraestructuras críticas en caso de ser damnificadas por un ataque; agrupa los dictámenes y directivas que sigue el Estado para movilizar sus capacidades operativas frente a ataques deliberados (LISA Institute).

2.2.2.8.2. Planes Estratégicos Sectoriales

Los planes estratégicos sectoriales son instrumentos de planificación con alcance nacional que permiten conocer, en cada uno de los doce sectores previstos en el anexo de la ley 8/2011, cuáles son los servicios esenciales, su funcionamiento, las vulnerabilidades del sistema y las medidas necesarias para su mantenimiento. Estos planes son elaborados por el Grupo de Trabajo por cada uno de los sectores y deben contener al menos los siguientes elementos: a) Análisis de riesgos, vulnerabilidades y consecuencias a nivel global; b) Propuestas de implantación de medidas organizativas y técnicas necesarias para prevenir, reaccionar y paliar las consecuencias; c) Propuestas de implantación de otras medidas

preventivas y de mantenimiento; d) Medidas de coordinación con el Plan Nacional de Protección de Infraestructuras Críticas.

Estos planes están clasificados también como secreto oficial. Se revisan cada dos años (art. 19, del Real Decreto 704/2011).

2.2.2.8.3. Planes de Seguridad del Operador

Los Planes de Seguridad del Operador son documentos estratégicos definidores de las políticas de los operadores críticos para garantizar la seguridad del conjunto de instalaciones de su propiedad o gestión. Deben establecer una metodología de análisis de riesgos que asegure la continuidad de los servicios brindados y en la que se recojan las medidas de seguridad frente a las amenazas tanto físicas como lógicas (art. 22, del Real Decreto 704/2011).

Mediante estos documentos se pretende que los operadores críticos cumplan con el Real Decreto 704/2011. El Plan de Seguridad del Operador define la política general del operador para garantizar la seguridad integral del conjunto de sistemas de su propiedad o gestión. Por ejemplo, en España el principal operador en transporte de electricidad es la empresa Red Eléctrica de España S.A. (CORREA-HENAO y YUSTA-LOYO, 2013, 101).

Estos planes están clasificados igualmente como secreto oficial. Se revisan cada dos años (art. 24, del Real Decreto 704/2011).

2.2.2.8.4. Planes de Protección Específicos

Los Planes de Protección Específicos son documentos, en donde se definen las medidas concretas ya adoptadas y las que adoptarán los operadores críticos para garantizar la seguridad física y lógica de sus instalaciones críticas. Estos planes son elaborados por cada operador crítico en el plazo de cuatro meses a partir de la aprobación del Plan de Seguridad del Operador.

Cada Plan de Protección Específico debe contemplar la adopción de medidas permanentes, temporales y graduales, determinadas por la activación del Plan Nacional de Protección de las Infraestructuras Críticas, o como consecuencia de comunicaciones de autoridades competentes (art. 25, del Real Decreto 704/2011).

Estos planes están clasificados igualmente como secreto oficial (art. 26, del Real Decreto 704/2011). Se revisan cada dos años (art. 27, del Real Decreto 704/2011).

2.2.2.8.5. Planes de Apoyo Operativo

Los Planes de Apoyo Operativo son documentos en donde se plasman las medidas concretas a aplicar por las administraciones públicas en apoyo a los operadores críticos. Su elaboración debe realizarse en un plazo de cuatro meses a partir de la aprobación del Plan de Protección Específico.

El Plan de Apoyo Operativo contiene las medidas planificadas de prevención, protección y reacción a adoptar por las unidades policiales y las Fuerzas Armadas en caso de activación del Plan Nacional de Protección de Infraestructuras Críticas, o bien, de confirmarse la existencia de amenaza inminente. Estas medidas son complementarias de aquellas graduales que hayan sido previstas por los operadores críticos en sus respectivos Planes de Protección Específicos.

Estos planes están clasificados también como secreto oficial (art. 31, del Real Decreto 704/2011). Se revisan cada dos años (art. 32, del Real Decreto 704/2011).

2.2.3. Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de redes y sistemas de información

Continuando con la normativa, es importante mencionar el Decreto-ley 12/2018 que tiene por objeto regular la seguridad de las redes y sistemas de información utilizados para la provisión de servicios esenciales y de los servicios digitales, y establecer un sistema de notificación de incidentes (art. 1). Este decreto se aplica a la prestación de servicios esenciales dependientes de redes y sistemas de información abarcados en los doce sectores estratégicos definidos en el anexo de la ley 8/2011.

Servicio esencial, a los efectos del Decreto-ley 12/2018, es el "servicio necesario para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las Instituciones del Estado y las Administraciones Públicas, que dependa para su provisión de redes y sistemas de información" (art. 3, c).

2.2.4. Real Decreto-ley 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de redes y sistemas de información

El Real Decreto 43/2021 tiene por objeto desarrollar el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, en lo concerniente al

marco estratégico e institucional de seguridad de las redes y sistemas de información, la supervisión del cumplimiento de las obligaciones de seguridad de los operadores de servicios esenciales y de los proveedores de servicios digitales, y la gestión de incidentes de seguridad (art. 1).

Es de aplicación el Real Decreto 43/2021, en lo que aquí interesa, a los servicios esenciales dependientes de las redes y sistemas de información abarcados en los sectores estratégicos definidos en el anexo de la ley 8/2011.

2.2.5. Límites de la "normativa PIC": aplicabilidad del art. 346, CP

La ley 8/2011, el Real Decreto 704/2011 y el Reglamento de Protección de las infraestructuras críticas -sintetizados con la frase "normativa PIC"- buscan dar seguridad a los planes de protección de las infraestructuras críticas en términos de derecho administrativo, pero no de derecho penal. Observa Jiménez Díaz que en caso de ataque a las infraestructuras críticas, resulta aplicable la figura de estragos prevista en el art. 346 del código penal:

"De este entramado normativo, llegamos a la conclusión de que estas normas tienen unos objetivos claros y marcados, entre los cuales no figura el establecimiento de sanciones en el caso de que se produzcan infracciones. Ya que esta normativa no tiene la función de sancionar la producción de determinados riesgos, sino que su función es la de establecer unos planes de protección sobre las infraestructuras mencionadas, para lograr una mayor seguridad. Por ello, se puede afirmar que la normativa PIC simplemente adelanta las barreras de protección con la creación de estos planes, pero se dejan las posibles sanciones al derecho penal. Por lo tanto, en el caso de que se produzca o intente cometer un ataque contra alguna de estas infraestructuras críticas o esenciales, se ha de acudir a la normativa penal para sancionarlo conforme al delito de estragos, ya que la normativa administrativa no impone sanciones en estos casos" (JIMÉNEZ DÍAZ, 2017, 9).

El art. 346.1, CP, dispone: "Los que provocando explosiones o utilizando cualquier otro medio de similar potencia destructiva, causaren la destrucción de aeropuertos, puertos, estaciones, edificios, locales públicos, depósitos que contengan materiales inflamables o explosivos, vías de comunicación, medios de transporte colectivos, o la inmersión o varamiento de nave, inundación, explosión de una mina o instalación industrial, levantamiento de los carriles de una vía férrea, cambio malicioso de las señales empleadas

en el servicio de ésta para la seguridad de los medios de transporte, voladura de puente, destrozo de calzada pública, daño a oleoductos, perturbación grave de cualquier clase o medio de comunicación, perturbación o interrupción del suministro de agua, electricidad, hidrocarburos u otro recurso natural fundamental incurrirán en la pena de prisión de diez a veinte años, cuando los estragos comportaran necesariamente un peligro para la vida o integridad de las personas".

Se advierte del contenido del art. 346.1, CP, que prácticamente todos los resultados materiales involucran alguno de los 12 sectores estratégicos contenidos en el anexo de la ley 8/2011. Por ejemplo, la perturbación del suministro de electricidad e hidrocarburos afecta al "sector 1" (Energía); la perturbación grave de cualquier medio de comunicación concierne al "sector 2" (Tecnologías de la Información y las Comunicaciones); la destrucción de aeropuertos, puertos, vías de comunicación, medios de transporte colectivos, se relacionan con el "sector 3" (Transporte); la perturbación o interrupción del suministro de agua afecta al "sector 4" (agua).

En el delito de estragos, el bien jurídico directo es la seguridad colectiva. La vida e integridad de las personas son bienes jurídicos de protección indirecta. El delito de estragos se verifica cuando concurren tres requisitos: a) conducta típica; b) resultado material; c) peligro (ROMEO CASABONA, SOLA RECHE y BOLDOVA PASAMAR, 2016, 578).

2.2.6. Código Penal Español

Las infraestructuras críticas han tenido consideración por el legislador español, quien las incluyó a partir del art. 264, CP. Veremos los preceptos a continuación.

2.2.6.1. art. 264, CP

El art. 264.1, CP, establece: "El que, por cualquier medio, sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese o hiciese inaccesibles datos informáticos, programas informáticos o documentos electrónicos ajenos, cuando el resultado producido fuera grave, será castigado con la pena de prisión de seis meses a tres años".

A su vez, el art. 264, apartado 2, CP, dispone: "Se impondrá una pena de prisión de dos a cinco años y multa del tanto al décuplo del perjuicio ocasionado, cuando en las conductas descritas concurra alguna de las siguientes circunstancias: ... 4.ª Los hechos hayan afectado

al sistema informático de una infraestructura crítica o se hubiera creado una situación de peligro grave para la seguridad del Estado, de la Unión Europea o de un Estado Miembro de la Unión Europea. A estos efectos se considerará infraestructura crítica un elemento, sistema o parte de este que sea esencial para el mantenimiento de funciones vitales de la sociedad, la salud, la seguridad, la protección y el bienestar económico y social de la población cuya perturbación o destrucción tendría un impacto significativo al no poder mantener sus funciones".

El art. 264, CP, contempla los llamados "ataques a la integridad de los datos", según la denominación empleada por el art. 4 del Convenio sobre Cibercriminalidad adoptado por el Consejo de Europa en Budapest el 23 de noviembre de 2001. La denominación abarca las conductas de borrar, dañar, deteriorar, alterar, suprimir o hacer inaccesibles datos informáticos, programas informáticos o documentos electrónicos, es decir, los elementos lógicos de un sistema informático. Sin embargo, corresponde resaltar que las escalas penales del art. 264.1, CP (prisión de seis meses a tres años) y 264.2, CP (prisión de dos a cinco años) son totalmente distintas.

Desde la reforma de 2015, el art. 264, apartado 2.4, CP, protege "el buen funcionamiento de infraestructuras críticas, públicas o privadas" (BARRIO ANDRÉS, 2020,76).

El art. 264, apartado 2.4, CP, tiene por objeto material los datos informáticos, programas informáticos o documentos electrónicos contenidos en un sistema que soporta una infraestructura crítica. "Datos" son las unidades básicas de información, cualquiera que sea su contenido, que al ser procesadas dan lugar a la información que resulta de la conexión de uno o más datos. "Programas" son el cuerpo sistemático de instrucciones legibles por la computadora que le permiten realizar una tarea concreta. "Documento electrónico" es el conjunto de datos creado informáticamente o susceptible de procesamiento informático (GÓMEZ TOMILLO, 2015, 351).

Entre los numerosos medios de ataque a los datos, programas o documentos electrónicos cabe mencionar: los *crash programs* o programas de destrucción progresiva, a través de los cuales es posible borrar una gran cantidad de datos en un breve lapso de tiempo; pueden ser de utilidades, escribirse por sí mismos o actuar como caballos de Troya generando rutinas dentro del sistema operativo o del programa de aplicación; las *time bombs* o bombas lógicas de actuación retardada, que destruyen los archivos luego de un

período de tiempo en razón de indicaciones precisas tales como la presencia de un dato, de una hora, de un código, de un nombre; el *superzapping* o uso no autorizado de un programa de utilidad para borrar los datos almacenados en el ordenador o en los soportes magnéticos; se pueden alterar registros sin que quede constancia de la modificación y aun en caso de descubrirse es difícil de detectar quién, cuándo y cómo se hizo; *cancer rutine*, consistente en introducir un conjunto de órdenes que generan su propia reproducción en otros programas arbitrariamente elegidos; pueden ser detectadas y sacadas, pero si permanece alguna el cáncer sigue extendiéndose; *virus programs* o virus, programas que pueden multiplicarse y contaminar otros programas que están en el disco duro y los programas de empresas durante la conexión, entre otros (GÓMEZ TOMILLO, 2015, 354).

El delito se consuma cuando se produce el borrado, el daño, la destrucción, el deterioro, la alteración, la supresión o inutilización de los datos informáticos, programas informáticos o documentos electrónicos. Admite tentativa.

Estamos ante un delito doloso que reclama el conocimiento y voluntad de destruir, alterar o inutilizar los datos informáticos, programas informáticos o documentos electrónicos. Pero no se requiere un ánimo especial.

El art. 264, apartado 2.4, CP, se limita a mencionar el término "infraestructuras críticas" y a incorporar una definición, pero no establece parámetros para determinar la valoración del daño. Incluso, algunos "servicios públicos esenciales" previstos en la agravante del apartado 2.3, CP, coinciden con los servicios de las infraestructuras críticas previstas en el apartado 2.4, CP (VELASCO NÚÑEZ y SANCHIS CRESPO, 2019, 51).

En este sentido, resulta razonable como guía para la mensuración del injusto recurrir a las ya mencionadas "causas de criticidad", previstas en el art. 2, apartado h, de la ley 8/2011. Pues, si la observancia de al menos una de las causas de criticidad es requisito para que una infraestructura resulte clasificable de "crítica", con mayor razón las causas de criticidad sirven para mensurar el daño a un sistema informático de una infraestructura que ya ha sido clasificada como crítica.

La escala penal prevista en el art. 264.2, CP, que trepa hasta los cinco años de prisión, tiene su origen en el art. 9.4, de la Directiva 2013/40/UE. Sin embargo, cinco años de prisión revela una mínima observancia de la citada Directiva. En efecto, resulta ser poco castigo teniendo en cuenta las causas de criticidad, previstas en el art. 2, apartado h, de la ley 8/2011.

Si se observa con agudeza, se advierte que el monto de cinco años de prisión se aleja incluso hasta de lo que ha de entenderse por delito grave conforme al art. 33, CP, es decir, delitos reprimidos con penas superiores a cinco años de prisión. Pues, el art. 33. 1, CP, dispone que "en función de su naturaleza y duración, las penas se clasifican en graves, menos graves y leves"; el art. 33.2, CP, establece un catálogo de castigos a los que considera "penas graves"; entre ellas, la "prisión superior a cinco años". Pero hay más: el art. 33.3, CP, dice expresamente que la "prisión de tres meses hasta cinco años" corresponde a una pena menos grave.

También resulta errada la pena en su mínimo, toda vez que el monto de dos años de prisión permite, para el caso de primera condena, que la pena sea dejada en suspenso, con lo cual, el hacker no pasa por la cárcel.

Todo ello demuestra que la escala penal de dos a cinco años de prisión resulta violatoria de la "prohibición de infraprotección". Cuando hablamos de "Untermassverbot" o "prohibición de infraprotección" (ROXIN y GRECO, 2020, 83), nos referimos a un "mandato de criminalización jurídico-constitucional" que "puede deducirse de los derechos fundamentales de la persona" (WESSELS, BEULKE y SATZGER, 2018, 2). Esta prohibición "representa el límite inferior de la libertad de valoración del legislador" (STAECHELIN, 2000, 289).

El concepto de "prohibición de infraprotección" fue desarrollado por el Tribunal Constitucional Federal alemán, en la conocida discusión en torno a la legislación sobre el aborto, en la oportunidad en que declaró inconstitucional la llamada solución de los plazos –impunidad del aborto en los tres primeros meses del embarazo-. Allí dijo el tribunal germano que "la prohibición de infraprotección (de la Constitución) impide renunciar libremente al uso del derecho penal y a los efectos protectorios de la vida humana que parten de él" (BVerfGE 88, 204, núm. 8, sentencia citada en NAUCKE, 2006, 106).

Según Roxin, la postura del Tribunal Constitucional Federal "merece aprobación para el caso de destrucción de bienes jurídicos fundamentales bajo los estrictos presupuestos mencionados; pues en otro caso el Estado se podría sustraer a su cometido de asegurar la coexistencia pacífica de los ciudadanos, y con ello se estaría desahuciando a sí mismo" (ROXIN, 2015, 65).

Hoy en día la "prohibición de infraprotección" no se limita al ámbito de la punibilidad del aborto, sino que se enmarca en una discusión mucho más amplia. Es opinión tradicional

que el Estado puede verse obligado a proteger determinados valores fundamentales mediante el empleo de normas penales ante amenazas o daños masivos (STAECHELIN, 2000, 290).

En nuestra opinión, si el daño informático a los datos informáticos, programas informáticos o documentos electrónicos de las infraestructuras críticas es tan devastador como el daño físico a tales estructuras, resulta razonable equipararlo a un estrago. Por ese motivo, sería correcto equiparar también la escala penal del daño a los datos informáticos y programas informáticos de las infraestructuras críticas con la escala penal prevista para el delito de estrago. Y es en este punto en donde el legislador español se encuentra en deuda con la Directiva 2013/40/UE, toda vez que la pena máxima debería ser mayor.

2.2.6.2. art. 264 bis, CP

El art. 264, apartado 2.4, CP, debe ser leído junto con el art. 264 bis, CP, en razón de que establece una escala penal agravada (prisión de tres a ocho años y multa del triplo al décuplo del perjuicio ocasionado) cuando en los hechos se afecta un sistema informático de una infraestructura crítica.

El art. 264 bis.1, CP, dispone: "Será castigado con la pena de prisión de seis meses a tres años el que, sin estar autorizado y de manera grave, obstaculizara o interrumpiera el funcionamiento de un sistema informático ajeno: a) realizando alguna de las conductas a que se refiere el artículo anterior; b) introduciendo o transmitiendo datos; o c) destruyendo, dañando, inutilizando, eliminando o sustituyendo un sistema informático, telemático o de almacenamiento de información electrónica. Si los hechos hubieran perjudicado de forma relevante la actividad normal de una empresa, negocio o de una Administración pública, se impondrá la pena en su mitad superior, pudiéndose alcanzar la pena superior en grado".

El art. 264 bis.2, CP, establece: "Se impondrá una pena de prisión de tres a ocho años y multa del triplo al décuplo del perjuicio ocasionado, cuando en los hechos a que se refiere el apartado anterior hubiera concurrido alguna de las circunstancias del apartado 2 del artículo anterior".

El delito previsto en el art. 264 bis, CP, contempla los "ataques contra la integridad del sistema", en la denominación del art. 5 del Convenio de Budapest, que consisten en obstaculizar o interrumpir, en modo grave y sin autorización, el funcionamiento de un sistema informático ajeno borrando, dañando, deteriorando, alterando, suprimiendo o

haciendo inaccesibles datos informáticos, programas informáticos o documentos electrónicos; introduciendo o transmitiendo datos o destruyendo, dañando, inutilizando, eliminando o sustituyendo un sistema informático.

Algunos de los medios para obstaculizar o interrumpir un sistema informático son: el *mail bomber*, proceso que bloquea la dirección del correo electrónico del usuario mediante el envío masivo de información; las *bombas ansi*, que manipulan el funcionamiento del teclado, asignando a las teclas funciones poco ortodoxas (GÓMEZ TOMILLO, 2015, 359); a veces se utilizan "redes botnet" o grupo de equipos informáticos que han sido infectados con software malicioso que permite su control remoto, obligándolos a enviar spam, propagar virus o realizar ataques de denegación de servicio distribuido (DDoS), sin el conocimiento o la autorización de los propietarios de los equipos. Por ello se los denomina *zombies* (BARRIO ANDRÉS, 2020, 85).

El delito se consuma con la obstaculización o interrupción del funcionamiento del sistema informático.

El art. 264 bis, CP, presenta numerosos problemas. En primer lugar, no establece criterio de gravedad de la conducta. Por ello, aquí también resulta útil recurrir a las causas de criticidad.

Algo mejor se ve la escala penal. Pues, un castigo que llega a ocho años de prisión se aproximaría más a la gravedad del injusto y de la culpabilidad. Por otro lado, el mínimo de tres años implica ya una pena de cumplimiento efectivo, es decir, que el hacker pasará por la cárcel. Igualmente, consideramos que la escala penal también resulta insuficiente frente al daño experimentado en las infraestructuras críticas.

Pero hay más. La decisión de si es aplicable la figura básica prevista en el art. 264, apartado 2.4, CP, o bien, la figura agravada del art. 264 bis, CP, resulta extremadamente difícil. Pues, muchos de los virus pueden afectar no sólo los datos y los programas sino también el sistema informático. Si se considera que el caso versa sobre un daño a un dato informático o programa informático de una infraestructura crítica (art. 264, apartado 2.4, CP), la pena mínima será de dos años de prisión; y si, en cambio, se considera que el caso se refiere a una destrucción de un sistema informático de una infraestructura crítica (art. 264 bis apartado 2, CP), la pena mínima será de tres años de prisión.

No compartimos en absoluto la distinción entre "daño a un dato informático o programa informático" y "destrucción de un sistema informático", la cual se presta a interpretaciones acomodaticias en desmedro de la seguridad jurídica.

2.2.6.3. art. 264 ter, CP

Otro precepto relacionado con la temática es el art. 264 ter, CP, que reprime con una pena de prisión de seis meses a dos años o multa de tres a dieciocho meses a quien "sin estar debidamente autorizado, produzca, adquiera para su uso, importe o, de cualquier modo, facilite a terceros, con la intención de facilitar la comisión de alguno de los delitos" previstos en los arts. 264 y 264 bis, CP, "un programa informático, concebido o adaptado principalmente para cometer alguno de los delitos a que se refieren los dos artículos anteriores"; o "una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información".

La reforma de 2015 ha incorporado aquí una especie de acto preparatorio en relación a los delitos previstos en los dos preceptos anteriores (MUÑOZ CONDE, 2015, 416). Sin embargo, también la escala penal de seis meses a dos años de prisión, en forma alternativa con la multa, resulta demasiado baja. Pues, se trata de una escala penal que transita todo su recorrido como pena en suspenso y que, por ende, no asusta a nadie. Menos aún si dicha escala de prisión resulta reemplazable por una multa. Es un castigo inadecuado teniendo en cuenta las causas de criticidad, previstas en el art. 2, apartado h, de la ley 8/2011.

Se advierte aquí igualmente que la escala penal de seis meses a dos años de prisión resulta violatoria de "prohibición de infraprotección".

2.2.6.4. art. 573, CP

Si el ataque informático al sistema de una infraestructura crítica se realiza con finalidad terrorista, resulta aplicable la agravante del terrorismo. Es importante destacar que el código penal español no se preocupa por definir el término "terrorismo", sino que se limita a fijar los elementos subjetivos que han de concurrir en la conducta ilícita concreta previamente tipificada para que pueda ser considerada terrorista (CERRADA MORENO, 2018, 25).

Las finalidades están previstas en el art. 573, CP, y son las siguientes: "1.ª Subvertir el orden constitucional, o suprimir o desestabilizar gravemente el funcionamiento de las

instituciones políticas o de las estructuras económicas o sociales del Estado, u obligar a los poderes públicos a realizar un acto o a abstenerse de hacerlo; 2.ª Alterar gravemente la paz pública; 3.ª Desestabilizar gravemente el funcionamiento de una organización internacional; 4.ª Provocar un estado de terror en la población o en una parte de ella".

Así como el legislador español no se ha preocupado por la definición de terrorismo, tampoco los jueces han sido particularmente exigentes con el principio de máxima determinación de la ley penal. El Tribunal Supremo ha dicho reiteradamente que no es necesario que exista un concepto legal de "terrorismo" para que puedan ser reprimidas como tales determinadas conductas: "La jurisprudencia de esta Sala del Tribunal Supremo igualmente mantiene la doctrina según la cual la determinación del carácter de actividad terrorista por la naturaleza de las acciones de quien las comete es respetuosa con la Constitución, dado que ésta no la define de modo completo, no siendo, por tanto, necesario que exista un concepto legal de terrorismo para que puedan ser castigadas como tales determinadas acciones" (STS 1025/2007 - ECLI:ES:TS:2007:1025).

Para el objeto de la presente investigación, tiene relevancia el art. 573, apartado 2, CP, el cual considera terrorismo los delitos informáticos previstos en los arts. 264 a 264 quater, CP, cuando se cometan con alguna de las cuatro finalidades ya mencionadas en el art. 573 apartado 1, CP.

Resulta objetable, ante todo, la remisión en paquete realizada por el legislador mediante el art. 573.2, CP. Pues, podría ser racional respecto del art. 264 bis, CP, que tipifica conductas graves, sobre todo cuando los ciberataques afectan a sistemas de infraestructuras críticas. Pero no ocurre lo mismo con las conductas previstas en el tipo básico del art. 264, CP. Hubiera sido más adecuado, en lugar de una remisión en bloque, haber hecho referencia únicamente a los arts. 264.2 y 264 bis (GORJÓN BARRANCO, 2021, 113).

Es cuestionable también la excesiva amplitud de las finalidades previstas en el art. 573.1, CP. La primera finalidad -subvertir el orden constitucional, etc.- viene redactada en conceptos tan imprecisos que permiten aplicar la legislación antiterrorista a hechos muy lejanos a la concepción tradicional que se tiene del terrorismo; no se especifica lo que ha de entenderse por "estructuras económicas o sociales del Estado", lo cual se opone al principio de taxatividad (CERRADA MORENO, 2018, 313).

La segunda meta -alterar gravemente la paz pública-, resulta hoy superflua al haberse agregado al art. 573, CP, mediante la Ley Orgánica 2/2015, la finalidad consistente en

"provocar un estado de terror en la población o parte de ella". Esta última meta representa más la esencia del terrorismo y engloba a la anterior, porque una población aterrorizada no puede estar en paz y, por ende, se habrá visto gravemente alterada su paz pública (CERRADA MORENO, 2018, 329).

La tercera finalidad -desestabilizar gravemente el funcionamiento de una organización internacional- también deja un amplio margen de discrecionalidad, la cual resulta igualmente contraria al principio de taxatividad.

El cuarto propósito -provocar un estado de terror en la población- hace referencia a un particular estado emocional que se apodera de sus víctimas, quienes no tienen problema alguno para identificar un atentado terrorista como tal (CERRADA MORENO, 2018, 332).

Surge de lo expuesto que la comisión de un delito informático previsto en los arts. 264, 264 bis y 264 ter contra las infraestructuras críticas con finalidades terroristas conduce a una pena de hasta doce años de prisión. Ello, sin dejar de desconocer que las finalidades terroristas presentan una deficiente técnica legislativa.

2.2.7. Enfoque desde el derecho procesal penal

Los ataques a los sistemas informáticos de las infraestructuras críticas son delitos graves, por más que las escalas penales previstas en los arts. 264, 264 bis, 264 ter y 573, CP, no sean las adecuadas. Son delitos graves, además, en función de las "causas de criticidad" previstas en el art. 2, apartado h, de la ley 8/2011.

Sin embargo, por más grave que sea el delito, no se debe olvidar que el derecho penal no le toca al hacker el sombrero. Esta idea ha sido tomada de una famosa frase que se atribuye Beling: "el derecho penal no le toca al delincuente un solo pelo" (MAIER, 1999, 84). Beling decía que el derecho procesal penal por sí sólo y asilado "no tendría ejecución en la realidad de la vida" (BELING, 1943, 1).

Las "causas de criticidad" permiten a las autoridades la adopción de medidas de investigación intrusivas respecto de ciertos derechos fundamentales previstos en el art. 18, CE, el cual reconoce los derechos al honor, a la intimidad personal, familiar y a la propia imagen (art. 18.1, CE), el derecho a la inviolabilidad domiciliaria (art. 18.2, CE), el derecho al secreto de las comunicaciones (art. 18.3, CE) y el derecho a la protección de datos (art. 18.4, CE).

Estamos ante hechos complejos, toda vez que resulta más difícil identificar a los autores de un ciberdelito, que investigar a los autores de un delito físico. El anonimato que ofrece internet sigue siendo atractivo para la inmensa mayoría de los hackers (ECKE, 2020, 3). Cada dispositivo conectado a internet tiene asignado una dirección IP que funciona como el Documento Nacional de Identidad de la computadora. La IP puede ser estática o dinámica. No es difícil detectarla ni seguirla porque es un dato público, pero existen técnicas para enmascarar tal asignación, como la posibilidad de conectarse a través de redes wi-fi abiertas, la utilización de *proxies* o VPNs, la creación de redes *botnet*, o la red Tor –*The onion router* o el enrutado cebolla (BARRIO ANDRÉS, 2020, 21).

A ello se agrega la volatilidad de las pruebas electrónicas. No se desconoce en esto otra circunstancia relevante: la trasnacionalidad delictiva. El ciberespacio no tiene fronteras. Dado que la internet es global, cualquiera puede actuar desde cualquier parte. Cuando se inicia una investigación en el país afectado contra los autores del ilícito, el proveedor puede encontrarse fuera de su jurisdicción penal, o se puede haber trasladado el contenido a otro servidor radicado en un tercer Estado. Por ello, son decisivos los convenios internacionales (BARRIO ANDRÉS, 2020, 14).

Tal como hemos visto, los componentes del Sistema de Protección de las Infraestructuras Críticas y los instrumentos de planificación asignan a éstas una seguridad reforzada. Por ello, para vencer las barreras de seguridad hacen falta ataques de alta complejidad y tecnología, de difícil detección. La única manera de investigar tales ciberataques es mediante las medidas tecnológicas que se encuentran previstas en la LECrim a partir de la Ley Orgánica 13/2015, de 5 de octubre.

2.2.7.1. Investigación tecnológica

La Ley Orgánica 13/2015 fue una reacción ante la sentencia del Tribunal Constitucional 145/2014, de 22 de septiembre, que puso de manifiesto la necesidad de una reforma legislativa que regule las medidas de investigación concretas que resulten necesarias para esclarecer los delitos cuyas pruebas están contenidas en dispositivos tecnológicos. En su histórica sentencia, el Tribunal Constitucional dijo:

"Es doctrina constante de este Tribunal (por todas, STC 49/1999, de 5 de abril, FJ 3) que aunque la literalidad de dicho precepto ("se garantiza el secreto de las comunicaciones y, en especial, las postales, telegráficas y telefónicas, salvo resolución judicial") puede inducir a

pensar que la única garantía que establece inmediatamente la Constitución es la exigencia de autorización judicial, un análisis más detenido de la cuestión pone de manifiesto lo contrario, ya que, por mandato expreso de la Constitución, toda injerencia estatal en el ámbito de los derechos fundamentales y las libertades públicas, que incida directamente sobre su desarrollo (art. 81.1 CE), o limite o condicione su ejercicio (art. 53.1 CE), precisa, además, una habilitación legal. Esa misma jurisprudencia dispone que la reserva de ley constituye "el único modo efectivo de garantizar las exigencias de seguridad jurídica en el ámbito de los derechos fundamentales y las libertades públicas", lo que "implica exigencias respecto del contenido de la Ley que, naturalmente, son distintas según el ámbito material de que se trate", pero que en todo caso determinan que "el legislador ha de hacer el 'máximo esfuerzo posible' para garantizar la seguridad jurídica", esto es, "la expectativa razonablemente fundada del ciudadano en cuál ha de ser la actuación del poder en aplicación del Derecho" (STC 49/1999, FJ 4). Profundizando en esa exigencia, en la STC 169/2001, 16 de julio, FJ 6, sostuvimos, con abundante cita de Sentencias del Tribunal Europeo de Derechos Humanos, en cuanto a las características exigidas por la seguridad jurídica respecto de la calidad de la ley habilitadora de las injerencias, que "la ley debe definir las modalidades y extensión del ejercicio del poder otorgado con la suficiente claridad para aportar al individuo una protección adecuada contra la arbitrariedad" (ECLI:ES:TC:2014:145).

La ley Orgánica 13/2015 ha establecido las siguientes medidas: la interceptación de las comunicaciones telefónicas y telemáticas, la captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos, la utilización de dispositivos técnicos de seguimiento, localización y captación de la imagen, el registro de dispositivos de almacenamiento masivo de información y los registros remotos sobre equipos informáticos.

2.2.7.2. Principios rectores

Las medidas de investigación se rigen por los principios rectores que se encuentran previstos en el art. 588 bis a, LECrim. Los veremos a continuación.

2.2.7.2.a) Legalidad

Este principio no se encuentra mencionado completamente en el art. 588 bis a.1, LECrim, sino tangencialmente mediante la alusión a "medidas de investigación reguladas en

el presente capítulo...". Pues, cuando el art. 588 bis a.1 dispone: "Durante la instrucción de las causas se podrá acordar alguna de las medidas de investigación reguladas en el presente capítulo", exige que la medida de investigación surja de la ley.

Por otra parte, los artículos restantes del tratamiento común (desde el art. 588 bis a hasta el 588 bis k), mencionan la autorización judicial, los requisitos para la resolución, el secreto de las actuaciones, la duración, las posibilidades de prórroga, el control judicial, etc., y de este modo, delimitan con suficiente precisión en qué situaciones puede disponerse esa medida y hasta qué límite.

2.2.7.2.b) Especialidad

El principio de especialidad ha sido definido por el legislador español en el art. 588 bis a.2: "El principio de especialidad exige que una medida esté relacionada con la investigación de un delito concreto. No podrán autorizarse medidas de investigación tecnológica que tengan por objeto prevenir o descubrir delitos o despejar sospechas sin base objetiva".

El delito se considera suficientemente identificado cuando existan indicios objetivos, esto es, que sean accesibles a terceros y con base real sin valoraciones personales (VELASCO NÚÑEZ y SANCHIS CRESPO, 2019, 273).

2.2.7.2.c) Idoneidad

El principio de idoneidad ha sido caracterizado por el legislador español en el art. 588 bis a.3: "El principio de idoneidad servirá para definir el ámbito objetivo y subjetivo y la duración de la medida en virtud de su utilidad".

Únicamente si la medida tecnológica es útil puede ser autorizada por el juez.

2.2.7.2.d) Excepcionalidad y necesidad

Los principios de excepcionalidad y necesidad vienen de la mano, y están formulados en el art. 588 bis a.4 con el siguiente tenor:

"En aplicación de los principios de excepcionalidad y necesidad solo podrá acordarse la medida:

a) cuando no estén a disposición de la investigación, en atención a sus características, otras medidas menos gravosas para los derechos fundamentales del investigado o encausado e igualmente útiles para el esclarecimiento del hecho, o

b) cuando el descubrimiento o la comprobación del hecho investigado, la determinación de su autor o autores, la averiguación de su paradero, o la localización de los efectos del delito se vea gravemente dificultada sin el recurso a esta medida".

Estos principios resultan vulnerados con peticiones sistemáticas y concesiones rutinarias de las medidas de investigación, según tiene dicho el Tribunal Supremo respecto de las intervenciones telefónicas: "De la nota de excepcionalidad se deriva que la intervención telefónica no supone un medio normal de investigación, sino excepcional en la medida que supone el sacrificio de un derecho fundamental de la persona, por lo que su uso debe efectuarse con carácter limitado, ello supone que ni es tolerable la petición sistemática en sede judicial de tal autorización, ni menos se debe conceder en forma rutinaria" (STS 982/2016, ECLI:ES:TS:2017:40).

2.2.7.2.e) Proporcionalidad

El principio de proporcionalidad ha sido caracterizado por el legislador español en el art. 588 bis a.5: "Las medidas de investigación reguladas en este capítulo solo se reputarán proporcionadas cuando, tomadas en consideración todas las circunstancias del caso, el sacrificio de los derechos e intereses afectados no sea superior al beneficio que de su adopción resulte para el interés público y de terceros. Para la ponderación de los intereses en conflicto, la valoración del interés público se basará en la gravedad del hecho, su trascendencia social o el ámbito tecnológico de producción, la intensidad de los indicios existentes y la relevancia del resultado perseguido con la restricción del derecho".

2.2.8. Registro remoto

Entre las medidas de investigación tecnológica incorporadas por la ley Orgánica 13/2015, existe una que tiene especial relevancia para la compleja investigación de los ciberataques a los sistemas informáticos de las infraestructuras críticas: el registro remoto. Pues, si bien es más invasiva, resulta más difícil de esquivar para los hackers, quienes deben utilizar dispositivos para cometer sus ataques y almacenar información, con lo cual existe una mayor probabilidad de éxito en la investigación (GONZÁLEZ PULIDO, 2022, 508).

Los presupuestos para la autorización judicial del registro remoto están previstos en el art. 588 septies a, LECrim. Hay dos notas esenciales que distinguen al registro remoto respecto de los registros directos: la clandestinidad y el carácter dinámico del registro

(Circular 5/2019, sobre registro de dispositivos y equipos informáticos, de la Fiscalía General del Estado). Veamos, entonces, los presupuestos.

2.2.8.a) Presupuestos del art. 588 septies a, LECrim.

"1. El juez competente podrá autorizar la utilización de datos de identificación y códigos, así como 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, siempre que persiga la investigación de alguno de los siguientes delitos:

a) Delitos cometidos en el seno de organizaciones criminales.

b) Delitos de terrorismo.

c) Delitos cometidos contra menores o personas con capacidad modificada judicialmente.

d) Delitos contra la Constitución, de traición y relativos a la defensa nacional.

e) Delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la telecomunicación o servicio de comunicación.

2. La resolución judicial que autorice el registro deberá especificar:

a) Los ordenadores, dispositivos electrónicos, sistemas informáticos o parte de los mismos, medios informáticos de almacenamiento de datos o bases de datos, datos u otros contenidos digitales objeto de la medida.

b) El alcance de la misma, la forma en la que se procederá al acceso y aprehensión de los datos o archivos informáticos relevantes para la causa y el software mediante el que se ejecutará el control de la información.

c) Los agentes autorizados para la ejecución de la medida.

d) La autorización, en su caso, para la realización y conservación de copias de los datos informáticos.

e) Las medidas precisas para la preservación de la integridad de los datos almacenados, así como para la inaccesibilidad o supresión de dichos datos del sistema informático al que se ha tenido acceso.

3. Cuando los agentes que lleven a cabo el registro remoto tengan razones para creer que los datos buscados están almacenados en otro sistema informático o en una parte del

mismo, pondrán este hecho en conocimiento del juez, quien podrá autorizar una ampliación de los términos del registro".

El art. 588 septies a, LECrim, ha sido tildado de "algo irreal" porque no hay contraseñas mágicas, ni súper usuarios para todo, ni un súper software que brinde acceso a todo. Por ello, era más adecuado hablar de uso de técnicas de intrusión y no limitarse a instrumentos concretos (VELASCO NÚÑEZ y SANCHIS CRESPO, 2019, 494).

El precepto también ha generado dudas en cuanto a su alcance. No parece que el tenor literal de la norma permita desarrollar un seguimiento continuo de la actividad del sospechoso investigado mediante ese dispositivo informático al que se tuvo acceso por vía remota, porque el legislador solamente permite el examen del contenido de un ordenador, pero no el rastreo de la actividad del usuario (OTAMENDI ZOZAYA, 2017, 144).

2.2.8.b) Subsunción en el catálogo

Consideramos que la investigación de un ciberataque a los sistemas informáticos de las infraestructuras críticas puede llevarse a cabo de mediante el registro remoto, toda vez que existe suficiente asidero legal para ello.

En primer lugar, la razón más sencilla es que el ciberataque a los sistemas informáticos de las infraestructuras críticas es un delito cometido a través de "instrumentos informáticos", según lo exige el art. 588 septies a.1, inc. e), LECrim. Esta es la vía natural para canalizar la medida de investigación. Pues, los preceptos del art. 264, 264 bis y 264 ter, CP, no dejan dudas en orden a que un ciberataque a cualquiera de los doce sectores estratégicos contenidos en el anexo de la ley 8/2011 torna operativa la medida del registro remoto de ordenadores.

En segundo término, el ciberataque puede responder a la finalidad terrorista prevista en el art. 573.2, CP, según lo exige el art. 588 septies a.1, inc. b), LECrim.

En tercer lugar, dado que el ciberataque puede ser cometido por organizaciones criminales, el registro remoto podría encontrar asidero en el art. 588 septies a.1, inc. a), LECrim.

Por último, también sería posible fundar el registro remoto en caso de concluir que el ciberataque afecta la defensa nacional en los términos del art. 588 septies a.1, inc. d), LECrim. Sin embargo, esta sería la vía más difícil, porque no todas las infraestructuras críticas conciernen a la defensa nacional.

2.2.8.c) Observancia de los principios rectores

La autorización del registro remoto para investigar un ciberataque a los sistemas informáticos de las infraestructuras críticas estará fundada, según lo dicho hasta aquí, en el catálogo de delitos que la habilitan (art. 588 septies a.1, LECrim). También estará fundada en los principios rectores (art. 588 bis a, LECrim). Veamos.

En lo que respecta al principio de legalidad, corresponde afirmar que el principio se cumple no sólo porque el registro remoto está previsto en la LECrim, sino también porque contiene una reglamentación rigurosa de las circunstancias en que resulta procedente.

El principio de especialidad exige que la medida de registro remoto sea autorizada una vez iniciado el proceso penal, con indicios objetivos de la gravedad del delito y no a modo de prevención.

El principio de idoneidad también se cumple, si se tiene en cuenta que, al igual que en toda investigación compleja, es necesario acceder a una gran cantidad de datos, en un tiempo máximo de un mes, prorrogable hasta tres meses, y que el registro remoto es útil para ello.

La observancia de los principios de excepcionalidad y necesidad es fácil, teniendo en cuenta que debido a la complejidad que presenta la investigación de ciberataques contra los sistemas informáticos de las infraestructuras críticas, no hay a disposición de la investigación medidas menos gravosas e igualmente útiles. Si se tiene en cuenta que los ataques informáticos son desarrollados por hackers, la no utilización de esta técnica haría mucho más difícil la determinación del autor y la averiguación de su paradero.

El principio de proporcionalidad igualmente se verifica, toda vez que, frente a un ciberataque a los sistemas informáticos de las infraestructuras críticas, la afectación de los derechos e intereses de los hackers no es superior al interés público y de terceros en el descubrimiento de semejante hecho. Se entiende que, a pesar de las escalas penales cuestionables, estamos ante un hecho punible grave, de un enorme ámbito tecnológico de producción, sobre lo cual habrá indicios de intensidad. La medida tendrá una importancia decisiva para el juzgamiento y, en su caso, castigo a los responsables.

2.3. PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS EN ARGENTINA

2.3.1. Tutela de infraestructuras críticas en Argentina

Si bien la República Argentina ha incorporado los delitos informáticos al Código Penal mediante la ley 26.388 de 2008, no existe hasta el momento un precepto penal específico similar al español. A continuación, analizaremos los preceptos legales vigentes con miras a determinar si, pese a su generalidad, permiten la subsunción de un ataque a los sistemas informáticos de las infraestructuras críticas.

2.3.2. Estado actual de la legislación vigente

La protección de las infraestructuras críticas presenta en Argentina un estado que podría calificarse como embrionario. A continuación, veremos las principales resoluciones, conceptos y preceptos legales sobre el tema.

2.3.2.1. Resolución 580/2011. Creación del Programa Nacional de Protección de Infraestructuras Críticas de Información y Ciberseguridad.

Las décadas de 1990 y 2000 significaron para la Argentina una actualización legal que fue consecuencia del comercio electrónico. Aparecieron numerosas leyes para acompañar los avances tecnológicos. Fue sancionada la ley 25.326 de protección de datos personales; la ley 25.506 de firma digital (BEKERMAN, 2021, 39). Luego vino la ley 26.388 de delitos informáticos, que ha modificado algunos delitos del código penal. Estaba claro que los avances tecnológicos trajeron grandes ventajas, pero que también la información y la infraestructura digital se encontraba ante nuevas amenazas (BEKERMAN, 2020, 1).

Fue en este contexto en que se conoció la Resolución 580/2011, cuyo art. 1 creaba el "Programa Nacional de Infraestructuras Críticas de información y Ciberseguridad" con el objetivo de elaborar un marco regulatorio específico que "propicie la identificación y protección de las infraestructuras estratégicas y críticas de las entidades y jurisdicciones definidas en el art. 8° de la Ley 24.156 y sus modificatorias, los organismos interjurisdiccionales, y las organizaciones civiles y del sector privado que así lo requieran, así como al fomento de la cooperación y colaboración de los mencionados sectores con miras al desarrollo de estrategias y estructuras adecuadas para un accionar coordinado hacia la implementación de las pertinentes tecnologías".

2.3.2.2. Resolución 1523/2019

Para adquirir panorámica sobre las infraestructuras críticas en Argentina resulta relevante la Resolución 1523/2019 porque establece una definición de infraestructuras críticas; fija criterios de identificación de infraestructuras críticas y menciona los sectores identificados.

2.3.2.2.1. Definición de Infraestructuras Críticas

El Poder Ejecutivo Nacional, a través de la entonces Secretaría de Gobierno de Modernización -Jefatura de Gabinete de Ministros- ha definido mediante la Resolución 1523/2019, Anexo 1, a las infraestructuras críticas como "aquellas que resultan indispensables para el adecuado funcionamiento de los servicios esenciales de la sociedad, la salud, la seguridad, la defensa, el bienestar social, la economía y el funcionamiento efectivo del Estado, cuya destrucción o perturbación, total o parcial, los afecte y/o impacte significativamente".

Años más tarde, la Resolución 28/2022 de la Secretaría Legal y Técnica, de fecha 23/05/2022, ha definido en el glosario a las infraestructuras críticas como: "Activos de carácter esencial e indispensable cuyo funcionamiento es imprescindible y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales".

Como se advierte, la definición contenida en la Res. 28/2022 es similar a la establecida en la Res. 1523/2019, pero establece mayores precisiones, sobre todo porque puntualiza que las infraestructuras críticas son "activos".

2.3.2.2.2. Causas de criticidad

Las "causas de criticidad" se denominan "criterios de identificación" en la legislación argentina; tales criterios están previstos en la resolución 1523/2019 y son:

2.3.2.2.2.a) impacto en la vida humana

Este impacto se verifica en que, debido a la afectación de un sistema informático, "se genere riesgo de pérdida de vida o grave amenaza a la salud e integridad física de las personas";

2.3.2.2.2.b) impacto económico

Este impacto se presenta cuando debido a la afectación de un sistema informático se produce "un daño o amenaza de daño grave, a la estructura productiva y/o financiera del país";

2.3.2.2.2.c) impacto en el medio ambiente:

Existe impacto cuando debido a la afectación de un sistema informático se afecta negativamente o daña gravemente el espacio en el que se desarrolla la vida de los seres vivos;

2.3.2.2.2.d) impacto en el ejercicio de los derechos humanos y de las libertades individuales

Este impacto existe en aquellos casos en que, mediante cualquier acción desarrollada a través de un sistema informático, "se restrinja o coarte indebidamente de manera colectiva, el pleno ejercicio de los derechos consagrados en los Tratados Internacionales, la Constitución Nacional o las leyes";

2.3.2.2.2.e) impacto público o social

Este impacto existe en aquellos casos en que debido a la afectación de un sistema informático se produzcan acontecimientos susceptibles de provocar grave conmoción en una parte significativa de la población;

2.3.2.2.2.f) impacto en el ejercicio de las funciones del Estado

Este impacto existe cuando debido a la afectación de un sistema informático, se afecte de manera sustancial el normal desempeño de los órganos de los poderes Ejecutivo, Legislativo o Judicial;

2.3.2.2.2.g) impacto en la soberanía nacional

Este impacto existe cuando mediante la afectación de un sistema informático se cuestione o restrinja el poder del Estado Nacional en el ámbito del territorio nacional;

2.3.2.2.2.h) impacto en mantenimiento de la integridad territorial nacional

Este impacto se verifica cuando mediante la afectación de un sistema informático, se vulneran las fronteras territoriales, marítimas o espaciales de la nación, sobre todo cuando dicho ejercicio se canaliza a través de la vía judicial.

Se advierte que muchas causas de criticidad argentinas (en particular, las letras “a”, “b”, “c” y “e”) coinciden con las españolas. Las demás (concretamente, las letras “d”, “f”, “g” y “h”) no tienen correlato con las españolas. Sin embargo, un catálogo tan extenso resulta cuestionable por su falta de justificación y su eventual superposición. Por ejemplo, el “impacto en el ejercicio de las funciones del Estado”, cuando se afecta el desempeño del Poder Judicial no parece diferir mucho del “impacto en el ejercicio de los derechos humanos y de las libertades individuales”.

2.3.3. Sectores identificados

La resolución 1523/2019 identifica 11 sectores: 1) Energía; 2) Tecnologías de Información y Comunicaciones; 3) Transportes; 4) Hídrico; 5) Salud; 6) Alimentación; 7) Finanzas; 8) Nuclear; 9) Químico; 10) Espacio; 11) Estado.

2.3.4 Código Penal Argentino

La ley 26.388, B.O. 25/6/2008, ha incorporado un grupo de delitos informáticos al código penal. No todos tienen relación con nuestro objeto de investigación.

Por ello, los preceptos legales en los que se podría subsumir un ataque al sistema informático de las infraestructuras críticas son, a resumidas cuentas, tres (SUEIRO, 2022, 580): el daño informático, previsto en el art. 183, párr. 2, CP; el daño informático agravado, tipificado en el art. 184, inc. 6, CP; y la interrupción de las comunicaciones “de otra naturaleza” -vale decir: comunicaciones electrónicas-, contemplado en el art. 197, CP.

A continuación, nos ocuparemos de estos preceptos.

2.3.4.1. art. 183, párr. 2, CP

El art. 183, párr. 2, CP, reprime con prisión de quince días a un año, a quien "alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños". Se trata del delito de "daño informático".

El daño informático presenta dos facetas: abarca el daño informático propiamente dicho -alterar, destruir o inutilizar datos, documentos, programas o sistemas informáticos- y también la introducción de programas destinados a generar daños, tal como ocurre con los virus informáticos (MOLINA, 2021, 614). Dentro de los virus informáticos se encuentran los caballos de Troya, bombas lógicas y gusanos, entre otros.

La víctima puede ser una persona física, un grupo de personas físicas o una persona jurídica (BUOMPADRE, 2012, 540). No es frecuente que el empleo de virus informáticos en redes telemáticas genere un perjuicio patrimonial único, ya que la alteración de un sistema informático ocasiona normalmente la afectación de datos de terceros (ABOSO, 2021, 1219).

Sin embargo, aquí no estamos ni ante la sombra de un servicio esencial. No se habla de energía, ni de salud, ni de servicio esencial alguno.

La escala penal que comienza en quince días y trepa hasta un año de prisión, además de permitir el cumplimiento en suspenso en todo su recorrido, resulta demasiado baja en comparación con los daños que experimentan los sistemas informáticos de las infraestructuras críticas. Se advierte aquí también entonces, una afectación a la prohibición de infraprotección. Nos remitimos a lo dicho anteriormente en cuanto a la "prohibición de infraprotección".

2.3.4.2. art. 184, inc. 6, CP

El art. 184, inc. 6, CP, dispone que la pena será de tres (3) meses a cuatro (4) años de prisión, si el hecho es ejecutado en "sistemas informáticos destinados a la prestación de servicios de salud, de comunicaciones, de provisión o transporte de energía, de medios de transporte u otro servicio público".

Estamos ante la figura de "daño informático agravado". El tipo penal parece ser más receptivo para la tutela penal de las infraestructuras críticas. Incluso, parte de la doctrina argentina interpreta que el daño informático a las infraestructuras críticas ya se encuentra contemplado en el art. 184, inc. 6, CP.

En este sentido, señalan Cherñavsky, Muniagurria y Moreira, que "si el daño se ejecuta sobre infraestructura crítica (art. 184, CP) la pena se agrava de tres meses a cuatro años. Se entiende que ellos son los servicios de prestación de servicios de salud, de comunicaciones, de provisión o transporte de energía, de modos de transporte u otro servicio público listado en el inc. 6°" (CHERÑAVSKY, MUNIAGURRIA Y MOREIRA, 2018, 149). Reclaman en relación al daño a los sistemas informáticos de las infraestructuras críticas que "una futura reforma prevea mayores penalidades".

La postura de Cherñavsky, Muniagurria y Moreira, que considera incluidas las infraestructuras críticas en el art. 184, CP, a pesar de que el precepto no las menciona expresamente, no resulta descabellada.

Pues, la misma situación se presenta en Alemania. Según el *Bundesamt für Bevölkerungsschutz und Katastrophenhilfe* (Oficina Federal para la Protección de la Población y Asistencia en caso de catástrofe), no existe en el StGB una regulación que contenga una referencia concreta y una definición de infraestructuras críticas. Sin embargo, la principal oficina encargada de proteger a la población en Alemania entiende que en el ámbito de los ciberdelitos –sin referencia concreta a las infraestructuras críticas- entra en consideración una punibilidad según el hecho y la finalidad perseguida conforme a los parágrafos 202a (espionaje de datos), 202b (interceptación de datos), 263a (fraude informático), 269 (falsificación de datos probatorios relevantes), 303a (alteración de datos) y 303b (sabotaje informático). El parágrafo 303b, párr. 4, oración 2, núm. 3, prevé un caso especialmente grave de sabotaje informático para hechos que afecten el abastecimiento de la población con bienes o servicios vitales, o la seguridad de la República Federal de Alemania. Dentro del abastecimiento de los servicios vitales se encuentran los hospitales, la industria energética y el sistema bancario (RENGIER, 2021, 488).

Referencias a la seguridad del abastecimiento de la población se encuentran, además, en el parágrafo 316 StGB (alteración de servicios públicos) y 317 StGB (interrupción de instalaciones de telecomunicaciones). Este último protege las instalaciones de telecomunicaciones de servicio público, en su calidad de servicios de interés público, frente a los riesgos concretos de su explotación.

Agrega el BBK que desde hace algún tiempo existen esfuerzos de algunos Estados Federados por tipificar ciberataques contra las infraestructuras críticas con penas más elevadas. En esta dirección, cabe citar el impreso del Consejo Federal 242/20 del

13/05/2020, en donde está contenida una fundamentación "para una protección jurídico-penal efectiva de las infraestructuras críticas contra los ciberataques" y para ello habría que redactar un nuevo parágrafo 202e. El impreso del Consejo Federal 336/16 del 23/09/2016 aborda también este tema. Hasta el momento no ha tenido lugar una reforma legal (correo electrónico enviado al autor en fecha 30 de marzo de 2023). En este contexto, no parece razonable afirmar que Alemania no tenga protegidas sus infraestructuras críticas debido a la ausencia de una referencia concreta a "infraestructuras críticas" en el código penal.

Sin embargo, tenemos tres objeciones frente a la interpretación que considera implícitamente incluidas las infraestructuras críticas en el art. 184, inc. 6, CP.

En primer lugar, el art. 184, inc. 6, CP, resulta más genérico y amplio que lo requerido para el caso, a tal punto que se ha dicho que lo protegido no es un servicio esencial sino todo servicio público. Así lo ha entendido Riquert: "Nuevamente, la intervención de la ley 26.388 para incluir en el nuevo y último inciso sexto a los sistemas informáticos que aun cuando no necesitan ser de propiedad pública (lo que cae bajo el inc. 5) estén destinados a la prestación de un servicio público. Puede tratarse de cualquier servicio público" (RIQUERT, 2022, 1679).

En segundo término, el art. 184, inc. 6, CP, además de confundir los servicios esenciales con los servicios públicos, parece considerarlos como compartimentos estancos sin tener en cuenta una característica fundamental de las infraestructuras críticas: la interdependencia, la cual ha sido definida en la Resolución 1523/2019, Anexo II, como "una relación bidireccional entre dos infraestructuras a través de las cuales el estado de cada infraestructura influye o se correlaciona con el estado de la otra". Mientras el legislador no recurra a términos más precisos, esta problemática será ineludible.

En tercer lugar, advertimos nuevamente que la tijera sancionatoria que comienza en tres meses de prisión y se abre hasta los cuatro años de prisión, resulta baja en comparación con los daños que experimentan los sistemas informáticos de las infraestructuras críticas. Advertimos igualmente entonces, una afectación a la prohibición de infraprotección.

Se ha cuestionado si realmente los servicios esenciales tienen que estar ubicados en el art. 184, inc. 6, CP, o si quizás, no deberían estar contemplados en art. 186, CP, que regula el estrago. Al respecto, observa Donna que la tipificación del daño causado a los sistemas informáticos destinados a los sistemas de salud, transporte, energía, transporte u otro servicio público, encuentra su justificación en razón de la importancia de estos. La pregunta

es –sostiene el catedrático argentino- "por qué no están en el título siguiente, esto es, en los delitos contra la seguridad pública" (DONNA, 2016, 829).

La postura de Donna olvida que el art. 186, CP, tampoco tiene asidero para los daños informáticos, toda vez que el art. 186, CP, está concebido para daños físicos. Si se considera que el daño sufrido por las infraestructuras críticas tiene errónea ubicación en los ciberdelitos patrimoniales, habría que crear un nuevo bien jurídico.

2.3.4.3. art. 197, CP

El art. 197, CP, reprime con prisión de seis (6) meses a dos (2) años, al que "interrumpiere o entorpeciere la comunicación telegráfica, telefónica o de otra naturaleza o resistiere violentamente el restablecimiento de la comunicación interrumpida".

Para que resulte aplicable la figura prevista en el art. 197, CP, la conducta debe haber creado necesariamente una situación de riesgo común para el servicio de comunicaciones (TAZZA, 2018, 436).

En nuestra opinión, el escenario es similar al que se presenta con el art. 183, CP: no estamos ni ante la sombra de un servicio esencial. Es bastante dudoso que el legislador haya pensado en las comunicaciones de las infraestructuras críticas tan sólo con haber agregado la frase "de otra naturaleza". Si con semejante formulación se pretende tutelar las infraestructuras críticas, habría que haberlo dicho expresamente. En esta tesitura, Gamarra propone la creación de una figura penal específica, que proteja de manera diferenciada las infraestructuras críticas que posibilitan los intercambios telemáticos modernos (GAMARRA, 2019, 256).

Por otra parte, la escala penal que comienza en seis meses y llega hasta los dos años de prisión, más allá de permitir dejar el cumplimiento de la pena en suspenso en toda su extensión, resulta demasiado baja en comparación con los daños que experimentan los sistemas informáticos de las infraestructuras críticas. Se advierte aquí también entonces, una afectación a la prohibición de infraprotección.

2.3.4.4. art. 41 quinquies, CP

La ley 26.734, publicada el 28/11/2011, incorporó el art. 41 quinquies, CP, con lo cual pretendía aprobar la evaluación que realiza el Grupo de Acción Financiera Internacional

(GAFI), de la cual Argentina es miembro. La consecuencia de ello fue la inclusión de una agravante en caso de terrorismo (DE LANGHE, 2019, 319).

Por tanto, si el daño informático es obra de un grupo terrorista, resulta aplicable la agravante prevista en el art. 41 quinquies, CP, que dispone: "Cuando alguno de los delitos previstos en este Código hubiere sido cometido con la finalidad de aterrorizar a la población u obligar a las autoridades públicas nacionales o gobiernos extranjeros o agentes de una organización internacional a realizar un acto o abstenerse de hacerlo, la escala se incrementará en el doble del mínimo y el máximo".

Se trata de una descripción normativa de extrema vaguedad, relacionada con los parámetros internacionales utilizados para la prevención y castigo de los delitos de terrorismo. No resulta claro quién y cómo habrá de constatar el nivel de terror en la población. Lo peor del asunto es que el mismo precepto, en su párrafo segundo, dispone que la agravante no resulta aplicable cuando los hechos tuvieran lugar en ocasión del ejercicio de derechos humanos y/o sociales, o de cualquier otro derecho constitucional. Esto mismo responde a la realidad argentina, que demuestra diariamente el corte de rutas, o vías de acceso público y paralización de servicios de transporte en el centro de la ciudad de Buenos Aires y otros puntos del país, con motivo de dar mayor difusión a los reclamos. La formulación legal resulta excesivamente amplia, y afecta el principio de taxatividad (ABOSO, 2021, 217).

2.3.5. art. 496, Anteproyecto de Reforma Integral al Código Penal de la Nación (Decreto P.E.N. n° 103/2017)

El último esfuerzo legislativo argentino –Anteproyecto de 2017- ha tipificado el daño a los sistemas de infraestructuras críticas en el art. 496, con el título "Daño masivo a sistemas informáticos, a infraestructura crítica del Estado, o como generador de situación de peligro grave para la sociedad".

El precepto reprime con prisión de uno (1) a cinco (5) años, si el hecho hubiere afectado a un número indiscriminado de sistemas informáticos, hubiere afectado el funcionamiento de servicios públicos esenciales o la provisión de bienes de primera necesidad, o hubiere creado una situación de peligro grave para la sociedad.

El art. 496 lleva el *nomen iuris* "infraestructura crítica del Estado", lo cual implica un avance. Además, el art. 496, inc. 2, del Anteproyecto 2017 contiene supuestos de daños a las

infraestructuras críticas, toda vez que allí menciona expresamente el "funcionamiento de servicios públicos esenciales".

Sin embargo, consideramos que los efectos devastadores de un sistema informático de las infraestructuras críticas resultan equiparables al estrago. Por ese motivo, resulta ser más adecuada la escala penal prevista en el delito de estrago. En este sentido, advierte Sueiro que no parece lógica la escala penal proyectada, porque un máximo de cinco años de prisión para conductas con efectos tan devastadores resulta insuficiente. Considera más razonable una escala penal similar a la prevista para el delito de estrago doloso (SUEIRO, 2022, 600).

El texto del art. 186, CP, reprime al que cause incendio, explosión o inundación:

"1º Con reclusión o prisión de tres a diez años, si hubiere peligro común para los bienes;

2º Con reclusión o prisión de tres a diez años el que causare incendio o destrucción por cualquier otro medio:

a) De cereales en parva, gavillas o bolsas, o de los mismos todavía no cosechados;

b) De bosques, viñas, olivares, cañaverales, algodonales, yerbatales o cualquiera otra plantación de árboles o arbustos en explotación, ya sea con sus frutos en pie o cosechados;

c) De ganado en los campos o de sus productos amontonados en el campo o depositados;

d) De la leña o carbón de leña, apilados o amontonados en los campos de su explotación y destinados al comercio;

e) De alfalfares o cualquier otro cultivo de forrajes, ya sea en pie o emparvados, engavillados, ensilados o enfardados;

f) De los mismos productos mencionados en los párrafos anteriores, cargados, parados o en movimiento;

3º Con reclusión o prisión de tres a quince años, si hubiere peligro para un archivo público, biblioteca, museo, arsenal, astillero, fábrica de pólvora o de pirotecnia militar o parque de artillería;

4º Con reclusión o prisión de tres a quince años, si hubiere peligro de muerte para alguna persona;

5º Con reclusión o prisión de ocho a veinte años, si el hecho fuere causa inmediata de la muerte de alguna persona".

A todo lo dicho, parece recomendable con miras a una futura reforma, que el nuevo tipo penal de daño al sistema informático de infraestructuras críticas tenga una escala penal

similar del delito de estrago (art. 186, CP) y una mensuración de la pena basada en las "causas de criticidad".

2.3.6. Necesidad de incorporar una figura penal

Consideramos que la República Argentina no tiene tipificado un precepto específico contra el daño al sistema informático de las infraestructuras críticas. El texto previsto en el art. 184, inc. 6, resulta insuficiente.

Por ello, es necesario incorporar un tipo penal referido al daño informático en el sistema informático de las infraestructuras críticas con una descripción técnicamente adecuada del contenido de ilícito y con una escala penal proporcional a la gravedad del hecho.

2.3.7. Enfoque desde el derecho procesal penal

Hemos visto que en Argentina los delitos informáticos fueron incorporados mayormente por la ley 26.388, la cual resulta insuficiente para concebir las infraestructuras críticas. Por ello, Argentina registra un retraso en la legislación penal en comparación con España.

Argentina no ha sido ajena a los ciberataques. Durante los días 24, 25, 26, 27 y 28 de octubre de 2016 fue víctima de un ciberataque que interrumpió el servicio de administración de justicia. No fue posible hacer uso del sistema informático del Poder Judicial de la Nación; quedó afectado el sistema de gestión judicial Lex 100 y el sistema de notificación electrónica, razón por la cual, la Corte Suprema de Justicia de la Nación declaró la inhabilidad de tales días ("El Consejo de la Magistratura denunció un hackeo al Poder Judicial, 28 de octubre de 2016, DPI Cuántico, dpicuantico.com/2016/10/28/el-consejo-de-la-magistratura-denuncio-el-hackeo-al-poder-judicial/).

A nivel procesal penal el retraso es mayor aún que a nivel penal. Pues, nunca se ha encarado en Argentina una reforma de derecho procesal penal que incorpore medidas de investigación tecnológica.

Ello podría tener su explicación hasta cierto punto. El primer código procesal que rigió en Argentina, el Código de Procedimiento en Materia Penal (ley 2372), fue sancionado el 4 de octubre de 1888 y estuvo vigente hasta el año 1991. Durante la mayor parte de su vigencia no hubo desarrollo tecnológico relevante.

Luego de 1991, cuando entró en vigencia el Código Procesal Penal de la Nación (ley 23.984), tampoco incluyó medidas de investigación tecnológica. Para la época de la sanción de la ley 23.984 –Código Levene-, las computadoras tenían poco desarrollo y no había internet en Argentina en forma masiva. La comercialización de internet comenzó en 1996.

Los debates acerca de las medidas de investigación tecnológica tuvieron inicio luego de 1996; a ello se añade que la discusión no es uniforme, sino que avanza más rápido en algunos códigos procesales penales de algunas provincias que en el Código Procesal Penal de la Nación.

El Convenio sobre Ciberdelincuencia, conocido como Convenio de Budapest, al cual la República Argentina adhirió mediante la ley 27.411 promueve la aplicación de medidas de investigación eficaces en materia de ciberdelitos. La Sección 2a del citado convenio, titulada "Derecho Procesal", fomenta el "registro y decomiso de datos informáticos almacenados" (art. 19) y la "recopilación en tiempo real de datos informáticos" (art. 20). Advertimos, pues, que esta es la segunda vez que el legislador argentino hace caso omiso al Convenio de Budapest: la primera vez fue en 2008, al momento de sancionar la ley 26.388. La segunda vez fue en 2017, paradójicamente, al momento de adherir al referido convenio.

Luego de la adhesión al Convenio de Budapest, resulta inexplicable que el Código Procesal Penal de la Nación no contenga medidas de investigación tecnológica. Pues, mientras los hackers avanzan rápidamente en la comisión de delitos a través de mecanismos digitales cada vez más sofisticados, los investigadores se ven entorpecidos por la ausencia de regulación de medidas de investigación adecuadas. Ello se intenta resolver invocando el principio de libertad probatoria, que según la Corte Suprema de Justicia de la Nación, implica que "el cuerpo del delito puede comprobarse por todos los medios de prueba" (CSJN-Fallos 183:216). Este principio se encuentra previsto también en el art. 134, CPPF: "Podrán probarse los hechos y circunstancias de interés para la solución correcta del caso, por cualquier medio de prueba, salvo que se encuentren expresamente prohibidos por la ley". Al hacer esto, sin embargo, se incurre en una interpretación forzada del principio de libertad probatoria, con miras a incorporar medidas de investigación no previstas en el código de forma (STRATIOTIS, 2022, 450).

Si las medidas de investigación tecnológica estuvieran reguladas en el Código Procesal Penal de la Nación y las infraestructuras críticas estuviesen protegidas por el Código Penal, las "causas de criticidad" permitirían a las autoridades argentinas la adopción de medidas

intrusivas en relación a los derechos fundamentales previstos en los arts. 18 y 19, Const. Nac. Pues, la fundamentación de una medida equivalente al registro remoto basada en los principios rectores establecidos en el art. 588 bis a, LECrim, ofrecería fundamento suficiente para una medida de investigación tecnológica en Argentina.

Se trata de hechos complejos, en los cuales es difícil identificar a los hackers. El anonimato de internet resulta especialmente bondadoso. A ello se agrega la volatilidad de la prueba electrónica.

No desconocemos otra dificultad, cual es la trasnacionalidad delictiva.

2.3.8. Allanamiento virtual

Hemos afirmado que una de las medidas más idóneas para la investigación de un hackeo a los sistemas informáticos de las infraestructuras críticas es el registro remoto. El equivalente funcional en Argentina es el "allanamiento virtual", el cual se utiliza para "extraer información alojada en un dispositivo electrónico de manera remota y subrepticia" (STRATIOTIS, 2022, 443).

Si bien el allanamiento virtual no se encuentra regulado en el Código Procesal Penal de la Nación, existen regulaciones en los códigos procesales de algunas provincias. Por ejemplo, el Código de Neuquén, cuyo art. 153 dispone:

"Artículo 153º Información digital. Cuando se hallaren dispositivos de almacenamiento de datos informáticos que por las circunstancias del caso hicieran presumir que contienen información útil a la investigación, se procederá a su secuestro, y de no ser posible, se obtendrá una copia. O podrá ordenarse la conservación de los datos contenidos en los mismos, por un plazo que no podrá superar los noventa (90) días. Quien deba cumplir esta orden deberá adoptar las medidas necesarias para mantenerla en secreto.
También podrá disponerse el registro del dispositivo por medios técnicos y en forma remota.
A cualquier persona física o jurídica que preste un servicio a distancia por vía electrónica, podrá requerírsele la entrega de la información que esté bajo su poder o control referida a los usuarios o abonados, o los datos de los mismos.

La información que no resulte útil a la investigación no podrá ser utilizada y deberá ser devuelta, previo ser puesta a disposición de la defensa, que podrá pedir su preservación. Regirán las limitaciones aplicables a los documentos".

Mendoza es otra provincia que viene trabajando sobre las medidas de investigación tecnológica y busca adecuar su código procesal penal a lo establecido por el Convenio de Budapest. Tiene un proyecto legislativo en trámite con aprobación del Senado. Se pretende incorporar a la ley 6730 -Código Procesal Penal- los arts. 29 bis, 216 bis, 220 bis, 220 ter, 220 quater y 224 ter. El proyecto incluye, además del agente encubierto informático, el registro de un sistema informático e incautación de datos ("El Senado aprobó la reforma del Código Procesal Penal para incorporar la figura de evidencia digital, 2 de agosto, 2022, https://www.senadomendoza.gob.ar/el-senado-aprobo-la-reforma-del-codigo-procesal-penal-para-incorporar-la-figura-de-evidencia-digital/).

Las regulaciones de Neuquén y Mendoza aportan una luz al final del túnel. Pues, resulta indispensable comenzar a legislar las medidas de investigación tecnológica para combatir ciberdelitos graves, particularmente con el registro remoto o allanamiento virtual, que afectan la intimidad y la privacidad (arts. 18 y 19, CN), y reclaman una regulación específica.

3. Conclusiones

3.1. Conclusiones en torno a la legislación española

Hasta el momento la protección de las infraestructuras críticas en España parece conformarse con la transposición de directivas europeas y la adopción de medidas técnicas y de derecho administrativo. Si bien el legislador español ha incorporado las infraestructuras críticas al Código Penal, no parece haber advertido el efecto devastador que produce el daño en sus sistemas informáticos a la hora de traducirlo a escalas penales.

Varias razones nos conducen a afirmar que el código penal español ha incorporado el daño informático a los sistemas de las infraestructuras críticas de manera deficiente. Veamos.

El art. 264, apartado segundo, CP, establece una escala penal de dos a cinco años que resulta insuficiente, si con ello se piensa en un castigo frente a ataques deliberados de tipo cibernético. Dejamos al margen los ataques físicos porque ya están reprimidos con el precepto de estrago, conforme el art. 346, CP.

El art. 264 bis, CP, establece una figura agravada con una escala penal que parece ser más proporcional (de tres a ocho años de prisión). No obstante, igualmente resulta insuficiente para los daños informáticos experimentados por las infraestructuras críticas. Además, el art. 264 bis, CP, contiene un tenor literal que hace muy difícil de desentrañar si resulta aplicable la figura básica prevista en el art. 264, CP, o bien, el tipo agravado del art. 264 bis, CP. Estamos ante una redacción que carece de parámetros racionales objetivos y se presta a interpretaciones acomodaticias en desmedro de la seguridad jurídica.

El art. 264 ter, CP, reprime la facilitación de un programa informático, o de una contraseña, para cometer un daño a las infraestructuras críticas con una pena de seis meses a dos años de prisión. También se trata de una escala penal demasiado baja.

La figura de terrorismo prevista en el art. 573, CP, conlleva una pena agravada, la cual trepa hasta los doce años de prisión. Lo que ocurre es que si el ataque viene en formato de atentado terrorista habrá que contar con dificultades adicionales para llevar a los terroristas a juicio.

En nuestra opinión, resulta más acorde con la importancia de las estructuras críticas la escala penal prevista para los delitos de estrago (art. 346, CP). No es coherente que un

ataque físico a una infraestructura crítica tenga una pena de diez a veinte años de prisión, mientras que un ataque a un sistema informático de una estructura crítica tenga una pena de dos a cinco años de prisión.

Los límites de rendimiento de los tipos penales junto a sus escalas penales también deben ser observados. Pues, aquí rige que "el derecho penal no le toca al hacker el sombrero". De allí que resulten esenciales las medidas de investigación tecnológica, en particular, el registro remoto y los convenios internacionales.

3.2. Conclusiones respecto de la legislación argentina

La legislación española ha dejado algunas enseñanzas que deberían ser aprovechadas por el legislador argentino. La primera de ellas reside en que la figura que tipifique el daño al sistema de las infraestructuras críticas debe poder deslindarse cuidadosamente de las figuras de daño informático simple (art. 183, CP) y daño informático agravado (art. 184, inc. 6, CP), de modo de evitar la superposición que hoy existe entre los arts. 264 y 264 bis del CP español.

Pues, si la futura reforma penal vuelve a confundir servicios esenciales con servicios públicos, o tratar los objetos de protección como compartimientos estancos, el precepto venidero sobre infraestructuras críticas podría quedar rápidamente vacío de contenido.

La segunda de las enseñanzas radica en que la escala penal prevista para el daño a las infraestructuras críticas debería ser algo "serio". Y en esto, se debería evitar el error existente en el art. 264 del CP español, que reprime el daño al sistema de las infraestructuras críticas con una pena que en su mínimo (dos años de prisión) permite que el condenado no concurra a la cárcel.

Dado que España admite dejar en suspenso la ejecución de penas privativas de libertad de hasta dos años (art. 80, apartado primero, CP español), este mismo razonamiento trasladado al CP argentino implica que la pena mínima no debería ser inferior a tres años y seis meses de prisión. Pues, lo que para España es dos años como límite a la pena privativa de libertad de ejecución en suspenso, para Argentina son tres años (art. 26, CP argentino).

La tercera de las enseñanzas pasa por tipificar la futura figura de daño al sistema de infraestructuras críticas con una escala penal similar a la prevista en el delito de estrago, pero con un mínimo de tres años y seis meses de prisión.

Una cuarta enseñanza consiste en aplicar las causas de criticidad a los fines de establecer graduaciones de pena.

La última enseñanza proviene del derecho procesal penal. Resulta imperioso acomodar el Código Procesal Penal de la Nación al derecho procesal del Convenio de Budapest. También es deseable que en un futuro cercano todas las provincias incorporen en su legislación de forma las medidas de investigación tecnológica. De este modo se superaría la crisis actual en que el principio de libertad probatoria se encuentra desbordado por las nuevas tecnologías.

Referencias bibliográficas

ABOSO, G. E., *Código Penal de la Nación. Comentado y Anotado*, 6a ed, Buenos Aires: Euros, 2021.

BARRIO ANDRÉS, M., *Ciberdelitos 2.0. Amenazas criminales en el ciberespacio*, 2a ed, Buenos Aires: Astrea, 2020.

BEKERMAN, U., "Algunas medidas de ciberseguridad en Argentina, Colombia, Cuba, Egipto, Francia, Grecia, Japón, Singapur y Turquía", *Diario DPI*, Suplemento Derecho y Tecnologías Nro. 66 –07.08.2020.

BEKERMAN, U. "Ciberseguridad en Argentina: La Protección de las infraestructuras críticas", en *Sistema penal e informática*, Riquert M. A (dirección), Sueiro, C. Ch. (Coordinación), t. 4, Buenos Aires: Hammurabi, 2021.

BELING, E., *Derecho Procesal Penal*, trad. de M. Fenech, Barcelona: Labor, 1943.

BELTRÁN, M. (Coord.) y SEVILLANO, F. (Coord.), *Ciberseguridad e infraestructuras críticas*, Madrid: RA-MA, 2021.

BLANCO, H., *Tecnología informática e investigación criminal*, Buenos Aires: Thomson Reuters La Ley, 2020.

BRITO ACUÑA, G., "Garantía de disponibilidad en infraestructuras críticas CNS/ATM", *Sinergia Académica*, 11/2020, vol. 2, núm. 1, pp. 1-10.

BUOMPADRE, J. E., *Manual de Derecho Penal. Parte Especial*, Buenos Aires: Astrea, 2012.

CERRADA MORENO, M., *El terrorismo. Concepto jurídico*, Barcelona: Bosch, 2018.

CHERÑAVSKY, N. A., MUNIAGURRIA, P. H. y MOREIRA, D. A, "A diez años de la ley de delitos informáticos. Balance y propuestas", en *Sistema penal e informática*, Riquert M. A. (dirección), Sueiro, C. Ch. (Coordinación), t. 1, Buenos Aires: Hammurabi, 2018.

CORREA-HENAO, G. J. y YUSTA-LOYO, J. M., "Seguridad energética y protección de infraestructuras críticas", Lámpsakos, julio-diciembre, 2013, Medellín - Colombia, pp. 92-108.

DE LANGHE, M., "Art. 41 "quinquies". Agravante genérica de las penas de los delitos cometidos con la finalidad de infundir el terror público", 275/371. En ZAFFARONI, E. R. (Dir.), *Código Penal y normas complementarias*, t. 2, 3a ed., Buenos Aires: Hammurabi, 2019.

DONNA, E. A., *Derecho Penal. Parte Especial*, t. II-B, 3a ed., Santa Fe: Rubinzal Culzoni, 2016.

ECKE, D., *Kritische Infrastrukturen in Deutschland. Bedrohung und Schutz*, 2020: Grin, https://www.grin.com/document/1003754.

FERNÁNDEZ FERNÁNDEZ, F. J, "Protección de infraestructuras críticas frente al ciberterrorismo, Trabajo fin de Máster, UNIR.

FERNÁNDEZ GARCÍA, E., "Derecho de la ciberseguridad de las infraestructuras críticas: más allá de la perspectiva penalista", *Revista Jurídica de Castilla y León*, 2022, n° 56, enero 2022, pp. 109-141.

GALINDO SIERRA, F. J., Protección de infraestructuras críticas: un análisis de derecho comparado, Facultad de Derecho, Universidad de Málaga, 2017, https://1library.co/document/qvl05l6r-protecci%C3%B3n-infraestructuras-cr%C3%ADticas-an%C3%A1lisis-derecho-comparado.html.

GAMARRA, S.E., "El tipo penal de interrupción de comunicaciones en el Anteproyecto de Código Penal. Ciberataques y protección de las infraestructuras críticas en la era digital", *Revista de Derecho Penal y Criminología*, 2019.

GÓMEZ TOMILLO, M. (director), *Comentarios prácticos al Código Penal*, t. III, Pamplona: Thomson Reuters, 2015.

GONZÁLEZ PULIDO, I. *Diligencias de investigación tecnológicas para la lucha contra la ciberdelincuencia grave* (tesis doctoral), Universidad de Salamanca, 2022.

GORJÓN BARRANCO, M. C., "Sabotaje informático a infraestructuras críticas: análisis de la realidad criminal recogida en los artículos 264 y 264 bis del Código Penal. Especial referencia a su comisión con finalidad terrorista", *Revista de Derecho Penal y Criminología*, 2021, n° 25, 3a Época, pp. 77-124.

GUTERRES, E. C., "Regulação de Riscos e Proteção de Infraestruturas Críticas: os novos ventos do fenômeno regulatório", *Revista de Direito, Estado e Telecomunicações*, Brasília, v. 8, n. 1, maio 2016, pp. 81-134.

JIMÉNEZ DÍAZ, V., *Delitos colectivos. Regulación del Delito de Estragos*, 2017, Universidad de Salamanca, Trabajo Fin de Grado.

KELSEN, H., *Teoría pura del derecho*, trad. de la 2a ed. alemana por R. Vernengo, México, D.F.: Porrúa, 1993.

LISA Institute (29 de abril de 2023). *Infraestructuras Críticas: definición, planes, riesgos, amenazas y legislación*, https://www.lisainstitute.com/blogs/blog/infraestructuras-criticas

MAIER, J. B. J., *Derecho Procesal Penal*, t. I, 2a ed., Buenos Aires: Editores del Puerto, 1999.

MOLINA, G. J., *Manual de Derecho Penal. Parte Especial*, Resistencia: Contexto, 2021.

MUÑOZ CONDE, F., *Derecho Penal. Parte Especial*, 20a ed., Valencia: tirant lo blanch, 2015.

NAUCKE, W., *Derecho Penal*. Una introducción, trad. de la 10a ed. alemana por L. G. Brond, Buenos Aires: Astrea, 2006.

OTAMENDI ZOZAYA, F., *Las últimas reformas de la Ley de Enjuiciamiento Criminal. Una visión práctica tras un año de vigencia*, Madrid: Dykinson, 2017.

RAMONET, I., *El imperio de la Vigilancia. Nadie está a salvo de la red global de espionaje*, trad. por M. Sacristán, Buenos Aires: Le Monde Diplomatique – Capital Intelectual, 2016.

RENGIER, R., *Strafrecht. Besonderer Teil* I, 23 ed., Múnich: Beck, 2021.

RIQUERT, M. A. (director), *Código Penal de la Nación, Comentado y Anotado*, t. II, 2a ed., Buenos Aires: Erreius, 2022.

ROMEO CASABONA, C. M., SOLA RECHE, E., BOLDOVA PASAMAR, M. A., (Coordinadores), *Derecho Penal. Parte Especial*, Granada: Comares, 2016.

ROXIN, C., *Derecho Penal, Parte General*, t. I, trad. de la 2a ed., por Luzón Peña y otros, Buenos Aires: Thomson Reuters, 2015.

ROXIN, C. y GRECO, L., *Strafrecht. Allgemeiner Teil*, t. I. 5a ed., Múnich: Beck, 2020.

Seguridad en entornos de ocio, Las infraestructuras críticas en el Código Penal: daños informáticos https://seguridadenentornosdeocio.com/2016/05/12/las-infraestructuras-criticas-en-el-codigo-penal-danos-informaticos/

STAECHELIN, G., "¿Es compatible la "prohibición de infraprotección" con una concepción liberal del derecho penal?, 289/304. En Instituto de Ciencias Criminales de Frankfurt, *La insostenible situación del Derecho Penal*, edición española por el Área de Derecho Penal de la Universidad Pompeu Fabra, Granada: Comares, 2000.

STRATIOTIS, D., "Los allanamientos remotos y el uso de drones", 443-476. En DUPUY, D. S., *Innovación en investigaciones digitales*, Buenos Aires: Hammurabi, 2022.

SUEIRO, C. Ch., "Ciberataques y la propuesta del Anteproyecto de reforma integral al Código Penal de la Nación", 569-604. En ABOSO, G. E, (Dir.), *Ciberdelitos. Análisis doctrinario y jurisprudencial*, Buenos Aires: elDial.com, 2022.

TAZZA, Alejandro, *Código Penal de la Nación Argentina Comentado. Parte Especial*, t. II, Santa Fe: Rubinzal Culzoni, 2018.

VELASCO NÚÑEZ, E. y SANCHIS CRESPO, C., *Delincuencia informática. Tipos delictivos e investigación. Con jurisprudencia tras la reforma procesal y penal de 2015*, Valencia: Tirant lo blanch, 2019.

WESSELS, J., BEULKE, W. y SATZGER, H., *Derecho Penal. Parte General*, trad. de la 46a ed. Alemana por Pariona Arana, R., Lima: Instituto Pacífico, 2018.

Jurisprudencia

STSJ CAT 1752/2023 - ECLI: ES: TSJCAT:2023:1752

STC 145/2014 - ECLI:ES:TC:2014:145

STS 982/2016 - ECLI:ES:TS:2017:40

STS 1025/2007 - ECLI:ES:TS:2007:1025

BVerfGE 88, 204

BVerfGE 39, 1, 45

CSJN-Fallos 183:216

Listado de abreviaturas

BBK	*Bundesamt für Bevölkerungsschutz und Katastrophenhilfe* (Oficina Federal para la Protección de la Población y Asistencia en caso de catástrofe)
B.O.	Boletín Oficial de la República Argentina
BVerfGE	*Entscheidung des Bundesverfassungsgerichts* (sentencia del Tribunal Constitucional alemán).
CE	Comunidad Europea; Constitución Española
CN	Constitución Nacional de la República Argentina
CNPIC	Centro Nacional para la Protección de las infraestructuras Críticas
CP	Código Penal
CPPF	Código Procesal Penal Federal de la República Argentina
CSJN-Fallos	Fallos de la Corte Suprema de Justicia de la Nación.
etc.	etcétera
ES	España
Incibe	Instituto Nacional de Ciberseguridad
LECrim	Ley de Enjuiciamiento Criminal española
PEN	Poder Ejecutivo Nacional
PIC	Protección de las infraestructuras Críticas
StGB	*Strafgesetzbuch* (Código penal de Alemania)
STS	sentencias del Tribunal Supremo
TS	Tribunal Supremo
UE	Unión Europa