Anuario de la Facultad de Derecho. Universidad de Extremadura 37 (2021): 75-118
ISSN: 0213-988X – ISSN-e: 2695-7728

Doi: https://doi.org/10.17398/2695-7728.37.75

DESAFÍOS JURÍDICOS INTERDISCIPLINARES DE LA CIBERSEGURIDAD NACIONAL: APUNTES *DE LEGE FERENDA*

INTERDISCIPLINARY LEGAL CHALLENGES OF NATIONAL CYBERSECURITY: "DE LEGE FERENDA" NOTES

EDUARDO FERNÁNDEZ GARCÍA[1]

Universidad Isabel I

Recibido: 10/11/2021 Aceptado: 30/12/2021

RESUMEN

Una sociedad hiperconectada como la actual española debe hacer frente al incremento de riesgos y amenazas que se ciernen sobre la seguridad pública y la seguridad nacional en el paso del mundo físico al lógico. El ciberespacio ha pasado a interesar al Derecho en distintas ramas. La ciberseguridad, en consecuencia, ha sido regulada parcialmente por normas administrativas y penales, pero algunas implicaciones constitucionales resultan de extraordinaria importancia, como ha puesto de relieve el conjunto de medidas adoptadas por la pandemia, deviniendo insuficiente la previsión de planes y normas anteriores. Una mirada crítica a la normativa vigente arroja resultados altamente insatisfactorios, por lo que sería deseable que el ordenamiento plantease a corto plazo

1 Profesor de Derecho de la Seguridad en la Universidad Isabel I (Burgos); Profesor asociado de Historia del Pensamiento y de los Movimientos Políticos y Sociales de la Universidad de León. Doctor por la Universidad de León; licenciado en Derecho; graduado en Ciencia Política y de la Administración; graduado en Geografía e Historia; graduado en Español Lengua y Literatura y graduado en Economía. Ha desempeñado diversos cargos públicos en relación con la seguridad y la protección civil y ha sido Diputado Nacional en el Congreso en las legislaturas X, XI y XII.

mayor capacidad de protección de los ciudadanos y de resistencia a los ciberataques, con escrupuloso respeto a los derechos fundamentales. Se propone aquí una metodología multidisciplinar de análisis de situación y un conjunto de propuestas legislativas que afectan a varios campos, y de ahí la necesidad de interdisciplinariedad jurídica, no exenta de una mirada politológica.

Palabras clave: interdisciplinariedad, Derecho de la ciberseguridad, reforma legislativa, paradigma de seguridad integral y global

ABSTRACT

A hyper-connected society such as the current Spanish one must face the increase in risks and threats that loom over public safety and national security in the transition from the physical to the logical world. Cyberspace has become an object of study of Law. Cybersecurity, consequently, has been partially regulated by administrative and criminal regulations, but some constitutional implications seem to have extraordinary importance, as the set of measures adopted by the pandemic has highlighted, due to the insufficient performance of previous plans and regulations. A critical vision of the current regulations yields highly unsatisfactory results, so it would be desirable for the legal system to propose, in the short term, greater capacity to protect citizens and resist cyberattacks, with scrupulous respect for fundamental rights. A multidisciplinary methodology for situation analysis and a set of legislative proposals that affect various fields are proposed here, therefore is postulated the need for legal interdisciplinarity, not exempt from a political perspective.

Keyword: interdisciplinarity, Cybersecurity Law, legislative reform, total and global security paradigm.

1. A MODO DE INTRODUCCIÓN: CIBERESPACIO, SEGURIDAD PÚBLICA Y DERECHO

Asistimos a un escenario en el que simultáneamente se produce un cierto asombro por parte de la opinión pública ante algunos notables y mediáticos ciberataques contra Administraciones Públicas españolas y se anuncian diversas iniciativas políticas e institucionales para modificar aspectos sustanciales del ordenamiento jurídico concernientes a la ciberseguridad en España, desde perspectivas complementarias, principalmente administrativa y penal. Es el momento de recordar que los retos jurídicos a los que se enfrenta la ciberseguridad en España no son menores que los desafíos tecnológicos, pero se producen con un mayor decalaje temporal entre la necesidad social y la respuesta legislativa. Este contexto es particularmente preocupante cuando se dibuja en relación con la seguridad nacional y la seguridad de las infraestructuras críticas, en ambos casos en el ciberespacio. Se aboga aquí por una variación de la mentalidad con la que se acomete el proceso de reforma legal a este respecto, particularmente en dos sentidos: de un lado, una mayor necesidad de interdisciplinariedad de la utilizada para las modificaciones legislativas en otras ramas del Derecho Público; de otro, una mayor celeridad para acompasarse al vertiginoso ritmo en el que se producen las modificaciones de las herramientas tecnológicas de comisión de ilícitos administrativos y penales.

La seguridad nacional en sus múltiples facetas, de mayor profundidad que la seguridad pública en el ciberespacio[2], ha tenido que acomodarse a los distintos dominios de operaciones en que han pasado a actuar las Fuerzas y Cuerpos de Seguridad y las Fuerzas Armadas. España asumió con rapidez que el desarrollo de un quinto dominio operativo diferente al espacial se estaba fortaleciendo con rapidez hace dos décadas y adaptó sus organismos públicos de seguridad a él. Lo hizo tanto en su faceta civil al servicio de la sociedad -así el Incibe- y de la

2 Ofelia Tejerina Rodríguez, "Seguridad pública en el mundo digital", en *Sociedad Digital y Derecho*, ed. Tomás de la Quadra-Salcedo y Fernández del Castillo y José Luis Piñar Mañas (Madrid: Ministerio de Industria, Comercio y Turismo, 2018), 553-72; María José Caro Bejarano, "Alcance y ámbito de la seguridad nacional en el ciberespacio", *Cuadernos de estrategia*, n.o 149 (2011): 47-82.

propia Administración Pública -como el Centro Criptológico Nacional-, como en su vertiente policial -con varios cuerpos policiales con unidades especializadas, el CNP, la Guardia Civil y algunas policías autonómicas, y el CNPIC- y militar -del Mando Conjunto de Ciberdefensa al Mando Conjunto del Ciberespacio desde 2020-. Con escrupulosa atención a las exigencias constitucionales[3], y a pesar de unos inicios titubeantes[4], el Derecho regulador de la seguridad, pública, ciudadana y nacional se ha acompasado a esa evolución[5] con un elevado grado de especialización, pero con unos tiempos muy diferentes a los de las innovaciones técnicas.

La pregunta inicial a la que responden varios condicionantes a los que atender a lo largo de este artículo es ¿cómo se controla -no sólo se regula- jurídicamente el ciberespacio como nuevo dominio de la seguridad nacional? Probablemente en tanto no se afronte realistamente una respuesta a ese interrogante lo único que se promoverá por las instancias políticas serán soluciones jurídicas muy parciales que no tienen presente que hay diferentes visiones conceptuales sobre este objetivo de dominio, tanto a escala regional como mundial, que impelen a una clarificación de la respuesta activa de las democracias avanzadas y del Estado democrático de Derecho frente a la nuda fuerza de algunos regímenes políticos de corte más autoritario, que no dudan en ocupar parcelas en el ciberespacio que comprometen la seguridad nacional de muchos países occidentales.

¿A los efectos de este articulo qué es el ciberespacio y qué notas reviste que modifiquen las previsiones ordinarias de protección del ordenamiento jurídico respecto a la seguridad nacional en el mundo físico? Semejantes preguntas indican desde el comienzo la necesidad de precisiones conceptuales anteriores incluso a abordar una metodología jurídica interdisciplinar para todas las

3 Ignacio Álvarez Rodríguez, "Constitución y Derecho del Ciberespacio", en *Nuevos retos de la ciberseguridad en un contexto cambiante*, ed. Covadonga Mallada Fernández (Cizur Menor: Aranzadi Thomson Reuters, 2019), 21-46.

4 Cesáreo Gutiérrez Espada, "¿Existe (ya) un derecho aplicable a las actividades en el ciberespacio?", en *Nuevas tecnologías en el uso de la fuerza: drones, armas autónomas y ciberespacio*, ed. María José Cervell Hortal (Cizur Menor: Thomson Reuters Aranzadi, 2020), 225-48.

5 Emilio Suñé Llinas, "Del derecho de la informática al derecho del ciberespacio y a la constitución del ciberespacio", *Estudios jurídicos* 2007 (2007).

reformas legislativas pendientes. En realidad, es necesaria una previa delimitación epistémica en atención a la peculiaridad de los bienes jurídicos concretos, que abarcaría simultáneamente distintas ramas del Derecho[6], puesto que no se puede mantener la imagen de estanqueidad y suficiencia de ninguna de ellas por sí sola[7] a la hora de configurar un auténtico derecho a la ciberseguridad[8].

No es suficiente una definición como la ofrecida para el campo de la ciberdefensa por la Cumbre de Varsovia de la OTAN en 2016[9], como esfera de interés e influencia en la que llevar a cabo actividades, funciones y operaciones que se entienden específicamente como misiones de control sobre el oponente, pues hay un componente de la seguridad nacional que se despliega en positivo para el disfrute de las libertades sin oponente a priori, más que el que desea limitar o impedir el ejercicio de los derechos constitucionales.

Son muchas las definiciones posibles, pero confluyen sobre un conjunto reducido de notas caracterizadoras que se han recogido expresamente en la Estrategia de Seguridad Nacional española 2017, además de su naturaleza virtual y artificial al ser creado por el ser humano: "el ciberespacio es un escenario con características propias marcadas por su componente tecnológico, fácil accesibilidad, anonimidad, alta conexión y dinamismo"; los mismos caracteres se han señalado reiteradamente por la doctrina como amplificadores de riesgos y amenazas[10] dada la inexistencia de fronteras geográficas y el posible uso clandestino sin necesidad de desplazamientos. Como repetidamente se ha puesto de manifiesto por los responsables españoles de la ciberseguridad es el medio ideal para el enfrentamiento asimétrico e híbrido.

---

6 Ver la conexión desde lo epistémico a lo metodológico en Adolfo Jorge Sánchez Hidalgo, *Epistemología y metodología jurídica* (Valencia: Tirant lo Blanch, 2019).

7 Claudio Souto, "La ficción de la autosuficiencia en los saberes jurídicos fundamentales", *Doxa: Cuadernos de Filosofía del Derecho*, n.o 3 (1986): 149-57.

8 Carlos Galán, "El derecho a la ciberseguridad", en *Sociedad Digital y Derecho*, ed. Tomás de la Quadra-Salcedo y Fernández del Castillo y José Luis Piñar Mañas (Madrid: Ministerio de Industria, Comercio y Turismo, 2018), 573-90.

9 Que venía a completar la de dos años antes en las *NATO Cyber Defence taxonomy and definitions*: "Dominio global formado por los sistemas TIC y otros sistemas electrónicos, su interacción y la información que es almacenada, procesada o transmitida por estos sistemas"

10 Ver Moisés Barrio Andrés, *Ciberdelitos. Amenazas criminales del ciberespacio* (Madrid: Reus, 2017), 33-40.

La tendencia incremental a la hiperconectividad[11] que caracterizaba en el último lustro a la sociedad española se ha intensificado profusamente debido a las restricciones de movilidad y conexión física introducidas normativamente como consecuencia de las recomendaciones sanitarias de distanciamiento social por la pandemia de Covid 19. Los requerimientos acumulados en la esfera técnica y la dimensión jurídica requieren el acompasamiento de dos paradigmas altamente exigentes. De un lado, lo que se fraguaba claramente como un diferente entorno de relaciones sociales y económicas al que debía adaptarse el ordenamiento jurídico ha devenido un condicionante absoluto para el actual paradigma de la seguridad integral, que afecta a la vez a la dimensión interna y externa o internacional que deben protegerse jurídicamente al mismo tiempo[12]. Empresas y Administraciones han tenido que aclimatarse a esta coyuntura, y parecen hacerlo mejor las primeras que las segundas, probablemente porque los instrumentos para implementar nuevas medidas sean de naturaleza muy distinta: planes en el caso de las compañías, normas jurídicas en el de las Administraciones Públicas. Por otra parte, del nuevo paradigma de la omniconectividad permanente se ha derivado la correlativa necesidad de mecanismos jurídicos que protejan los derechos constitucionales, tanto frente a las eventuales extralimitaciones y ataques antijurídicos que posibilita el uso irrestricto de tecnologías muy disruptivas, pero a la vez enormemente invasivas, como frente a los mecanismos telemáticos igualmente amplios de los poderes públicos en la persecución de los ciberdelitos.

Del ruego de los sectores técnicos para actualizar las leyes y reglamentos que regulan el Derecho de la Ciberseguridad se ha pasado a una necesidad social ampliamente sentida, lo que demanda una pronta puesta al día de las principales normas, tanto administrativas como penales y procesales. Cuando ya empiezan a circular propuestas concretas y se sugiere dar forma a textos articulados que pasarán al Parlamento entre la presente legislatura nacional y la siguiente,

11 Ángel Gómez de Ágreda, "Ciberseguridad en un mundo hiperconectado", en *Ciberseguridad. Un nuevo reto para el Estado y los gobiernos locales*, ed. Dolors Canals i Ametller (Madrid: Wolters Kluwer, 2021), 29-62.
12 Daniel Fernández Bermejo y Gorgonio Martínez Atienza, *Ciberseguridad, ciberespacio y ciberdelincuencia* (Cizur Menor: Aranzadi Thomson Reuters, 2018), 88.

convendría subrayar la necesidad de que las reformas legislativas previstas se acompasasen a una realidad social y tecnológica extraordinariamente cambiante en apenas un lustro. Esta realidad no conoce de compartimentos estancos, ni entre parcelas sociales afectadas -económicas, jurídicas, éticas, técnicas- ni siquiera entre países. El anonimato y la larga distancia en la que se cometen los ciberataques dan cuenta intuitiva de las dificultades a las que se enfrentan el Derecho Penal y el Derecho Procesal Penal. Al primero se demandan respuestas más ágiles que las previstas para los ciberdelitos de nuevo cuño introducidos en 2015; al segundo, una eficacia en la persecución del delito dentro del necesario contexto garantista de los derechos constitucionalmente consagrados, que apenas se está ensayando por vía de la cooperación judicial internacional.

Se llama la atención sobre la enorme disparidad entre los ciberataques y ciberincidentes gestionados por los servicios públicos españoles, pues solamente Incibe reportó el pasado año más de ciento treinta mil incidentes, frente a los procedimientos judiciales abiertos en el orden penal por ciberdelitos, que habiéndose incrementado notablemente, apenas pasan de los once mil. Tal diferencia en las cifras pone de manifiesto la existencia de una amplísima zona gris de elevada impunidad que convendría ir reduciendo paulatinamente para evitar que la incidencia en la dimensión económica sea mayor, minando la confianza del consumidor y la seguridad jurídica de las transacciones online que el Derecho Mercantil había conseguido introducir normativamente en España y en el ordenamiento comunitario.

2. PROTECCIÓN INTEGRAL DEL BIEN JURÍDICO E INTERDISCIPLINARIEDAD

La principal reclamación aquí contenida a la hora de abordar la reforma legal futura de la ciberseguridad nacional en España es que se vincule a una comprensión global e integral. Esto es, a una noción susceptible de proteger a un tiempo a la sociedad frente a las amenazas e ilícitos provenientes de todo el mundo y en todos los sectores de la actividad social de la seguridad nacional,

que constituye en definitiva un único, aunque poliédrico, bien jurídico a proteger. Esa demanda genérica se traduce en las aludidas dos exigencias simultáneas de multidisciplinariedad entre el Derecho y otras ciencias y saberes, y de interdisciplinariedad entre diferentes ramas jurídicas, que van más allá de la tradicional ampliación de la respuesta penal a la prevención administrativa, pasando por unas exigencias de agilidad procesal que difícilmente pueden ser solventadas con la óptica de un solo país. Veamos sucintamente estos tres aspectos y sus implicaciones antes de pasar a propuestas de reforma legal concreta.

La frecuente controversia sobre el bien jurídico a proteger no puede resolverse restrictivamente para vincularlo de manera exclusiva a la integridad del Estado y sus manifestaciones de soberanía. Esto es lo que frecuentemente ha venido sucediendo al contemplar los tipos penales de los delitos del título XXIII del Código Penal y del Título I del Libro II del Código Penal Militar, delitos todos ellos atinentes al espionaje o la traición, desde la rúbrica de la paz, la independencia y la defensa del Estado, que deviene en el Código Penal Militar también seguridad del Estado.

Por una parte, el bien jurídico a proteger no es exclusivamente el ciberespacio como dominio operativo de la seguridad. Por otra, tampoco pueden serlo exclusivamente parcelas como la paz o la independencia de España que, por relevantes que resulten individualmente, han de contemplarse conjuntamente como contexto del normal desenvolvimiento de la sociedad. Esta ha sido la consideración habitual al afrontar el relato de los bienes jurídicos considerados uno a uno en cada tipo penal del Título XXIII. Esta perspectiva meramente dogmática se revela insuficiente al atender al objeto final de la protección integral de España como Estado, es cierto, pero fundamentalmente de la sociedad española como comunidad activa escenario del ejercicio de los derechos fundamentales. Se entiende adecuadamente esta idea al considerar que el art. 17.1 C erige la dupla libertad/seguridad al unísono.

Cabe apuntar dos precisiones sobre la esencia del bien jurídico vulnerable. No lo puede ser todo el ciberespacio, dada la intangibilidad, especialmente a efectos de fronteras, y su inmensidad en contenidos, datos y acciones posibles.

Si esta fue la consideración inicial en momentos de menor extensión lógica del ciberespacio[13], ya no es posible si sopesamos la inconmensurabilidad de los datos disponibles, los intercambios informáticos realizados cotidianamente y la ampliación de la capacidad de procesamiento mundial que crece exponencialmente. El aparente estancamiento de la famosa Ley de Moore sobre la duplicación cada dos años de la capacidad de los chips de los microprocesadores ya no es el problema; ni tampoco es el enfoque adecuado a escala global cuando se tiene en cuenta la interrelación entre minería de datos sectorizada, *big data*[14], *blockchains*[15], *Internet of Things* e Inteligencia Artificial[16]. Particularmente relevante es esta última dimensión, que amenaza con incorporarse mediante un potencial uso autónomo de ciberarmas por medio de programas automatizados sin la intervención humana[17].

13 Jorge Alexandre González Hurtado, "Un nuevo bien jurídico protegido en el uso y disfrute de la tecnología: la seguridad en los sistemas de información", *La ley penal: revista de derecho penal, procesal y penitenciario*, n.o 107 (2014): 4.

14 Iniciado como seguridad de los datos susceptibles de requerirse en la defensa nacional: González Hurtado; Manuel Navarro Ruiz, "La seguridad se convierte en el principal reto de Big Data", *Byte España*, n.o 238 (2016): 8-9; José Francisco Aldana Montes et al., *Big data: seguridad y gobernanza* (Madrid: García Maroto Editores, 2018); Joan Gené Badia, Pedro Gallo, y Itziar de Lecuona Ramírez, "Big data y seguridad de la información", *Atención primaria: Publicación oficial de la Sociedad Española de Familia y Comunitaria* 50, n.o 1 (2018): 3-5. En la actualidad se desarrolla específicamente como big data aplicada a la seguridad nacional y la defensa: José Antonio Carrillo Ruiz et al., "Big data en los entornos de defensa y seguridad", *Pre-bie3*, n.o 6 (2013); Jesús Alcantarilla, ""Big Data" en los departamentos de seguridad, una oportunidad para un nuevo modelo", *Seguritecnia*, n.o 434 (2016): 48-49; Ricardo Malhado, "Big Data y sistemas cognitivos están cambiando el paradigma de seguridad", *Red seguridad: revista especializada en seguridad informática, protección de datos y comunicaciones*, n.o 78 (2017): 42-44.

15 Antonio Requena Jiménez, "Blockchain como disrupción para aplicaciones de seguridad", *Revista SIC: ciberseguridad, seguridad de la información y privacidad* 26, n.o 127 (2017): 114-16; Vicente Moret Millás, "Blockchain and National Security", *Revista de privacidad y derecho digital* 5, n.o 18 (2020): 97-128.

16 Marc Valls Estefanell, "La inteligencia artificial y su encaje en las Estrategias de Seguridad Nacional", *bie3: Boletín IEEE*, n.o 12 (2018): 472-85; Félix Arteaga Martín, "Contexto estratégico de la inteligencia artificial", en *La inteligencia artificial, aplicada a la defensa*, 2019, 153-72; José Carlos de la Fuente Chacón, "La inteligencia artificial y su aplicación en el mundo militar", en *La inteligencia artificial, aplicada a la defensa*, 2019, 69-98; Enrique Cubeiro Cabello, "Inteligencia artificial para la seguridad y defensa del ciberespacio", en *Usos militares de la inteligencia artificial, la automatización y la robótica*, 2020, 97-130; Daniel (dir.) Terrón Santos y José Luis (dir.) Domínguez Álvarez, *Inteligencia artificial y defensa: nuevos horizontes* (Aranzadi Thomson Reuters, 2021).

17 Peter W Singer, "Ciberarmas y carreras de armamentos: un análisis", *Vanguardia dossier*, n.o 54 (2015): 42-47; Jairo Eduardo Márquez Díaz, "Armas cibernéticas. Malware inteligente para ataques dirigidos", *Revista Ingenierías USBMed* 8, n.o 2 (2017): 48-57.

Pero tampoco puede ser el bien a proteger cada ámbito social considerado individualmente. La seguridad nacional no ampara parcialmente la soberanía nacional, el ejercicio de derechos constitucionales, el funcionamiento de las instituciones, la economía, las finanzas, la distribución de energía, el medioambiente o cualesquiera otras actividades, sino a la sociedad que las disfruta.

Más inadecuada resulta una visión del bien jurídico transida de componentes puramente tecnológicos. No es posible trasladar al ámbito jurídico la concepción técnica estrecha de proteger confidencialidad + integridad + disponibilidad de las redes. Dado que es imposible en el momento actual limitar el crecimiento del ciberespacio hacia relaciones sociales y jurídicas antes no reguladas por el ordenamiento, los riesgos y amenazas consecuentes al incremento de las vulnerabilidades introducidas por esa ampliación tienen necesariamente que incorporarse al bien jurídico protegido.

La seguridad nacional integral (seguridad pública, seguridad ciudadana, seguridad militar, seguridad económica y ciberseguridad) compone un acervo plural e interrelacionado esencialmente, sobre el que se vuelca una atención global a un mosaico de entornos que el art. 10 Ley 32/2015 de 28 de septiembre, de Seguridad Nacional (LSN) denomina ámbitos de especial interés de la Seguridad Nacional, por ser básicos para preservar derechos y libertades y el suministro de bienes y servicios, entre los que destacadamente encontramos el ciberespacio. Este es, en puridad, el bien jurídico a proteger, en su infraestructura y en sus servicios, que es tanto como decir en su existencia física, lógica y en el eficaz funcionamiento operativo para la sociedad y las instituciones[18]. El modelo sería en el caso español el de la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la Protección de las Infraestructuras Críticas (LPIC) con dos cambios relevantes: tendría que ser llevado desde las infraestructuras a los datos y servicios y desde sectores específicos a toda la seguridad nacional.

18 Edgar Iván Colina Ramírez, "La seguridad como bien jurídico", *Cuadernos de la Guardia Civil: Revista de seguridad pública*, n.o 56 (2018): 41-60.

Fácilmente se comprenden las complejas implicaciones de esa visión esférica del bien jurídico a proteger al considerar que no son intercambiables las categorías de ciberincidente, ciberataque, ciberdelito y comisión por medios telemáticos de otros delitos, por supuesto, todos ellos proyectados exclusivamente sobre la seguridad nacional. Cuando se analiza de forma desagregada el total de incidencias registradas, estudiadas y clasificadas por Incibe y Centro Criptológico Nacional se percibe que los fenómenos a los que se refiere este artículo son únicamente ciberataques y delitos del título XXIII CP cometidos por medios telemáticos.

Frecuentemente la perspectiva dogmática ha llevado a erigir la precisión sobre el bien jurídico en el núcleo central sobre el que pivota toda seguridad. Así ha sido al configurar los ciberdelitos y así parece plantearse en estos momentos cualquier reforma que amplíe la protección en el ciberespacio. Este procedimiento que parte siempre del bien jurídico plantea, sin embargo, en la actual demanda social dos inconvenientes. Por una parte, es excesivamente tributario de una perspectiva penalista, que no rinde igual utilidad en la dimensión preventiva del Derecho Administrativo. Por otra, el desbordamiento de los límites conocidos que la tecnología posibilita en estos momentos alcanza también a esta cuestión, siendo difícil de puntualizar un solo bien jurídico a proteger cuando simultáneamente los ciberataques afectan a infraestructuras materiales, a servicios intangibles y a derechos relacionados con ambos.

Por todo ello, cuando se demandan simultáneamente multidisciplinariedad e interdisciplinariedad es precisamente para una adecuada protección integral del bien jurídico a proteger como un todo en sus implicaciones realistas en una sociedad abierta.

Partiendo de la especial consideración del ciberespacio como *locus delicti commisi*[19] es necesario ampliar el enfoque jurídico para las reformas de otros

19 Puede verse a este respecto y en relación con las notas caracterizadoras antes expuestas para el ciberespacio de la Estrategia Nacional de Seguridad española, la clásica caracterización del ciberespacio como lugar de comisión del delito del Curtis E. Lemay Center en "Introduction to cyberspace operations" de 2011.

sectores del ordenamiento que se anuncian ya. Este artículo menciona algunas propuestas concretas *de lege ferenda* de cara a ese inmediato e imprescindible proceso y las elabora partiendo de la doble premisa epistémica en la preparación técnica de los anteproyectos de ley.

De un lado, multidisciplinariedad. No han sido infrecuentes las dudas incluso sobre la posibilidad de una cooperación multidisciplinar[20], ni las incomprensiones desde diversas Ciencias Sociales que han venido trabajando con la seguridad en el ciberespacio como objeto de estudio antes que el Derecho, ni tampoco los reproches respecto al papel que este último estaba llamado a desempeñar desde tiempo atrás y que está aún pendiente de desarrollo. Dadas las diversas perspectivas implicadas, no se trata tanto de desdibujar los límites entre disciplinas[21] como de aproximar sus contenidos[22].

Analizar el estado de la cuestión a este respecto permite apreciar la variedad de análisis concurrentes: politológicos, sociológicos, tecnológicos de ingeniería e informática, económicos, policiales y militares, que demandan una multidisciplinariedad horizontal y cooperativa[23]. En definitiva, junto con el Derecho están llamadas a aportar puntos de vista complementarios principalmente la Ingeniería informática, la Ingeniería de las Telecomunicaciones y la Ciencia Política; la primera para las soluciones técnicas que afectan a los servicios, la gran asignatura pendiente en estos momentos; la segunda para la integridad de las redes, en lo que se ha avanzado notablemente en tiempo reciente; y la tercera para definir una auténtica política pública de la seguridad, en la que la ciberseguridad está llamada en lo inmediato a ocupar el espacio prevalente.

20 Minor E Salas, "Interdisciplinariedad de las ciencias sociales y jurídicas: ¿impostura intelectual o aspiración científica?", *Revista de ciencias sociales*, n.o 113 (2006): 68.
21 Serena Baldin, "Diritto e interdisciplinarietà: note sulla integrazione metodologica con le altre scienze sociali", *Revista General de Derecho Público Comparado*, n.o 25 (2019).
22 Miguel Ángel Ciuro Caldani, "Reflexiones básicas sobre integrativismo e interdisciplina en el Derecho (un planteo interdisciplinario de la interdisciplina)", *Revista de Filosofía Jurídica y Social*, n.o 37 (2016): 61-85.
23 Antonio Barreto Rozo, "La interdisciplinariedad horizontal. Las formas económica, social, política y jurídica de construir realidades", *Co-herencia: revista de humanidades* 13, n.o 24 (2016): 43-58.

De otro, junto a la multidisciplinariedad a la hora de abordar la redacción de los textos articulados y el conjunto de informes previos que han de dar forma en los primeros pasos del *iter* legislativo a los anteproyectos de ley, se postula aquí la necesidad de interdisciplinariedad jurídica. Particularmente porque existen unos límites prefijados tanto por el Derecho Constitucional como por el Derecho Internacional Público. Que disciplinas con objetos de estudio tan acreditados como los del Derecho Administrativo, del Derecho Penal y del Derecho Procesal estén llamadas a confluir en un mismo campo analítico demanda establecer previamente mecanismos de comunicación normativos. Y hacerlo pausada y consensuadamente, en lugar de mediante la habitual fórmula de las leyes ómnibus que tanta improvisación y aleatoriedad han introducido en algunos sectores del Derecho Administrativo, lo que proyectado sobre el ámbito penal no acarrearía sino desprotección y discrecionalidad de graves implicaciones constitucionales. Aunque se han dado los primeros pasos para incorporar en las normas sobre seguridad los puentes desde el mundo físico al lógico y se ha modulado conceptualmente cómo inciden en la naturaleza de los ilícitos[24] no se recoge enteramente el conjunto de exigencias que la visión holística incorporada en la LSN demanda.

Puede aducirse que la especial naturaleza de la norma penal requiere un encauzamiento ad hoc que impide la penetración de otras perspectivas jurídicas más laxas, que son las que en estos momentos trazan las conexiones y la delimitación entre la seguridad global, la seguridad pública y la seguridad nacional. En este articulo interesa particularmente la última, pero es imposible hoy acotarla de tal modo que no tenga intensas vinculaciones tutelares con una seguridad integral que abraza simultáneamente aspectos administrativos y penales.

España se incorporó tardíamente a la dotación de documentos doctrinales completos atinentes a la seguridad nacional, a la definición del interés nacional y a la actualización periódica de sus medios en atención a la revisión de las

24 Juan José González Rus, "Los ilícitos en la red (I): hackers, crackers, cyberpunks, sniffers, denegación de servicio y otros comportamientos semejantes", en *El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales*. (Granada: Comares, 2006), 241-71.

amenazas. Más tardíamente aún ha hecho las primeras adaptaciones legislativas al marco internacional, señaladamente al europeo, proceso que está en buena manera aún inconcluso. Es decir, que el Derecho ha ido muy por detrás de otras disciplinas, como las ciencias militares, las Relaciones Internacionales y las ingenierías informática y de telecomunicaciones al convertir el ciberespacio en un objeto de estudio consistente. Puede confiarse en que ese retraso relativo se compense en lo inmediato con una puesta al día decidida de los instrumentos jurídicos de protección de la sociedad en el entorno cibernético.

3. TRANSPOSICIÓN DEL ORDENAMIENTO COMUNITARIO Y PERSPECTIVA CRÍTICA DE LA NORMATIVA VIGENTE EN ESPAÑA

¿Es la queja sobre la insuficiencia y el desfase de la normativa española de ciberseguridad un lamento excesivamente subjetivo de los operadores jurídicos o existe algún indicio objetivable de dicho desacoplamiento entre realidad socioeconómica y norma jurídica? Dos parecen ser los más elocuentes.

En primer lugar, la tradicional espera del legislador español a la evolución en ordenamientos más dinámicos a estos efectos, señaladamente los anglosajones y el propio comunitario. Respecto a los primeros se aducen dos impedimentos principales para seguir su estela: la pertenencia a sistemas jurídicos tan diferentes que la importación directa de soluciones parciales suele ocasionar desajustes de segundo orden aún mayores, diferidos en el tiempo. Y que el parámetro de prevención absoluta se ha sobreelevado legislativamente sobre la protección de las libertades fundamentales y de las garantías procesales para su preservación, en nombre de una seguridad nacional omnímoda, especialmente en el caso norteamericano. Por tanto, es la diferencia entre el acervo comunitario en materia de ciberseguridad y la normativa española un criterio más cercano y ampliamente asumido sobre la necesidad genérica de introducir mejoras y la obligación específica de transposición de las novedades. El indiscutible ejemplo de la Directiva NIS es ejemplo suficiente para evitar mayores digresiones.

Por otra parte, existe un criterio objetivo interno, de tipo más cuantitativo, que permite apreciar claramente el desajuste entre el problema social y la respuesta jurídica en atención a diferentes clases de sanciones o condenas. Se ha mencionado el desfase entre ciberataques registrados y clasificados, investigaciones policiales, procedimientos judiciales penales abiertos y condenas. El porcentaje de incremento de las últimas es mucho menor que el alza relativa de los ciberataques, por lo que esa brecha, lejos de contenerse con más medios tecnológicos disponibles, se ha venido aumentando año a año. Debe tenerse presente que un porcentaje muy alto de los procedimientos judiciales y las condenas tienen que ver con los delitos contra el patrimonio, por lo que si se analizan los procedimientos instruidos por ciberataques contra la seguridad nacional, estos son prácticamente inexistentes y los incoados se refieren más a la integridad de las infraestructuras que a la prestación de servicios esenciales, por lo que sigue existiendo un sesgo, persistente en el caso español, más matizado en la directiva comunitaria, entre redes y datos. Por más que se hacen ingentes esfuerzos por acrecentar la denominada cultura de la ciberseguridad, se ha venido a aceptar generalizadamente una especie de relajación de la respuesta penal frente a graves ataques a un bien jurídico tan sensible como el de la seguridad nacional. La mejor manifestación de esta censurable tendencia es que ataques que hubieran merecido inmediata y contundente respuesta en el mundo físico -por ejemplo, el traspaso de las fronteras, el uso no autorizado del espacio aéreo o el ataque contra infraestructuras militares- se contemplan laxamente cuando se producen en el ciberespacio.

3.1. La restringida protección penal

Si bien para el Derecho Penal es posible contemplar el ciberespacio[25] en conjunto y no solamente a efectos del empleo de métodos de comisión telemáticos de los delitos, no se ha producido en el ámbito de la protección penal de la

25 Lorenzo Picotti, "Ciberespacio y Derecho penal", en *Libro homenaje al profesor Dr. Agustín Jorge Barreiro*, ed. Gonzalo Basso, vol. 2 (Madrid: Servicio de Publicaciones de la Universidad Autónoma de Madrid, 2019), 1191-1204.

seguridad nacional un esfuerzo de adaptación de las normas similar al que se ha operado para la seguridad pública. En este último se ha ido dando cabida en las más recientes reformas a la paulatina contemplación del uso de las nuevas tecnologías de la telecomunicación y las nuevas herramientas informáticas para la comisión dolosa de hechos típicos que estaban ya recogidos en el Código Penal y de nuevos ilícitos. Respecto de los primeros, la capa ciber utilizada para la comisión variaba parcialmente algunos elementos objetivos de los tipos penales, como se observa particularmente en el caso de estafas o apropiaciones indebidas; en relación con los segundos, el cambio de visión introducido por la Ley Orgánica 1/2015 parece un modelo adecuado, aunque insuficiente.

Consideremos como posibles ejemplos las novedades incluidas para los delitos de interceptación de las transmisiones de datos, los delitos informáticos relacionados con la propiedad intelectual e industrial y los de intrusión informática regulados en los artículos 197 bis, 197 ter, 197 quater, 197 quinquies y ss. y 270 y ss del CP. Todos ellos han incorporado una doble novedad: la existencia del ciberespacio como lugar de comisión de los delitos, y la imprescindible utilización de medios telemáticos en las modalidades de comisión más tecnificadas. Nada de esto está presente en el tenor literal del Código Penal ni del Código Penal Militar para los delitos relativos a la seguridad nacional. Si se atiende a la redacción de todos los artículos del título XXIII CP y se considera la traza histórica, sorprende negativamente la invariable literalidad de muchos de ellos desde el Código Penal de 1870, y aún para algunos desde el de 1848. En aras a la necesaria concisión no es posible detenerse en este momento en ellos, pero cuando se analizan los delitos de traición, espionaje, injerencia en la soberanía o revelación de secretos relativos a la Defensa Nacional, todos vinculados con la seguridad nacional, se aprecia que se sigue manteniendo hoy el concepto de infraestructuras esenciales para la seguridad que estaba plenamente vigente en los códigos decimonónicos. Si tenemos en cuenta que la incorporación de las últimas infraestructuras susceptibles de atacarse para debilitar la seguridad nacional eran los aeródromos, que se introdujeron en el Código Penal de 1928, en plena dictadura primorriverista, se comprende el desfase que impide relacionar perspectiva alguna de ciberseguridad con la seguridad nacional apreciada penalmente.

No hay únicamente inconvenientes de tipo dogmático. El mayor impedimento que cabe achacar a la ley penal para proporcionar una adecuada protección en el ciberespacio la seguridad nacional deriva principalmente de la distancia que se percibe entre los medios tecnológicos y la finalidad de política criminal que debería perseguir una normativa más actualizada y realista. Esta habría de ser la orientación que pudiera darse a una nueva redacción de los artículos de ese título XXIII CP para apreciar más adecuadamente la singularidad del elemento objetivo del tipo[26]. Así pues, del mismo modo que se ha afirmado con carácter general, la perspectiva penal está particularmente necesitada de puentes interdisciplinares[27] para una protección integral de la seguridad nacional. De forma particularmente intensa se proyecta aquí la insuficiencia hasta este momento en el paso de una visión dogmática a otra de política criminal más comprensiva y amplia, que acreciente el campo de protección que sociedades tan abiertas como la española plantean en estos momentos como desafío principal para los poderes públicos[28].

Con particular vinculación con la visión penal surgen las severas restricciones e inconvenientes derivados de las exigencias procesales y la inexistencia de normas de auténtica proyección internacional o transnacional, más allá de los tibios intentos hasta ahora impulsados por algunas organizaciones internacionales de ámbito territorial limitado y de escasa especialización temática.

3.2. Protección administrativa

Afortunadamente se ha superado ya un interés parcial del Derecho Administrativo que se relacionaba únicamente con una visión de la administración

26 María Pilar Serrano Ferrer, *El reflejo de las nuevas tecnologías en el derecho penal y otros destellos* (Cizur Menor: Aranzadi Thomson Reuters, 2016), cap. 2 Internet como medio comisivo.
27 Diana Patricia Arias Holguín, "Contexto, interdisciplinariedad y dogmática penal", en *Liber amicorum: estudios jurídicos en homenaje al profesor doctor Juan Ma. Terradillos Basoco* (Valencia: Valencia : Tirant lo Blanch, 2018), 49-62.
28 Fernando Miró Llinares, *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio* (Madrid: Marcial Pons, 2012), 191-95.

militar[29]. Si la defensa del sistema es reactiva en la perspectiva penalista, es más preventiva en el ordenamiento administrativo. Comenzando por la existencia de un abanico mayor de medidas que pueden ser implementadas para la protección de la seguridad nacional, y que van desde una doctrina constante, revisada y comparada con los países del entorno de seguridad y defensa europea y atlántica, hasta unas normas más precisas para la protección de infraestructuras y de servicios necesarios para el desarrollo normal de la vida, pasando por planes aprobados, homologados e implementados de forma rigurosa por las distintas autoridades intervinientes en la seguridad nacional. Además, esta pluralidad de mecanismos se aplica simultáneamente sobre las misiones militares, el trabajo policial y las operaciones de inteligencia.

Son tres los campos sobre los que se ha proyectado esta ampliación de la atención administrativista sobre la ciberseguridad nacional de naturaleza tuitiva. En todos ellos ha habido una primera preocupación en los Estados que han sufrido mayores quebrantos a la seguridad nacional en forma de terrorismo y espionaje, pero ese interés no se ha convertido en norma positiva hasta la intervención de las instancias comunitarias. En uno de tales campos con menor énfasis (la asignación de parámetros estratégicos vinculados con un ámbito de seguridad europeo como el fijado por la PESC), pero decididamente en los dos restantes (la regulación administrativa de las infraestructuras críticas y la normativa sobre integridad de las redes y sistemas).

Ya se ha abundado en la primera de esas líneas, que lleva a la fijación de estrategias de seguridad nacional compartibles para aquellos Estados que participan en dos mecanismos tan relevantes como Schengen, para la dimensión policial, y las misiones bajo paraguas UE, para la dimensión militar. En relación con este último aspecto se buscaba una mayor homogeneización de las decisiones estratégicas dentro de un marco jurídico más estable que el proporcionado para la OTAN por el *Manual de Tallin 2.0 sobre Derecho Internacional aplicable a las ciberoperaciones*, que sigue basado en el respeto a la soberanía estatal,

29 Juan Díaz del Río Durán, "La ciberseguridad en el ámbito militar", *Cuadernos de estrategia*, n.o 149 (2011): 215-56.

la diligencia debida, la no intervención como principio general porque se espera un correlato, el de la responsabilidad internacional de los Estados, que raramente se da en las confrontaciones híbridas actuales. Basta ver su definición de ciberataque como operación cibernética ofensiva o defensiva de la que se espera que pueda causar pérdidas de vidas humanas, lesiones a las personas y daños o destrucciones de bienes, para inferir su inadecuación por seguir siendo tan formalista y tan tributario de la visión del art. 49 del del *Protocolo Adicional I a los Convenios de Ginebra relativo a la protección de las víctimas de los conflictos armados internacionales*.

Fruto de esa diferente mentalidad es la sucesiva aprobación de las estrategias de seguridad nacionales de España y de la aludida jurídificación en la LSN. Mejor aún, la aprobación de la Estrategia Nacional de Ciberseguridad por la Orden Ministerial PCI/487/2019, y el alineamiento de muy diferente normativa sectorial que incide en la ciberseguridad, como la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, o el Real Decreto que regula el esquema Nacional de Seguridad en el ámbito de la administración electrónica.

En el mismo sentido positivo ha de valorarse la creación del Sistema de Seguridad Nacional, del Departamento de Seguridad Nacional y del Consejo Nacional de Ciberseguridad como organismos de apoyo basados en la habilitación de la ya antigua Ley del Gobierno de 1997.

El segundo de los ejes mencionados se refiere a la transposición y ampliación en el ordenamiento administrativo español de la normativa de protección en el ciberespacio de las infraestructuras críticas, la Directiva 2008/114/CE del Consejo, de 8 de diciembre de 2008, sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección. La Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas y el Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas han conseguido el mayor grado de protección en las normas

administrativas, que debería ser modelo a seguir para cualquier regulación futura, puesto que se ha desarrollado un auténtico sistema con una Comisión Nacional para la Protección de las Infraestructuras Críticas creada en 2014 y que en los años sucesivos ha declarado sectores, operadores e infraestructuras, llevando un grado de ciberprotección muy avanzado.

La necesidad de establecer una gobernanza multinivel en relación con la seguridad nacional se percibe claramente en las infraestructuras críticas de titularidad pública que se refieren a servicios esenciales prestados en España a través de la administración de las Comunidades Autónomas y que requieren un complemento normativo a la legislación básica estatal a través de la legislación de desarrollo autonómico, como ocurre en materia de industria, gestión hospitalaria o transportes.

El tercero de esos ejes, también traspuesto a nuestro ordenamiento, es el relativo a la adaptación de la Directiva 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información o directiva NIS (*Network and information security*) [30]. Indudablemente ha supuesto una mejora de la protección integral de la ciberseguridad[31], pero aun así manifiesta una cierta insuficiencia de la protección de las redes e infraestructuras, incluso cuando se habla de los sistemas, porque tiene que abarcar además los datos y también la prestación de los servicios, sobre todo cuando se trata de la implementación de servicios públicos, que es lo que preocupa a los ciudadanos.

En este momento se procede por la Comisión Europea a la reevaluación de la directiva NIS[32]. El juicio que esta ha merecido en España ha puesto de manifiesto el desacoplamiento con otras normas españolas administrativas aplicables, como el Reglamento de Protección de Datos, mucho más que la falta de

30 Jesús Fernández Acevedo, "Directiva NIS y la transposición al derecho interno", en *Aspectos jurídicos de la ciberseguridad*, 2020, 91-101.

31 Vicente Moret Millás, "Aspectos relativos a la incorporación de la Directiva NIS al ordenamiento jurídico español", *bie3: Boletín IEEE*, n.o 5 (2017): 733-51.

32 Félix Arteaga Martín, "La evaluación y la revisión de la Directiva NIS: la Directiva NIS 2.0", *Análisis del Real Instituto Elcano (ARI)*, n.o 19 (2021).

apoyo para su implementación de las Administraciones Públicas españolas. La propia Comisión Europea reconoce el desfase de la normativa comunitaria como consecuencia del considerable aumento de la conectividad y del incremento de la digitalización, por lo que en estos momentos es prioritario incorporar en las normas españolas que hayan de adoptarse la regulación de las actividades de los proveedores de servicios digitales. Otro reto pendiente de definir fuera de las infraestructuras críticas se refiere al intercambio de información entre actores públicos y privados concesionales.

4. PROPUESTAS *DE LEGE FERENDA*

Siendo parcial, insuficiente y en cierto modo obsoleta la regulación actual, se hace imprescindible acometer algunas reformas legislativas de gran calado y en los tiempos comprometidos políticamente. Estos parecen haberse alterado sustancialmente por los cambios de prioridades introducidos por la pandemia de Covid 19; pero resultaría un error aprovechar la ocasión para diferir la resolución de las disfunciones más graves ya detectadas y unánimemente criticadas por los operadores técnicos y jurídicos de la ciberseguridad. La intensificación de los ciberataques sufridos por usuarios domésticos y empresariales palidece ante la profundidad y la notoriedad mediática de los padecidos por el sector público estatal y autonómico durante las épocas de más severa restricción durante los sucesivos estados de alarma, como los ataques de *ransomware* sobre la red de hospitales públicos y la paralización de los servicios del Servicio Público de Empleo estatal pusieron de manifiesto descarnadamente. En este tiempo los ciberatacantes de toda condición, presumiblemente también aquellos que pueden servir a intereses de países ajenos a la esfera de libertades de la UE, no han cejado en su empeño por paralizar el normal desenvolvimiento de los servicios públicos esenciales e incluso por obstaculizar la operatividad de las fuerzas de seguridad. Por tanto, lejos de relajarse la necesidad de contar con un ordenamiento actualizado robusto, esta se encuentra en el punto más alto desde la multiplicación de los ataques sobre infraestructuras críticas.

Se apuntan catorce modificaciones de la actual regulación, que se agrupan, para una mejor comprensión de las sinergias buscadas y de las interacciones positivas necesarias, en sugerencias provenientes de necesidades exógenas, apuntes para la perfección de la protección administrativa de la ciberseguridad, propuestas de ampliación de la protección penal para los casos más graves de conculcación de los derechos individuales y de alteración de los servicios públicos, así como de brecha de la seguridad nacional y, finalmente, recomendaciones para mejorar la cooperación judicial en la persecución de los delitos cometidos en el ciberespacio desde países situados fuera del espacio Schengen, puesto que solucionar ese déficit se antoja en la actualidad imposible.

Las primeras derivan principalmente de la estrategia de política pública a adoptar por las autoridades nacionales españolas en consonancia con las exigencias de seguridad del contexto europeo. Los segundos de la adaptación a un perfeccionamiento creciente de la normativa supranacional de protección de los consumidores de servicios TIC y de las infraestructuras esenciales, especialmente en el ámbito comunitario. Las terceras de la obsolescencia del tenor literal del Código Penal al recoger los elementos objetivos, especialmente las conductas típicas, de los delitos contra la independencia del Estado y contra la Defensa Nacional. Las últimas de la imposibilidad de hacer avanzar los procedimientos judiciales por medio de imputaciones eficaces cuando las acciones iniciales de comisión de los delitos se han producido en territorios pertenecientes a Estados que no las persiguen por lagunas en su propia normativa o por simple dejadez, cuando no por abierta complicidad e incluso promoción de tales conductas por sus propios intereses estratégicos.

4.1. PROPUESTAS CON RENDIMIENTO PARCIALMENTE EXTRAJURÍDICO

El debate social y político condiciona enormemente las propuestas jurídicas, dado que el arsenal tecnológico actual posibilita acciones muy invasivas de los ciberatacantes que vulneran las libertades públicas, pero a la vez los instrumentos informáticos disponibles para los poderes públicos permitirían tanto anticiparse como contraatacar con riesgo cierto de extralimitación, por lo que el celo

en la defensa de los derechos individuales afectados por ciberataques no puede contrarrestarse por el uso ilimitado de la fuerza informática disponible para los aparatos policiales, militares y de inteligencia de los Estados de Derecho. En esta estrecha, débil y polémica franja se deben situar estas propuestas que desde lo jurídico limiten la amplia capacidad coactiva e intervencionista de la tecnología actual.

Las cuatro primeras propuestas de reforma normativa tienen por objeto aproximar interés nacional, planes estratégicos y regulación positiva. Se refieren: 1º) a la juridificación de los mecanismos de la seguridad nacional también en materia de ciberseguridad; 2º) la uniformización en normas positivas de la terminología necesaria para aplicar las normas penales subsumiendo situaciones fácticas en las que la tecnología es altamente especializada; 3º) favorecer en términos constitucionalmente irreprochables la capacidad preventiva que toda ley de seguridad demanda, máxime cuando están en juego varios de los derechos fundamentales que hacen reconocible nuestra sociedad como una democracia avanzada; 4º) acompasar la capacidad reactiva a los principios de legalidad y proporcionalidad, con la incidencia especial de la denominada legítima defensa anticipada en evitación de las últimas consecuencias de los ciberataques severos contra la seguridad interior del Estado.

La primera propuesta tiene que ver con la necesidad de adecuar la visión política al ordenamiento jurídico también a los efectos de la regulación de la ciberseguridad nacional. Debe constatarse la reluctancia mantenida desde los tiempos de la Transición hasta hoy a expresar en términos jurídicos las propuestas políticas sobre seguridad nacional. Basta considerar el lapso temporal entre las primeras formulaciones estratégicas de seguridad nacional y la aprobación de la Ley 32/2015 de 28 de septiembre, de Seguridad Nacional (LSN). Por un inconsistente poso histórico, las cuestiones relacionadas con la seguridad han preferido sustanciarse en la esfera de los documentos doctrinales y, en último caso, de la planificación pública, pero la dirección de los servicios policiales, de inteligencia, y en menor medida, militares, se han mostrado refractaria a la juridificación pormenorizada de estas cuestiones, probablemente por no querer atarse en la operativa práctica. En tal sentido, la LSN marca un camino adecuado

que no puede detenerse en este momento, sino profundizarse para darle mayor soporte a la Estrategia de Seguridad Nacional y a la Estrategia de Ciberseguridad Nacional. Las actualmente vigentes beben directamente en las fuentes de la LSN de 2015 y son respectivamente de 2017 y 2019.

Sería aconsejable que cuando toque su actualización, ya próxima, pudiera hacerse con mayor grado de exigibilidad coercitiva que el actual, que evitaría problemas como los vividos recientemente con la pandemia, pues no hay que olvidar que en la vigente Estrategia de Seguridad Nacional se consignan a la vez la vulnerabilidad del ciberespacio entre las amenazas y las pandemias entre los desafíos. Es de esperar que, si se produce un problema de seguridad cibernética de dimensiones tan importantes como el de la seguridad sanitaria reciente, no se tenga que recurrir a la improvisación de medidas como la declaración del estado de alarma, que tantas controversias constitucionales ha provocado. Dicho de otra forma, juridificar estas cuestiones permitiría, si es que llega el caso de su aplicación por un ciberataque crítico a escala masiva, una protección más incontrovertida de la seguridad nacional.

La segunda se relaciona con la construcción de un léxico especializado, absolutamente imprescindible para avanzar con seguridad jurídica en este momento, pues, en efecto, no deriva esta necesidad tanto de una adecuación técnica, sino de la necesidad de erradicación de la inseguridad jurídica al calificar conductas ilícitas. Sin embargo, no es precisamente el contenido jurídico el más problemático a la hora de forjar este vocabulario. Como en puridad tampoco es exclusivamente un problema de léxico, sino también de su significado. El avance técnico vertiginoso que ofrecen las nuevas tecnologías abre simultáneamente enormes posibilidades de comisión de ilícitos que se diferencian únicamente por los procedimientos de comisión en detalles mínimos.

Está indudablemente necesitada de actualización la Guía de Seguridad del Centro Criptológico Nacional CCN-STIC-401 que contiene el Glosario y Abreviaturas. Se trata de un documento pocas veces utilizado en el mundo técnico, por considerarlo parcialmente insuficiente y obsoleto, y menos aún en el mundo jurídico, por la elevada inclusión de aspectos propios de la ingeniería que se

escapan a una fácil comprensión de los profanos en esta materia. Sin embargo, es absolutamente crucial que desde ambos campos se hiciesen aportaciones significativas para su precisión. El objetivo no es primariamente mejorar la documentación aplicable, sino hacer comprensible a especialistas de ambas disciplinas las peculiaridades de significado de los términos utilizados cotidianamente.

La urgencia de esta mayor precisión se percibe claramente cuando se pasa del debate doctrinal a la reforma legal, particularmente la que está llamada a perfilar las respuestas más inmediatas del sistema ante los ciberataques y su análisis forense, momento en el que se revela con toda crudeza que técnicos y juristas no aluden a las mismas realidades con nombres semejantes, o incluso que carecen de algunos términos que sería importante precisar de cara a una exigencia de responsabilidades de contenido jurídico o económico. Urge, en consecuencia, vincular más estrechamente semántica y léxico, tarea que no corresponde a los lingüistas, sino a quienes hacen uso de ese vocabulario para identificar, clasificar, contrarrestar, reponer y auditar los ciberataques, que son en algunas de estas fases técnicos, y en la última, juristas. Lo que es una constante necesidad en el campo jurídico[33], se convierte en este caso, por la presencia decisiva de elementos tecnológicos, en una verdadera barrera para la protección del bien jurídico integral de la seguridad nacional.

Cualquier jurista que haya debido realizar una calificación de ciberataques, bien con carácter preventivo en el Derecho Administrativo, bien reactivamente en el Derecho Penal, se ha enfrentado a una maraña de siglas, neologismos y anglicismos que ha solventado a los técnicos la necesidad de invenciones de términos equivalentes en español, a la vez que ha incorporado inmediatamente las novedades surgidas en la esfera internacional del ciberespacio en la que se produce la práctica totalidad de los ciberincidentes, pero que dificultan en extremo su traslación al ámbito jurídico. Particularmente cuando se trata de aplicar esas palabras con el mecanicismo que requiere la acreditación procesal de un soporte

33 Rafael García Pérez, "¿Desde cuándo se cometen delitos?: relaciones entre léxico y sintaxis en la evolución histórica de la lengua del derecho penal", en *Palabras, norma, discurso*, ed. Luis Santos Río (Salamanca: Universidad de Salamanca, 2005), 509-20.

probatorio tantas veces dificultado en el paso entre los términos tecnológicos y los conceptos jurídicos penales. La necesaria aplicación del principio de legalidad para las sanciones, tanto administrativas como penales, requiere ajustar necesariamente las definiciones y taxonomías de las conductas perseguibles en los ciberataques para poder subsumirlas en tipos penales que no deban ser aplicados por analogía, especialmente cuando se trata de distinguir entre autoría y participación. En este momento se está lejos de alcanzar un nivel óptimo en esas clasificaciones, en unas ocasiones porque la utilización indebida de la tecnología va tan rápido que no da tiempo a incorporar jurídicamente las nuevas formas comisivas y en otros casos porque hay una abierta contradicción entre la terminología técnica y la semántica jurídica, especialmente en lo que se refiere a la aceptación del riesgo (ver la implicación en la certificación de funciones de la *risk acceptance*) y la actuación responsable (en relación con la autoría el *privilege creep* por escalada no definida de privilegios).

La tercera reforma legislativa debería centrarse en el problema de la prevención, que a diferencia de otras esferas del ordenamiento penal resulta indispensable, pues inhabilitaría la protección real de la sociedad española esperar a la efectiva puesta en riesgo de la ciberseguridad nacional, no digamos ya con un nivel de afectación paralizante de las infraestructuras públicas críticas como la distribución de energía, la red hospitalaria o la distribución de alimentos.

Se trata de favorecer en términos constitucionalmente irreprochables la capacidad preventiva que toda ley de seguridad demanda, máxime cuando están en juego varios de los derechos fundamentales que hacen reconocible nuestra sociedad como una democracia avanzada. Estamos, por supuesto, muy lejos de los debates sociales y jurídicos apreciados en Estados Unidos con ocasión de la creación de Homeland Security en 2002 con la Administración Bush tras los ataques a las Torres Gemelas o de la asunción de capacidades de monitorización muy amplias por la NSA. El garantista sistema instaurado en España para el funcionamiento del CNI con supervisión judicial permanente de sus operaciones por la Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia, es indudablemente el modelo a seguir. Pero establecida una cautela como la contemplada en el art. 12 de la Ley

11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, efectuada a través del art. 342 bis LOPJ, nada impide el escrupuloso respeto a las libertades constitucionales también para las operaciones que requieran una cierta anticipación para evitar las consecuencias más nocivas de la efectiva producción de los resultados dañosos para la seguridad nacional. De ahí la conveniencia de eludir la generación de daños concretos que tantas veces se ha vinculado con la visión penalista. En materia de ciberseguridad nacional, contemplar las amenazas efectivas desde la producción de sus resultados acarrea irreparables perjuicios para el sistema de seguridad integral y puede que también incontables daños sociales al bien jurídico que, tal como se ha definido, requiere asimismo protección preventiva[34].

Sería posible de este modo una reorientación de política criminal preventiva que no incurriera en el trance de identificar la naturaleza de estos delitos exclusivamente con la producción de daños efectivos en la comisión telemática[35], sino que permitiera contemplar simultáneamente daños y riesgos[36].

Cuanto no ha podido avanzarse en el derecho preventivo, ha tratado de volcarse sobre el derecho retributivo, empezando por la capacidad para responder a los ciberataques y terminando por las sanciones y penas. Desde el punto de vista de las capacidades, los organismos públicos especializados en ciberdefensa cuentan con CERTs y CESIRTs, equipos de respuesta tanto policiales como militares, perfectamente preparados para cualquiera de estas eventualidades, ya sean amenazas, ya ciberataques.

Convendría acompasar la capacidad reactiva a los principios de legalidad y proporcionalidad, con la incidencia especial de la denominada legítima defensa anticipada. Pero es que si nos atenemos a la estricta aplicación de la *NATO AJP*

34 José Luis González Cussac, "Estrategias legales frente a las ciberamenazas", *Cuadernos de estrategia del Ministerio de Defensa* 149 (2011): 85-127.

35 Mariana Noelia Solari Merlo, "El legislador penal ante la innovación tecnológica: los daños informáticos en el dilema entre la reflexión filosófica y la práctica jurídico científica", en *Moderno discurso penal y nuevas tecnologías: memorias [del] III Congreso Internacional de Jóvenes Investigadores en Ciencias Penales, 17, 18 y 19 de junio de 2013*, ed. Fernando Pérez Álvarez (Salamanca: Ediciones Universidad de Salamanca, 2014), 201-17.

36 Edgar Iván Colina Ramírez, *Sobre la legitimación del derecho penal del riesgo* (Barcelona: J.M. Bosch Editor, 2014), 119-35.

3-12 Cyberspace operations de 8 de junio de 2018 que sustituyó a la *3-20 Joint doctrine for cyberspace operations*, y al *UE Concept on cyberdefence for EU-led military Operations and Missions*, revisado en abril de 2019, documentos ambos que vinculan a España, en la práctica la respuesta se produciría cuando los daños fuesen efectivos, graves y cuantiosos. Incluso para los tipos de ciberataques menos dañinos se estaría ante pasos indefectibles en el eje vulnerabilidad – riesgo – amenaza – ataque – que tendría a partir de ahí dos caminos: recuperación o respuesta.

¿Cuál es el que se debe privilegiar en las democracias occidentales? Antes de contestar convendría tener presentes algunas implicaciones de la visión conceptual rusa y la práctica de la *deziformatsiya*, la desinformación deliberada que, como han puesto de relieve los informes del Real Instituto Elcano, para una opinión pública sorprendida en España se emplea como método militar asimétrico e indirecto en la guerra híbrida, que tiene su antecedente en las denominadas "medidas activas" y se define como una acción cuyo fin es "desacreditar y debilitar a los oponentes y distorsionar su percepción de la realidad". No se trata de simples *fake news* dispersas, sino de una estrategia deliberada y orquestada para distorsionar la percepción de la realidad, aprovechando las posibilidades de la posverdad. Comparar esa estrategia con las occidentales desvela la importancia de adecuar los mecanismos de respuesta por los que aquí se aboga, con la diferencia de que en el marco de la UE siempre se haría dentro de los límites constitucionales y del respeto a los derechos humanos que falta en la contraparte atacante. ¿Cuál va a ser la respuesta europea al proyecto Lakhta ruso y sus granjas de trolls: anticipación, contraataques, respuesta o simple recuperación?

4.2. PROPUESTAS CON RENDIMIENTO ADMINISTRATIVISTA

¿Es suficiente una perspectiva reactiva ante ciberataques crecientemente graves? Probablemente la respuesta venga mejor por la continuación de la senda ya emprendida de ampliación y adaptación de las normas antes relacionadas de naturaleza administrativa, que por una reforma del Código Penal que se antoja casi imposible en el actual clima parlamentario. Tres vías son aconsejables: 1º)

resolver el problema de la segmentación del bien jurídico integral de la seguridad nacional en microbienes tangibles -como la integridad territorial o el dominio físico de las infraestructuras- o sectoriales -como redes y datos-; 2º) la facilitación de los mecanismos de alerta temprana al incorporarse a planes necesarios por mandato legal; 3º) la posible ampliación del modelo de seguridad física y de ciberseguridad de las infraestructuras críticas.

Es el momento de acompasar la protección administrativa a lo que operadores públicos y usuarios entienden como ciberseguridad. Aquellos pueden ser titulares de infraestructuras, pero las poseen para garantizar la integridad del ciberespacio. Todos, unos y otros -a los que hay que sumar los operadores privados- quieren que la garantía sea del suministro de servicios, por lo que en torno a este debería girar cualquier futura ampliación de la denominada impropiamente normativa de ciberseguridad, el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, que adaptó la Directiva NIS. El primer paso, reciente, pues se contiene en el Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, es adecuado, pero insuficiente a su vez. En buena medida se centra en el aspecto orgánico de las autoridades intervinientes. Otros dos contenidos, en cambio, avanzan en buena dirección: la supervisión y la comunicación de incidentes. Pero aquí se aboga por un cambio más profundo, que afecta incluso al nombre, y que denote que se va más allá de las redes y sistemas para centrarse en datos, servicios y usos.

En segundo lugar, es el momento de trasladar la buena práctica del establecimiento de mecanismos de alerta temprana desde los planeas a las normas. Mientras se queden en los primeros, por mucho que se desarrollen, solo servirán voluntaristamente para considerar la interrelación entre prevención, anticipación y respuesta. Si pasasen a exigirse normativamente de manera generalizada se podría estandarizar sus contenidos, homologar mejor su implementación obligatoria, e incorporar a una respuesta inmediata que, sin duda, redundaría en una más eficaz contención y recuperación.

La puesta en marcha del SAT o Servicio de Alerta Temprana del CCN-CERT en 2008 buscaba incluso pasar de la detección rápida a la anticipación, con una identificación inmediata de anomalías en las dependencias administrativas. Existe, por tanto, una práctica de acción preventiva y correctiva que ha servido eficazmente a la mayor contención posible de las intrusiones. Se trata ahora de perfeccionarla, generalizarla y exigirla para cualquier operador cuyo trabajo condicione la seguridad nacional. La experiencia de SAT INET para identificar patrones de tipos de ataques y amenazas en el tráfico de datos y en los flujos de información dentro de los organismos de seguridad españoles, a modo de sonda individual que recolecta información y la filtra para evitar afecciones al sistema central es la pauta a generalizar. Para ello tiene que salir de la dimensión dispositiva de la planificación pública de los CERTS gubernamentales para incrustarse definitivamente en la obligatoria de las exigencias normativas.

La tercera propuesta tiene que ver con una mejor articulación entre regulación de la gestión y de la auditoría, una vez más con el modelo de ciberseguridad de las infraestructuras críticas. Se han ido sustituyendo progresivamente las prácticas de homologación que provenían de los planes de Protección Civil hacia las más específicas de certificación, propias del mundo de la ciberseguridad. El definitivo avance en la generalización de clasificaciones, terminología y métricas que requiere la norma procesal solo será enteramente útil si se alcanza este paso, al menos en los planes de contingencia y de recuperación en entornos OT (Operation Technology).

La auditoría no es solo del hardware y del software, sino de su rendimiento, vulnerabilidades, eventuales configuraciones mejoradas, ciberseguridad perimetral y otros aspectos operativos. Exista ya una Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información, aunque se trata de elevar su rango normativo si se quieren evitar sucesos como la grave afección del SEPE en marzo de 2021.

4.3. Propuestas con rendimiento penalista

La enorme diferencia entre ataques en la red y procedimientos abiertos en el orden jurisdiccional penal demuestra la insustancialidad de la normativa vigente, a la vez que suscita un debate apenas sugerido hoy en sede parlamentaria sobre la ampliación de la ley penal: 1º) la inadecuación y obsolescencia de algunos elementos objetivos de los tipos actuales 2º) el debate sobre los tipos penales abiertos o cerrados en los delitos contra la seguridad nacional, la independencia del estado, la paz y la Defensa nacional; 3º) en qué medida se desdibuja el esquema de la autoría por los condicionantes de trazabilidad en delitos cometidos a larga distancia y por medios humanos y materiales interpuestos o mediatos.

La primera cuestión se refiere a la inadecuación de la regulación de determinadas conductas que impiden proporcionar certezas sobre la protección de la seguridad nacional comprometida en la proyección exterior del Estado por la presencia en foros y teatros de operaciones con normativas diferentes a la nuestra, o bajo mando directo de organizaciones internacionales con diferente ordenamiento jurídico rector de sus operaciones, y ello aunque existiera una autorización o mandato parlamentario en España.

Los delitos de espionaje[37], revelación de secretos y traición deberían ver variada su redacción profundamente para acoger las modalidades comisivas en el ciberespacio o con utilización de medios telemáticos, que varían significativamente la autoría. Es difícil imaginar una exfiltración de información contenida en papel en un momento en que se ha digitalizado desde la cartografía hasta las herramientas de ataque y defensa. Pero nuestro Código Penal sigue anclado en una redacción hecha cuando no existía siquiera la máquina de escribir.

¿Cómo delimitar supuestos muy frecuentes de coautoría y de autoría mediata en acciones que necesariamente requieren una acumulación de actos, si algunos de ellos están automatizados en la programación informática y no se

37 Diego Navarro Bonilla, "Espionaje, seguridad nacional y relaciones internacionales", *Colección de estudios internacionales*, n.o 14 (2014): 1-45.

desarrollan con total conocimiento de los intervinientes en la ejecución? ¿Cómo modular el fundamento último de la punición del partícipe en estas modalidades de comisión telemática a larga distancia y con extraterritorialidad, especialmente en casos de accesoriedad cualitativa? ¿Cómo contemplar la cooperación necesaria, imprescindible, de los técnicos que habilitan redes, pero no lanzan el ciberataque? ¿Cómo acotar debidamente el *iter criminis* especial de estos delitos en el ciberespacio con una visión obsoleta de un derecho penal del enemigo que resulta inconciliable hoy con la capacidad tecnológica? No es lugar para detenerse en propuestas de redacción que corresponderán al legislador, oídos los expertos técnicos, pero sí de decir que no admite más dilación afrontar esta reforma, a la vista de los graves quebrantos para la seguridad nacional que algunos sonoros y mediáticos casos de filtraciones han ocasionado a nuestros aliados atlánticos.

Algunos de los episodios que a continuación se referirán de interferencia en el normal desenvolvimiento de los procesos democráticos electorales en los países europeos han tenido su origen en Rusia, incluso sin prejuzgar la eventual participación de algunos aparatos de inteligencia del Kremlin. Los que han conseguido un mayor impacto no lo han hecho penetrando las redes militares de España, Francia, Reino Unido, Italia o Alemania, sino agitando sus opiniones públicas ante acontecimientos puntuales que generaban enorme malestar. Se trata de procesos deliberadamente promovidos, que vistos desde las legislaciones nacionales penales de los países afectados resultaron claramente susceptibles de persecución por comisión dolosa de diversos ilícitos penales relacionados con la sedición, la independencia exterior del Estado por los delitos electorales y que habían sido perpetrados mediante una ingeniería social[38] todavía necesitada de regulación específica.

38 Javier Alonso García, *Derecho penal y redes sociales* (Madrid: Aranzadi, 2015); Jorge Eduardo Miceli, Omar Gabriel Orsi, y Nicolás Rodríguez García, *Análisis de redes sociales y sistema penal* (Tirant lo Blanch, 2017); Juan Periago Morant, "TICS y Redes Sociales en derecho penal: pensamiento analítico", en *IN-RED 2019: V Congreso de Innovación Educativa y Docencia en Red*, 2019, 488-501.

¿Demanda el ciberespacio y las modalidades comisivas telemáticas de las amenazas híbridas una mayor generalización de tipos penales abiertos? Este es un debate en curso que debería mantenerse en los estrictos términos jurídicos de delimitación de la autoría y no abrir inconvenientes contaminaciones políticas ante la posibilidad de variar algunos elementos objetivos en los delitos contra la seguridad nacional y la independencia del Estado. La presión de los operadores técnicos siempre apunta hacia la apertura de los tipos penales, lo que no es únicamente una preocupación relacionada con los delitos contra la seguridad nacional[39]. No es esta, sin embargo, la línea apuntada en este artículo cuando se reclama una mayor juridificación de las estrategias de seguridad nacional, porque es tan delicado el conjunto de derechos que puede resultar afectado por la aplicación de las situaciones de interés para la seguridad nacional que contemplan los artículos 23 y 24 LSN, que se dificultaría el enjuiciamiento[40] de algunas conductas que se refieren más a la habilitación del substrato tecnológico utilizado para la comisión del delito, que a esta última.

4.4. Propuestas con rendimiento procesal

Cuatro son las principales sugerencias en este apartado: 1º) un deseable mimetismo entre trazabilidad tecnológica y nexo causal de la imputación; 2º) un mejor tratamiento de las implicaciones de la transnacionalidad de algunas acciones delictivas; 3º) demandar una respuesta conjunta en el seno de la Unión Europea, en tanto que la seguridad nacional está igualmente comprometida en este ámbito, como reiteradamente ha considerado el Parlamento Europeo; 4º) perfeccionar la capacidad de auditoría forense exigida ahora por las normas administrativas y los planes públicos, de manera que pase de los contenidos

39 Ángel Torío López, "Tipicidad. Referencia a la teoría de los tipos abiertos", en *Vinculación del juez a la ley penal*, ed. José Jiménez Villarejo (Madrid: Consejo General del Poder Judicial, 1995), 7-34.

40 Daniel Gustavo Gorra, "¿Los jueces crean derecho cuando "definen" los tipos penales abiertos?", *Revista de Derecho Penal y Criminología*, n.o 7 (2014): 199-206.

técnicos a la conformación de soportes probatorios inatacables en los procedimientos penales.

En relación con la primera cuestión, en nuestro país y en el conjunto de la Unión Europea se ha constatado la enorme dificultad de acreditar fehacientemente un reparto de responsabilidades ante la comisión de ilícitos penales mediante un soporte probatorio suficiente como para prosperar la acusación en sede judicial[41]. Si tomamos los episodios más impactantes para el funcionamiento de las empresas en relación con los ciberdelitos contra el patrimonio esta es ya una dificultad notable, más por las implicaciones reputacionales que por verdaderas dificultades de averiguación, pues muchas grandes compañías, una vez solventada la brecha de seguridad de sus sistemas, prefieren afrontar pagos a las víctimas que promover la condena penal a los delincuentes para evitar noticias alarmantes sobre las vulnerabilidades de sus operaciones en el ciberespacio. Pero cuando se pasa de esa esfera a la de los delitos aquí analizados contra la seguridad nacional -quizás con la sola excepción del ciberterrorismo[42]-asistimos a una auténtica incapacidad probatoria, bien sea por las dificultades de indagación de la autoría -sirva de ejemplo el ataque al SEPE de marzo de 2021- o porque se topa con una eventual responsabilidad de agentes que pudieran actuar por cuenta de terceros Estados que les confieren inmunidad -véase el episodio de la injerencia rusa a través de casi cinco mil bots en apoyo del desafío secesionista catalán entre el 29 de septiembre y el 19 de octubre de 2017-, ejemplos enormemente didácticos para comprender la verdadera naturaleza del reto al que España se enfrenta para garantizar la ciberseguridad nacional.

De ahí la relación con la segunda propuesta, que tiene que ver con las frustrantes cortapisas impuestas a la persecución, investigación y enjuiciamiento de los ciberataques contra la seguridad nacional cuando se producen desde el extranjero. Una vez más la injerencia rusa sirve para ejemplificar los problemas surgidos ante acciones que constituyen ilícitos penales de acuerdo con el Código

41 Sara Arrazola Ruiz, "La ciberdelincuencia como fenómeno jurídico. Su tratamiento procesal", *Revista Aequitas: Estudios sobre historia, derecho e instituciones*, n.o 18 (2021): 371-402.
42 Vicente Pons Gamon, "Ciberterrorismo: amenaza a la seguridad. Respuesta operativa y legislativa, nacional e internacional" (UNED, 2018), 117-58.

Penal español y que pueden tener distinto tratamiento en otros Derechos a efectos de su persecución dentro de las fronteras de terceros Estados, con un tratamiento práctico muy distinto entre los delitos perseguibles de acuerdo a las normas del Derecho Penal Internacional y aquellos que no han adquirido un estatuto jurídico tan consolidado y son únicamente perseguibles a tenor de las legislaciones nacionales.

En los hechos más alarmantes fallan las previsiones construidas por el Derecho Internacional Público para otros escenarios, tangibles o intangibles pero abiertos y carentes del anonimato que caracteriza este[43]. Basta considerar la doctrina internacionalista, más que la letra de los acuerdos internacionales y la escasa jurisprudencia disponible sobre los denominados "hechos del Estado" al reputar responsable a un Estado del comportamiento de individuos que actúan bajo instrucciones, dirección o control, puesto que en este caso es más probable que se dé ante la inacción y la deliberada inhibición u omisión de control del Estado que por mandato expreso.

Occidente constató mediante trazabilidad tecnológica inequívoca la procedencia rusa de los ataques sobre las elecciones presidenciales norteamericanas en 2016, las elecciones presidenciales francesas, las elecciones generales alemanas, la campaña electoral del Brexit y el desafío independentista catalán -injerencia rusa que fue analizada incluso en el Senado de los Estados Unidos-, todas estas últimas intervenciones promovidas por la agencia rusa IRA en 2017. Pero ante todos y cada uno de esos eventos la negativa a aceptar responsabilidades del gobierno ruso se amparaba no en su desconocimiento de tales hechos, sino la imposibilidad de monitorizarlos, como puso de manifiesto la tensa reunión entre los presidentes Putin y Macron en Versalles. Algo parecido constató España cuando el CERT Gubernamental intervino en el ciberataque de *ransomware* Netwalker evitando la encriptación maliciosa de las redes de hospitales públicos españoles en plena incidencia dura de la pandemia. En ambos casos

43 Martha Lliana Sánchez Lozano, *Los retos del derecho internacional humanitario para los conflictos armados en el ciberespacio* (Bogotá: Grupo Editorial Ibáñez, 2018), cap. 4 Propuestas de solución para los retos planteados en conflictos armados en el ciberespacio.

saber de dónde proceden los ciberataques y poder llevar a cabo una imputación formal son cosas muy distintas.

Igual dificultad de aplicación práctica de los principios del Derecho Internacional Público plantea la definición para el uso de la fuerza en el ciberespacio de los tres conceptos clave de gravedad, inmediatez e intrusión, que darían lugar a un uso de la fuerza mediante respuesta de ciberarmas en caso de legítima defensa. E incluso en supuestos de inminencia, en los más controvertidos casos de legítima defensa anticipada que, por definición, en el ciberespacio se multiplicarían infinitamente dada la inmediatez entre la perpetración del ciberataque y sus consecuencias, a diferencia de lo que sucede en el mundo físico que requiere movimientos de grupos o tropas.

Finalmente, entre estas dificultades de aplicación de las previsiones del Derecho Internacional Público, resalta la imposibilidad de aplicación *stricto sensu* del principio de proporcionalidad como complemento al principio de necesidad, puesto que la asimetría de medios es parte inescindible de la guerra híbrida en el ciberespacio.

No son esos los únicos obstáculos procesales, porque se puede recordar igualmente la compleja determinación de la competencia jurisdiccional territorial penal, con enorme dificultad para precisar en relación con el artículo 14.2 LECr el lugar de comisión del delito cuando el ataque pasa por las redes y servidores de distintos países.

Existe ya una preocupación palpable de la Unión Europea que ha venido a completar la parcial visión de la OTAN[44], que contempla la seguridad desde la perspectiva militar. La imbricación de ese interés en la seguridad en una acción conjunta se ha beneficiado de un rápido cambio de mentalidad. Si fue evidente en la conformación de la Política Exterior y de Seguridad Común entre los tratados de Maastricht y Lisboa, está necesitada de mayor refuerzo tras los atentados yihadistas sufridos por una pluralidad de Estados miembros. Fruto de esa

44 Nestor Ganuza Artiles, "Situación de la ciberseguridad en el ámbito internacional y en la OTAN", *Cuadernos de estrategia*, n.o 149 (2011): 165-214.

ocupación existen incipientes mecanismos cooperativos[45], que están llamados a intensificarse, porque las amenazas en el ciberespacio están ocupando paulatinamente el lugar de las amenazas en el mundo físico.

No se puede cerrar esta enumeración de propuestas sin mencionar la conveniencia del desarrollo de la capacidad forense[46] y la auditoría: camino emprendido desde la técnica al Derecho. Se trata de perfeccionar la capacidad de auditoría forense para permitir imputaciones con suficiente soporte probatorio[47]. Este es en la actualidad el principal obstáculo al que se enfrenta la persecución de los delitos con eficacia preventiva, por ejemplarizante. Cuando las averiguaciones policiales revelan que el origen del ciberdelito está en España, los procedimientos judiciales son los habituales, con una gran continuidad entre la investigación policial, la instrucción, el enjuiciamiento y la eventual condena. Aunque siempre es deseable una mejor dotación de medios humanos y materiales, no parece que el escollo se encuentre en la formación y dotación de unidades especializadas en delitos telemáticos, también contra la seguridad, en los cuerpos policiales integrales (la Brigada de Investigación Tecnológica del Cuerpo Nacional de Policía, el Grupo de Delitos Telemáticos de la UCO y el Grupo de Ciberinteligencia y Ciberterrorismo de la Guardia Civil, la Unidad de Ciberseguridad Policial de los Mossos d'Esquadra y la Sección Central de Delitos en Tecnologías de la Información de la Ertzaintza). No obstante, a diferencia de lo que sucede en los ciber delitos contra el patrimonio, los delitos cometidos en el ciberespacio contra la seguridad y la Defensa Nacional suelen tener origen territorial fuera de las fronteras nacionales, habitualmente en países con escasa cultura e instrumentos obligatorios de cooperación judicial internacional.

---

45 Antonio Manrique de Luna Barrios, "El rol de la Unión Europea en el ámbito de la paz y de la seguridad regional e internacional", en *Retos del Derecho ante las nuevas amenazas*, ed. Susana de Tomás Morales (Madrid: Dykinson, 2016), 387-96.

46 Andres Caro Lindo, "Reto en ciberseguridad: análisis forense de discos", en *Actas de las primeras Jornadas Nacionales de Investigación en Ciberseguridad: León, 14, 15, 16 de septiembre de 2015. I JNIC2015* (León: Área de Publicaciones Universidad de León, 2015), 148-55.

47 Andrés Sánchez Magro, "El ciberdelito y sus implicaciones procesales", en *Principios de derecho de internet* (Valencia: Tirant lo Blanch, 2005), 293-324; Ignacio Flores Prada, *Criminalidad informática: (aspectos sustantivos y procesales)* (Valencia: Tirant lo Blanch, 2012); Moisés Barrio Andrés, *Delitos 2.0: Aspectos penales, procesales y de seguridad de los ciberdelitos* (Madrid: Wolters Kluwer, 2018).

Aunque el Convenio de Budapest sobre la Ciberdelincuencia de 23 de noviembre de 2001, ratificado por España en 2010, constituyó un hito importante en la cooperación internacional en la persecución de los delitos tecnológicos[48], ha quedado parcialmente desfasado y después de dos décadas muestra su absoluta inadecuación para los niveles de ataques y conectividad actuales. Se impone una actualización para mejorar la investigación[49] en la fase de instrucción que facilite las vistas.

5. CONCLUSIONES

Expuestas las razones que parecen abonar una modificación importante en varias direcciones de las normas vigentes en materia de ciberseguridad, e incluso su extensión más allá de los límites actuales, corresponde apuntar sucintamente las principales conclusiones que hilan estas reflexiones, sin necesidad de enumerar de nuevo las medidas desgranadas en el apartado anterior.

La primera es la constatación del desfase normativo por obsolescencia de la regulación pensada para instrumentos tecnológicos menos maduros e invasivos que los actuales. Los cambios del tenor literal de los artículos del Código Penal obedecían tradicionalmente a razones dogmáticas, mientras que aquí parecen venir aconsejados por motivos de política criminal. No se trata de buscar una mayor punición, sino una mejor definición de los elementos objetivos del tipo penal, precisando particularmente las conductas dolosas con una pluralidad de intervinientes y una sucesión de actos de ejecución. Respecto a la normativa administrativa, se aprecia una mayor actualización constante, por lo que se trata

48 Andrés Díaz Gómez, "El delito informático, su problemática y la cooperación internacional como paradigma de su solución: El Convenio de Budapest", *Revista electrónica del Departamento de Derecho de la Universidad de La Rioja, REDUR*, n.o 8 (2010): 169-203; Francisco Jiménez García, "La ciberseguridad en el marco internacional. El sistema del Convenio de Budapest de 2001 sobre la ciberdelincuencia adoptado en el Consejo de Europa", en *La protección y seguridad de la persona en internet: aspectos sociales y jurídicos* (Madrid : Reus, 2014, 2014), 49-79.

49 José María Asencio Gallego, "Los delitos informáticos y las medidas de investigación y obtención de pruebas en el convenio de Budapest sobre la ciberdelincuencia", en *Justicia penal y nuevas formas de delincuencia* (Valencia: Tirant lo Blanch, 2017), 44-67.

únicamente de incluir mecanismos de anticipación a la producción efectiva de daños graves a la seguridad nacional.

La segunda es la necesidad de evitar una compartimentación perniciosa como la actual, lo que solo se logrará mediante soluciones jurídicas interdisciplinares que pretendan una eficacia mayor de la persecución penal de los delitos y de la investigación policial en los casos de mayor afección de la extraterritorialidad y el anonimato proporcionados por el ciberespacio. Para ello deben intensificarse los puentes entre la perspectiva procesal, la norma penal y el sustrato administrativo y tecnológico.

La tercera es la necesidad de proyectar la amplitud normativa de la Ley de Seguridad Nacional sobre los próximos cambios. Su mayor flexibilidad para acoger esos acercamientos interdisciplinares jurídicos puede informar eficientemente las reformas legislativas simultáneas que en el futuro inmediato agilicen los mecanismos de resiliencia y recuperación frente a ciberataques graves a la ciberseguridad nacional respecto a alguna normativa administrativa, al Código Penal y a la Ley de Enjuiciamiento Criminal.

La cuarta es la conveniencia de acometer algunas de las reformas propuestas en este artículo en un razonable y corto plazo, dentro de la presente legislatura estatal las más urgentes, aprovechando la necesidad de transponer las oportunas modificaciones que se introduzcan en la normativa comunitaria que puedan afectar a las herramientas utilizadas en el ciberespacio y que tienen connotaciones de ciberseguridad, que indefectiblemente terminan por afectar a la seguridad nacional.

REFERENCIAS BIBLIOGRÁFICAS

Alcantarilla, Jesús. "«Big Data»" en los departamentos de seguridad, una oportunidad para un nuevo modelo". *Seguritecnia*, n.º 434 (2016): 48-49.

Aldana Montes, José Francisco, José Manuel García Nieto, Juan Carlos Gonzalvez, y Ismael Navas Delgado. *Big data: seguridad y gobernanza*. Madrid: García Maroto Editores, 2018.

Alonso García, Javier. *Derecho penal y redes sociales*. Madrid: Aranzadi, 2015.

Álvarez Rodríguez, Ignacio. "Constitución y Derecho del Ciberespacio". En *Nuevos retos de la ciberseguridad en un contexto cambiante*, editado por Covadonga Mallada Fernández, 21-46. Cizur Menor: Aranzadi Thomson Reuters, 2019.

Arias Holguín, Diana Patricia. "Contexto, interdisciplinariedad y dogmática penal". En *Liber amicorum: estudios jurídicos en homenaje al profesor doctor Juan Ma. Terradillos Basoco*, 49-62. Valencia: Valencia: Tirant lo Blanch, 2018.

Arrazola Ruiz, Sara. "La ciberdelincuencia como fenómeno jurídico. Su tratamiento procesal". *Revista Aequitas: Estudios sobre historia, derecho e instituciones*, n.º 18 (2021): 371-402.

Arteaga Martín, Félix. "Contexto estratégico de la inteligencia artificial". En *La inteligencia artificial, aplicada a la defensa*, 153-72, 2019.

Arteaga Martín, Félix. "La evaluación y la revisión de la Directiva NIS: la Directiva NIS 2.0". *Análisis del Real Instituto Elcano (ARI)*, n.º 19 (2021).

Asencio Gallego, José María. "Los delitos informáticos y las medidas de investigación y obtención de pruebas en el convenio de Budapest sobre la ciberdelincuencia". En *Justicia penal y nuevas formas de delincuencia*, 44-67. Valencia: Tirant lo Blanch, 2017.

Baldin, Serena. "Diritto e interdisciplinarietà: note sulla integrazione metodologica con le altre scienze sociali". *Revista General de Derecho Público Comparado*, n.º 25 (2019).

Barreto Rozo, Antonio. "La interdisciplinariedad horizontal. Las formas económica, social, política y jurídica de construir realidades". *Co-herencia: revista de humanidades* 13, n.º 24 (2016): 43-58.

Barrio Andrés, Moisés. *Ciberdelitos. Amenazas criminales del ciberespacio*. Madrid: Reus, 2017.

Barrio Andrés, Moisés. *Delitos 2.0: Aspectos penales, procesales y de seguridad de los ciberdelitos*. Madrid: Wolters Kluwer, 2018.

Caro Bejarano, María José. "Alcance y ámbito de la seguridad nacional en el ciberespacio". *Cuadernos de estrategia*, n.º 149 (2011): 47-82.

Caro Lindo, Andres. "Reto en ciberseguridad: análisis forense de discos". En *Actas de las primeras Jornadas Nacionales de Investigación en Ciberseguridad: León, 14, 15, 16 de septiembre de 2015. I JNIC2015*, 148-55. León: Área de Publicaciones Universidad de León, 2015.

Carrillo Ruiz, José Antonio, Jesús Marco de Lucas, Juan Carlos Dueñas López, Fernando Cases Vega, José Cristino Fernández, Guillermo González Muñoz De Morales, y Luis Fernando Pereda Laredo. "Big data en los entornos de defensa y seguridad". *Pre-bie3*,

n.º 6 (2013).

Ciuro Caldani, Miguel Ángel. "Reflexiones básicas sobre integrativismo e interdisciplina en el Derecho (un planteo interdisciplinario de la interdisciplina)". *Revista de Filosofía Jurídica y Social*, n.º 37 (2016): 61-85.

Colina Ramírez, Edgar Iván. "La seguridad como bien jurídico". *Cuadernos de la Guardia Civil: Revista de seguridad pública*, n.º 56 (2018): 41-60.

Colina Ramírez, Edgar Iván. *Sobre la legitimación del derecho penal del riesgo*. Barcelona: J.M. Bosch Editor, 2014.

Cubeiro Cabello, Enrique. "Inteligencia artificial para la seguridad y defensa del ciberespacio". En *Usos militares de la inteligencia artificial, la automatización y la robótica*, 97-130, 2020.

Díaz del Río Durán, Juan. "La ciberseguridad en el ámbito militar". *Cuadernos de estrategia*, n.º 149 (2011): 215-56.

Díaz Gómez, Andrés. "El delito informático, su problemática y la cooperación internacional como paradigma de su solución: El Convenio de Budapest". *Revista electrónica del Departamento de Derecho de la Universidad de La Rioja, REDUR*, n.º 8 (2010): 169-203.

Fernández Acevedo, Jesús. "Directiva NIS y la transposición al derecho interno". En *Aspectos jurídicos de la ciberseguridad*, 91-101, 2020.

Fernández Bermejo, Daniel, y Gorgonio Martínez Atienza. *Ciberseguridad, ciberespacio y ciberdelincuencia*. Cizur Menor: Aranzadi Thomson Reuters, 2018.

Flores Prada, Ignacio. *Criminalidad informática: (aspectos sustantivos y procesales)*. Valencia: Tirant lo Blanch, 2012.

Fuente Chacón, José Carlos de la. "La inteligencia artificial y su aplicación en el mundo militar". En *La inteligencia artificial, aplicada a la defensa*, 69-98, 2019.

Galán, Carlos. "El derecho a la ciberseguridad". En *Sociedad Digital y Derecho*, editado por Tomás de la Quadra-Salcedo y Fernández del Castillo y José Luis Piñar Mañas, 573-90. Madrid: Ministerio de Industria, Comercio y Turismo, 2018.

Ganuza Artiles, Nestor. "Situación de la ciberseguridad en el ámbito internacional y en la OTAN". *Cuadernos de estrategia*, n.º 149 (2011): 165-214.

García Pérez, Rafael. "¿Desde cuándo se cometen delitos?: relaciones entre léxico y sintaxis en la evolución histórica de la lengua del derecho penal". En *Palabras, norma, discurso*, editado por Luis Santos Río, 509-20. Salamanca: Universidad de Salamanca, 2005.

Gené Badia, Joan, Pedro Gallo, y Itziar de Lecuona Ramírez. "Big data y seguridad de la información". *Atención primaria: Publicación oficial de la Sociedad Española de Familia y Comunitaria* 50, n.º 1 (2018): 3-5.

Gómez de Ágreda, Ángel. "Ciberseguridad en un mundo hiperconectado". En *Ciberseguridad. Un nuevo reto para el Estado y los gobiernos locales*, editado por Dolors Canals i Ametller, 29-62. Madrid: Wolters Kluwer, 2021.

González Cussac, José Luis. "Estrategias legales frente a las ciberamenazas". *Cuadernos de estrategia del Ministerio de Defensa* 149 (2011): 85-127.

González Hurtado, Jorge Alexandre. "Un nuevo bien jurídico protegido en el uso y disfrute de la tecnología: la seguridad en los sistemas de información". *La ley penal: revista de derecho penal, procesal y penitenciario*, n.º 107 (2014): 4.

González Rus, Juan José. "Los ilícitos en la red (I): hackers, crackers, cyberpunks, sniffers, denegación de servicio y otros comportamientos semejantes". En *El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales.*, 241-71. Granada: Comares, 2006.

Gorra, Daniel Gustavo. "¿Los jueces crean derecho cuando "definen" los tipos penales abiertos?" *Revista de Derecho Penal y Criminología*, n.º 7 (2014): 199-206.

Gutiérrez Espada, Cesáreo. "¿Existe (ya) un derecho aplicable a las actividades en el ciberespacio?" En *Nuevas tecnologías en el uso de la fuerza: drones, armas autónomas y ciberespacio*, editado por María José Cervell Hortal, 225-48. Cizur Menor: Thomson Reuters Aranzadi, 2020.

Jiménez García, Francisco. "La ciberseguridad en el marco internacional. El sistema del Convenio de Budapest de 2001 sobre la ciberdelincuencia adoptado en el Consejo de Europa". En *La protección y seguridad de la persona en internet: aspectos sociales y jurídicos*, 49-79. Madrid: Reus, 2014, 2014.

Malhado, Ricardo. "Big Data y sistemas cognitivos están cambiando el paradigma de seguridad". *Red seguridad: revista especializada en seguridad informática, protección de datos y comunicaciones*, n.º 78 (2017): 42-44.

Manrique de Luna Barrios, Antonio. "El rol de la Unión Europea en el ámbito de la paz y de la seguridad regional e internacional". En *Retos del Derecho ante las nuevas amenazas*, editado por Susana de Tomás Morales, 387-96. Madrid: Dykinson, 2016.

Márquez Díaz, Jairo Eduardo. "Armas cibernéticas. Malware inteligente para ataques dirigidos". *Revista Ingenierías USBMed* 8, n.º 2 (2017): 48-57.

Miceli, Jorge Eduardo, Omar Gabriel Orsi, y Nicolás Rodríguez García. *Análisis de redes sociales y sistema penal*. Tirant lo Blanch, 2017.

Miró Llinares, Fernando. *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio*. Madrid: Marcial Pons, 2012.

Moret Millás, Vicente. "Aspectos relativos a la incorporación de la Directiva NIS al ordenamiento jurídico español". *bie3: Boletín IEEE*, n.º 5 (2017): 733-51.

Moret Millás, Vicente. "Blockchain and National Security". *Revista de privacidad y*

derecho digital 5, n.º 18 (2020): 97-128.

Navarro Bonilla, Diego. "Espionaje, seguridad nacional y relaciones internacionales". *Colección de estudios internacionales*, n.º 14 (2014): 1-45. https://dialnet.unirioja.es/servlet/extart?codigo=6509142.

Navarro Ruiz, Manuel. "La seguridad se convierte en el principal reto de Big Data". *Byte España*, n.º 238 (2016): 8-9.

Periago Morant, Juan. "TICS y Redes Sociales en derecho penal: pensamiento analítico". En *IN-RED 2019: V Congreso de Innovación Educativa y Docencia en Red*, 488-501, 2019.

Picotti, Lorenzo. "Ciberespacio y Derecho penal". En *Libro homenaje al profesor Dr. Agustín Jorge Barreiro*, editado por Gonzalo Basso, 2:1191-1204. Madrid: Servicio de Publicaciones de la Universidad Autónoma de Madrid, 2019.

Pons Gamon, Vicente. "Ciberterrorismo: amenaza a la seguridad. Respuesta operativa y legislativa, nacional e internacional". UNED, 2018.

Requena Jiménez, Antonio. "Blockchain como disrupción para aplicaciones de seguridad". *Revista SIC: ciberseguridad, seguridad de la información y privacidad* 26, n.º 127 (2017): 114-16.

Salas, Minor E. "Interdisciplinariedad de las ciencias sociales y jurídicas: ¿impostura intelectual o aspiración científica?" *Revista de ciencias sociales*, n.º 113 (2006): 55-69.

Sánchez Hidalgo, Adolfo Jorge. *Epistemología y metodología jurídica*. Valencia: Tirant lo Blanch, 2019.

Sánchez Lozano, Martha Lliana. *Los retos del derecho internacional humanitario para los conflictos armados en el ciberespacio*. Bogotá: Grupo Editorial Ibáñez, 2018.

Sánchez Magro, Andrés. "El ciberdelito y sus implicaciones procesales". En *Principios de derecho de internet*, 293-324. Valencia: Tirant lo Blanch, 2005.

Serrano Ferrer, María Pilar. *El reflejo de las nuevas tecnologías en el derecho penal y otros destellos*. Cizur Menor: Aranzadi Thomson Reuters, 2016.

Singer, Peter W. "Ciberarmas y carreras de armamentos: un análisis". *Vanguardia dossier*, n.º 54 (2015): 42-47.

Solari Merlo, Mariana Noelia. "El legislador penal ante la innovación tecnológica: los daños informáticos en el dilema entre la reflexión filosófica y la práctica jurídico científica". En *Moderno discurso penal y nuevas tecnologías: memorias [del] III Congreso Internacional de Jóvenes Investigadores en Ciencias Penales, 17, 18 y 19 de junio de 2013*, editado por Fernando Pérez Álvarez, 201-17. Salamanca: Ediciones Universidad de Salamanca, 2014.

Souto, Claudio. "La ficción de la autosuficiencia en los saberes jurídicos fundamentales".

Doxa: Cuadernos de Filosofía del Derecho, n.º 3 (1986): 149-57.

Suñé Llinas, Emilio. "Del derecho de la informática al derecho del ciberespacio y a la constitución del ciberespacio". *Estudios jurídicos* 2007 (2007).

Tejerina Rodríguez, Ofelia. "Seguridad pública en el mundo digital". En *Sociedad Digital y Derecho*, editado por Tomás de la Quadra-Salcedo y Fernández del Castillo y José Luis Piñar Mañas, 553-72. Madrid: Ministerio de Industria, Comercio y Turismo, 2018.

Terrón Santos, Daniel (dir.), y José Luis (dir.) Domínguez Álvarez. *Inteligencia artificial y defensa: nuevos horizontes*. Aranzadi Thomson Reuters, 2021.

Torío López, Ángel. "Tipicidad. Referencia a la teoría de los tipos abiertos". En *Vinculación del juez a la ley penal*, editado por José Jiménez Villarejo, 7-34. Madrid: Consejo General del Poder Judicial, 1995.

Valls Estefanell, Marc. "La inteligencia artificial y su encaje en las Estrategias de Seguridad Nacional". *bie3: Boletín IEEE*, n.º 12 (2018): 472-85.

EDUARDO FERNÁNDEZ GARCÍA
Área de Historia del Derecho y de las Instituciones
Facultad de Criminología
Universidad Isabel I. Burgos
eduardo.fernandez.garcia@ui1.es
https://orcid.org/ 0000-0002-9225-1071