Icade. Revista de la Facultad de Derecho | nº 109 | 1-19 [enero-junio 2020] [ISSN 2341-0841]
DOI: 10.14422/icade.i109.y2020.001

CIBERSEGURIDAD Y ESTADO AUTONÓMICO

Cybersecurity and Autonomic State

Francisco Martínez Vázquez
Universidad Pontificia Comillas
E-mail: fvazquez@comillas.edu

Autor

La protección de la seguridad en el ciberespacio se ha convertido en una prioridad para los poderes públicos, que exige el desarrollo de políticas adecuadas para prevenir y contrarrestar las amenazas que se materializan en el mundo virtual. El Estado es el actor principal en el campo de la ciberseguridad, sin perjuicio de la dificultad para delimitar las actuaciones en un espacio que, por definición, no puede acotarse a través de fronteras y jurisdicciones. En los Estados descentralizados se plantea el debate sobre el alcance de las competencias de las entidades subestatales en materia de ciberseguridad, especialmente cuando los Gobiernos, organismos y servicios públicos regionales y locales destacan cada vez más como objeto de las acciones maliciosas en el espacio virtual. En España, la delimitación de competencias entre el Estado y las Comunidades Autónomas ha sido precisada por el Tribunal Constitucional en la STC 142/2018, de 20 de diciembre, en coherencia con su doctrina y con la concepción racional del sistema de seguridad nacional.

Protecting security in cyberspace has become a priority for public authorities, which requires the development of adequate policies to prevent and counteract threats that materialize in the virtual world. The State is the main actor in the field of cybersecurity, without prejudice to the difficulty in delimiting actions in a space that, by definition, cannot be bounded across borders and jurisdictions. In decentralized states, the debate on the scope of the powers of sub-state entities in cybersecurity is raised, especially when regional and local governments, agencies and public services increasingly stand out as the object of malicious actions in virtual space. In Spain, the delimitation of powers between the State and the Autonomous Communities has been specified by the Constitutional Court in STC 142/2018, of December 20, in coherence with its doctrine and with the rational conception of the national security system.

Resumen

ciberespacio; ciberseguridad; ciberamenazas; infraestructuras críticas; incidentes; seguridad pública; Estado autonómico

cyberspace; cybersecurity; cyber threats; critical infrastructure; incidents; public safety; Autonomic State

Key words

Recibido: 29/04/2020. Aceptado: 27/05/2020

Fechas

1. La seguridad del ciberespacio como bien colectivo constitucionalmente relevante

1.1. Ciberseguridad, ciberamenazas y usos ilícitos del ciberespacio

En su obra *El nomos de la tierra*, Carl Schmitt afirmaba que "el derecho es terrenal y vinculado a la tierra (…) el mar no conoce tal unidad evidente de espacio y derecho, de ordenación y asentamiento" (Schmitt, 2002, p. 22). A mediados del siglo pasado, el autor establecía una elaborada construcción partiendo de la premisa de que cualquier ordenamiento se basa en una localización, asentamiento o territorio determinado.

No ha pasado un siglo desde aquellas certeras palabras y ya no podemos compartir esa contundente afirmación inicial, desde el momento en que existe una dimensión en la que se desarrolla intensamente la vida, que no es ni siquiera susceptible de delimitación y, muchos menos, de apropiación. El ciberespacio es el lugar más poblado del planeta en el que interactúa casi un 60% de la población mundial, más de 4.500 millones de personas en un entorno sin fronteras, que se resiste a cualquier definición con categorías jurídicas tradicionales.

En el ciberespacio se desarrolla la comunicación personal y el acceso a información con una velocidad y un alcance sin precedentes, el comercio internacional, los servicios públicos, las relaciones internacionales y también el crimen y la guerra. Como señala la primera conclusión del *Informe de la Ponencia para el estudio de diversas cuestiones relativas a la ciberseguridad en España*, aprobado por la Comisión Mixta de Seguridad Nacional de las Cortes Generales[1], "la profundidad y relevancia de los cambios que la disrupción digital está produciendo en los sistemas económicos, los sistemas políticos, los modelos comerciales y, en general, en las relaciones sociales, supone una transformación integral de la realidad que conocemos".

La Estrategia de Seguridad Nacional (2017)[2] describe este entorno afirmando que "la conectividad genera un mayor intercambio y movimiento de mercancías, personas, bienes, servicios y capitales, configurando un espacio funcional distinto al puramente geográfico". La ciberdependencia es, sin duda, uno de los rasgos de la sociedad contemporánea: un mundo hiperconectado que necesita para el desarrollo cotidiano de toda clase de actividades apoyarse en redes y tecnologías digitales que se convierten, así, en imprescindibles.

Recientemente, la crisis provocada por la pandemia del patógeno COVID-19 no ha hecho sino confirmar que el ciberespacio es una dimensión absolutamente necesaria en todos los órdenes de la actividad humana, pues no solo se ha convertido en el único medio de comunicación interpersonal en situaciones de restricción drástica de la movilidad, sino que ha demostrado ser una alternativa real en el mundo laboral y también, en muchos casos, el medio que ha hecho posible el funcionamiento de las instituciones públicas, a través de votaciones telemáticas en el Congreso de los Diputados o reuniones virtuales del Consejo de Ministros.

1 Boletín Oficial de las Cortes Generales, XII Legislatura, sección Cortes Generales, número 277, 13 de marzo de 2019.

2 Real Decreto 1008/2017, de 1 de diciembre, por el que se aprueba la Estrategia de Seguridad Nacional 2017.

El ciberespacio se resiste a someterse a las categorías jurídicas tradicionales, insuficientes para las relaciones que se desarrollan en un entorno en el que se han desvanecido los límites espaciales y, por tanto, es difícil definir el ordenamiento aplicable y el alcance de la jurisdicción de los Estados, probablemente porque Schmitt tenía razón: el Derecho está "vinculado a la tierra".

Si el ciberespacio es un entorno para el desarrollo de toda clase de relaciones y negocios jurídicos, es evidente que se presta también a usos maliciosos y, en muchos casos, delictivos, que pretenden obtener algún tipo de beneficio a partir de actuaciones que se desarrollan en el ecosistema virtual y que constituyen actos ilícitos de variada naturaleza. En efecto, la interdependencia en que se desenvuelve la vida digital genera también nuevos riesgos y nuevas amenazas. La Estrategia de Seguridad Nacional (2017) antes citada afirma que, en este mundo global e hiperconectado, "la distancia entre situaciones de normalidad y crisis es cada vez menor".

Nos enfrentamos, afirma Caro Bejarano (2011) "a un nuevo campo de batalla dentro de la seguridad que es el ciberespacio, donde se producen comportamientos o fenómenos ya conocidos, pero empleando técnicas nuevas; y también fenómenos nuevos que surgen de la propia idiosincrasia del ciberespacio y en donde, en ocasiones, no están claras las fronteras entre activismo y delincuencia". En la misma línea, observa Alonso Lecuit (2018) que "la Red se ha convertido en un escenario de competición geopolítica y económica entre Estados donde se entremezclan ciberataques, ciberdelitos y desinformación con un propósito desestabilizador".

En este contexto, surgen los conceptos de ciberseguridad y ciberamenazas y otros tantos construidos con el prefijo "ciber", que aluden a actuaciones que se desarrollan en el entorno virtual y que constituyen nuevos ámbitos que deben ser sometidos, en la medida de lo posible, a regulación y que constituyen, asimismo, objeto de actuaciones de los poderes públicos.

La Unión Internacional de las Telecomunicaciones aprobó en 2008 una definición amplia de ciberseguridad en su Recomendación UIT–T X.1205, que comprende, a su vez, la definición de otros conceptos relacionados. Así, la ciberseguridad se definiría como "el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciberentorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno. Las propiedades de seguridad incluyen una o más de las siguientes: disponibilidad, integridad, que puede incluir la autenticidad y el no repudio y confidencialidad".

En términos más sintéticos, el Reglamento sobre la Ciberseguridad de la Unión Europea[3] define la ciberseguridad en su artículo 2.1 como "todas las actividades necesarias para la protección de las redes y sistemas de información, de los usuarios de tales sistemas y de otras personas afectadas por las ciberamenazas".

La Estrategia de Seguridad Nacional (2017) afirma que "es creciente la actividad tanto por parte de Estados, que persiguen la expansión de sus intereses geopolíticos a través de acciones de carácter ofensivo y subversivo, como de organizaciones terroristas, grupos de crimen organizado y actores individuales".

La protección de la seguridad del ciberespacio y la lucha contra las ciberamenazas se han convertido en una prioridad dentro de las políticas públicas de seguridad y defensa, si bien con las evidentes dificultades derivadas de la insuficiente regulación de esa "cuarta dimensión", nacida como "un ámbito en el cual no hay leyes que lo regulen, ya que por definición nació exento, en principio, de la acción estatal" (Moret Millás, 2017).

La premisa de este trabajo es que la ciberseguridad constituye, en la actualidad, una función de los poderes públicos encaminada a proveer un bien colectivo de interés constitucional, en tanto que manifestación de la seguridad pública. Sin perjuicio de lo anterior, en todos los Estados descentralizados se ha planteado la necesidad de delimitar las competencias en el ámbito de la ciberseguridad, con la particularidad de que las políticas públicas en este campo están relacionadas con títulos materiales diversos, como son la defensa, la seguridad pública y la lucha contra el crimen, la inteligencia, las relaciones internacionales o las telecomunicaciones. En España este mismo debate ha llegado al Tribunal Constitucional que, como veremos, ha delimitado las competencias entre el Estado y las Comunidades Autónomas en materia de ciberseguridad en la STC 142/2018, de 20 de diciembre.

1.2. El Estado en peligro en el ciberespacio: amenazas híbridas

El ciberespacio, el espacio marítimo y el espacio aéreo y ultraterrestre son espacios comunes globales, según la terminología que utiliza la Estrategia de Seguridad Nacional (2017). "Conectan el mundo y permiten el libre flujo de personas, bienes, información, servicios e ideas", afirma el documento estratégico, al tiempo que añade que tales espacios "se caracterizan por no tener fronteras físicas, la ausencia general de soberanía y jurisdicción por parte de los Estados, la difícil atribución de acciones delictivas y su débil regulación".

Paradójicamente, el Estado se desenvuelve mal en el ciberespacio, a pesar de lo cual desarrolla una actividad cada vez más intensa en esta dimensión y está expuesto a amenazas de diversa naturaleza que comprometen su soberanía en el mundo digital. Los ciberataques ocurridos en Estonia en 2007, en Georgia en 2008 o el *malware Stuxnet*, que afectó el programa nuclear iraní (2010), no fueron meros ciberincidentes, sino que constituyen los primeros y más claros ejemplos de agresiones en el entorno digital realizadas por actores estatales o por actores patrocinados por Estados.

3 Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo de 17 de abril de 2019 relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) n. o 526/2013 (Reglamento sobre la Ciberseguridad).

El 15 de febrero de 2018, un comunicado de prensa de la Casa Blanca[4] afirmaba que el ciberataque conocido como *NotPetya* había sido lanzado por Rusia respondiendo al objetivo del Kremlin de desestabilizar Ucrania. El ataque se calificaba como el más destructivo de la historia. Una de las compañías que sufrió gravísimas pérdidas económicas a raíz de este incidente, superiores a 1.300 millones de dólares, fue la farmacéutica Merck, que, naturalmente, reclamó la correspondiente indemnización a las compañías con las que tenía suscritos contratos de seguro. Las compañías de seguros se negaron a asumir tales indemnizaciones, con el argumento de que el siniestro estaba fuera del ámbito asegurado en las pólizas, pues el incidente debía calificarse como un acto de guerra (*act of war*). La empresa farmacéutica ha acudido a los tribunales de New Jersey, iniciado lo que puede ser un interesante *leading case* en cuanto a la naturaleza jurídica de estas agresiones entre Estados, que constituyen claros ejemplos de amenazas híbridas con numerosas consecuencias en el ámbito jurídico, incluido, por supuesto, el derecho del seguro (Pérez López, 2020).

En este contexto de amenazas híbridas (Galán, 2018), la pregunta inevitable es si estamos hablando exclusivamente de un escenario de confrontación entre Estados o, por el contrario, en el ciberespacio no son válidas las categorías del orden westfaliano y debemos asumir que un conjunto de actores sin fácil adscripción a intereses o patrocinios estatales son capaces de los más graves ataques y perturbaciones.

En el ciberespacio las reglas tradicionales de relación entre Estados resultan absolutamente insuficientes. Como afirma Galán (2018, p. 6) "no podemos considerar el ciberespacio como una frontera, sino como un verdadero ámbito operativo —un dominio— que representa un desafío a la idea tradicional de seguridad".

En este contexto, es evidente que las amenazas híbridas e incluso las agresiones que afectan a la soberanía e integridad del Estado o a sus infraestructuras críticas forman parte del ámbito estatal de actuaciones cubierto por la competencia material sobre la defensa, ámbito de actuación reservado por antonomasia al Estado como actor exclusivo. Así, desde la Cumbre de Bucarest de 2008, la OTAN impulsó la necesidad de mejorar su capacidad de ciberdefensa, la necesidad de los Estados de la alianza de mejorar la protección de los sistemas de información crítica desplegados en sus territorios y la exigencia para ambas partes, la OTAN y los Estados, de mejorar la coordinación, intercambio de información y apoyo mutuo en materia de ciberdefensa.

La reflexión se plantea respecto de aquellos incidentes que se producen en el ciberespacio y que no puede calificarse, al menos inicialmente, como actos de guerra híbrida, especialmente cuando afectan a las infraestructuras, organismos o servicios de entidades regionales o locales.

1.3. Who does what: el debate sobre Cyber Federalism en Estados Unidos

En efecto, la pregunta "quién hace qué" es oportuna en aquellos casos en que las agresiones en el ciberespacio afectan exclusivamente a entes subestatales, como es el caso de entidades locales o gobiernos regionales. El ejemplo más evidente lo encontramos en Estados Uni-

4 Recuperado de https://www.whitehouse.gov/briefings-statements/statement-press-secretary-25/

dos, donde los ataques contra gobiernos locales se incrementaron notablemente a partir de 2018 y, sobre todo, en 2019. En 2018 un ataque de *ransomware* paralizó la ciudad de Atlanta durante varias semanas y desde entonces se produjeron una media de seis ataques al mes contra instituciones y organismos públicos locales, en algunos casos de grandes ciudades. El gobernador de Louisiana llegó a declarar el estado de emergencia como consecuencia de un ataque de *ransomware* que afectó a las infraestructuras estratégicas y servicios esenciales del Estado. A finales de 2019, los únicos Estados cuyas agencias públicas no habían sido atacadas por *ransomware* eran Delaware y Kentucky.

Frente a lo que se podría creer desde un paradigma clásico de las relaciones internacionales, las amenazas y las agresiones en el ciberespacio desbordan el papel del Estado como único titular de competencias para desarrollar políticas públicas de seguridad colectiva y plantean el necesario debate acerca del papel que las entidades locales y regionales deben jugar en la protección del ciberespacio o el alcance, en su caso, de las competencias regionales y locales en materia de ciberseguridad.

El presidente Obama aprobó en 2013 la *Executive Order 13636* cuyo objeto era la mejora de la ciberseguridad de las infraestructuras críticas y que dio paso, tres años después, el 26 de julio de 2016, a la aprobación de la *Presidential Policy Directive (PPD) 41: United States Cyber Incident Coordination*[5], que establece mecanismos de coordinación en manos del Gobierno Federal para prevenir y responder al impacto de los ciberataques.

Tan solo unos meses después de la aprobación de la PPD 41, la comunidad de inteligencia de Estados Unidos informaba de los intentos de influir a través de las redes sociales y el uso malicioso del ciberespacio en los resultados de las elecciones presidenciales de noviembre de 2016, lo que tuvo como inmediata consecuencia la declaración por parte del Departamento de *Homeland Security* de la infraestructura electoral como infraestructura crítica, protegida por el Plan Nacional de Protección de Infraestructuras Críticas del Gobierno Federal. Esta consideración de los procesos electorales como infraestructura crítica permite al Gobierno Federal proporcionar asistencia a los gobiernos estatales y locales en sus respectivas elecciones. Sin embargo, algunos gobiernos estatales interpretaron que el paso dado por el Departamento de Interior invadía las competencias de los Estados y era un intento de establecer un control federal sobre sus procesos electorales. En realidad, esta polémica sacó a la luz la inexistencia de una regulación clara de las competencias de los Estados y de los gobiernos locales en la prevención y respuesta a ciberataques contra sus instituciones, procesos o agencias.

En efecto, en el ámbito de la seguridad pública y, por extensión, de la ciberseguridad, el debate federal no ha estado exento de controversias desde la creación del propio Departamento de *Homeland Security* en 2003, que fue una profunda revisión del modelo de agencias públicas de seguridad creado por la *National Security Act* de 1947. La controversia sobre el alcance de las competencias del Gobierno Federal frente a las que corresponden a los gobiernos estatales y locales ha sido especialmente intenso en el ámbito de la seguridad interior, donde siguen sin estar claras las líneas divisorias entre lo poderes de unos y otros (Morag, 2011).

5 Recuperado de https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident

La tesis de los defensores de la primacía de las competencias federales en situaciones de crisis (Waxman, 2002) postula la superación, tras los atentados del 11 de septiembre de 2001, de la vigencia de la cláusula *anti-commendering*, que había fijado el Tribunal Supremo en *Printz v. United States* (1997). Esta posición se contrapone a la de quienes defienden la amplitud de las competencias de los estados y gobiernos locales para hacer frente a los incidentes que afectan a la seguridad interior (Nivola, 2002).

En el ámbito del ciberespacio, el debate es todavía más complejo pues es inevitable pensar que la dimensión internacional de la amenaza y la dificultad para explicar los incidentes desde las tradicionales categorías espaciales que condicionan la delimitación de competencias ha llevado a la constatación de que no cabe una simplista atribución de potestades exclusivas al Gobierno o al Congreso Federal y que tan importante es la cooperación internacional como la adecuada colaboración entre agencias y organismos locales y estatales (Finklea, 2013). También se ha argumentado a favor del fortalecimiento de las competencias de los gobiernos estatales en materia de ciberseguridad, partiendo de la idea de que tanto la comunidad internacional como el Gobierno Federal han resultado, en la práctica, poco eficaces en la protección frente a ciberamenazas, de donde se desprende la conveniencia de que los Estados sean autosuficientes en este campo (Glennon, 2012).

En definitiva, el ritmo al que se producen los avances tecnológicos y, por tanto, la evolución permanente de las amenazas en el ciberespacio revela la insuficiencia de los criterios tradicionales de delimitación de competencias en Estados descentralizados, donde las cláusulas y principios que hasta ahora permitían delimitar el campo de actuación reservado en exclusiva al Estado se muestran disfuncionales cuando se aplican a las políticas públicas en materia de ciberseguridad.

Asimismo, la intensidad y frecuencia con la que han sido atacadas las infraestructuras, servicios y organismos públicos infraestatales, singularmente en Estados Unidos, ha suscitado un creciente interés en la aclaración del marco jurídico de intervención de las diferentes administraciones públicas para garantizar una protección eficaz y eficiente frente a las amenazas que, como todo en el ciberespacio, no responden a un criterio de adscripción territorial ni pueden, por tanto, doblegarse a las categorías jurídicas de un Derecho público que, citando nuevamente a Carl Schmitt, es "terrenal y vinculado a la tierra".

2. La ciberseguridad en el sistema de seguridad nacional

Si acotamos el perímetro del debate al caso de España, podemos preguntarnos cómo se configura el mapa de distribución de competencias en materia de ciberseguridad entre el Estado y las Comunidades Autónomas, para lo cual parece oportuno partir de un somero examen de la regulación de la ciberseguridad en el sistema de seguridad nacional y una descripción de lo que se denomina el "modelo de gobernanza de ciberseguridad".

Nuestra Constitución anticipó con encomiable intuición, y con algo de inspiración en la Constitución portuguesa de 1976, que la tecnología podría prestarse a una utilización ilícita, al establecer en el artículo 18.4 CE que "la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".

Este precepto constitucional sirvió como fundamento a las sucesivas leyes orgánicas de protección de datos personales, hasta llegar a la actualmente vigente Ley Orgánica 3/2018,

de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, en la que es evidente la convergencia de este campo del ordenamiento con la protección de la seguridad en el ciberespacio, algo que no plantearon por razones obvias ni la Ley Orgánica 5/1992, de 29 de octubre, reguladora del tratamiento automatizado de datos personales ni la Ley Orgánica 15/1999, de 5 de diciembre, de protección de datos personales. En título X de la Ley Orgánica 3/2018, introducido por vía de enmienda durante la tramitación parlamentaria de la iniciativa en el Congreso de los Diputados, recoge en el artículo 82 el que denomina derecho a la seguridad digital, en virtud del cual "los usuarios tienen derecho a la seguridad de las comunicaciones que transmitan y reciban a través de Internet". Es importante no perder de vista que muchas de las acciones ilícitas que se desarrollan en el ciberespacio tienen como objetivo la obtención ilegal de toda clase de datos personales para su utilización al servicio de los más variados fines, desde la extorsión o la suplantación de identidad a la venta en la *darkweb*. Por consiguiente, a pesar de haber nacido antes de la expansión de la sociedad de la información, el régimen jurídico de la protección de datos personales complementa, en buena medida, el de la ciberseguridad, con el objetivo coincidente de proteger el espacio virtual frente a usos maliciosos.

Fuera del ámbito de la protección de datos personales, entre las primeras referencias legislativas a la ciberseguridad debemos destacar lo dispuesto en el artículo 4 b) de la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, que atribuye al servicio de inteligencia español la misión de "prevenir, detectar y posibilitar la neutralización de aquellas actividades de servicios extranjeros, grupos o personas que pongan en riesgo, amenacen o atenten contra el ordenamiento constitucional, los derechos y libertades de los ciudadanos españoles, la soberanía, integridad y seguridad del Estado, la estabilidad de sus instituciones, los intereses económicos nacionales y el bienestar de la población". Bajo esta rúbrica, es evidente que encuentra acomodo, como no podía ser de otro modo, toda la actividad que el Centro Nacional de Inteligencia realiza en el ciberespacio que, en el caso de España, a diferencia de Alemania, es una competencia exclusiva del Estado pues no existen servicios o agencias regionales de inteligencia, a diferencia de las *Landesbehörde für Verfassungsschutz* existentes en siete länder alemanes, cuyo ámbito de actuación y recursos son "modestos" (Schallbruch & Skierka, 2018).

En cuanto a las primeras referencias a lo que hoy denominamos ciberseguridad en nuestro ordenamiento jurídico, el artículo 42.2 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, ya derogada, ordenó al Gobierno la aprobación por Real Decreto del Esquema Nacional de Seguridad, cuyo objeto se definía como "la política de seguridad en la utilización de medios electrónicos" en el ámbito de la citada ley, constituido por los principios básicos y requisitos mínimos que permitan una protección adecuada de la información. En cumplimiento de este mandato, se aprobó el Real Decreto 3/2010, de 8 de enero, por el que se regula el esquema nacional de seguridad en el ámbito de la Administración electrónica.

Un importante salto cualitativo en la regulación de la ciberseguridad llegará de la mano de la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas, que constituye un relevante hito en la adopción de un nuevo paradigma de la seguridad pública basado en la prevención y en la creación del sistema de protección de infraestructuras críticas (artículo 5). La ley se dicta al amparo de la competencia exclusiva del Estado en materia de seguridad pública (artículo 149.1.29ª) y desvela en su preámbulo que su objeto es "regular la protección de las infraestructuras críticas contra ataques deliberados

de todo tipo (tanto de carácter físico como cibernético)". La Ley 8/2001 fue desarrollada por el Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.

Tras la aprobación de la primera Estrategia de Seguridad Nacional en 2013, la regulación, por primera vez en nuestro ordenamiento jurídico, del Sistema de Seguridad Nacional, diseñado con vocación integradora de todas las dimensiones de la seguridad pública, llegará con la importante Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, cuyo artículo 10 define los ámbitos de especial interés de la Seguridad Nacional como "aquellos que requieren una atención específica por resultar básicos para preservar los derechos y libertades, así como el bienestar de los ciudadanos, y para garantizar el suministro de los servicios y recursos esenciales" y enumera, a continuación, a título ejemplificativo, varios de esos ámbitos, comenzando precisamente por la ciberseguridad. La Ley 36/2015 se ampara en los títulos previstos en el artículo 149.1.4.ª y 29.ª CE, que atribuyen al Estado la competencia exclusiva en materia de defensa y Fuerzas Armadas y en materia de seguridad pública.

Ese mismo año se aprobaron dos leyes de enorme relevancia en la regulación de nuestro sector público, como son la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas y la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público. Aunque el contenido de ambas es mucho más amplio que la seguridad de los entornos digitales, no es menos cierto que se trata de leyes que consagran los principios, garantías y normas de funcionamiento de un sector público que se relaciona con los ciudadanos por medios digitales y que se basa en estas mismas tecnologías para ordenar las relaciones interorgánicas o interadministrativas, lo cual comporta una serie de exigencias en materia de seguridad de la información que enriquecen el entramado regulatorio de la ciberseguridad en España. Así, el artículo 156.2 de la Ley 40/2015 es el que otorga nueva sede legislativa al Esquema Nacional de Seguridad, al establecer que "el Esquema Nacional de Seguridad tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de la presente Ley, y está constituido por los principios básicos y requisitos mínimos que garanticen adecuadamente la seguridad de la información tratada".

La segunda Estrategia de Seguridad Nacional, aprobada por Real Decreto 1008/2017, de 1 de diciembre, asume como finalidad "garantizar un uso seguro de las redes y los sistemas de información y comunicación a través del fortalecimiento de las capacidades de prevención, detección y respuesta a los ciberataques, potenciando y adoptando medidas específicas para contribuir a un ciberespacio seguro y fiable".

El siguiente hito normativo de enorme importancia en la regulación de la ciberseguridad en España llega de la mano de Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, que transpone al ordenamiento jurídico español la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, conocida como Directiva NIS. El Real Decreto-ley, dictado al amparo de las competencias exclusivas del Estado en materia de régimen general de telecomunicaciones y seguridad pública (artículo 149.1.21.ª y 29.ª CE) incorporó a nuestro ordenamiento jurídico una directiva comunitaria cuya vocación es, claramente, unificar las obligaciones en materia de ciberseguridad de los operadores públicos y privados de la Unión Europea. Se trata, afirma Moret Millás, "de una norma centrada precisamente en alcanzar unos determinados estándares comunes de ciberseguridad en toda la Unión Europea, para lo cual se precisa establecer una regulación del sector que supone la imposición

de forma gradual de obligaciones y de procedimientos de control de dichas obligaciones, así como de designar a las autoridades competentes para efectuar esa labor y, en su caso, imponer las sanciones previstas en la norma" (Moret Millás, 2018).

El Real Decreto-ley 12/2018 establece el régimen aplicable a los operadores de servicios esenciales, definidos con arreglo al criterio de la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas y a los proveedores de servicios digitales, definidos conforme a lo dispuesto en la letra a) del anexo de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

Entre las obligaciones que crea la norma destaca la de designar a un responsable de la seguridad de la información (la figura del CISO), que puede ser una persona, unidad u órgano colegiado, como punto de contacto y, sobre todo, la de notificar los incidentes que puedan tener efectos perturbadores significativos y que afecten a las redes y sistemas de información empleados en la prestación de los servicios indicados, tanto si se trata de redes y servicios propios como si lo son de proveedores externos (artículo 19).

La trasposición a nuestro ordenamiento jurídico de la Directiva NIS ha supuesto un "cambio radical en el panorama del marco jurídico de la ciberseguridad" (Moret Millás, 2018) y un avance decisivo en la convergencia de las obligaciones exigibles en toda la Unión Europea en materia de ciberseguridad, todo ello sin perjuicio de la necesidad de concretar muchos de los aspectos de esta nueva normativa en el desarrollo reglamentario del Decreto-ley.

Con el precedente de la Estrategia de Ciberseguridad Nacional de 2013, el Consejo de Seguridad Nacional aprobó la Estrategia de Ciberseguridad Nacional en sintonía con la Estrategia de Seguridad Nacional (2017). El capítulo 5 de este importante documento concreta la estructura de la ciberseguridad en el marco del Sistema de Seguridad Nacional y desarrolla lo que se denomina el modelo de "gobernanza de la ciberseguridad". La estrategia menciona, así, al Consejo de Seguridad Nacional, el Comité de Situación, único para el conjunto del Sistema de Seguridad Nacional ante situaciones de crisis, el Consejo Nacional de Ciberseguridad, la Comisión Permanente de Ciberseguridad, el Foro Nacional de Ciberseguridad y las Autoridades públicas competentes y CSIRT de referencia nacionales. En este último componente de la estructura se menciona expresamente a los CSIRT de las Comunidades Autónomas, de las Ciudades Autónomas, de las Entidades Locales y de sus organismos vinculados o dependientes.

Asimismo, la segunda línea de acción recogida por la Estrategia responde al objetivo de "garantizar la seguridad y resiliencia de los activos estratégicos para España" y menciona entre las medidas a adoptar "potenciar, en el marco de sus competencias, la progresiva implicación y creación de infraestructuras de ciberseguridad en las Comunidades Autónomas, las Ciudades Autónomas, de las Entidades Locales y de sus organismos vinculados o dependientes, que cooperarán y se coordinarán con las estructuras nacionales en pro de la mejora de la ciberseguridad nacional".

Esta referencia de la Estrategia de Ciberseguridad Nacional a las Comunidades Autónomas, Ciudades Autónomas y Entidades Locales recoge el parecer del Informe de la Ponencia constituida en el seno de la Comisión Mixta de Seguridad Nacional para el estudio de diversas cuestiones relativas a la ciberseguridad en España, que fue aprobado en la sesión de la Comisión Mixta de Seguridad Nacional celebrada el 28 de febrero de 2019, con modificaciones al informe inicial elevado por la ponencia, precisamente en el sentido de incluir en

la tercera conclusión una referencia a "la progresiva implicación de las Comunidades Autónomas en este esfuerzo mediante la creación de sus propias estructuras de ciberseguridad" y una nueva conclusión 23.ª con el siguiente tenor literal: "Asimismo, se considera necesario alcanzar un acuerdo amplio que permita incrementar la ciberseguridad de las entidades locales especialmente de las más pequeñas, con la colaboración de la Federación Española de Municipios y Provincias y la cooperación de las Comunidades Autónomas. En este sentido, también se considera imprescindible lograr una progresiva adecuación de los esfuerzos presupuestarios del Estado, de las Comunidades Autónomas y las Entidades Locales para hacer frente, con las debidas garantías, a los retos que plantea la ciberseguridad".

En última instancia, debemos referirnos al Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones, que modifica la Ley 9/2014 General de Telecomunicaciones y habilita al Gobierno, con carácter excepcional y transitorio, para asumir la gestión directa o la intervención de las redes y servicios de comunicaciones electrónicas en determinados supuestos excepcionales que puedan afectar al orden público, la seguridad pública y la seguridad nacional. Como certeramente ha señalado Moret Millás (2020), este fortalecimiento de las potestades del Estado es importante pero no tan novedoso, pues "ya se aplicaba a los supuestos que afectasen a la seguridad pública y la defensa nacional y ahora se amplía a la seguridad nacional y el orden público como causas legitimadoras de esa intervención".

Este recorrido por la normativa española sobre ciberseguridad nos permite concluir que las normas jurídicas dedicadas a esta materia han sido aprobadas en el ámbito de la competencia exclusiva del Estado y pretenden una regulación homogénea de todas las cuestiones concernientes a la seguridad del ciberespacio.

Es difícil definir en este entramado normativo el ámbito de regulación en manos de las Comunidades Autónomas, a pesar de lo cual es evidente que debe haberlo, si la Estrategia de Ciberseguridad Nacional alude expresamente a la creación de sus propias estructuras de ciberseguridad.

En todo caso, es importante precisar que la Ley 8/2011 incluye a las Comunidades Autónomas y las Ciudades con Estatuto de Autonomía en el Sistema de Protección de Infraestructuras Críticas (artículo 5.d) y de manera especial permite a aquellas Comunidades Autónomas que ostenten competencias estatutariamente reconocidas para la protección de personas y bienes y para el mantenimiento del orden público ejercer las facultades que reglamentariamente se determinen respecto a la protección de las infraestructuras críticas de su territorio.

Asimismo, la Ley 36/2015, de Seguridad Nacional, contempla en su disposición adicional tercera que "los órganos competentes de las distintas Administraciones públicas revisarán, en el plazo de seis meses desde la entrada en vigor de esta ley, sus normas y procedimientos de actuación para adecuar y coordinar su funcionamiento en el Sistema de Seguridad Nacional", implicando así a los Gobiernos y Administraciones autonómicas al Sistema de Seguridad Nacional, del que no tendría sentido alguno que quedasen excluidos.

La controversia se ha suscitado precisamente a raíz de la aprobación por el Parlamento de Cataluña de la 15/2017, de 25 de julio, de la Agencia de Ciberseguridad de Cataluña, que constituye el objeto del pronunciamiento del Tribunal Constitucional en la materia, recogido en la STC 142/2018, de 20 de diciembre, en la que nos detendremos a continuación.

Totalmente diferente es el modelo del *Basque Cybersecurity Centre*, Centro Vasco de Ciberseguridad, que se define como una iniciativa integrada en la Agencia Vasca de Desarrollo Empresarial, regulada por Decreto 160/2018, de 13 de noviembre, por el que se aprueban los estatutos de "SPRI-Agencia Vasca de Desarrollo Empresarial". No existe una norma jurídica que defina claramente la naturaleza o competencias de este Centro de Ciberseguridad, lo que evita las contradicciones que en su día supuso la creación de la Agencia de Ciberseguridad de Cataluña, si bien no proporciona una mínima base de seguridad jurídica a la actividad desarrollada por el mencionado organismo, del que solo se conoce su adscripción a la Agencia Vasca de Desarrollo Empresarial.

3. Las competencias del Estado en materia de ciberseguridad

3.1. Los conceptos constitucionales de seguridad ciudadana, seguridad pública y seguridad nacional

La delimitación de las competencias del Estado y las Comunidades Autónomas aconseja partir de los conceptos de seguridad ciudadana, seguridad pública y seguridad nacional, tal como han sido perfilados en la jurisprudencia constitucional.

Así, Freixas y Remotti (1995) advirtieron hace años que "el Tribunal Constitucional no ha realizado una interpretación que permita sistematizar y diferenciar el alcance del orden público, la seguridad pública y la seguridad ciudadana". No obstante, la jurisprudencia del Tribunal Constitucional califica la seguridad ciudadana como un bien jurídico constitucionalmente protegido. Así, la STC 105/1988 se refiere a "un valor e interés constitucionalmente legítimo" mientras que la STC 196/1987 califica "la persecución y castigo de los delitos, la defensa de la paz social y de la seguridad ciudadana" como "bienes reconocidos en los artículos 10.1 y 104.1 de la Constitución" y la STC 55/1990 define ese bien jurídico con la "prevención y lucha contra la criminalidad, el mantenimiento del orden y la seguridad pública", mientras que la STC 325/1994 sostiene que la seguridad ciudadana es un "bien jurídico de ámbito colectivo, no individual". La STC 155/2013, de 10 de septiembre, en su fundamento jurídico tercero, afirma que la seguridad ciudadana comprende "tanto el mantenimiento de la paz pública en el sentido más físico del término, como los servicios y acciones instrumentales a la altura de los riesgos que amenazan la paz pública en nuestros días, que no son los del pasado siglo".

El concepto de seguridad pública, por su parte, aparece mencionado en el artículo 149.1.29ª CE, precisamente como competencia exclusiva del Estado, a lo que se añade "sin perjuicio de la posibilidad de creación de policías por las Comunidades Autónomas en la forma que se establezca en los respectivos Estatutos en el marco de lo que disponga una ley orgánica".

El Tribunal Constitucional (por todas, la STC 87/2016) ha postulado una interpretación restrictiva del concepto "seguridad pública", al afirmar "que no toda seguridad de personas y bienes, ni toda normativa encaminada a conseguirla o a preservar su mantenimiento, puede englobarse en aquella, pues, si así fuera, la práctica totalidad de las normas del Ordenamiento serían normas de seguridad pública".

Con arreglo a esta premisa, la jurisprudencia constitucional define la seguridad pública como "la actividad dirigida a la protección de personas y bienes (seguridad en sentido estricto) y al mantenimiento de la tranquilidad u orden ciudadanos"; aunque no se limita a regular "las actuaciones específicas de la llamada Policía de seguridad", pues "la actividad policial es una parte de la materia más amplia de la seguridad pública" que "abarca un amplio espectro de actuaciones administrativas" (STC 86/2014, FFJF 2 y 4, entre otras) e incluye "un conjunto plural y diversificado de actuaciones, distintas por su naturaleza y contenido, aunque orientadas a una misma finalidad tuitiva del bien jurídico así definido" (STC 235/2001, FJ 6).

Por su parte, el concepto de seguridad nacional se ha incorporado al Derecho positivo a través del artículo 3 de la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, a tenor del cual: "a los efectos de esta ley se entenderá por Seguridad Nacional la acción del Estado dirigida a proteger la libertad, los derechos y bienestar de los ciudadanos, a garantizar la defensa de España y sus principios y valores constitucionales, así como a contribuir junto a nuestros socios y aliados a la seguridad internacional en el cumplimiento de los compromisos asumidos".

El Tribunal Constitucional ha tenido ocasión de pronunciarse sobre el concepto de seguridad nacional desde la perspectiva de la distribución de competencias entre el Estado y las Comunidades Autónomas: "la seguridad nacional no es una competencia nueva, sino que se integra en las competencias estatales de defensa y seguridad pública" (STC 184/2016, de 3 de noviembre de 2016, sobre diversos preceptos de la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional).

3.2. Delimitación de competencias en materia de ciberseguridad: la doctrina de la STC 142/2018, de 20 de diciembre

A partir de estas definiciones podemos identificar el concepto constitucional de seguridad del ciberespacio o ciberseguridad en la propia doctrina del Tribunal Constitucional, estrechamente ligado al concepto de seguridad nacional, como destacó el ATC 29/2018, de 20 de marzo, en su Fundamento Jurídico 5, que alude al artículo 10 de la Ley de Seguridad Nacional, conforme al cual la ciberseguridad es uno de los "ámbitos de especial interés de la seguridad nacional... que requieren una atención específica, por resultar básicos para preservar los derechos y libertades, así como el bienestar de los ciudadanos, y para garantizar el suministro de los servicios y recursos esenciales".

Asimismo, el Tribunal Constitucional ha relacionado las políticas públicas en materia de ciberseguridad con las competencias relativas al régimen general de las telecomunicaciones. A ambas cuestiones se refiere la STC 142/2018, de 20 de diciembre, que resolvió el recurso de inconstitucionalidad interpuesto por el presidente del Gobierno contra la Ley 15/2017, de 25 de julio, de la Agencia de Ciberseguridad de Cataluña.

Este relevante pronunciamiento considera el concepto de ciberseguridad como "sinónimo de la seguridad en la red" y lo define como "una actividad que se integra en la seguridad pública, así como en las telecomunicaciones" y también como "un conjunto de mecanismos dirigidos a la protección de las infraestructuras informáticas y de la información digital que albergan". El Tribunal Constitucional afirma que "la evolución de las tecnologías de la información y de la comunicación ha hecho que las redes y sistemas de información desem-

peñen actualmente un papel crucial en nuestra sociedad, siendo su fiabilidad y seguridad aspectos esenciales para el desarrollo de las actividades económicas y sociales".

A partir de esta premisa, la Sentencia revisa los preceptos impugnados de la Ley del Parlamento de Cataluña 15/2017, de 25 de julio, de la Agencia de Ciberseguridad de Cataluña, para concretar el alcance de las competencias de las Comunidades Autónomas en materia de Ciberseguridad.

El fundamento jurídico cuarto repasa la normativa aprobada por el Estado en materia de ciberseguridad y concluye de la misma que "afecta a cuestiones relacionadas con la seguridad pública y la defensa, las infraestructuras, redes y sistemas y el régimen general de telecomunicaciones". La seguridad del ciberespacio, en consecuencia, no puede reconducirse a un único título de competencias materiales debido al carácter "transversal e interconectado" de las tecnologías de la información y las comunicaciones. El juicio de constitucionalidad sobre la Ley catalana 15/2017 se basa, por tanto, en la el examen de la regulación de la Agencia Catalana de Ciberseguridad a la luz de la doctrina sobre tales títulos, lo que se reduce sustancialmente a la contraposición entre la competencia exclusiva del Estado en materia de seguridad pública y telecomunicaciones y la competencia de la Generalitat de Cataluña en materia de organización de su Administración, así como en la competencia ejecutiva en materia de comunicaciones electrónicas y en la competencia exclusiva en materia de comercio, todo ello conforme a los artículos 150, 140.7 y 121.1 a) del Estatuto de Autonomía de Cataluña.

En primer lugar, en lo relativo al alcance de la competencia exclusiva del Estado en materia de seguridad pública (artículo 149.1.29ª CE) la Sentencia califica como "doctrina consolidada" la plasmada en la STC 148/2000, de 1 de junio, en virtud de la cual la competencia exclusiva del Estado solo se encuentra limitada por las competencias que las Comunidades Autónomas hayan asumido respecto a la creación de su propia policía, en los términos que contemplan las normas del bloque de la constitucionalidad y, en particular, el Estatuto de Autonomía y la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad.

La Sentencia enfatiza que las competencias derivadas de la creación de cuerpos policiales autonómicos se ejercen "de acuerdo con lo dispuesto en la legislación estatal" o "en el marco de la legislación estatal", lo que ciertamente es el tenor literal de los apartados 1 y 3 del artículo 164 del Estatuto de Autonomía de Cataluña, si bien no es tan claro ese carácter subordinado en el apartado 4 de dicho precepto, según el cual "la Generalitat participa, mediante una Junta de Seguridad de composición paritaria entre la Generalitat y el Estado y presidida por el Presidente de la Generalitat, en la coordinación de las políticas de seguridad y de la actividad de los cuerpos policiales del Estado y de Cataluña, así como en el intercambio de información en el ámbito internacional y en las relaciones de colaboración y auxilio con las autoridades policiales de otros países". No parece muy lógico que el Estado sea titular de una competencia exclusiva en materia de seguridad pública con la única limitación que implica la existencia de un cuerpo policial autonómico que actúa en el marco de la legislación estatal y, en cambio, el órgano de coordinación de las políticas de seguridad sea una Junta de Seguridad presidida por el presidente de la Generalitat, lo que induce a pensar que la subordinación es más bien la inversa a la que predica el Estatuto de Autonomía.

En todo caso, aclara la Sentencia que no basta la relación de una función con la materia seguridad pública, sino que es precisa una delimitación en sentido negativo, como es que no exista "vinculación específica con la competencia derivada de la creación de la policía

autonómica, cuyo ámbito competencial no comporta sólo una referencia orgánica, sino también funcional".

En segundo lugar, las competencias del Estado en materia de ciberseguridad se vinculan con la competencia exclusiva estatal en materia de telecomunicaciones y de régimen general de comunicaciones, prevista en el artículo 149.1.21 CE. La Sentencia aclara que la competencia ejecutiva de la Generalitat en materia de comunicaciones electrónicas (artículo 140.7 del Estatuto de Autonomía de Cataluña) no puede perturbar ni menoscabar la competencia exclusiva del Estado para "ordenar normativamente y asegurar la efectividad de las comunicaciones, ni tampoco la dimensión técnica vinculada al uso del dominio público radioeléctrico que está en manos del Estado, que es su titular".

Como tercera idea, la Sentencia analiza la competencia esgrimida por el representante procesal de la Generalitat para sustentar la constitucionalidad de la Ley 15/2017, que es la potestad de autoorganización de la Comunidad Autónoma, inherente al concepto mismo de autonomía, como destacó la STC 111/2016, de 9 de junio. El Tribunal Constitucional es muy claro a este respecto, pues delimita el objeto de la litis en torno a las funciones atribuidas por la Ley 15/2017 a la Agencia de Ciberseguridad de Cataluña y no a la existencia misma de la Agencia, lo que implica un implícito y necesario reconocimiento a la potestad de las Comunidades Autónomas para crear, en el ámbito de sus competencias, órganos encargados de la protección de la seguridad del ciberespacio. De este modo, adquiere pleno sentido la previsión contenida en la Estrategia de Ciberseguridad Nacional (2019), que insta a potenciar la creación de infraestructuras de ciberseguridad en las Comunidades Autónomas, Ciudades Autónomas y Entidades Locales, así como en sus organismos vinculados y dependientes. También se entiende así el reconocimiento explícito a la creación por las Comunidades Autónomas de sus propias estructuras de ciberseguridad, que la Comisión Mixta de Seguridad Nacional introdujo en el *Informe de la Ponencia para el estudio de diversas cuestiones relativas a la ciberseguridad en España*. Si la doctrina constitucional se hubiese sustentado en consideraciones orgánicas y no funcionales, tales apelaciones a las estructuras autonómicas de ciberseguridad resultarían incompatibles con la Constitución.

A partir de estas consideraciones, la Sentencia declara la inconstitucionalidad del artículo 2.1 de la Ley 15/2017 por la amplitud con que define el objeto de la Agencia de Ciberseguridad de Cataluña, a la que encomienda "garantizar la ciberseguridad en el territorio de Cataluña, entendida como la seguridad de las redes de comunicaciones electrónicas y de los sistemas de información". Afirma el Tribunal Constitucional que es contraria a la Constitución una "garantía general y omnicomprensiva de la ciberseguridad", cuyo tenor literal parece excluir cualquier otra intervención pública para proteger el ciberespacio.

Por la misma razón, se declara la inconstitucionalidad de un inciso del artículo 2.3, según el cual en la ejecución de los objetivos fijados en el apartado 2, la Agencia "puede ejercer sus funciones con relación a las personas físicas y jurídicas situadas en Cataluña". Nuevamente la amplitud en la definición de las funciones de la Agencia conduce a la declaración de inconstitucionalidad.

Asimismo, se declara la inconstitucionalidad del inciso "planificar, gestionar, coordinar y supervisar la ciberseguridad en Cataluña, estableciendo la capacidad preventiva y reactiva necesaria para paliar los efectos de los incidentes de ciberseguridad que afecten al territorio de Cataluña, así como las pruebas que puedan organizarse en materia de ciberseguridad y continuidad" (artículo 2.4.b) de la Ley 15/2017) por cuanto su redacción no se circunscribe

a la Administración de la Generalitat y su sector público, sino que por su amplitud invade las competencias exclusivas del Estado en materia de seguridad pública.

Finalmente, se impone un criterio de interpretación conforme a la Constitución del apartado 2 del artículo 2 de la Ley 15/2017, que ha de ser entendido "en el sentido de que el objetivo que persigue la Agencia se relaciona con la necesidad de proteger las redes y sistemas de información de la Administración de la Generalitat y de su sector público y los de los particulares y otras administraciones públicas que se relacionan por medios electrónicos con dicha administración, no es contrario al orden constitucional de distribución de competencias".

El resto de los preceptos impugnados por el Abogado del Estado resultan conformes a la Constitución pues todos ellos delimitan correctamente el ámbito de actuación que corresponde a la Generalitat de Cataluña en relación con la protección del ciberespacio y que se circunscribe a la ciberseguridad del Gobierno, de la Administración autonómica y de su sector público dependiente, así como de quienes se relacionen por medios electrónicos con la Generalitat. Lo mismo sucede con el mandato de colaboración con el resto de autoridades con competencias en materia de ciberseguridad, que no es sino "concreción del principio general de cooperación que informa el Estado autonómico" y con el deber de colaborar con Jueces y Tribunales y con el Ministerio Fiscal.

En definitiva, el Tribunal Constitucional en la STC 142/2018 confirma que la protección del ciberespacio es de tal complejidad que no es posible la delimitación excluyente de competencias en sentido absoluto, sino, como en tantas ocasiones, una convivencia de funciones y políticas públicas de diverso alcance territorial, en sintonía con la propia arquitectura constitucional del Estado autonómico.

El Estado no excluye el ejercicio de competencias autonómicas en materia de ciberseguridad, sino que promueve activamente la implicación de las Comunidades Autónomas en la protección del ciberespacio y la creación de sus propias estructuras para el desarrollo de estas funciones, circunscritas, eso sí, a la protección de la seguridad de las infraestructuras y redes de la administración autonómica y de quienes se relacionan con ella a través de tecnologías digitales. Así se deduce del marco diseñado por la Estrategia de Ciberseguridad Nacional (2019).

No es compatible, sin embargo, con este diseño constitucional una regulación de las competencias sobre la seguridad del ciberespacio en términos tan amplios que permita deducir de ella precisamente lo contrario, esto es, la exclusión de las competencias del Estado en materia de ciberseguridad respecto de todo lo que suceda en el "ciberespacio catalán", un concepto, por lo demás, de imposible concreción.

4. Conclusiones

El ciberespacio se ha consolidado como una dimensión en la que se desenvuelve de manera cotidiana la actividad de los ciudadanos y de los poderes públicos, con la dificultad que implica someter a regulación un entorno virtual cuya principal característica es que no se pliega a nuestras categorías convencionales de definición de la jurisdicción en el espacio. Esta dificultad alcanza también a la intervención de los poderes públicos para proteger la seguridad del ciberespacio, así como para prevenir y perseguir aquellas acciones ilícitas que

se desarrollan en el mismo y que, en la actualidad, pueden resultar tan nocivas o más que las conductas ilícitas en el mundo físico.

En los Estados descentralizados, las políticas públicas en el ámbito de la ciberseguridad deben respetar el marco constitucional de distribución de competencias, no como una imposición caprichosa sino como un diseño coherente con los principios y valores constitucionales que subyacen en cada modelo de organización territorial. Así, en Estados Unidos se ha abierto un enriquecedor debate sobre el alcance de las competencias del Gobierno Federal y el Congreso en materia de ciberseguridad y, por consiguiente, sobre los poderes de los estados y los gobiernos locales en este ámbito, lo que resulta especialmente relevante si tenemos en cuenta el impactante número de incidentes cibernéticos que se producen contra infraestructuras, organismos o servicios públicos estatales o locales.

En España el marco normativo de la ciberseguridad se ha desarrollado en un espacio corto de tiempo, acomodándose a una estructura racional y coherente, como es la que diseña la Estrategia de Seguridad Nacional (2017) y la Estrategia de Ciberseguridad Nacional (2019), en sintonía con las normas aprobadas por la Unión Europea para garantizar unos estándares homogéneos de ciberseguridad entre los Estados miembros.

En este contexto, las competencias en materia de ciberseguridad se reconducen a dos títulos materiales exclusivos del Estado, como son la seguridad pública (artículo 149.1.29ª CE) y las telecomunicaciones y régimen general de las comunicaciones (artículo 149.1.21ª CE). No obstante, tales competencias del Estado no pueden interpretarse en un sentido excluyente sino necesariamente compatible con la existencia de estructuras autonómicas en materia de ciberseguridad, incardinadas en el ámbito de protección de las infraestructuras y redes utilizadas por los poderes públicos autonómicos y por quienes se relacionan con ellos a través de medios digitales y sin perjuicio de las competencias correspondientes a los cuerpos de seguridad autonómicos, allí donde existan. Esta es, en términos sintéticos, la doctrina expresada por el Tribunal Constitucional en la STC 142/2018, de 20 de diciembre, que declaró la inconstitucionalidad de aquellos preceptos de la Ley 15/2017, de 25 de julio, de la Agencia de Seguridad de Cataluña. El juicio de inconstitucionalidad no se basa en la existencia de un órgano autonómico con competencias en materia de ciberseguridad, pues tales estructuras son promovidas activamente en la Estrategia de Ciberseguridad Nacional.

Por el contrario, la decisión del Tribunal se basa en la definición absolutamente amplia de las competencias de la citada Agencia de Ciberseguridad de Cataluña, en términos imposibles de conciliar, ni siquiera por vía interpretativa, con la existencia misma de funciones del Estado en la materia, lo cual, además de resultar inconstitucional pone de manifiesto que se optó por la solución menos razonable a los desafíos de esa cuarta dimensión a la que llamamos ciberespacio.

Si algo caracteriza el nuevo escenario virtual en el que se desenvuelve buena parte de nuestra actividad y en el que pasamos cada día más tiempo es que se resiste a doblegarse a las viejas y herméticas categorías jurídicas basadas en la presencia en el territorio. En el ciberespacio, como en el mar, puede decirse que "sobre la ola, todo es ola" (Schmitt, 2002).

Bibliografía

Alonso Lecuit, J. (2018, noviembre 13). Evolución de la agenda de ciberseguridad de la Unión Europea. *Análisis del Real Instituto Elcano 121/2018*.

Recuperado de: http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/ari121-2018-lecuit-evolucion-agenda-ciberseguridad-union-europea.

Caro Bejarano, M. J. (2010). Alcance y ámbito de la seguridad nacional en el ciberespacio. *Cuadernos de Estrategia*, *149*, 47-82. Ministerio de Defensa.

Finklea, K. (2013, enero 17). *The Interplay of Borders, Turf, Cyberspace, and Jurisdiction: Issues Confronting U.S. Law Enforcement, en Congressional Research Service*. Recuperado de: https://www.researchgate.net/publication/289731810_The_interplay_of_borders_turf_cyberspace_and_jurisdiction_Issues_confronting_US_law_enforcement.

Freixas, T., & Remotti, J. C. (1995). La configuración constitucional de la seguridad ciudadana. *Revista de Estudios Políticos*, *87*, 141-162.

Galán, C. (2018, diciembre 13). Amenazas híbridas: nuevas herramientas para viejas aspiraciones. *Análisis del Real Instituto Elcano 20/2018*. Recuperado de: http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/dt20-2018-galan-amenazas-hibridas-nuevas-herramientas-para-viejas-aspiraciones.

Glenon, M. (2012). State-level Cybersecurity. *Policy Review*, *171*, febrero-marzo 2012. Recuperado de: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1997565.

Morag, N. (2011). *Comparative Homeland Security: Global Lessons*. New Jersey: Editorial Wiley.

Moret Millás, V. (2017, abril). Conflictos armados, ciberespacio y el derecho internacional: el derecho de la guerra en ciberoperaciones militares. *Ejército. Revista del Ejército de Tierra Español*, *912*, 28-33.

Moret Millás, V. (2018, octubre 11). Un nuevo escenario jurídico para la ciberseguridad en España: el Real Decreto-Ley 12/2018, de Seguridad de las redes y sistemas de información. *Diario La Ley, 9277, Sección Tribuna*. Editorial Wolters Kluwer. Recuperado de: https://diariolaley.laleynext.es/Content/Documento.aspx?params=H4sIAAAAAAAAEAFXMuwrDMAxG4bfxrLpQkkFT_Ajeixr9BlMjFecCefumS6BnPnxVlVOmszjcI1HY0ZfqxpFuA43xEcwVOU28maJUg_6WWo7kcz4-4CJtQcDL_f0nPS9hbpCeZMUkDabSOfcNX2kIqP56AAAAWKE.

Moret Millás, V. (2020, enero). El Real Decreto-Ley 14/2019: una nueva regulación del ciberespacio en clave nacional. *Análisis del Real Instituto Elcano 4/2020*. Real Instituto Elcano. Recuperado de: http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/ari4-2020-moret-real-decreto-ley-14-2019-nueva-regulacion-ciberespacio-en-clave-nacional.

Nivola, P. (2002, mayo 13). Reflections on Homeland Security and American Federalism. *Brookings*. Recuperado de: https://www.brookings.edu/articles/reflections-on-homeland-security-and-american-federalism/.

Pérez López, I. (2020, marzo 6). Cyber-risk and cyber-insurance (II): silent cyber, an ongoing revolution?. *Insuralex*. Recuperado de: https://insuralex.com/cyber-insurance-lawyers-spain-risk/.

Schallbruch, M., & Skierka, I. M. (2018, agosto). Cybersecurity in Germany. *Digital Society Institute, ESMT Berlín*. Recuperado de: https://www.researchgate.net/publication/326514651_The_German_View_on_Cybersecurity.

Schmitt, C. (2002). *El nomos de la tierra en el Derecho de Gentes del "Ius publicum europaeum"*. Granada: Editorial Comares.

Waxman, S. (2002). Federalism, Law Enforcement, and the Supremacy Clause: The Strange Case of Ruby Ridge. *Georgetown Law Faculty Publications and Other Works*, *289*. Recuperado de: https://scholarship.law.georgetown.edu/facpub/289.