MERCEDES FUERTES

METAMORFOSIS DEL ESTADO

Maremoto digital y ciberseguridad

Marcial Pons

MADRID | BARCELONA | BUENOS AIRES | SÃO PAULO

2022

ÍNDICE

PRIMER ACTO

Las nuevas tecnologías están impulsando saltos notables en el desarrollo de la Humanidad. Cambios en las relaciones personales, multitud de innovaciones en las actividades comerciales e industriales... Al mismo tiempo nos muestran una mayor vulnerabilidad social. Las injerencias en los sistemas informáticos son constantes. Amenazas y riesgos inesperados aparecen en las comunicaciones electrónicas con trepidante celeridad. Los números de ataques y daños que recogen diferentes informes públicos son muy elevados y no dejan de aumentar. Hemos de ocuparnos, además de preocuparnos, de tan extrema fragilidad[1].

La peculiar configuración de la Red, con sus diversos nodos, servidores, asignaciones de rutas y destinos que facilitan la transmisión ágil y versátil de la comunicación, no implica que sea en toda su extensión intocable, que su actividad sea siempre permanente y constante, que sus efectos resulten en todo caso predecibles, cercanos a la perfección. Es una obra humana y, como tal, imperfecta. Riesgos, imprevistos,

---

[1] El Centro Criptológico Nacional facilita relevante información, por ejemplo, puede verse su informe *Ciberamenazas y tendencias. Septiembre 2020,* disponible en *https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/5377-ccn-cert-ia-13-20-ciberamenazas-y-tendencias-edicion-2020/file.html*. También está disponible el *Informe anual de seguridad nacional 2020* con datos significativos sobre las tendencias y hábitos en Internet por la población española, las nuevas amenazas, así como otros desafíos y actuaciones. Igualmente, la Agencia Europea, ENISA, publica informes anuales sobre el panorama de amenazas. Los últimos «ENISA Threat Landscape 2020» pueden consultarse en su página web *https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends*.

accidentes, se suceden y pueden originar una cierta parálisis del tráfico de Internet. Y, con ello, la interrupción de numerosas actividades y servicios cada vez más dependientes de una adecuada conexión. Recuerdo ahora solo un ejemplo, entre los miles que hemos vivido: en junio de 2021 se produjo una especie de ceguera parcial de Internet. Durante un tiempo significativo —y ante un ordenador los minutos evocan la eternidad y el apagón duró un par de horas— resultó imposible acceder a muchas páginas oficiales de distintos Gobiernos, de grandes empresas multinacionales, de medios de comunicación, porque se había «caído», se había «apagado» la red de servidores de la empresa a la que estaban conectados (Fastly). La causa que luego se apuntó fue la simple actualización del sistema que había aceptado un usuario. Esto es, el mero acto instantáneo de pulsar un interruptor, en lugar de mejorar una función, apagó esos servidores y, con ello, no solo el pequeño espacio donde estaban alojados, centenares de empresas y millones de usuarios se vieron afectados quedando a oscuras.

Sin embargo, lo que más alarma son los ataques voluntarios. Afectan a personas, a pequeñas y grandes empresas e, incluso, a las instituciones y organismos del Estado. La fortaleza casi inexpugnable que exhibía en otras épocas el poder resulta ahora burlada. Los altos muros de esa alcazaba o fortaleza, las sólidas vigas de las que presumía la morada del Leviatán parecen de cartón piedra ante la facilidad con la que se traspasan por unos espectros, esas corrientes eléctricas que impulsan una numeración que se convierte en datos, protocolos y programas que mueven tanta información.

De manera sobria y con cierta sordina aparecen noticias sobre los secuestros de sistemas informáticos que, ora se sospecha que proceden de servicios especializados de algunos países como Rusia, Corea del Norte o China, ora están protagonizados por quienes dan vida a una especie renovada de salteadores de caminos. Un ejemplo: en enero de 2022 un investigador norteamericano perturbó durante varios días el tráfico de Internet en Corea del Norte y bloqueó páginas webs de ese Gobierno. Una persona en solitario cuya motivación fue desprestigiar a un gobierno totalitario y también reaccionar a un ataque que habían sufrido varios informáticos norteamericanos sin que los servicios de seguridad estadounidenses hubieran abierto investigación alguna ni reaccionado.

Nadie está exento de ese riesgo: parlamentos, departamentos ministeriales, grandes ayuntamientos, salas de tribunales, grandes y pe-

queñas empresas, además de los ciudadanos... Con aparente facilidad y generando un absoluto desconcierto tales bandoleros se deslizan a través de lo que podría ser una especie de «butrón» informático y, tras pasearse por el circuito, consiguen información, manipulan datos y archivos, interceptan comunicaciones..., incluso logran paralizarlo, impidiendo que sus legítimos titulares accedan a sus datos, expedientes, archivos, esto es, secuestran el sistema y exigen el pago de un rescate en monedas virtuales. El desconcierto es mayúsculo.

Los ataques no dejan de multiplicarse. Antes de la pandemia ya conocimos el preocupante chantaje a hospitales para que pudieran volver a acceder a la historia clínica de sus pacientes. En medio de esta inquietante situación leemos cómo se atacan sanatorios con trágicas consecuencias y cómo se perturba el trabajo de investigadores para diseñar vacunas al espiarse la actividad de algunos laboratorios. Lo mismo que se multiplican los asaltos contra entidades financieras y aseguradoras. Y podría seguir recordando el robo a grandes o pequeñas empresas de información comercial o el espionaje industrial, ya que distintos tipos de botines interesan a los delincuentes y al mercado de información que generan[2].

Dejando a un lado en este momento las ofensivas que derivan de preocupantes tensiones geopolíticas (p. ej., en Ucrania), subrayo cómo la actuación de estos nuevos guerrilleros solitarios nos recuerda la teoría del partisano de Carl Schmitt: todo nuevo espacio ocasiona guerras en las que aparece ese combatiente aislado que, con una lucha irregular, desprecia el nuevo orden que se intenta instaurar[3].

Un abanico abierto de motivaciones con gran cromatismo impulsa esos ataques individuales. Por ejemplo, el afán de enriquecimiento,

---

[2] En marzo de 2020 Europol difundió un documento alertando del incremento de riesgos durante la pandemia, por ejemplo, el ataque al Hospital Universitario de Brno (Chequia) que obligó a redirigir a los pacientes y a posponer operaciones (*Europol: Pandemic profiteering. How criminals exploit the COVID-19 crisis*). En septiembre, un ataque informático a un hospital de Düsseldorf originó, entre otras consecuencias nocivas para muchos enfermos, el retraso en la atención a una paciente que falleció. Las autoridades alemanas tienen todavía abierta la investigación. Sobre la escalada del espionaje industrial y el robo de secretos comerciales, la Comisión Europea publicó en diciembre de 2018 un estudio accesible a través de Internet: *https://op.europa.eu/en/publication-detail/-/publication/b3b5fcfb-4541-11e9-a8ed-01aa75ed71a1/language-en/format-PDF/source-90181868*.

[3] C. Schmitt, *Teoría del partisano. Acotación al concepto de lo político*, Madrid, Trotta, 2013, p. 79.

similar al que movía los abordajes de los piratas. Tal es el caso de los secuestros del sistema informático de empresas o ayuntamientos que solo se levantan a cambio del correspondiente pago. También advertimos cómo la ayuda y la financiación de «terceros poderosos» facilita esa actividad similar a la de los espías, saboteadores... lo que resaltó otro teórico de los partisanos, Rofl Schroers[4]. Igualmente hay que contar con la vanidad pretenciosa de quienes quieren conseguir un destacado logro para llamar la atención. En fin, también hay quien se presenta como heredero de aquellos partisanos que, en otros siglos, de manera aislada o espontánea combatían fuera de las reglas de la guerra con el fin de poner de manifiesto la debilidad del sistema político, social o económico. Porque así como el objetivo del partisano era el soldado uniformado, hoy es lo que representa la estructura social, ya sean las instituciones públicas, ya determinadas corporaciones económicas.

No obstante, les separa una nota muy relevante. Frente a los alardes románticos con los que se ha dibujado a esos antiguos guerrilleros que se levantaron, por ejemplo, en España contra la ocupación francesa de Napoleón, hoy día, los «bandidos informáticos» carecen de ese halo que adorna la defensa de otros ciudadanos indefensos o más pobres. Simplemente paralizan la actividad normal, generan desolación al robar datos o ingentes sumas de dinero manipulando los apuntes contables en las entidades financieras. El poder de perturbación, de grave alteración en el funcionamiento de servicios básicos, de nuestras relaciones económicas y sociales, es mayúsculo. Introducen un notable desconcierto mediante perfectas falsificaciones. No aludo a la propagación de bulos y embustes que confunden la realidad. Me refiero a la alteración de las páginas oficiales del *BOE*, a la suplantación de las declaraciones de responsables políticos en la Asamblea de las Naciones Unidas o de otros cargos directivos, como consejeros ejecutivos de bancos, con el fin, como hemos conocido, de simular una orden para transferir millones a un banco alojado en un paraíso fiscal. Vemos nítidamente su imagen, reconocemos su genuino timbre de voz y, sin embargo... sin embargo, sus palabras han sido adulteradas.

---

[4] La obra de Carl Schmitt entra en debate en muchas ocasiones con las tesis sostenidas por R. Schroers en su libro *Der Partisan; ein Beitrag zur politischen Anthropologie,* Köln, Kiepenheuer & Witsch, 1961, pues para Carl Schmitt los partisanos se caracterizan por la irregularidad de su lucha, su movilidad, más que por incorporarse a una resistencia general que defendía la tierra, aspecto central en la tesis de Schroers. Ambos destacan el compromiso o activismo político.

Bien se advierte en estos nuevos partisanos la condición de «enemigos absolutos». Enemigos de las bases de nuestra civilización.

Nadie pone en duda que los avances tecnológicos han traído mejoras en el sistema sanitario, educativo, en los servicios... han impulsado prosperidad pero, al mismo tiempo, no somos espíritus ingenuos que ignoremos que tales progresos consiguen erradicar o minorar los riesgos de malhechores y criminales. Resulta imprescindible que el poder proteja a la sociedad de tales partisanos, de los miles de ataques informáticos que perpetran[5].

Estamos ante una «guerra sin límites» que demanda un nuevo *nomos*[6].

La vulnerabilidad de la Red, la debilidad de tantos servicios que dependen del buen funcionamiento de los sistemas informáticos, los ataques conscientes y tantas otras contingencias muestran la necesidad de acopiar instrumentos jurídicos para garantizar uno de los primeros fines del Estado: el orden público. Hobbes, ante «los desórdenes de la época» se inspiró en el libro de Job para sacar del mar al omnipotente monstruo Leviatán.

Nada más lejos de mi pensamiento que aludir a un poder soberano ilimitado. Si he invocado al Leviatán, es por la deuda inmensa hacia la estructura artificial del cuerpo del Estado que Hobbes justificó y que permitió avanzar en el Derecho público. Ante los «desórdenes» de nuestra época, Hobbes hoy trataría de diseñar ese artilugio en lugar de con cobre con otros materiales como el silicio, el grafeno y otros elementos singulares[7]. Dejémosle a un lado entretenido, porque

---

[5] La enorme repercusión que han tenido algunos ataques está incrementando la conciencia de atender a unas mínimas medidas de seguridad en este entorno digital que, como nueva atmósfera, nos engloba. Así, aparece reflejado, entre otros documentos, en los estudios sobre la ciberseguridad y confianza del ciudadano en la red que publica el Observatorio Nacional de las Telecomunicaciones y la Sociedad de la Información (se encuentran disponibles en la página web de este organismo: *https://www.ontsi.red.es/es*).

[6] En este sentido, resultan ilustrativas las consideraciones que hace tiempo apuntó R. Campione en su libro *El nomos de la guerra. Genealogía de la «guerra justa»*, Valencia, Tirant lo Blanch, 2009.

[7] Expone con gran intuición consideraciones sobre los cambios jurídicos por la automatización R. Campione, en su libro *La plausibilidad del Derecho en la era de la inteligencia artificial: filosofía carbónica y filosofía silícica del Derecho*, Madrid, Dykinson, 2020.

mi discurso quiere ser fruto de esta época. Interesa que, ante la tempestad digital, el Derecho acopie técnicas que garanticen la confianza, que este mundo tan dependientemente interconectado mantenga la seguridad y el bienestar de una sociedad democrática.

Explicaré en las siguientes páginas al lector que me acompañe los instrumentos que se empiezan a consolidar. He diseñado un itinerario temporal. En lugar de sistematizar ya las medidas existentes, he considerado que el Tiempo es un buen maestro cuyo ritmo nos permite tomar mejor conciencia de cada paso en las concretas circunstancias de cada momento.

Y empiezo el recorrido recordando uno de los primeros constipados, si se me permite la expresión, con un virus que generó cierta convulsión mundial.

I. LA FRAGMENTADA Y ESTRECHA PERSPECTIVA INICIAL

La sucesión de tecnologías ha ido saltando a la escena de la actualidad de manera trepidante. Con originalidad se presentan nuevos aparatos, con imaginación se mejoran, con celeridad se innovan. Del mismo modo que la solución de problemas e interrupciones, la corrección de defectos y errores ha impulsado su desarrollo. En este sentido, resulta obligado recordar como hito reseñable, entre los acontecimientos singulares que convulsionaron a los técnicos de comunicaciones y avivaron la preocupación por la seguridad, la aparición del «gusano de Morris» en 1988. Un programa informático que aprovechó la vulnerabilidad de las conexiones, que se replicaba de manera automática a los ordenadores conectados y que puso de manifiesto, entre otros riesgos, la debilidad de las contraseñas, la celeridad de la expansión de los virus informáticos en un par de segundos[8].

Este acontecimiento incrementó la toma de conciencia por la seguridad. No solo por la industria productora, también lógicamente por los propios científicos y técnicos, así como por los usuarios más interesa-

[8] Sobre la estructura del «gusano de Morris» y los efectos que generó, así como sobre el proceso contra su autor, existe numerosa bibliografía. Sirva la mera referencia al resumen de A. Jajoo, *A study on the Morris worm,* disponible en la base de datos *researchgate.net.*

dos en los avances. Durante la década de los años noventa se extendieron catálogos de buenas prácticas dirigidas a asegurar la integridad de las comunicaciones, se concretaron pautas de gestión y las asociaciones de normalización comenzaron a publicar sus estándares específicos[9].

En el Derecho de la Unión Europea las previsiones sobre seguridad se alojaban en cada sector concreto: medidas especiales para las instalaciones o industrias, otras apropiadas a los servicios bancarios, otras peculiares para el comercio electrónico, otras especiales para la firma digital o certificados de confianza... La regulación estaba fragmentada y las invocaciones a la seguridad en tales disposiciones eran genéricas pues se trasladaba a las autoridades nacionales su precisión. La normativa sobre telecomunicaciones solo establecía con carácter general el objetivo de conseguir la «seguridad e integridad» de la red y de la comunicación, lo que se materializaba con los estándares y las buenas prácticas de actuación asumidas por las propias empresas[10].

Es con el cambio de milenio cuando desde el Consejo Europeo se impulsa la elaboración de una propuesta integral que tiene como fruto el documento de la Comisión «Seguridad de las redes y de la información: propuesta para un enfoque político europeo». Recogía un amplio espectro de medidas como la protección a las Administraciones públicas, apoyo tecnológico, incorporación de certificaciones técnicas, conexión de centro de alertas y emergencias, fomento de buenas prácticas, mejora de la educación digital y realización de campañas de concienciación[11].

Además, ante el riesgo de que proliferaran técnicas de seguridad heterogéneas, así como especificaciones diversas en las previsiones de seguridad —cosa que entorpecería la consolidación de un mercado interior de las telecomunicaciones— se impulsó la creación de un centro especializado. Nace así la Agencia Europea de Seguridad de las Redes

---

[9] Los técnicos reconocen la importante labor realizada por el Gobierno británico con las denominadas guías BS 7799; así como los trabajos de la Organización de Normalización Internacional, con la serie ISO 27001 y la Comisión Electrónica Internacional.

[10] En este sentido puede leerse en la Directiva 2002/21, de 7 de marzo, que establece el marco común de las redes y servicios de comunicaciones electrónicas y que tiene su origen en la Comunicación de la Comisión (2000), 393, de 23 de agosto.

[11] Fue el Consejo Europeo celebrado en Estocolmo en marzo de 2001 el que incitó la preparación del proyecto que publicó la Comisión: «Seguridad de las redes y de la información: propuesta para un enfoque político europeo» [COM (2001) 298, de 6 de junio].

y la Información, que se conoce por su acrónimo en inglés: ENISA (*European Network and Information Security Agency*). Se alojó en Heraclión, la capital de Creta, teniendo también una sede en Atenas. Su misión se concretó en analizar amenazas e incidentes a través del seguimiento de las normas técnicas existentes y de la información que recabara; en asesorar a las instituciones europeas, especialmente a la Comisión, con criterio profesional y técnico; en fomentar la cooperación entre instituciones, Estados, empresas, investigadores, en fin, en contribuir a incrementar el conocimiento sobre la seguridad de las redes con la descripción de buenas prácticas u otras actividades [12].

La configuración inicial fue muy modesta. Un dato incontestable: ha sido la única de todas las agencias europeas que se creó con un mandato temporal, inicialmente de cinco años, sometiéndose a la incertidumbre de su desaparición. Periódicamente se discutía su actuación para revalidar y prorrogar su vigencia [13].

A pesar de tan cauta posición como centro de asesoramiento su creación fue discutida por Reino Unido. El Tribunal de Justicia de la Unión Europea desestimó el recurso en una interesante sentencia en la que analizó los contornos de la competencia europea con el fin de armonizar las legislaciones de los Estados miembros. Porque tal armonización no está constreñida de manera exclusiva con instrumentos que atraigan la actuación de los Estados miembros. La armonización atribuye a las instituciones europeas un suficiente margen de apreciación para desplegar otras técnicas jurídicas y, en ellas, puede resultar adecuada la creación de un organismo europeo. En este caso, además, la justificación era sólida. La ciberseguridad constituye una preocupación seria ante las amenazas mudables, ha de atenderse la rápida reparación de las averías, la pronta resolución de las interrupciones de servicios y, sobre todo, la prevención de las disparidades que puedan surgir ante la enorme complejidad técnica. Por ello, resultaba plausible la creación de un centro especializado que realizara estudios y análisis con proyección para toda Europa [14].

---

[12] Su primera regulación se contiene en el Reglamento Europeo 460/2004, de 10 de marzo.

[13] El Reglamento 1007/2008, de 24 de septiembre, prorrogó su vigencia durante ocho años; el Reglamento 580/2011, de 8 de junio, otro año y medio, y el Reglamento 526/2013, de 21 de mayo, previó su vigencia hasta junio de 2020.

[14] La Sentencia tiene fecha de 2 de mayo de 2006 (C-217/04, ECLI:EU:C:2006:279).

Han tenido que mostrarse inoperancias en la descoordinación ante ataques informáticos, las deficiencias en el mercado de productos, para que se haya modificado su estatuto jurídico, se haya suprimido su temporalidad y se hayan ampliado sus funciones. Entre otras, facilitar el establecimiento de un marco de certificación de ciberseguridad en todos los países europeos[15]. Un cambio muy significativo. Pero permítame el lector que aparte hacia un fondo lateral del escenario menos iluminado a ENISA. En ese fondo de escenario irá desenvolviendo con rigor sus funciones, redactando sustanciosos informes y guías prácticas, organizando ejercicios y simulaciones de ataques, así como otras actividades para investigadores, empresarios y representantes de los Estados miembros.

Desplazo a la agencia ahora porque, atraídos por el fuerte oleaje y el incremento de las mareas digitales, se aprobaron disposiciones que requieren de una especial atención.

II. PRESERVAR LO MÁS SAGRADO

Los atroces atentados terroristas (las torres gemelas de Nueva York o la estación de Atocha en Madrid) urgieron la necesidad de introducir medidas adecuadas que fortalecieran una mayor seguridad. La fragilidad de la sociedad era manifiesta.

Una desconcertante vulnerabilidad que encuentra paralelismos en otras muchas épocas históricas. Mencioné ya cómo Hobbes escribe su *Leviatán* motivado por los «desórdenes» de su época. Ahora apunto las similitudes con la Alta Edad Media porque en amplias zonas de Europa se sucedían los atropellos y actos vandálicos, de barbarie o devastación. En aquellos tiempos, la necesidad de contar con una mínima seguridad y tranquilidad, así como posiblemente el amparo de la influencia cristiana, consiguieron que se extendieran unas pautas rudimentarias de mandatos y compromisos evitando una violencia desparramada.

---

[15] La regulación vigente se contiene en el Reglamento Europeo 2019/881, de 19 de abril, relativo a ENISA y a la certificación de ciberseguridad. Téngase simplemente en cuenta que con antelación a esta regulación los empresarios debían someterse a las regulaciones nacionales, conseguir los correspondientes sellos de seguridad y abonar distintas tasas.

Conviene recordar lo que algunos historiadores alojan en los Sínodos de Charroux y Puy a finales del siglo x, a saber, la proclamación de ciertas prohibiciones: que no se saquearan las iglesias, que no se golpeara a los clérigos y a aquellos aldeanos cuando no portaban armas, que no se robaran los animales de los pastores... Mandatos y compromisos a los que se van adhiriendo nobles, vasallos, siervos y campesinos en homenajes y ceremonias religiosas.

Ha de subrayarse que ese cese de hostilidades se dirigió, en primer lugar, a proteger las iglesias, los monasterios y sus entornos, los cementerios, los *loca sacra.* Los beneficios de esa «tregua» se fueron extendiendo a quienes se acercaban a lugares de culto, a los peregrinos, a quienes portaban un *conductus*... Respirar esa mínima tranquilidad, una situación carente de violencia, hizo que se fueran ampliando tales «treguas» como ondas en un estanque. *Loca sacra* no eran ya solo los lugares religiosos, sino también aquellos otros abiertos donde empezaban a desenvolverse las relaciones comerciales y el intercambio de bienes: se declararan treguas durante la celebración de ferias y mercados. Y a partir de ahí ese concepto se fue expandiendo a otras estancias y lares.

Si hace mil años preocupaba garantizar la ausencia de violencia en las iglesias y mercados, hoy nos ocupa evitar los ataques, minorar los riesgos de tantas instalaciones esenciales necesarias para el desarrollo de nuestras creencias en una sociedad abierta, así como las relaciones de servicios que circulan por las redes de comunicación.

Y ese empeño ocupó a la Unión Europea y a sus Estados miembros. Había que analizar la debilidad de nuestros *loca sacra* y asegurarlos, de manera especial ante la creciente expansión de las redes tecnológicas. Por ello, el Consejo de Jefes de Estado y de Gobierno, de junio de 2004, encargó a la Comisión Europea la preparación de una estrategia que protegiera, entre otros elementos, las llamadas «infraestructuras críticas».

En aquellos años tal locución —«infraestructuras críticas»— era deudora de las primeras previsiones jurídicas que se habían aprobado en Estados Unidos. Hacía tiempo que, dentro de la lucha contra el terrorismo, se analizaban los riesgos de interdependencia de servicios esenciales con las nuevas tecnologías. Se apuntaba directamente a la necesidad de defender los sistemas digitales, además de las instalaciones físicas en su conjunto. Por ello, la luz de esa expresión enfocaba

únicamente a la red y al sistema de comunicación de los que dependía el correcto funcionamiento de servicios esenciales [16].

Nadie ponía en duda que la progresiva tecnificación de tantos servicios como el abastecimiento de agua o de energía, la distribución de alimentos o medicamentos, etc., incorporaba nuevos elementos y, con ello, nuevos riesgos a los que había que atender para evitar la interrupción de los suministros o el desabastecimiento. Siguiendo el sencillo símil del cuerpo humano, del mismo modo que cada órgano o tejido genera sus propias células de defensa, esto es, un sistema «inmunitario» ante agresiones externas, así hemos de preocuparnos de manera inexcusable de la seguridad de los sistemas informáticos y de las redes con el fin de impedir las nuevas modalidades de ataques.

1. Qué es crítico para Europa lo indican los Estados

Fruto de ese mandato del Consejo Europeo, la Comisión publicó a los pocos meses una Comunicación que incluía propuestas de mejora en la prevención, la preparación y la respuesta frente a atentados terroristas. Después un Libro Verde en el que se describió un programa de protección a partir del cual se fue concretando un plan de actuación, la configuración de grupos de expertos, diseño de medidas de intervención, una red de información para facilitar el inmediato conocimiento de una alerta que afectara a infraestructuras críticas y, además, se elaboró una directiva para identificar y proteger las infraestructuras críticas europeas [17].

---

[16] Una decisión del presidente de Estados Unidos de 21 de junio de 1995 dirigida a luchar contra el terrorismo creó un comité para analizar las infraestructuras críticas. Una nueva Decisión de 22 de mayo de 1998 (PDD 62) estableció previsiones específicas en un apartado sobre «*critical infrastructure protection*». El espectacular desarrollo tecnológico y, sobre todo, trágicos atentados terroristas, generaron la aprobación de otras disposiciones, entre las que resalta la Directiva de 2003, que regula la política nacional de protección, hoy recogidas en el marco de ciberseguridad nacional.

[17] La referencia de esa Comunicación de la Comisión sobre protección de las infraestructuras críticas en la lucha contra el terrorismo es COM (2004) 702, de 20 de octubre. La información sobre la Red de información de alertas de las infraestructuras críticas [CIWIN por su denominación en inglés, *vid.* COM (2004) 676, de 27 de octubre], puede consultarse en *https://ec.europa.eu/home-affairs/what-we-do/networks/critical_infrastructure_warning_information_network_en.* La Directiva es

Su aprobación culminó a finales de 2008, esto es, un año después del espectacular ciberataque que sufrió Estonia. Recordemos que se inutilizaron múltiples servicios y hubo de aislarse de manera absoluta ese país de Internet para reconstruir sus redes y ello, además, con la ayuda de la OTAN. Urgía establecer, por consiguiente, un marco común para evitar o, al menos, reaccionar ante riesgos transnacionales.

Sabemos que los Estados mantienen la responsabilidad de garantizar la seguridad en su territorio en el esquema de distribución de competencias establecido en el Tratado de Lisboa. Al «alto representante de la Unión para asuntos exteriores y política de seguridad» se le atribuyen solo competencias sobre aquellos aspectos que puedan alojarse en lo que se entiende por «seguridad común».

Ello supone, siguiendo esa lógica, que corresponde en primer término a cada Estado la protección de las infraestructuras críticas. Sin embargo, aquellas cuyo funcionamiento tengan relevancia europea han de contar con unas medidas complementarias de protección. De ahí la competencia de la Unión para configurar un instrumento que otorgue seguridad. Y, en este caso, tal instrumento es un trípode porque se asienta en tres pies, a saber: uno, pautas similares para identificar qué infraestructuras son críticas; dos, obligaciones específicas a las empresas afectadas, y tres, una organización que supervise el adecuado cumplimiento y facilite la asistencia necesaria.

En resumen, cada Estado es competente dentro de su territorio para reconocer aquellos elementos digitales que son cruciales teniendo en cuenta varios criterios: el posible número de afectados, el impacto económico y ambiental que un ataque genere, las consecuencias de carácter público como la perturbación en el desarrollo normal de la vida cotidiana, la inseguridad y fragilidad generada, así como la existencia de alternativas o la extensión de efectos según persista la agresión... Aspectos que atenderán a las directrices y horquillas de incidencias que proponga la Comisión Europea.

---

la núm. 2008/114, de 8 de diciembre, sobre identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección. De manera previa, la Comisión había publicado un Libro Verde sobre un programa europeo para la protección de las infraestructuras críticas [COM (2005) 576, de 17 de noviembre] que describe las distintas opciones y alternativas que se debatieron en estudios previos y varias sesiones.