IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

www.uoc.edu/idp

ARTÍCULO

# El Derecho del ciberespacio. Una aproximación

Ignacio Álvarez Rodríguez
Universidad Complutense de Madrid

Fecha de presentación: abril de 2019
Fecha de aceptación: julio de 2019
Fecha de publicación: noviembre de 2019

## Resumen

El presente texto es una aproximación crítica al Derecho del ciberespacio. A tal fin, se estudian en el mismo las normas principales que lo componen, tanto nacionales como internacionales, para posteriormente abordar algunos problemas que la comunidad de expertos ha detectado sobre ambos sectores. Finaliza con unas conclusiones que sintetizan los hallazgos resultantes.

## Palabras clave

derecho, ciberespacio, *soft-law*

## Tema

derecho público, derecho constitucional

## *An Analysis of Cyberspace Law*

### *Abstract*

*This text is a critical analysis of Cyberspace Law. To that end, the main regulations which constitute it in the national and international sectors are studied, in order to subsequently address various problems which have been detected by the community of experts in both these sectors. At the end of the text, conclusions are set out which give a summarisation of the resultant findings.*

### *Keywords*

*law, cyberspace, soft law*

### *Subject*

*public law, constitutional law*

## 1. A modo de introducción: el Derecho del ciberespacio

El ciberespacio se puede definir como «el espacio global en el entorno de la sociedad de la información que consiste en el conjunto interdependiente de infraestructuras de TIC, y que incluye internet, las redes de telecomunicaciones, los sistemas informáticos y los procesadores y controladores integrados propios del internet de las cosas (IoT)»[1]. Consecuentemente, el Derecho del ciberespacio son las normas que regulan dicho espacio, tanto nacionales como internacionales. Estamos, pues, dentro del espacio no físico donde se interconectan e interrelacionan las redes de comunicación e información que internet une. Internet es la red que crea y canaliza esa conexión. Los ordenadores (portátiles, de mesa, *smartphones*, etc.) son los aparatos físicos que permiten la misma[2]. Ambos mundos se conectan en permanente evolución y transformación[3].

La presente contribución tiene por objeto acercar al lector cuáles son las principales normas que regulan en España el ciberespacio y qué problemas plantean a juicio de los expertos. A tal fin se expone, en primer lugar, las normas nacionales. En segundo lugar, se hace lo propio con las normas internacionales. En tercer lugar, se abordan las críticas referidas. Se cierra el presente texto con una reflexión final sometida al mejor parecer doctrinal.

## 2. Derecho nacional del ciberespacio

La llamada «red nacida libre»[4] necesita, como cualquier lugar de interacción humana, de normas. De las vigentes en España, ¿cuáles son las más reseñables?

### 2.1. Constitución

En primer lugar, destaca la norma fundamental. Son muchos los preceptos que conforman el nivel primario de protección jurídico-ciberespacial. Por ejemplo, los referidos a los derechos fundamentales (especialmente los contemplados en los artículos 17, 18, o 24). Verbigracia, los que regulan las misiones atribuidas tanto a las Fuerzas Armadas (artículo 8) como a las fuerzas y cuerpos de seguridad del Estado (artículo 104 y siguientes CE), así como las propias del Poder Judicial (artículos 117 y siguientes), y de la Fiscalía (artículo 124 CE)[5]. Otra muestra la tenemos en la distribución de competencias entre Gobierno y Comunidades Autónomas (artículos 148 y 149)[6].

La Constitución, como norma suprema, se aplica por entero en el ciberespacio. Hay dos datos que corroboran la aseveración. Primero, no solo tenemos el derecho fundamental al *habeas data* conforme al visionario artículo 18.4 CE, sino que la última jurisprudencia comunitaria y constitucional nos reconoce ser titulares del llamado «derecho al olvido»[7]. Y segundo, recordemos que nuestros jueces y tribunales garantizan todos los derechos y libertades, también en el ciberespacio.

1. Véase M. Barrio (2018, pág. 25)).
2. El Diccionario de la Real Academia Española define el ciberespacio como el «ámbito artificial creado por medios informáticos». Véase https://dle.rae.es/?id=98Wdd57. [Fecha de consulta: 14 de mayo de 2019].
3. D. Fernández Bermejo y G. Martínez Atienza (2018, pág. 113).
4. P. García Mexía (2017, pág. 68).
5. Véase F. Zea y Ó. Pastor (2013, pág. 84-86)) y J. Jordán (2013, pág. 156-165).
6. Según el Tribunal Constitucional, la ciberseguridad y la ciberdefensa a nivel nacional son competencia exclusiva del Estado y no de las Comunidades Autónomas (STC 184/2016).
7. Artículo 18.4 CE: «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». El Tribunal Constitucional dijo que tal precepto reconocía un «auténtico derecho fundamental» al *habeas data*. Véase J. Alguacil González-Aurioles (2001, pág. 365-388). La sentencia del Tribunal de Justicia de la Unión Europea es la dictada en el asunto *Google contra España* (asunto C-131/12) de 13 de mayo de 2014. La primera resolución del Tribunal Constitucional que la aplica es la STC 58/2018, de 4 de junio.

Valgan como ejemplo las condenas por manifestaciones vejatorias o insultantes en la red, haciendo bueno el límite del insulto a la libertad de expresión, único formal y claramente enunciado en la jurisprudencia constitucional[8].

## 2.2. Legislación

No es ningún secreto que en los últimos tiempos se han dictado numerosas normas con rango de ley que afectan al ciberespacio.

Dejando ahora de lado las que traen a nuestro país la nueva normativa europea de protección de datos, destaca la Ley de seguridad nacional (2015), auténtica *norma paraguas* que pretende crear un sistema de seguridad nacional estructurado y eficaz, explicitando tanto el objeto y sujetos llamados a ejercer las tareas en seguridad como los órganos competentes, así como las gestiones de eventuales crisis y el destino de recursos suficientes. De dicha norma se extrae que el peso de tales tareas recae, sin duda alguna, en el Poder Ejecutivo[9].

También destacan las diferentes modificaciones que se han introducido en el Código Penal, en la Ley de enjuiciamiento criminal, y en la Ley de protección de la seguridad ciudadana (las tres de 2015), donde se endurecen las penas de algunos delitos telemáticos o donde se regula cómo, cuándo, dónde y con qué objetivos cabe proceder a la intervención policial de equipos a distancia, la forma de custodiar los *hardware* incautados o la regulación de la figura del *agente encubierto* en redes y foros[10].

Tiene su importancia la Ley de infraestructuras críticas (2011), porque en ella se establecen qué administraciones se encargan de la protección y aseguramiento de equipos, sistemas, edificios y estructuras que se consideran especialmente sensibles (de ahí lo de «críticas») desde el punto de vista social[11].

Sin minusvalorar la importancia del resto del paquete legislativo (la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico; la Ley 59/2003, de 19 de diciembre, de firma electrónica; la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos), en materia de ciberseguridad se antoja capital tanto la Ley reguladora del Centro Nacional de Inteligencia como la Ley reguladora del control judicial previo del Centro Nacional de Inteligencia (ambas de 2002), donde se establece el régimen jurídico básico del espionaje español[12]. Otro tanto puede decirse de la Ley de secretos oficiales (1968), donde se regula las *materias clasificadas*[13], que pueden ser de dos tipos: materias calificadas de *secreto* y materias calificadas de carácter *reservado*[14], en atención al grado de importancia de la información.

## 2.3. Reglamentación y Administraciones Públicas

No cabe ninguna duda de que los reglamentos en materia de ciberseguridad son realmente numerosos.

Es relevante el Reglamento por el que se aprueba la *Estrategia de seguridad nacional 2017*, donde se sientan los pilares de la seguridad en España[15]. Una idea preside la regulación: la ciberseguridad es objetivo general y línea de

8. Sobre el particular puede verse J. Urías (2019), *pássim*.
9. Por poner algunos ejemplos, el artículo 4.1. establece que «la Política de Seguridad Nacional es una política pública en la que bajo la dirección del Presidente del Gobierno y la responsabilidad del Gobierno, participan todas las Administraciones Públicas (...)». El artículo 12 establece como órganos competentes en la materia, además de las Cortes Generales...: «b) El Gobierno; c) El Presidente del Gobierno; d) Los Ministros; e) El Consejo de Seguridad Nacional; f) Los Delegados del Gobierno en las Comunidades Autónomas y en las ciudades con Estatuto de Autonomía de Ceuta y Melilla». El artículo 14, por su parte, nos dice que: «Corresponde al Gobierno: a) Establecer y dirigir la Política de seguridad nacional y asegurar su ejecución; b) Aprobar la Estrategia de seguridad nacional y sus revisiones mediante real decreto, en los términos previstos en esta ley; c) Efectuar la Declaración de recursos
10. F. Bueno (2015, pág. 1-10).
11. Véase G. Correa y J. M. Yusta (2013, pág. 92-108).
12. 12. Cfr. J. L. González (2014, pág. 151-186).
13. Artículo segundo: «A los efectos de esta Ley podrán ser declarados "materias clasificadas" los asuntos, actos, documentos, informaciones, datos y objetos, cuyo conocimiento por personas no autorizadas pueda dañar o poner en riesgo la seguridad del Estado o comprometa los intereses fundamentales de la Nación en materia referente a la defensa nacional, la paz exterior o el orden constitucional».
14. Véase A. L. Alonso de Antonio (2015, pág. 219-243) y la monografía de L. M. Díez-Picazo (1998).
15. Real Decreto 1008/2017, de 1 de diciembre.

acción principal de la seguridad nacional. A nivel organizativo, es importante el Reglamento por el que se establece la organización básica de las Fuerzas Armadas, y donde se ubica al Mando Conjunto de Ciberdefensa bajo la dirección del Estado Mayor[16]. Goza de importancia capital el Reglamento de protección de las infraestructuras críticas. A título informativo conviene recordar que el Catálogo de infraestructuras críticas está calificado de *secreto*, por lo que no es ni puede ser de dominio público[17].También debemos recordar la norma[18] que regula el Esquema nacional de seguridad en el ámbito de la Administración Electrónica y la norma que hace lo propio con el Esquema nacional de interoperabilidad en el ámbito de la Administración Electrónica[19]. Es de cierta relevancia el Reglamento por el que se regula el Centro Criptológico Nacional[20]. Esta es una de las administraciones públicas más importantes en materia de ciberseguridad y queda bajo la supervisión directa del Director del CNI. Finalmente, destaca el Reglamento de desarrollo que desarrolla la Ley de secretos oficiales que, aunque no contiene ni podía contener disposiciones específicas en la materia, sigue en vigor y, por ende, aplicado[21].

Quienes ejecutan sus dictados en su actividad cotidiana son las administraciones públicas, auténtica columna vertebral, por lo que procede dedicarles unas líneas.

Desde el ámbito civil se sigue un mismo esquema: uno o varios ministerios tienen dentro de su organigrama diversos negociados que velan, en sus respectivos ámbitos competenciales, por la ciberseguridad. Los principales ministerios son el de Defensa, Interior, Innovación y Ciencia, e Industria; y los organismos que tienen adscritos van desde el Departamento de Seguridad de Presidencia del Gobierno, hasta el INCIBE (Instituto para la Ciberseguridad); desde el CCN-CERT (Centro Criptológico Nacional-Centro de Respuesta Temprana), el CNPIC (Centro Nacional de Protección de Infraestructuras Críticas, y el mismo CNI, hasta las unidades referidas de Policía Nacional y Guardia Civil, la Unidad de Delitos Telemáticos de la Fiscalía General del Estado, o la Oficina de Seguridad del Internauta (Ministerio de Industria). También destacan las unidades que las policías autonómicas dedican a fines de ciberseguridad.

Desde el ámbito militar destacan, por un lado, las diferentes unidades ubicadas en cada uno de los ejércitos. A título de ejemplo podemos citar el COVAM (Centro de Operaciones y Vigilancia de Acción Marítima), dependiente de la Armada; el COVE (Centro de Operaciones de Vigilancia Espacial), dependiente del Ejército del Aire; y el CESEGET (Centro de Seguridad del Ejército de Tierra), dependiente del Ejército de Tierra. Recordemos, de nuevo, el Mando Conjunto de Ciberdefensa, principal órgano militar en la materia.

## 3. Derecho internacional del ciberespacio

Las normas internacionales que rigen para España en materia ciberespacial presentan una similitud y una diferencia con las nacionales. La similitud es que también de estas se predica su obsolescencia, por haber sido pensadas para el mundo físico de antaño. La diferencia es que aquí opera la divisoria entre *hard-law* (Derecho vinculante para los estados, fundamentalmente los tratados internacionales) y las normas de *soft-law* (recomendaciones no vinculantes), siendo estas últimas las que permiten un mayor margen de acción y, por ende, las preferidas de los estados.

### 3.1. Organización de las Naciones Unidas

La Organización de las Naciones Unidas nació con la misión de garantizar la paz y la estabilidad internacionales. El mundo de 1945 era un mundo en el que la violencia, el empleo de los ejércitos y la conquista de territorios había sido una constante que se quería dejar atrás. Así fue como se enunció el principio del no uso de la fuerza en las relaciones internacionales. Con las nuevas capacidades ciberespaciales, la pregunta se antoja obvia: ¿y qué sucede si un estado decide librar una ciberguerra? ¿Sabemos qué

16. Real Decreto 872/2014, de 10 de octubre
17. Real Decreto 704/2011, de 20 de mayo.
18. Real Decreto 3/2010, de 8 de enero.
19. Real Decreto 4/2010, de 8 de enero.
20. Real Decreto 421/2004, de 12 de marzo.
21. Decreto 242/1969, de 20 de febrero.

es esa ciberguerra? ¿Hay ciberarmas? ¿Y ciberataques internacionales?

La realidad jurídica internacional demuestra que no existe, a día de hoy, ninguna norma de *hard-law* que regule este tipo de comportamientos. Así que tenemos que interpretar la principal norma en la materia: la Carta de las Naciones Unidas.

El uso de la fuerza está regulado en sus artículos 2.4. y 51. El principio internacional indiscutido es el no uso de la fuerza en las relaciones internacionales. Pero cabe una excepción: la legítima defensa. Si un estado es atacado, puede defenderse del ataque sufrido. ¿Bajo qué condiciones? Primero, debe haber sufrido un «ataque armado» (que aquí debería ser entendido como un «ciberataque armado»). Segundo, debe cumplir con los requisitos de necesidad (no hay otro medio de responder), proporcionalidad (ajustar la respuesta a los efectos y daños reales causados por el ataque/ciberataque) y oportunidad (responder en un tiempo razonable sin dilatar la respuesta). Y, aunque a primera vista parece que las nuevas amenazas en el ciberespacio casan mal con estas exigencias, las conclusiones de los expertos no excluyen que pueda alegarse legítima defensa en el ciberespacio[22]. Cuestión incluso más peliaguda es saber si los estados tienen eso que se ha llamado *legítima defensa preventiva*, es decir, golpear antes de ser golpeado ante un ataque inminente. Ya vimos el poco consenso que suscita esta tesis en la comunidad internacional al hilo de la última guerra de Irak, sin ir más lejos.

¿Cabrían usos de la fuerza adicionales, entendidos aquí como ciberuso de la fuerza? En principio, sí, en aplicación análoga de la normativa internacional. En primer lugar, cabría si lo autoriza el Consejo de Seguridad de las Naciones Unidas. Ejemplos en el mundo físico de autorización y no autorización los tenemos en las últimas guerras de Afganistán e Irak. Pero el proceso para obtener dicha autorización es largo y complejo y uno de los cinco miembros permanentes del Consejo podría vetar la resolución e impedirlo, por lo que los estados parece que están recurriendo a *otros métodos*. En segundo lugar, algunos estados alegan la conocida como *responsabilidad de proteger* (el famoso principio de *injerencia humanitaria*). Según esta visión, todo estado tendría la facultad de adentrarse en el espacio físico –y por extensión, virtual– de un tercer estado, si tiene constancia de que ese estado está violando los derechos humanos de su propia población. Ejemplos (bastante discutibles) serían los casos de Libia o Siria[23]. Sea como fuere, en el ciberespacio las cosas resultan más enrevesadas. Ni siquiera algo que en su día se consideró el primer *ciberarma* de la historia (el troyano Stuxnet), se tiene por tal en el principal grupo de expertos internacionales en la materia[24].

Por lo demás, la ONU sigue trabajando en la materia, aunque con resultados desiguales. Buena muestra de ello es el *Informe del Grupo de Expertos sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional*, de 2015, que ha sido ratificado por el G-20[25]. En este se realiza una defensa de la multilateralidad, la cooperación, la transparencia, y la ayuda mutua, recordando que cuando los estados empleen las TIC quedan sometidos al ordenamiento internacional, tanto en todo aquello que suceda en su territorio como en toda relación internacional que establezca con terceros estados o actores no estatales. También aboga por un uso pacífico y seguro del ciberespacio. Cuando en 2017 los expertos volvieron a reunirse para actualizar sus contenidos, no consiguieron ponerse de acuerdo en la nueva versión[26].

Si se diera el caso de que se desatara una ciberguerra, en principio debería aplicarse a las hostilidades el llamado Derecho internacional humanitario, cuya principal misión es limitar y regular qué se puede hacer y qué no se puede hacer en la batalla, en aras de proteger tanto a la población e infraestructuras civiles como a los no combatientes. Esta rama del Derecho internacional público está compuesta por los cuatro Convenios de Ginebra de 1949, a los que se suman los Protocolos de 1977, además de varias nor-

22. C. S. Yoo (2015, pág. 181).
23. Véase J. Vericat (2017, pág. 112-120).
24. C. S. Yoo (2015, pág. 186).
25. El Informe se ha consultado aquí: https://www.un.org/disarmament/es/los-avances-en-la-informatizacion-y-las-telecomunicaciones-en-el-contexto-de-la-seguridad-internacional/ [Fecha de consulta: 11 de junio de 2019].
26. Véase J. Nye (2018, 18 de marzo). (en línea) https://elpais.com/elpais/2018/03/16/opinion/1521229334_966187.html. [Fecha de consulta: 11 de junio de 2019].

mas sectoriales. Cabe recordar que estas normas fueron pensadas para el mundo físico anterior a la explosión de internet y sus consecuencias, por lo que las dudas sobre cómo aplicarlas a las nuevas situaciones perviven[27].

### 3.2. Organización del Tratado del Atlántico Norte

La Organización del Tratado del Atlántico Norte (OTAN) es la principal alianza defensiva trenzada por el mundo occidental. Desde 1949 en activo, estamos ante una coalición militar de países que se comprometen a prestarse apoyo mutuo en caso de sufrir un ataque armado (en respuesta a los ataques del 11-S, los Estados Unidos de América invocaron precisamente el artículo 5 del Tratado, que permite que los socios ayuden a responder al ataque)[28]. Una de sus principales razones de ser era contener el bloque soviético, que también había firmado su propia alianza militar mediante el Pacto de Varsovia (hoy en día extinguido).

Desde hace algunos años, la OTAN ha declarado el ciberespacio como un ámbito operativo más. Y, en consecuencia, intenta realizar los consiguientes esfuerzos para adaptar las capacidades militares de sus socios a las nuevas realidades. Uno de esos esfuerzos son las llamadas Reglas de enfrentamiento del ciberespacio. Estas reglas (en inglés, *Rules of Engagement*, abreviadas ROE) son las normas que regulan un eventual ciberconflicto en el espacio OTAN[29]. En realidad, lo que hacen es volcar la normativa internacional existente en el ámbito ciberespacial[30].

Por último, debe destacarse que en el marco de la OTAN se ha auspiciado la creación del Centro de Excelencia para la Cooperación en Ciberdefensa de la OTAN. Este centro realiza diversas tareas relacionadas con la ciberdefensa, especialmente por medio de los *ciberejercicios*, donde periódicamente los miembros de la Alianza ponen a prueba sus redes de información y comunicación al objeto de detectar vulnerabilidades y acometer mejoras. En los últimos años destacan *Locked Shields* y *Cyber Coallition* (2016), así como *Crossed Swords* (2017)[31]. La principal norma de *soft-law* se ha elaborado bajo sus auspicios. Hacemos alusión al Manual de Tallin (versión 1.0 y 2.0, de 2013 y 2017, respectivamente), elaborados por una veintena de expertos en Derecho internacional bajo el liderazgo de M. Schmitt[32].

### 3.3. Unión Europea

La Unión Europea está haciendo diversos esfuerzos a la hora de adaptarse a las *nuevas* realidades.

En la materia que nos ocupa cabe destacar, en primer lugar, la Estrategia de ciberseguridad (2013), también norma de *soft-law* que pretende garantizar un ciberespacio abierto, protegido y seguro[33]. Para ello, llama a la cooperación entre los estados miembros y a no permitir que se produzcan ciberataques desde sus territorios. En dicha Estrategia también se tiene en cuenta que las TIC constituyen actualmente la base del crecimiento económico, a la vez que se erigen como un elemento clave en sectores como las finanzas, la sanidad, la energía o los transportes. Además, este ciberespacio abierto y libre ha favorecido el intercambio de información y de ideas, así como una integración política y social en todo el mundo[34].

27. Véase L. R. Blank (2015).
28. Artículo 5 de la Organización del Tratado del Atlántico Norte: «Las Partes convienen que un ataque armado contra una o contra varias de ellas, acaecido en Europa o en América del Norte, se considerará como un ataque dirigido contra todas ellas y, en consecuencia, acuerdan que si tal ataque se produce, cada una de ellas, en ejercicio del derecho de legítima defensa individual o colectiva, reconocido por el artículo 51 de la Carta de las Naciones Unidas, asistirá a la Parte o Partes así atacadas, adoptando seguidamente, individualmente y de acuerdo con las otras Partes, las medidas que juzgue necesarias, incluso el empleo de la fuerza armada para restablecer y mantener la seguridad en la región del Atlántico Norte. Todo ataque armado de esta naturaleza y toda medida adoptada en consecuencia se pondrán inmediatamente en conocimiento del Consejo de Seguridad. Estas medidas cesarán cuando el Consejo de Seguridad haya tomado las medidas necesarias para restablecer y mantener la paz y la seguridad internacionales». Véase G. Colom Piella (2012, pág. 287-304).
29. Se han consultado aquí: https://www.ccdcoe.org/research/ [Fecha de consulta: 10 de junio de 2019].
30. Una crítica de tal extremo puede leerse en J. Miguel (2017, pág. 1-16).
31. Se han estudiado aquí: https://www.ccdcoe.org/training/ [Fecha de consulta: 10 de junio de 2019].
32. Se pueden leer las dos versiones aquí: https://www.ccdcoe.org/about-us/ [Fecha de consulta: 10 de junio de 2019].
33. Véase H. Wagener (2014, pág. 1-19)
34. Comisión Europea (2013, 7 de febrero) (en línea) http://europa.eu/rapid/press-release_IP-13-94_es.htm).. [Fecha de consulta: 11 de junio de 2019].

No cabe duda que esto ha comportado nuevos riesgos y vulnerabilidades, que deben ser enmendadas y prevenidas en la medida de lo posible. Los sucesos que tuvieron lugar al hilo de dos modalidades recientes de *ransomware* (WannaCry y NotPetya), con más de 300.000 equipos informáticos infectados y severos daños económicos a sus espaldas dieron la oportunidad a la UE de volver a insistir en la condena en firme de las «ciberactividades maliciosas». Así, las Conclusiones del Secretario General del Consejo de la UE, de 16 de abril de 2018, no dejaron lugar a dudas[35]. Comienza por recordar la importancia de un ciberespacio global, abierto, libre, estable y seguro. También recuerda que en el ciberespacio rige el Estado de derecho y los derechos fundamentales, en aras del bienestar social, el crecimiento económico, la prosperidad y la integridad de nuestras sociedades libres y democráticas. Incide en la importancia de seguir las recomendaciones dadas en su día en las *Conclusiones sobre el Marco de la Respuesta Diplomática conjunta a las Ciberactividades Maliciosas*[36], que apuestan por la prevención de conflictos, la cooperación y la estabilidad interestatal.

### 3.4. Consejo de Europa

Finalmente, debemos hacer una breve alusión a lo que sucede en el marco del Consejo de Europa, organización de la mayor importancia en lo que se refiere a la protección de los derechos humanos gracias, entre otros instrumentos, al Convenio Europeo de Derechos Humanos y a su principal garante, el Tribunal Europeo de Derechos Humanos[37].

Uno de sus principales hitos normativos es el Convenio contra la ciberdelincuencia (2004, en vigor en España desde 2010), también llamado Convenio de Budapest. Esta norma es el primer tratado internacional creado para combatir la delincuencia en internet y los delitos informáticos. Cuenta en su nómina, además de con los estados miembros del Consejo, con los Estados Unidos de América. Lo que hace este tratado es recoger una serie de crímenes y delitos que los estados firmantes se obligan a refrendar y castigar en sus normas. Goza de un Protocolo adicional, donde se tipifica como delito actos racistas y xenófobos cometidos por medio los sistemas informáticos. El tratado está respaldado por el Comité del Convenio sobre ciberdelincuencia, que supervisa su aplicación, y por la Oficina del programa sobre ciberdelincuencia en Bucarest, que apoya a países de todo el mundo con programas de capacitación[38].

Otro de esos hitos es el Convenio para la protección de los niños contra la explotación y el abuso sexual (2007, en vigor en España desde 2010). Es sabido que este es uno de los puntos más oscuros y macabros de la red y uno de los que concita mayores esfuerzos contra su erradicación[39].

También existen algunas disposiciones que afectan al ciberespacio en el Convenio de Prevención del Terrorismo (2005, en vigor en España desde 2009), con su protocolo adicional de 2015. Por medio del mismo, los estados se comprometen a tipificar como delitos la provocación pública para cometer delitos de terrorismo, y el reclutamiento y entrenamiento de terroristas por medio de internet. El protocolo, por su parte, contiene medidas para enfrentarse a los llamados «combatientes terroristas extranjeros»[40].

Ni que decir tiene que el enfoque que se privilegia desde esta organización es la protección de los derechos humanos en el marco del ciberespacio, defendiendo que las personas son las verdaderas protagonistas de internet, debiendo tener garantizado un acceso y uso libre y seguro. De muestra, dos botones jurisprudenciales. En primer lugar, el asunto *Yeldimiri contra Turquía*, decidido por la sentencia del Tribunal Europeo de Derechos Humanos de 18 de diciembre de 2012, donde viene a reconocer que el ciudadano turco tiene frente al Estado un «derecho a internet libre»[41]. En segundo lugar, la sentencia del mismo Tribunal, de 13 de septiembre de 2018, que decidió el asunto *Big Brother Watches and Others contra United Kingdom*,

35. Véase https://eur-lex.europa.eu/oj/direct-access.html?locale=es [Fecha de consulta: 10 de junio de 2019].
36. Véase https://eur-lex.europa.eu/oj/direct-access.html?locale=es [Fecha de consulta: 10 de junio de 2019].
37. Pueden consultarse los trabajos recogidos en dos obras colectivas que ya son clásicas en el iuspublicismo español, tanto en J. García Roca y P. Santolaya Machetti (2014) como en I. Lasagabaster (2015).
38. Véase J. M. Asencio Gallego (2017, pág. 44-67).
39. Sobre el mismo puede verse los diversos trabajos compilados en C. Villacampa Estiarte y T. Aguado-Correa (2015).
40. Véase Consejo De Europa (2014) (en línea) https://edoc.coe.int/en/ [Fecha de consulta: 11 de junio de 2019].
41. Véase P. García Mexía (2017, pág. 79).

donde declaró que las instituciones estatales solo pueden vigilar las comunicaciones si cumplen con las garantías pertinentes[42].

## 4. Problemas en torno al Derecho del ciberespacio

La comunidad de expertos parece estar de acuerdo en que la regulación jurídica del ciberespacio plantea algunas dudas y problemas. Sin ánimo de exhaustividad, señalaremos a continuación algunos de los más recurrentes.

### 4.1. Problemas comunes

Los problemas comunes son predicables tanto de las normas nacionales como de las internacionales.

Debemos empezar por ese movimiento activo y dinámico que defiende que el Estado debe alejarse del ciberespacio[43]. Y ello porque este es de los últimos reductos, si no el último, que quedan de libertad auténtica y real. A lo sumo aceptan que en el caso de que hiciera falta normas, la misma red se autorregularía mejor de lo que cualquier ente público o privado pudiera hacerlo. Así que cualquier Constitución, Ley, Reglamento o Tratado internacional serían vistos, independientemente de su contenido o de sus buenas intenciones, como algo intrínsecamente negativo.

Sin prejuzgar si este planteamiento acierta o yerra, la verdad es que conviene partir del principio de realidad. Esto es, la realidad demuestra que el ciberespacio ya está regulado por normas, quizá porque esa ha sido la tónica dominante de la sociedad humana, desde la prehistórica hasta la actualidad. Ya lo dice el aforismo *ubi societas, Ibi ius*[44]. Arriba se ha hecho referencia a algunas de ellas con la mirada puesta en España, pero hay cientos de normas en otros estados y en otras organizaciones internacionales que regulan el ciberespacio. Es más, la tendencia constatable es que el mundo físico y el mundo virtual no pueden ser tratados como lugares paralelos y desconectados, sobre todo en lo que se refiere a combatir fenómenos de criminalidad[45].

El otro gran reclamo de la comunidad de expertos es la demanda de nuevas normas para las nuevas realidades (o de interpretaciones flexibles y audaces de las vigentes). Sobre todo porque aquellos que pretenden hacer el mal son expertos en buscar y rebuscar las vulnerabilidades del sistema a dañar[46]. Conviene recordar que todo derecho, por más novedoso que pretenda ser, siempre irá uno o dos pasos por detrás de la realidad social que regula[47]. Así ha sido siempre y así seguirá siendo. Finalmente, cabe decir que la buena norma es la que se cumple y no la que se incumple. Dicho con otras palabras: una cultura del cumplimiento se retroalimenta a sí misma. ¿Cuál es el camino para llegar a cumplir las normas? Cumplirlas. Tan difícil o tan complicado como eso[48].

### 4.2. Problemas específicos

Siguiendo el esquema del inicio, y comenzando por las normas nacionales, se suele argüir que la regulación es escasa, confusa, parcial y obsoleta. No se puede objetar mucho a este parecer, más allá de un par de reflexiones.

Primero, quizá no haya un problema de normas sino un problema de lo que hay detrás de las normas (y este presenta varias caras). Si tenemos en cuenta que la cultura de la ciberseguridad está en plena construcción, se tendrá mucho terreno ganado[49]. Por ejemplo, no es lo mismo la delincuencia particular que se comete en la red (fundamentalmente ligada a las injurias y amenazas, a los delitos sexuales y a las pequeñas estafas), que la delincuencia organizada (que se dedica a explotar vulnerabilidades para causar daños masivamente, sobre todo contra patrimonios)[50].

42. Véase E. Salamanca Aguado (2014, pág. 1-26).
43. Véase M. Barrio (2018, pág. 42 y siguientes).
44. Véase M. De La Válgoma (2006, pág. 1-16).
45. Véase F. Almenar Pineda (2017, pág. 30-35).
46. Un repaso en profundidad de todas estas implicaciones puede verse en A. Gómez De Ágreda (2019).
47. Véase J. F. Sánchez Barrilao (2018, pág. 234 y siguientes).
48. Véase M. Fuertes (2013, pág. 69).
49. Véase M. Barrio (2018, pág. 13-21).
50. Véase E. Casas (2017, pág. 31 y siguientes).

Segundo, una perogrullada que no por obvia debe ser arrinconada: no hay norma que sustituya la conciencia, la decisión y la responsabilidad individual. No hay norma que valga en la soledad nocturna de una habitación. Tal y como se ha dicho con acierto, «nuestra forma de pensar internet afecta a nuestra manera de utilizar internet»[51].

Respecto a las normas internacionales, tiene especial protagonismo todo lo que se mueve entre bambalinas. Aquí podemos diferenciar dos planos: el político y el jurídico.

En el plano político, las relaciones internacionales están marcadas por los intereses permanentes y no por las alianzas eternas[52]. Los estados buscan situarse en el mejor lugar dentro de la escena internacional. Por eso las potencias compiten entre sí, sobre todo a la hora de obtener buenos recursos, resultando el ciberespacio el *lugar* idóneo para ello.

En ese tablero geoestratégico, la sociedad internacional tiene un auténtico reto en China, una vez más. El país asiático conjuga los avances tecnológicos y el sistema político autoritario con una pasmosa facilidad[53]. Y es que el modelo chino ha dado un salto de gigante, demostrando que «(...) internet se puede convertir en una red jerarquizada, con puertas de entrada de fácil bloqueo, donde la censura y la intromisión en la privacidad y el control de los contenidos es perfectamente posible, pero sin acabar con el desarrollo de la innovación (...)»[54]. Es decir, puedes ser una potencia digital plenamente competitiva, con empresas punteras en el *top ten* en innovación digital y ciberespacial, a la par que un sistema no democrático basado en el control masivo, la censura de contenidos inapropiados, y la tecnodictadura. En suma: «frente a la creencia de que internet por su propia naturaleza era único e indivisible y no podía ser fragmentado y, por tanto, estaría basado en un único modelo acorde a los valores de la sociedad liberal, estamos viendo surgir con pujanza un contramodelo autoritario y restrictivo que responde muy bien a valores contrarios a la cultura democrática»[55].

Otro problema lo plantean las *operaciones de falsa bandera*, cada vez más en auge y empleadas para confundir a la sociedad internacional e instigar la acción de terceros[56]. Los estados a veces dicen que hacen cosas que no hacen y otras veces no reconocen las cosas que sí que hacen. ¿Por qué quieren los estados influir en el ciberespacio? Exactamente por la misma razón por la que pretenden influir en el espacio físico tradicional: para ganar mentes y adeptos a la causa. Probablemente, la época de conquistar territorios a sangre y fuego ya ha pasado y ahora se trata de ganar un buen posicionamiento en el entorno ciberespacial[57]. No es ninguna exageración decir que los estados –o alguien a sueldo de los estados– suelen estar detrás de algunas de las ciberacciones más sonadas. Y lo hacen por motivos concretos: obtención fraudulenta de datos, destrucción o alteración de sistemas y servidores, filtraciones interesadas de documentos y robo de tecnología. Es lo que algún autor califica de «guerra híbrida»[58].

En el plano jurídico, las críticas son dos. La primera reside en las complicaciones que presenta la autoría de presuntas ilicitudes en el ciberespacio. Sabemos que en Derecho internacional el principal responsable jurídico es el Estado. Entonces, ¿qué pasa si una empresa es atacada desde el territorio de un tercer estado sin que este sepa o pueda impedirlo? ¿Ante quien se dirige la empresa? ¿Y qué sucede si un estado lanza un ciberataque encubierto? Si a eso se le suma que, en verdad, no sabemos todavía qué es un ciberataque, un ciberarma o un ciberuso de la fuerza, tenemos la situación actual, con los estados moviéndose como pez en el agua por las zonas grises. Lo cual tiene sentido con la segunda crítica. Se dice que buena parte de las «mejores normas» no son vinculantes (como el Manual de Tallin). Pero si se quiere hacer normas propiamente dichas, una de las características principales de las normas internacionales por antonomasia –los tratados internacionales– dependen de la voluntad de los estados, que tienen a su disposición diversos mecanismos para redactarlas a la medida de sus necesidades (y, en último extremo, pueden

51. Así lo expresa A. Manilla (2018, pág. 102).
52. Es de obligada consulta P. Baños (2017, 2018).
53. Véase D. Ramírez Morán (2017, pág. 8-15).
54. La larga cita se ha extraído de C. López Blanco (2019, pág. 36).
55. Véase C. López Blanco (2019, pág. 37).
56. Véase E. Frattini (2016).
57. Véase Y. N. Harari (2018, pág. 193).
58. Véase Y. Quintana (2018, pág. 1).

salvar su ratificación activando las reservas oportunas). Así que, a la larga, quizá no sea del todo malo que haya normas de *soft-law*.

Hay que añadir un ingrediente adicional. Y es que la vergüenza y los intereses de diversa índole suelen actuar de escudo. La confesión pública se interpreta como una debilidad y la debilidad es intolerable –al menos a juicio de la típica mentalidad de poder tradicional– por lo que buena parte de los ciberdelitos no se denuncian. Y si no se denuncian es como si no existieran. Al no existir, ¿cómo se van a perseguir? Los expertos advierten que, de seguir así, la paz internacional será imposible a largo plazo[59].

La comunidad de expertos coincide en que hay que replantearse reconstruir el edificio jurídico del ciberespacio, pero sin abandonar los pilares que nos vienen gobernando desde el año 1945[60]. No por ello hay que pecar de impaciencia: los primeros acuerdos de control nuclear tardaron veinte años en fructificar[61].

## 5. A modo de conclusión

Las conclusiones del estudio realizado en las líneas anteriores son las siguientes.

En primer lugar, no cabe duda de que se puede hablar, como una rama del Derecho con entidad propia, del Derecho del ciberespacio. Ese Derecho del ciberespacio está compuesto por diferentes normas nacionales (especialmente tres fuentes: Constitución, leyes, y reglamentos) e internacionales (entre las que hay diversas normas de *soft-law* que provienen de diferentes organizaciones internacionales a las que pertenecemos) y su expansión va en permanente aumento.

En segundo término, quizá en parte por esta expansión tan impresionante, la práctica y el desarrollo del ciberespacio y de las normas que se le aplican, ha dado lugar a una serie de críticas desde la comunidad de expertos, que se han sintetizado en torno a unos problemas comunes y a unos problemas específicos.

Dentro de los primeros destacan dos sectores. Recogiendo la esencia de la mejor filosofía *hacker*, hay quienes sostienen que la mejor norma respecto al ciberespacio es la que no se hace. El ciberespacio, según su visión, es y debe seguir siendo un lugar libre de injerencias externas. El otro sector del debate, con un punto mayor de realismo y pragmatismo, sostiene que es necesario adoptar una batería de normas, tanto nacionales como internacionales, porque el ciberespacio del siglo XXI las demanda.

Dentro de los segundos, como problema específico de las normas nacionales se arguye una regulación un tanto confusa, parcial y obsoleta, a la que se le oponen algunos argumentos atendibles (como por ejemplo el que defiende que no es un problema de normas sino de lo que hay detrás de las mismas). En el caso de las normas internacionales, la crítica es tanto política como jurídica. Política, porque nos encontramos en plena partida de ajedrez en el tablero internacional, donde los estados tienen diversos intereses y actúan en consecuencia, optimizando recursos y minimizando costes. Así se explican algunas actuaciones de ciertos países asiáticos o las ejecutadas bajo *falsa bandera*. Jurídica, porque la principal regulación se basa en las recomendaciones *soft-law*, no vinculantes por definición, amén de los añadidos quebraderos de cabeza de hacer encajar las normas antiguas a las realidades del siglo XXI.

59. Al menos, así lo defiende J. Nye (2015) (en línea) https://www.projectsyndicate.org/commentary/cyber-war-and-peace/spanish. [Fecha de consulta: 12 de junio de 2019].
60. Véase M. Robles (2016, pág. 1-43).
61. Sigue este criterio J. Nye (2018) (en línea). https://elpais.com/elpais/2018/03/16/opinion/1521229334_966187.html. [Fecha de consulta: 14 de mayo de 2019].

## Referencias bibliográficas

ALGUACIL GONZÁLEZ-AURIOLES, J. (2001) «La libertad informática. Aspectos sustantivos y competenciales (SSTC 290 y 292/2000)». *Teoría y Realidad Constitucional*, núm. 7. https://doi.org/10.5944/trc.7.2001.6543

ALMENAR PINEDA, F. (2018) *Ciberdelincuencia*. Lisboa: Juruá Editorial.

ALONSO DE ANTONIO, Á. L. (2015) «La Ley de Secretos Oficiales». *Foro: Revista de ciencias jurídicas y sociales*, núm. 1, vol. 18.

ASENCIO GALLEGO, J. M. (2017). «Los delitos informáticos y las medidas de investigación y obtención de pruebas en el convenio de Budapest sobre la ciberdelincuencia». En FERNÁNDEZ LÓPEZ, M. (coord.); ASENCIO GALLEGO, J. M. (dir) *Justicia penal y nuevas formas de delincuencia*. Valencia: Tirant lo Blanch.

BAÑOS, P. (2018). *El dominio mundial. Elementos del poder y claves geopolíticas*. Barcelona: Ariel.

BAÑOS, P. (2017). *Así se domina el mundo. Desvelando las claves del poder mundial*. Barcelona: Ariel.

BARRIO, M. (2018). *Ciberderecho. Bases estructurales, modelos de regulación e instituciones de gobernanza de Internet*. Valencia: Tirant lo Blanch.

BARRIO, M. (2017). «Fricciones entre Internet y Derecho». *Claves de razón práctica*, núm. 255.

BLANK, L. R. (2015) «Cyberwar versus Cyber Attack: The Role of Rethoric in the Application of Law to Activities in Cyberspace». En J. D. OHLIN; K. GOVERN; C. FINKELSTEIN (ed.) *Cyberwar. Law and Ethics for Virtual Conflicts*. Oxford: Oxford University Press. https://doi.org/10.1093/acprof:oso/9780198717492.003.0006

BUENO, F. (2015) «Comentarios y reflexiones sobre la Ley Orgánica 13/2015 de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica». *Diario La Ley*, núm. 8627.

CASAS, E. (2017). «Delincuencia en la Red». *Claves de razón práctica,* núm. 255.

COLOM PIELLA, G. (2012). «La evolución del Enfoque Integral de la OTAN en la gestión de crisis», *Revista CIDOB d'afers internacionals*, núm. 97-98.

COMISIÓN EUROPEA (2013, 7 de febrero) *Plan de ciberseguridad de la UE para proteger una red abierta plena de libertad y de oportunidades en línea*. (en línea) http://europa.eu/rapid/press-release_IP-13-94_es.htm). [Fecha de consulta: 11 de junio de 2019].

CONSEJO DE EUROPA (2014) *Protección de los derechos humanos en Internet* (en línea) https://rm.coe.int/16804c177e [Fecha de consulta: 11 de junio de 2019].

CORREA, G.; YUSTA, J. M. (2013). «Seguridad energética y protección de infraestructuras críticas». *Lámpsakos*, núm. 10.

DÍEZ-PICAZO, L. M. (1998). *Sobre secretos oficiales*. Madrid: Civitas.

Fernández BermeJO, D.; MARTÍNEZ ATIENZA, G. (2018). *Ciberseguridad, ciberespacio y ciberdelincuencia* (pág. 113). Cizur Menor: Thomson Reuters-Aranzadi.

FRATTINI, E. (2016). *Manipulando la historia. Operaciones de falsa bandera: del Maine al golpe de Estado en Turquía,* Barcelona: Planeta.

FUERTES, M. (2013). «Internet: la paz del camino». *El Cronista,* núm. 37, pág. 68.

GARCÍA MEXÍA, P. (2017). *La Internet Abierta.* Madrid: RDU Ediciones.

GARCÍA ROCA, J.; SANTOLAYA MACHETTI, P. (dir.) (2014). *La Europa de los Derechos. El Convenio Europeo de Derechos Humanos* (3.ª ed.) Madrid: CEPC.

GÓMEZ DE ÁGREDA, Á. (2019). *Mundo Orwell.* Barcelona: Ariel.

GONZÁLEZ, J. L. (2014). «Intromisión en la intimidad y CNI: Crítica al modelo español de control judicial previo». *Inteligencia y seguridad: Revista de análisis y prospectiva*, núm. 15.

HARARI, Y. N. (2018). *21 Lecciones para el siglo XXI*. Barcelona: Debate.

JORDÁN, J. (2013). «Ciberdefensa y tecnologías para la defensa». *Política Exterior*, núm. extra 155, vol. 27.

LASAGABASTER, I. (dir.) (2015) *El Convenio Europeo de Derechos Humanos. Comentario Sistemático.* (3.ª ed.) Cizur Menor: Civitas.

LÓPEZ BLANCO, C. (2019) «China y la venganza del nibelungo». *Letras Libres*, núm. 211.

MANILLA, A. (2018). *Ciberadaptados*. Madrid: La Huerta Grande.

MIGUEL, J. (2017). «La integración del ciberespacio en el ámbito militar». *Análisis GESI,* núm. 35.

NYE, J. (2018, 18 de marzo). «Nuevas normas para la seguridad». *El País* (en línea) https://elpais.com/elpais/2018/03/16/opinion/1521229334_966187.html. [Fecha de consulta: 11 de junio de 2019].

NYE, J. (2015) «Ciberguerra y Ciberpaz». *Project Syndicate* (en línea) https://www.projectsyndicate.org/commentary/cyber-war-and-peace/spanish. [Fecha de consulta: 12 de junio de 2019].

QUINTANA, Y. (2018). «Ciberseguridad, una cuestión de Estados», *Política Exterior,* núm. 185.

RAMÍREZ Morán, D. (2017). «Ciberseguridad en China». *Boletín del Instituto de Estudios Estratégicos,* núm. 1.

ROBLES, M. (2016). «El ciberespacio: presupuestos para su ordenación jurídico internacional». *Revista Chilena de Derecho y Ciencia Política,* núm. 1, vol. 7. https://doi.org/10.7770/rchdcp.v1i1.1025

SALAMANCA AGUADO, E. (2014). «El respeto a la vida privada y a la protección de datos personales en el contexto de la vigilancia masiva de comunicaciones». *Revista del Instituto Español de Estudios Estratégicos*, núm. 4.

SÁNCHEZ BARRILAO, J. F. (2018). «La neutralidad de Internet como objeto constitucional». En VALLS PRIETO, J. (coord.) *Retos jurídicos por la sociedad digital.* Cizur Menor: Thomson Reuters-Aranzadi.

TOHARIA, J. J. (2006). «Las profesiones jurídicas». En Díez-Picazo, L. M. (coord.). *El oficio de jurista.* Madrid: Siglo XXI.

URÍAS, J. (2019). *Libertad de expresión. Una inmersión rápida.* Barcelona: Tibidabo Ediciones.

VÁLGOMA, M. De La (2013). *El Derecho explicado a los jóvenes.* Barcelona: Paidós.

VERICAT, J. (2017). «Libia y el nuevo intervencionismo». *Política Exterior,* núm. 180, vol. 31.

VILLACAMPA ESTIARTE, C.; AGUADO-CORREA, T. (coord) (2015). *Delitos contra la libertad e indemnidad sexual de los menores: adecuación del Derecho español a las demandas normativas supranacionales de protección.* Cizur Menor: Thomson Reuters Aranzadi.

WAGENER, H. (2014). «La ciberseguridad en la Unión Europea». *Boletín del Instituto de Estudios Estratégicos,* núm. 77 (bis).

YOO, C. S. (2015). «Cyber Espionage or Cyberwar? International Law, Domestic Law and Self-Protective Measures». En J. D. OHLIN; K. GOVERN; C. FINKELSTEIN (ed.) *Cyberwar. Law and Ethics for Virtual Conflicts.* Oxford: Oxford University Press. https://doi.org/10.1093/acprof:oso/9780198717492.003.0009

ZEA, F.; Pastor, Ó. (2013). «La organización de la ciberdefensa militar en España y el perfeccionamiento de sus capacidades». *Revista SIC: ciberseguridad, seguridad de la información y privacidad*, núm. 104.

**Cita recomendada**

ÁLVAREZ RODRÍGUEZ, Ignacio (2019). «El Derecho del ciberespacio. Una aproximación». *IDP. Revista de Internet, Derecho y Política*. N.º 30, págs.. 1-13. UOC [Fecha de consulta: dd/mm/aa
https://dx.doi.org/10.7238/idp.v0i30.3201



**Sobre el autor**

Ignacio Álvarez Rodríguez
ialvarez1@ucm.es
Profesor Ayudante Doctor de Derecho Constitucional
Universidad Complutense de Madrid