ieee.es
Instituto Español de Estudios Estratégicos

Documento
Opinión

124/2015 17 noviembre de 2015

*Margarita Robles Carrillo**

EL CIBERESPACIO Y LA CIBERSEGURIDAD: CONSIDERACIONES SOBRE LA NECESIDAD DE UN MODELO JURÍDICO

EL CIBERESPACIO Y LA CIBERSEGURIDAD: CONSIDERACIONES SOBRE LA NECESIDAD DE UN MODELO JURÍDICO

Resumen:

La articulación de un modelo jurídico del ciberespacio no es una opción, sino una necesidad, incluso un imperativo. Operar mediante una mera traslación de las normas existentes desde el espacio físico al mundo virtual es insuficiente y erróneo. La eficacia del derecho como instrumento de ordenación de la vida en sociedad depende de su capacidad para responder a las coordenadas y singularidades propias de la realidad que está llamado a regular. El ciberespacio no solo es una realidad diferente, sino que también es una realidad capacitada para alterar la naturaleza y el funcionamiento de la realidad no virtual.

Abstract:

Building a legal model of cyberspace is not an option, but a necessity, even an imperative. Operate by a mere transfer of existing standards from the physical world to the virtual space is insufficient and erroneous. The effectiveness of the law as an instrument of management of social life depends on its ability to respond to the coordinates and singularities of reality that is called to regulate. Cyberspace is not just a different reality but also a reality that is changing the nature and operation of the preexisting realities.

Palabras clave:

Ciberespacio, ciberseguridad, modelo jurídico, aproximación constitucional.

Keywords:

Cyberspace, cybersecurity, legal model, constitutional approach.

INTRODUCCIÓN

En la década de los sesenta del siglo pasado, Paul Baran propuso la sustitución de las instalaciones y de los sistemas de comunicaciones centralizados por un sistema reticular de comunicación y un método de división y conmutación de la información en bloques, que se encuentra en el origen de ARPANET en 1969, rebautizado como INTERNET en los noventa. Desde entonces, las tecnologías de la información y de la comunicación (TIC) han avanzado a una velocidad imparable. Hace tiempo que el ciberespacio es una realidad, pero no una realidad cualquiera, básicamente, por dos motivos principales: su extraordinaria capacidad de expansión en el tiempo y en el espacio y, junto a ello, su singular y compleja interacción con el mundo no virtual.

En 1996, John Perry Barlow hacía pública la *Declaración de independencia del ciberespacio* que, además de incluir una severa crítica hacia los gobiernos, identificaba los problemas causados por una acción precipitada de los Estados para reglamentar este ámbito proclamando la necesidad de una nueva civilización del ciberespacio. En su alegato a favor de la libertad, condenaba la soberanía afirmando que *«Debemos declarar nuestros "yos" virtuales inmunes a vuestra soberanía, aunque continuemos consintiendo vuestro poder sobre nuestros cuerpos. Nos extenderemos a través del planeta para que nadie pueda encarcelar nuestros pensamientos. Crearemos una civilización de la Mente en el Ciberespacio. Que sea más humana y hermosa que el mundo que vuestros gobiernos han creado antes»*.

Esa pretendida inmunidad a la soberanía, en la medida en que se ha podido manifestar, no ha producido los efectos esperados en términos de libertad, ni tampoco en el camino hacia una civilización de la mente. El ciberespacio combina espacios donde el control estatal puede llegar a ser prácticamente absoluto[1] con otros en los que su ausencia o sus limitaciones sirven más a la causa de la criminalidad que a la de la libertad. Sin ir más lejos, el dilema que plantea la protección de datos personales en la era del *big data*[2] constituye un buen ejemplo de la pobre materialización de las expectativas lanzadas en el Manifiesto Barrow.

---

[1] No hace mucho, la catástrofe de Tianjin servía como argumento a la Administración del Ciberespacio de China (CAC) para cerrar en torno a medio centenar de páginas webs acusándolas de crear pánico entre la población por difundir información sin verificar o difundir rumores. Es una manifestación más de la llamada política de «tolerancia cero» y del alcance del control gubernamental chino.

[2] Mientras numerosos Estados y organizaciones internacionales y, entre ellas, singularmente, la Unión Europea, se afanan en establecer un régimen normativo en materia de protección de datos personales capacitado para operar en el contexto que impone el ciberespacio, no dejan de sucederse ciberataques consistentes precisamente en la difusión de esos datos. El asunto Ashley Madison podría pasar a la historia como uno de los casos emblemáticos en los que se ha podido llegar al suicidio como consecuencia de la divulgación de esos datos. Por su parte, la expansión del negocio del "big data" parece no conocer límites. "Big Data: el gran tesoro oculto del automóvil" (falta referencia) es el título de un artículo publicado recientemente en prensa en el que se identifica la automoción como la segunda industria por generación de datos y el impacto que pueden tener en las diversas áreas pronosticándole, como suele ser habitual, un futuro prometedor.

Prácticamente dos décadas después de ese Manifiesto, el contraste entre el avance tecnológico y la situación de relativo *impasse* en el plano jurídico empieza a ser alarmante. Es cierto que abundan las aportaciones doctrinales desde la ciencia jurídica y también lo es que los operadores jurídicos, los agentes y las instituciones internacionales y nacionales están trabajando en la solución jurídica de los problemas que plantea el ciberespacio. Pero también es verdad que se trata, en mayor medida, de reacciones frente a situaciones o problemas concretos y puntuales que de afrontar el verdadero reto de proceder a la articulación de un modelo jurídico para el ciberespacio. Ni la traslación mecánica del derecho existente al ciberespacio, ni la multiplicación de acciones con la consiguiente dispersión de los esfuerzos, que está caracterizando la actuación de las organizaciones internacionales y organismos nacionales, son suficientes para responder al desafío de ordenar jurídicamente el ciberespacio. Es necesario un planteamiento global sobre su régimen jurídico que ha de partir del conocimiento previo de su naturaleza.

UNA APROXIMACIÓN A LA NATURALEZA DEL CIBERESPACIO Y LA CIBERSEGURIDAD

El análisis del modelo jurídico del ciberespacio y de la ciberseguridad exige un acercamiento previo a su naturaleza por un doble motivo: de un lado, para huir de cualquier planteamiento formalista sobre la norma jurídica y, de otro, para destacar la función del derecho como instrumento de ordenación de la realidad social cuya efectividad depende de su potencial para organizar y racionalizar esa realidad, que será mayor cuanto mayor sea su capacidad de adecuación a las particularidades de la misma y a sus necesidades de regulación normativa. La norma jurídica no es intemporal y universalmente válida, ni tampoco siempre eficaz. Un ordenamiento jurídico no es extrapolable en el tiempo ni en el espacio a realidades sociales diferentes porque el derecho solo puede cumplir su función de racionalización de la vida en sociedad si se ajusta y responde a esa realidad social. Desde esa perspectiva, el ciberespacio muestra una naturaleza infinitamente más compleja que el espacio no virtual.

El ciberespacio: algo más que otro espacio

El ciberespacio constituye un escenario táctico, estratégico y operativo diferente de los espacios terrestre, marítimo, aéreo y exterior[3], que ha sido calificado en la doctrina, como uno de los *Global Commons*. Desde esa categorización, el discurso ha progresado y se ha perfeccionado como muestra la construcción teórica realizada por Gómez de Ágreda. A partir de esa propuesta inicial[4], el autor avanza en la comprensión de la naturaleza de

[3] Sobre su condición como "quinto dominio", puede verse JOYANES AGUILAR, l., "Introducción: estado del arte de la ciberseguridad", en *Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio*, *Cuadernos de Estrategia*, nº 149, diciembre 2010, 29-34.

[4] GÓMEZ DE ÁGREDA, A., "*Global Commons* en la era de la incertidumbre", *Boletín de Información del CESEDEN*, nº 317, 2010, 53-62.

ciberespacio cuestionando doblemente el recurso a aquella categoría: en un primer momento, constata las características singulares del ciberespacio respecto de los otros *Global Commons* para marcar sus diferencias[5]; y, después, procede a identificar la «esencia» del ciberespacio como el elemento verdaderamente distintivo. Como advierte certeramente Gómez de Ágreda, su esencia se encuentra en el modo en que altera las realidades de los otros dominios, su capacidad para interactuar con las otras realidades y modificar la percepción de las mismas y su naturaleza como aglutinante catalizador que provoca alteraciones en los demás entornos y en la comprensión de los mismos[6]. Esa naturaleza singular del ciberespacio desborda la idea de *Global commons* y este concepto, a su vez, se muestra incapaz de aprehender esa naturaleza singular.

Con una aproximación metodológica distinta, la calificación del ciberespacio como bien público tiene una doble virtualidad. En primer lugar, el recurso a esa categoría permite explicar la singularidad genética, funcional y sistémica del ciberespacio, destacando dos características insuficientemente apreciadas pero determinantes desde la perspectiva de su segurización entendida como el proceso y la garantía de su seguridad[7]. Como explican Mulligan y Schneider, «Cybersecurity is non-rivalrous and non-excludable so, by definition, it is a public good. It is non-rivalrous because one user benefiting from the security of a networked system does not diminish the ability of any other user to benefit from the security of that system. And it is non-excludable because users of a secure system cannot be

[5] Además de su artificialidad e inmaterialidad, Gómez de Ágreda pone el acento en el núcleo de la cuestión cuando explica que "La principal diferencia entre la interacción de los *commons* físicos entre ellos y la que se produce entre el Ciberespacio y los ámbitos físicos es que aquéllos pueden ejercer una cierta capacidad de control sobre los demás, generalmente en un sentido vertical descendente, mientras que el influjo que tiene el mundo virtual sobre el real es mucho más completo ya que puede determinar la posibilidad de utilización de los otros o bien actuar como multiplicador de sus capacidades" (GÓMEZ DE AGREDA, A., "El ciberespacio factor transversal en los *Global Commons*", en REQUENA Y DÍEZ DE REVENGA, M. (coord.), *La seguridad y la defensa en el actual marco socio-económico: nuevas estrategias frente a nuevas amenazas*, Madrid, Instituto Universitario General Gutiérrez Mellado, 2011, 1321-1331.

[6] GÓMEZ DE ÁGREDA, A., *The force of change*, http://deagreda.blogspot.com.es/2013/10/la-naturaleza-del-ciberespacio.html.

[7] La expresión «segurización» tiene, al menos, una doble acepción. Por una parte, a partir de los trabajos de la Escuela de Copenhague, el término *securitization* sirve para designar el proceso mediante el cual una cuestión se convierte en un problema de seguridad mediante un proceso definido como «an intersubjective process in the sense that it is only when the audience accepts a securitizing actor´s speech act that an issue will become securitized. When an issue is securitized, it becomes prioritized about `normal politics´ and `extraordinary means´ are necessary to address the problem» (MACKENZIE, M., "Securitizing Sex?", *International Feminist Journal of Politics*, vol. 12, n.º 2, 2010, 202-221, en concreto, pg. 204). Por otra parte, segurización se puede definir como el proceso y el resultado de garantizar la seguridad, de donde se extrae el verbo «segurizar» que se utiliza indistintamente junto con el de «securizar», procedentes del anglicismo *to secure*. Los equivalentes oficiales en castellano, asegurar o garantizar, no consiguen trasladar el significado del término inglés, en particular, cuando se trata de temas de ciberespacio y seguridad informática, razón por la cual se está extendiendo el uso de aquella expresión en la práctica.

easily excluded from benefits security brings»[8]. Esta característica significa, asimismo, que "excluding individuals from enjoying the benefits of cybersecurity is infeasible or uneconomical"[9]. En segundo lugar, la consideración del ciberespacio como un bien público es un argumento concluyente para la definición de una política pública como opción de técnica y de política legislativa[10]. Desde esa perspectiva, el modelo jurídico del ciberespacio ha de construirse en un contexto normativo natural y normalizado en el que se reconoce su naturaleza como bien público global y autónomo[11], al tiempo que se aleja de los planteamientos originales o convencionales focalizados en el derecho penal o en el derecho de los conflictos armados[12]. Por la fuerza de los hechos, por pura mecánica o por necesidad, la impronta de esos sectores del ordenamiento jurídico ha sido mayor y prácticamente protagónica en el ciberespacio cuando ambos han de ser, por definición, un último recurso, y ha desplazado de su lugar natural al resto de los sectores del ordenamiento jurídico.

---

[8] MULLIGAN, D. K. y SCHNEIDER, F. B., "Doctrine for cybersecurity", *Daedalus*, vol. 140, nº 4, 70–92, 2011, en concreto, pg. 75. Cooter y Siegel advierten que "cybersecurity is non-rival, because when an individual benefits from good security measures in a computer system, this benefit does not diminish the ability of other users to benefit from the security of the same system. Similarly, the security from a Cyber attack enjoyed by one individual does not detract from the security enjoyed by another individual. Further, protecting the digital rights, patents, copyrights, and trademarks of one group of professionals should not diminish the same rights to another group of professionals. Cybersecurity is also non-excludable, because individual users of a secure system cannot be easily excluded from benefits that this security brings. For example, if the government enhances security measures against a cyber attack, everyone will be able to benefit from these measures" (COOTER, R. D. y SIEGEL, N.S., "Collective action federalism: A general theory of article I, section 8", *Stanford Law Review*, vol. 63, nº 1, 2010, 112-185).

[9] ASLLANI, A., WHITE, Ch. S. y ETTKIN, L., "Viewing Cybersecurity As A Public Good: The Role Of Governments, Businesses, And Individuals", *Journal of Legal, Ethical and Regulatory Issues*, vol. 16, nº 1, 2013, 7-14, en concreto, pg. 9.

[10] En efecto, "Approaching cybersecurity as a public good represents a sensitive starting point toward creating an appropriate legal framework. It justifies the role of federal, state, and local governments to implement policies and initiatives that improve the cybersecurity of individuals and organisations" (ASLLANI, A., WHITE, Ch. S. y ETTKIN, L., "Viewing Cybersecurity As A Public Good: The Role Of Governments, Business, And Individuals", *Journal of Legal, Ethical and Regulatory Issues*, vol. 16, nº 1, 2013, 7-4, en concreto, pg. 9). Sobre la definición de un sistema público de seguridad cibernética siguiendo el modelo sanitario pueden verse: ROWE, J., LEVITT, K. y HOGARTH, M., "Towards the Realization of a Public Health Model for Shared Secure Cyber-Space", *Conference: Proceedings of the 2013 workshop on New security paradigms workshop*. DOI: 10.1145/2535813.2535815.

[11] Como explica Molina Mateos, "Tal vez el Derecho tenga ya asumido como bienes dignos de protección jurídica muchos de los elementos materiales e inmateriales que componen el Ciberespacio, como es el caso de la información, la tecnología o ciertas relaciones humanas, pero no lo hace con el conjunto como realidad autónoma a pesar de que, desde todas las perspectivas, es reconocido como un activo indiscutible para la humanidad que demanda ser protegido legalmente (MOLINA MATEOS, J.M., "Aproximación jurídica al ciberespacio", *Boletín Electrónico del Instituto español de Estudios Estratégicos*, Documento de análisis 57/2015, 08 de junio de 2015, 1-20, en concreto, pg. 7).

[12] Sobre esas diferentes aproximaciones convencionales y no convencionales y apostando por el principio "Regulatory Problems, Regulatory Solutions", véase SALES, M.A., "Regulating Cyber-Security", *Northwestern University Law Review*, vol. 107, nº 4, 2013, 1503-1568.

El régimen jurídico del ciberespacio no se agota en la ciberseguridad. Operar con esa pretendida identidad sería reducir el derecho a un derecho a/de la seguridad. El ciberderecho no se limita a la ciberseguridad y la ciberseguridad solo es un sector dentro de aquel conjunto más amplio y heterogéneo. Aunque el ciberespacio sea calificado como bien público, el ciberderecho está formado por un derecho público y un derecho privado, mientras que la ciberseguridad es esencialmente una cuestión pública, como lo es la seguridad ciudadana y la seguridad nacional[13]. La ciberseguridad muestra, además, algunas otras particularidades propias manifestándose como fenómeno multidimensional.

La ciberseguridad: un fenómeno multidimensional

El ciberespacio es un dominio caracterizado por su artificialidad, relativa inmaterialidad y permeabilidad, capilaridad o transversalidad. Esos caracteres, junto con lo que se ha denominado su esencia, esto es, su capacidad para alterar el resto de las realidades, hacen que la seguridad en el ciberespacio o la ciberseguridad sean un problema, asimismo, como el propio ciberespacio, capilar y transversal, pero que dista mucho de ser un problema artificial o inmaterial.

La ciberseguridad no es sólo la seguridad del ciberespacio entendido como un espacio más y, en consecuencia, no puede comprenderse como tal mediante una extrapolación mecánica de los parámetros tradicionales que han operado en los otros dominios como la seguridad territorial, marítima, aérea o medioambiental. La ciberseguridad implica un nuevo paradigma de seguridad global, inclusiva y comprehensiva de la totalidad de los escenarios que se van a ver afectados por la impronta que introduce la existencia y la utilización del ciberespacio.

[13] Ello no implica una traslación automática de los esquemas de funcionamiento de las políticas públicas tradicionales, sino su adaptación al ciberespacio. Sales hace una interesante propuesta de partenariado público-privado en los siguientes términos: «All private firms might be asked to provide a baseline level of cyber-security-modestly effective (and modestly expensive) defenses that are capable of thwarting intrusions by adversaries of low to medium sophistication. The government would then assume responsibility for defending public utilities and other sensitive enterprises against catastrophic attacks by foreign militaries and other highly sophisticated adversaries. This division of labor —basic security provided by firms, supplemental security provided by the government— is in a sense the opposite of what we see in realspace criminal law. In realspace, the government offers all citizens a baseline level of protection against criminals in the form of police officers, prosecutors, and courts. Individuals may supplement these protections at their own expense, such as by installing alarm systems in their homes or hiring private security guards. This arrangement also is consistent with our intuitions about the respective roles of government and the private sector in times of conflict. Consider another realspace analogy: in World War II, factories were not expected to install anti-aircraft batteries to defend themselves against Luftwaffe bombers. Nor should we expect power plants to defend themselves against foreign governments' cyber-attacks. Protecting vital national assets from destruction by foreign militaries is a quintessential, perhaps *the* quintessential, government function» (SALES, M.A., "Regulating Cyber-Security", *Northwestern University Law Review*, vol. 107, nº 4, 2013, 1503-1568, en concreto, pg. 1518).

En realidad, el concepto de seguridad puede ser calificado como la categoría que ha sufrido una mayor evolución en cuanto a su alcance, naturaleza y contenido en términos sociológicos, jurídicos y políticos desde el final de la II Guerra Mundial hasta la actualidad. En esa evolución, el concepto clásico de seguridad vinculado a la existencia, independencia e integridad territorial del Estado ha coexistido con otros paradigmas de seguridad, que se han adicionado a aquel primero con objeto de dotarlo de un contenido material más amplio —seguridad económica, seguridad ideológica, seguridad alimentaria o seguridad medioambiental, entre otras— y más adaptado a la realidad contemporánea o que, directamente, han aspirado a sustituirlo como ocurre con el concepto de seguridad humana[14].

El ciberespacio impone un nuevo paradigma de seguridad que encaja directamente en el propósito y el efecto de sustitución, característico de la fórmula «seguridad humana», más que en el modelo de ampliación material del objeto y los contenidos de la seguridad. Pero, con una apreciable y significativa diferencia: la ciberseguridad se está imponiendo, más que como una opción, por la fuerza de los hechos o por un principio de efectividad, mientras que la seguridad humana se ha movido, más y generalmente, en el plano de los ideales que en el de las realidades. Es un prototipo de seguridad que no se adiciona, como un componente más, al modelo existente sino que está llamado a sustituirlo y debe ser capacitado a esos efectos en la medida en que ya lo está transversalizando, modificando sus parámetros funcionales y afectando a los estructurales hasta el punto de que no cabe ya hablar de un modelo de seguridad sin ciberseguridad porque esta constituye, como el propio ciberespacio, un fenómeno multidimensional en lo económico, lo social y lo jurídico.

En efecto, el ciberespacio incorpora un nuevo *modelo económico*, la llamada Economía del Conocimiento[15], característica de la era de la globalización y articulada sobre la base de las TIC, que se superpone y transversaliza a los anteriores[16]. Si el modelo económico de la

[14] En este caso, «La búsqueda de un modelo de seguridad común y comprensiva, multidimensional e interdependiente, integradora y globalizadora, propugnado desde diversas corrientes doctrinales de pensamiento, conduce a la formulación de un nuevo concepto, la seguridad humana, con vocación de sustituir al anterior basándose en el axioma de que la persona, y no el Estado, es el sujeto último de la seguridad. Los pilares esenciales de la seguridad humana son la ausencia de amenazas —peligros vitales— la ausencia de necesidades —vulnerabilidades sociales— y la ausencia, en la medida de lo posible, de desastres naturales con consecuencias sociales devastadoras. La seguridad humana traduce libertad respecto de las necesidades básicas y libertad respecto a los miedos» (ROBLES CARRILLO, M., "La integración de la perspectiva de género en el análisis de los conflictos armados y la seguridad", *Cuadernos de Estrategia*, nº 157, 2012, 53-88, en concreto, 66). Véase, asimismo, KRAUSE, K. y WILLIAMS, M.C., *Critical Security Studies*, Londres, UCL Press, 1997, 43-45.

[15] Ese modelo se plasma en la Estrategia de Lisboa adoptada en 2000 por la UE con el objetivo de convertir a la UE en la economía basada en el conocimiento más competitiva y dinámica del mundo. Sobre la cuestión, puede verse ROBLES CARRILLO, M. "La reactivación de la Estrategia de Lisboa", *Revista Española de Derecho Europeo*, nº 16, 2005, 497-546.

[16] Para un sobresaliente análisis de la problemática estructural que plantea el ciberespacio en los ámbitos económicos, industriales, tecnológicos y sociales, véase DE SALVADOR CARRASCO, L., "Los problemas estructurales en el planteamiento de la ciberseguridad", *Boletín Electrónico del Instituto español de Estudios*

sociedad de servicios asume un papel protagónico y relega progresivamente al modelo industrial que, a su vez, había hecho lo propio con el modelo de la sociedad rural, la economía del conocimiento no se limita a desplazar a sus predecesores, sino que interfiere directamente en ellos modificando sus parámetros de organización y funcionamiento. No solo es un sector más que se adiciona a los anteriores sino que, sobre todo, altera sus dinámicas estructurales y funcionales[17]. El concepto mismo de ciberseguridad no es, ni puede ser, ajeno a las necesidades de *segurización* de ese sistema económico porque también a esas exigencias ha de dar respuesta el modelo de ciberseguridad.

El ciberespacio introduce también un nuevo *modelo socio-político*, la Sociedad del Conocimiento, interconectado y global en el que destaca el principio de diversidad como categoría conceptual y como realidad, que aparece sublimada con todas sus consecuencias positivas y negativas con lo que ello implica, en términos muy básicos, para la mera coexistencia social. La internacionalización de la vida social y la globalización han dado una mayor visibilidad a ese fenómeno que, siendo lógico y natural, no era tan potencial y realmente conflictivo cuando la estructura socio-política y territorial del Estado ofrecía una protección primaria básica a la diversidad cultural, religiosa, étnica, política o social y, sobre todo, controlaba o limitaba sus efectos negativos.

La organización y gestión de esa diversidad intensa y plural es imprescindible para garantizar la coexistencia y la convivencia social, pero es más compleja en el ciberespacio por dos motivos: porque se produce, primero, una extrapolación a la globalidad ciberespacial de esas múltiples diversidades particulares y porque, en segundo lugar, esa eclosión es naturalmente mayor por el tamaño, impacto e intensidad de los contrastes entre esas diversidades y particularismos. Con anterioridad, el conflicto intercultural estaba relativamente localizado en términos de espacio, tiempo o contenidos[18], pero en el ciberespacio se universaliza, multiplica y radicaliza con consecuencias no siempre previsibles. El caso Charlie Hebdo es un ejemplo dramático en ese sentido porque el atentado en Francia fue seguido de sucesivos actos de represalia contra cristianos y musulmanes en distintos lugares del mundo, mientras que, en varios países, incluida Turquía, se bloquearon por decisión judicial las webs en cuestión. La capacidad de proyección en el espacio y en el tiempo universaliza los hechos y multiplica sus efectos perversos evidenciando el alcance de la diversidad y su difícil

Estratégicos, Documento de análisis 09/2014, 03 de julio de 2014, 1-27.

[17] Aunque no parece necesario citar ejemplos, por tratarse de un fenómeno sobradamente conocido, no está de más mencionar dos casos distintos inmersos igualmente en esa dinámica como son los sectores agrícola y bancario. En el primero, no son iguales la estructura y el funcionamiento de una empresa agrícola antes y después de la incorporación de las TIC aunque solo sea por el hecho de que publicita y vende sus productos a través de Internet, se amplía su mercado y cambian las reglas de competencia. Tampoco es igual la prestación de servicios, por ejemplo, en el sector bancario. El modelo de negocio tradicional centrado en torno a la relación del cliente con su sucursal se está viendo sustituido a un ritmo imparable por la fórmula del *eBanking*.

[18] El conflicto intercultural era el resultado, generalmente, de situaciones muy localizadas como el fenómeno de la inmigración o temporales o excepcionales como las misiones internacionales realizadas en determinados países terceros.

coexistencia en el ciberespacio. En un contexto completamente distinto, ya hace tiempo, también el caso Yahoo fue un exponente claro de la eclosión del conflicto de la diversidad que implica el ciberespacio cuando enfrenta la defensa de la libertad de expresión, amparada en la Primera Enmienda estadounidense, con la prohibición de la apología del nazismo establecida en Francia. En el conflicto normativo sobre la posibilidad o no de aplicación extraterritorial de las normas subyace la diversidad de concepciones socio-históricas, políticas y culturales que justifica la diferencia entre la norma estadounidense y la europea[19].

En definitiva, los cambios en el modelo económico global y, sobre todo, en los patrones sociales, políticos y culturales, por el mero hecho de que han de funcionar en esa convivencia obligada que impone el ciberespacio, obligan a una reflexión de fondo sobre el propio *modelo jurídico* en el entendimiento de que el derecho ha de ser el instrumento de ordenación de esa vida social que se muestra diferente en este sistema global. Hay un segundo argumento que conduce a la misma conclusión: los cambios en los parámetros tradicionales de organización jurídico-política derivados de la superación del marco estatal que implica el ciberespacio. Son cambios que, en el plano teórico, afectan a componentes básicos de la estructura jurídica, como el marco de aplicación de la legislación estatal y el ámbito de ejercicio de la jurisdicción del Estado, y que, en la práctica, resultan necesarios y urgentes ante la alarmante combinación de crecimiento de la criminalidad y de persistencia de la impunidad en el ciberespacio.

UN MODELO JURÍDICO PARA EL CIBERESPACIO

Un cambio de paradigma

El ciberespacio impone, junto con los cambios económicos o sociales, la necesidad de reorganizar el *modelo jurídico* para ordenar esta realidad difícilmente aprehensible con los esquemas tradicionales de organización del derecho en torno al Estado. No se trata únicamente de un debate sobre la traslación de las normas del espacio físico al virtual o sobre la creación de normas específicas para conformar un ciberderecho.

El modelo jurídico en vigor, haciendo abstracción de sus especificidades regionales, funcionales y sistémicas, se construye sobre el concepto de Estado como categoría jurídico-política que determina el ámbito de aplicación de la legislación y de ejercicio de la jurisdicción resultantes de su poder soberano, compartimentando el conjunto de la sociedad internacional y organizando la convivencia entre esos sujetos estatales a través de las

[19] Como es sabido, los Estados miembros del Consejo de Europa y los demás Estados Partes en el Convenio sobre la Ciberdelincuencia, abierto a la firma en Budapest el 23 de noviembre de 2001, hubieron de redactar en 2003 un Protocolo adicional al Convenio sobre la ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos porque Estados Unidos no habría dado su consentimiento al Convenio de Budapest de haber estado incluidos en dicho tratado.

normas de Derecho internacional público. Legislación y jurisdicción están territorial y personalmente limitadas dentro de la esfera de las competencias estatales[20]. El Derecho internacional constituye una garantía del respeto de esas competencias y ofrece mecanismos para la posible solución de los conflictos competenciales, pero no establece reglas definitivas y generalmente aceptadas en materia de distribución horizontal de competencias entre los Estados sobre legislación o jurisdicción. Esta es la situación de estructuración y funcionamiento molecular del derecho antes de la aparición del ciberespacio, pero cambia necesariamente, después, con su evolución y desarrollo.

En ese contexto, la prioridad estriba en determinar el alcance de las competencias del Estado en el ciberespacio y en establecer mecanismos operativos y eficaces de solución de los conflictos positivos o negativos de competencias que puedan surgir en el marco de ejercicio de las actividades ciberespaciales. No hay que olvidar que, aunque las competencias de un Estado siempre han tenido como límite las competencias de los demás, el ciberespacio implica un cambio de paradigma a esos efectos por tres razones principales: una, impone límites diferentes al ejercicio de dichas competencias; dos, comporta obstáculos al ejercicio legítimo de las propias; y, tres, definitivamente, crea un escenario distinto del que se ha conocido hasta ahora, que se caracterizaba por la presencia de núcleos competenciales estatales relativamente autónomos en el ejercicio de la legislación y la jurisdicción y con normas internacionales de solución de los conflictos competenciales y no, en sentido estricto, normas de «ordenación» o «imposición» de la distribución competencial misma a nivel internacional. No es igual ordenar o racionalizar un ámbito material determinado que limitarse, en el buen sentido, a ofrecer reglas para resolver los conflictos que puedan aparecer en el mismo, como se ha hecho hasta ahora desde el ordenamiento jurídico internacional[21]. Ni en el Derecho internacional se ha consensuado aún el *corpus* jurídico aplicable, ni la concurrencia de ordenamientos internos es una fórmula válida como instrumento de ordenación, regulación y, en definitiva, racionalización que es la función que el derecho ha de cumplir en el ciberespacio. Ni siquiera la intervención misma del derecho internacional —en su alcance y en su contenido— en el ciberespacio ha sido aún objeto de consenso.

Las consecuencias son mayores de lo que aparentemente podría pensarse. Como advierte Sales, «The poor state of America's cyber-defenses is partly due to the fact that the analytical framework used to understand the problem is incomplete. The law and policy of cyber-security are undertheorized. Virtually all legal scholarship approaches cyber-security from the standpoint of the criminal law or the law of armed conflict. Given these analytical

[20] Como explica Shackelford, «cyberspace has eroded the connection between territory and sovereignty» (SHACKELFORD, S.J.,"From Nuclear War to Net War: Analogizing Cyber Attacks in International Law", *Berkeley Journal of International Law*, vol. 27, nº1, 2009, 191-251, en concreto, pg. 214).

[21] RABOIN, B., «Corresponding Evolution: International Law and the Emergence of Cyber Warfare», *Journal of the National association of Administrative Law Judiciary*, vol. 31, nº 2, 2011, 601-668, en concreto, pgs. 64 y ss.

commitments, it is inevitable that academics and lawmakers will tend to favor law enforcement and military solutions to cyber-security problems. These are important perspectives, but cyber-security scholarship need not run in such narrow channels. An entirely new approach is needed»[22].

La ordenación jurídica del ciberespacio no es una necesidad. Es un imperativo[23]. No se trata solo de aplicar analógicamente el derecho creado para el mundo físico porque en muchos casos es factible, pero también en muchos otros esa fórmula no resulta válida. El crecimiento exponencial de la cibercriminalidad es una señal de alarma en esa dirección, como también lo es el alarmante incremento de la impunidad en el ciberespacio. Dos motivos más que suficientes para enfrentarse al dilema y al desafío jurídico que implica el ciberespacio.

El dilema del iceberg

El ciberespacio es, ante todo y a pesar de su reconocida pero relativa inmaterialidad, una realidad cuantificable en datos. Las estadísticas oficiales ofrecen, con preocupante periodicidad, resultados sobre la actividad ilícita en el ciberespacio que, en un balance global, permiten llegar a una doble y aparentemente contradictoria conclusión: por una parte, una coincidencia generalizada cuando se trata de constatar el aumento cuantitativo y cualitativo y este, en concreto, en el sentido tanto de diversificación, como de especialización de la criminalidad cibernética; y, en segundo lugar, una falta de sincronía cuando se trata de especificar los resultados concretos sobre el origen, las modalidades, el alcance y la naturaleza precisa de dicha actividad más allá de su calificativo genérico como ciberdelincuencia[24]. En cierta medida, ello se explica por lo que cabría denominar el dilema del iceberg, que solo permite apreciar una parte del problema y de su realidad y que, en el marco de la ciberseguridad, viene propiciado además por la combinación de una doble circunstancia:

- La presencia de lo que cabría denominar quizás eufemísticamente el «microdelito», esto es, una actividad delictiva destinada a la obtención de un beneficio económico, dirigida a una multitud de víctimas y traducida en un perjuicio económico mínimo para cada una de ellas, por separado, razón por la cual generalmente no es objeto de denuncia, pero sí puede serlo de enormes beneficios. Un perjuicio económico individual de escasa cuantía

[22] SALES, M.A., "Regulating Cyber-Security", *Northwestern University Law Review*, vol. 107, nº 4, 2013, 1503-1568, en concreto, pg. 1507.

[23] GÓMEZ DE ÁGREDA, A., "Ciberdespacio", *Boletín Electrónico del Instituto español de Estudios Estratégicos*, Documento de análisis 57/2013, 19 de junio de 2013, 1-9.

[24] Así, «El principal problema es definir e identificar en su caso si es ciberguerra, ciberespionaje o ciberterrorismo cuando se produce una ciberagresión. Es muy difícil identificar al agresor y decidir si se trata de una acción de guerra (*casus belli*), de un acto de terrorismo o de una acción criminal» (FELIU ORTEGA, L., "La ciberseguridad y la ciberdefensa", *El ciberespacio. Nuevo escenario de confrontación*, Monografías del CESEDEN, nº 126, febrero 2012, 32-65, en concreto, pg. 529).

combinado con una pluralidad de víctimas se convierte en una garantía de rentabilidad económica y de una alta probabilidad de impunidad, esto es, un crimen prácticamente perfecto o, cuando menos, cercano a la perfección por los altos beneficios y los escasos riesgos.

- La singularidad de lo que podría denominarse «macrodelincuencia» —más por oposición o diferenciación respecto del caso anterior y por sus propias víctimas que por la precisión misma del concepto— dirigida a grandes sociedades, empresas, entidades o marcas que, siendo damnificadas, acaban por no denunciar para evitar la pérdida de prestigio que supondría la difusión de sus brechas de seguridad y las afectaciones económicas directas y colaterales y, en su caso, no hay que excluirlo, para eludir las eventuales responsabilidades que pudieran derivarse de la insuficiente o deficiente protección que no ha permitido neutralizar la actividad cibercriminal.

Pero el dilema del iceberg solo es un componente más, y no necesariamente el principal, de lo que cabría denominar el desafío jurídico del ciberespacio.

El desafío jurídico

El ciberespacio modifica los parámetros tradicionales de comprensión de la actividad delictiva y de su prevención, persecución, represión o sanción desde el punto de vista jurídico, no solo por las cuestiones relativas a la determinación de la legislación y la jurisdicción aplicables, sino también por el problema que plantea la calificación de la legalidad o ilegalidad de las actividades ciberespaciales. Lo que es ilícito en un sitio puede no serlo en otro o a la inversa pero, siendo ello hasta cierto punto lógico y comprensible, no se materializa igual que en el espacio físico, principalmente, por tres motivos: uno, por el alcance y la intensidad de la interconexión dentro del ciberespacio; dos, por su capilaridad con el mundo físico; y, tres, por la capacidad de proyección en el tiempo y el espacio de las acciones cibernéticas. En el mundo físico, la identificación de la naturaleza y la calificación del ilícito plantean en términos generales una mayor simplicidad, tanto por las propias características del ilícito como por las del medio en el que opera, pero no ocurre igual en el ciberespacio.

La determinación del ilícito depende de la combinación de dos variables fundamentales: uno, el contenido mismo y la naturaleza del hecho y, dos, la legislación aplicable que, a su vez, une al elemento estrictamente normativo el componente axiológico, entendiendo dentro de esa categoría el conjunto de las tradiciones sociales, políticas, culturales, étnicas, religiosas o de cualquier otra índole que determinan el sentido de la norma jurídica en cada caso[25]. Un mismo hecho puede ser o no ser ilícito dependiendo de la legislación del Estado

[25] Dos ejemplos ilustrativos: el contenido material de una maternidad subrogada o el diseño de una viñeta con una caricatura son idénticos en cualquier sitio pero la realización de esos hechos supondrá o no un ilícito en función de la legislación de cada Estado.

de manera que quien está sometido a su legislación y jurisdicción puede conocer la legalidad o ilegalidad de sus acciones y actuar en consecuencia, incluso, cuando trasciende la frontera del Estado en la medida en que se encuentra sometido a la competencia personal del propio Estado y a la territorial del Estado de localización.

Esta dinámica no es realmente extrapolable al ciberespacio por sus mismas características estructurales y funcionales y por la propia proyección potencialmente ilimitada en el espacio y en el tiempo de las acciones ciberespaciales. Simplemente, el hecho lícito realizado por un sujeto en origen puede convertirse en un ilícito en su trayectoria y en su destino[26]. En sentido contrario, un acto puede ser ilícito en origen y legal o permisible en su destino[27].

Los elementos constitutivos del ilícito tampoco han de ser necesariamente los mismos. En el ordenamiento jurídico internacional, el hecho ilícito se compone de un elemento objetivo —la violación de una obligación internacional— y de otro subjetivo —la atribución de ese hecho a un sujeto de derecho internacional—, sin necesidad de incorporar los componentes de intencionalidad (culpa o dolo) o daño (la violación misma de la obligación constituye un daño). El ilícito civil y el ilícito penal responden a una construcción diferente que, además, es también diferente en los distintos ordenamientos jurídicos, lo que complica doblemente la determinación de la licitud o ilicitud de los hechos.

En términos generales, al tratarse de un espacio global, los hechos del ciberespacio pueden catalogarse dentro de algunas categorías genéricas: ilícitos internacionales o internos y, dentro de ellos, ilícitos civiles o penales. El contenido del ilícito internacional se determina en función de las obligaciones asumidas internacionalmente por los Estados pero, en el derecho interno, la determinación de la ilicitud depende de la legislación de cada Estado. Un hecho puede ser simultáneamente lícito e ilícito como consecuencia de la pluralidad de ordenamientos intervinientes en el ciberespacio, por la inexistencia de un único régimen jurídico y por la alteración que impone esta realidad en el funcionamiento y puede que hasta en la esencia misma del derecho.

En realidad, por esa combinación de circunstancias, el ciberespacio puede suponer la modificación de la calificación de un acto como legal o ilegal y sacralizar esa situación anómala en la medida en que puede permanecer de modo indefinido en el espacio global con esa calificación dual y contradictoria. Pero si esta segunda variable, aunque relativamente comprensible por las diferencias lógicas existentes entre las legislaciones de los Estados, puede introducir disfunciones en la ordenación jurídica del ciberespacio, con la primera, el contenido y naturaleza del acto, la situación también es compleja.

[26] Lamentablemente conocidas son las consecuencias, por ejemplo, de realizar una viñeta con una caricatura que, siendo un acto lícito de conformidad con la legislación del Estado donde se realiza, constituye un ilícito en muchos otros Estados en donde se proyecta gracias a la globalización que implica el ciberespacio.
[27] Los límites impuestos al ejercicio de la libertad de expresión o de la libertad religiosa pueden hacer ilícita una acción en origen que, sin embargo, es perfectamente legal en los países de destino.

El problema de la calificación

En principio, hay que distinguir tres grandes categorías de actos: una primera formada por aquellos hechos delictivos que no tienen, por el momento, posibilidad de proyectarse en el ciberespacio (la autoría material de un asesinato o una violación); una segunda incluye los actos ilícitos que reproducen o resultan equiparables a sus homólogos del mundo físico (fraude o estafa); y una tercera, potencialmente más complicada por sus consecuencias desde una perspectiva jurídica, que engloba los actos que no admiten una adscripción automática dentro de una categoría en atención exclusivamente a su contenido y naturaleza.

En principio, este problema se manifiesta esencialmente respecto del ilícito penal. En el ámbito civil se exige la «intencionalidad» en la comisión del acto contrario a derecho, además de la causación de un daño. Esa exigencia permite discriminar los hechos lícitos de aquellos supuestos en los que se trata de un ilícito porque, en estos casos, debe existir la intención de contrariar la legalidad. En cambio, en lo penal, el ilícito está definido y castigado como tal legalmente, su existencia no depende de la intención del autor, aunque esta pueda servir para la modulación de la responsabilidad o para la categorización del delito, según se defina como doloso o culposo, y tampoco se requiere la producción de un daño, como demuestra la penalización de la tentativa. La no exigencia de «intencionalidad» como elemento constitutivo del hecho ilícito penal, junto con el principio básico de que el desconocimiento de la ley no exime de su cumplimiento, supone que es, en este marco, donde aparece con mayor nitidez el problema de la calificación de los actos cibernéticos como actos lícitos o ilícitos.

En efecto, materialmente, un mismo hecho puede o no constituir un acto lícito y, si es ilícito, puede ser considerado delito, espionaje, terrorismo o, incluso, una acción bélica. Un ciberataque, por sí mismo, no admite necesariamente una única y definitiva calificación. El contenido y la naturaleza del acto cibernético no determina esa calificación, sino que un mismo hecho es susceptible de ser catalogado como un acto legal o como un delito o un acto de espionaje, terrorista o bélico en función de cuatro variables principales: el autor, el destinatario, la intención y los efectos.

En un artículo titulado «Hacktivism: Cyber Activisme or Cyber Crime?», George O'Malley subraya la necesidad de diferenciar entre los conceptos de *hacker* y de *hacktivist* indicando que «in contrast to a malicious hacker who hacks a computer with the intent to steal private information or cause other harm, hacktivists engage in similar forms of disruptive activities to highlight political or social causes. For the hacktivist, hacktivism is an Internet-enabled strategy to exercise civil disobedience»[28]. En su opinión, «Legitimate hacktivism should not

[28] O'MALLEY, G., "Hacktivism: Cyber Activisme or Cyber Crime?", *Trinity College Law Review*, vol. 16, 2013, 137-

be associated with criminal behaviour»[29]. El autor analiza varias modalidades de ciberataque y, dentro de ellas, las que podrían ser consideradas lícitas o ilícitas.

Sin entrar en un análisis pormenorizado[30], que excedería el propósito de este trabajo, la obtención de información puede ser una actividad perfectamente lícita o, por el contrario, una actividad de espionaje, delictiva, terrorista o bélica[31], en función de las circunstancias que impone el contexto, la autoría, la intención o sus efectos. Un ataque de Denegación de Servicio (DoS) podría ser, efectivamente, un acto legítimo de protesta o un acto ilegal que puede ser un acto delictivo o de otra naturaleza en función de aquellas coordinadas. Un ataque de Denegación Distribuida de Servicio (DDoS) no admitiría la calificación de lícito si, en su realización, utiliza redes o sistemas sin el conocimiento de sus propietarios o responsables. Un ataque de desfiguración de sitios web (Website Defacement) también podría ser un delito, un acto terrorista o bélico en función de cuáles sean los autores, la intención y los efectos. Hay técnicas como el *phishing*, el *sniffing* o el *spaming* o los *botnets* que, por su propia naturaleza, no admitirían la definición como actos lícitos pero, dentro de su ilicitud, no siempre es fácil su calificación en una determinada categoría.

En el mundo solo físico, los actos pueden ser objeto de un proceso de adscripción relativamente sencillo y, en cualquier caso, suficientemente experimentado y contrastado, que permite calificar un hecho ilícito dentro de categorías también relativamente precisas —acto criminal, acto terrorista, acto de espionaje o acto de guerra— definidas sobre la base del contenido material del acto y encajadas en conceptos jurídico-políticos consolidados como la idea de seguridad pública y ciudadana, seguridad y defensa nacional o la definición del estado de guerra o de la situación de paz. En cambio, en el mundo cibernético, el virtual y el físico transversalizado por el anterior, no cabe operar con esas mismas categorías y en los mismos términos y un hecho puede ser calificado de diferente forma en función del sujeto, la intención y los efectos[32].

160, en concreto, pg. 140.

[29] Según el autor, "It is submitted that forms of hacktivism which: 1) are expressive in nature, 2) are performed without anonymity, with actors willing to take responsibility, 3) have a legitimate purpose, 4) proportionately balances the damage or disruption with the benefits to be achieved, and 5) are non-violent, should receive protection as a legitimate form of protest under the protection of freedom of expresión" (O'MALLEY, G., "Hacktivism: Cyber Activisme or Cyber Crime?", *Trinity College Law Review*, vol. 16, 2013, 137-160, en concreto, pgs. 158 y 160).

[30] Para una ilustrativa exposición de las amenazas, incluyendo su adscripción a categorías delictivas, véase PÉREZ CORTÉS, M., "Tecnologías para la defensa en el ciberespacio", *El ciberespacio. Nuevo escenario de confrontación*, Monografías del CESEDEN, nº 126, febrero 2012, 242-306, en concreto, pg. 265-275.

[31] Para una definición de estas actividades, véanse URUEÑA CENTENO, F.J., "Ciberataques, la mayor amenaza actual", *Boletín Electrónico del Instituto español de Estudios Estratégicos*, Documento de análisis 09/2015, 16 de enero de 2015, 1-18; SÁNCHEZ MEDERO, G., "Cibercrimen, ciberterrorismo y ciberguerra: los nuevos desafíos del siglo XX", *Revista CENIPEC*, vol. 31, 2012, 241-267.

[32] Shackelford ejemplifica con el caso Estonia la dificultad de calificar los ciberataques como cibercrimen, ciberterrorismo o ciberguerra (SHACKELFORD, S.J.,"From Nuclear War to Net War: Analogizing Cyber Attacks in International Law", *Berkeley Journal of International Law*, vol. 27, nº1, 2009, 191-251, en concreto, pgs. 232-

Esta situación resulta especialmente problemática cuando se trata de calificar ciberataques que pueden atentar contra la seguridad pública o ciudadana o ir más allá y afectar a la propia seguridad nacional, exigiendo una respuesta en términos de defensa nacional. En esos supuestos, la calificación resulta esencial porque la reacción en cada caso habría de ser diferente si se opera desde el modelo convencional y dominante de gestión de la seguridad que opera sobre dos parámetros fundamentales a esos efectos: la distinción entre el estado de guerra y la situación de paz y la diferenciación de las funciones constitucionales de las Fuerzas y Cuerpos de Seguridad del Estado y de las Fuerzas Armadas respecto de cada una de esas situaciones.

La superación del modelo tradicional de guerra y la generación de nuevas modalidades de conflicto no convencionales, como la guerra híbrida o asimétrica[33], se suman a la potencialidad que ofrece el ciberespacio para que un único sujeto, desde cualquier lugar y con escasos medios pueda llegar a alcanzar una capacidad delictiva e, incluso, destructiva inimaginable en el mundo precibernético[34]. Sin entrar en otros ejemplos, simplemente un ataque a una infraestructura crítica puede afectar a la seguridad pública pero también a la propia seguridad nacional y exigir una respuesta en términos de defensa nacional. La frontera entre seguridad pública y seguridad nacional se difumina en el mundo cibernético cuando cualquier acto puede ser una amenaza a la primera, a la segunda o a ambas. Ni los modelos tradicionales de seguridad, ni las formas convencionales de disuasión, ni siquiera las medidas de distensión, pueden resultar operativos ante esta multiplicación y diversificación de la amenaza[35]. Hay una atomización del riesgo y lo que se ha denominado

---

233).

[33] Sobre la guerra híbrida, SÁNCHEZ HERRÁEZ, P. "La nueva guerra híbrida: un somero análisis estratégico", *Boletín Electrónico del Instituto español de Estudios Estratégicos*, Documento de análisis 54/2014, 29 de octubre de 2014, 1-16.

[34] Como sostiene certeramente Raboin, «the emergence of Cyber warfare is more than just another evolutionary step in the development of wartime strategy and methodology; instead, they argue that it represents a fundamental transformation in the very nature of the concept of war itself. The notion that cyber warfare will alter the inherent nature of war is ultimately rooted in the conceptual idea that cyber warfare does not merely change the weaponry of modem wars, but that it represents a radical shift in the nature of the wartime battlefield. Whereas every historical evolution of warfare has occurred within the common sphere of the physical, tangible world, cyber warfare redefines the central wartime battlefield. Yet, the consequences of actions within this new Cyber warfare battlefield are unique because although they occur in the intangible domain of computer networks and information streams, the effects of the actions taken within that domain have very "real" effects in the physical world of our everyday reality» (RABOIN, B., "Corresponding Evolution: International Law and the Emergence of Cyber Warfare", *Journal of the National association of Administrative Law Judiciary*, vol. 31, nº 2, 2011, 601-668, en concreto, pg. 604).

[35] Gómez de Ágreda advierte que el ciberespacio «vive en un *estado permanente de agresión* en el que todos los usuarios, sea cual sea su nivel, son susceptibles de recibir ataques con relativa independencia de su grado de protección». En su opinión, el efecto igualador que ejerce el ciberespacio sobre sus usuarios «amplía hasta el infinito el número de agresores potenciales mientras que las dificultades en la trazabilidad en tiempo real (o, al menos, útil) de dichos ataques hace que sus autores sean *relativamente invulnerables a medidas disuasorias*» (GÓMEZ DE ÁGREDA, A., "El ciberespacio como escenario de conflictos. Identificación de las

una afganización del ciberespacio[36], donde coexisten burbujas de seguridad y de insurgencia, que cambian los parámetros de organización y gestión de la seguridad[37]. La capacidad de reacción del Estado ha de adecuarse a esa situación atenazada, además, por la impronta del factor tiempo característica del ciberespacio y por el problema adicional de la trazabilidad que contribuyen a extremar la vulnerabilidad. El ciberataque suele requerir, por definición, una respuesta rápida, si no inmediata, y el principio de resiliencia entendido en términos genéricos como la capacidad de neutralizar, restaurar y reaccionar se sitúa, por ello, en el núcleo de cualquier sistema de seguridad cibernética. La cuestión estriba en determinar a quién corresponderá la respuesta y cómo se articulará si con el ciberespacio se difuminan las fronteras entre seguridad pública y seguridad nacional afectando a la distribución tradicional de funciones entre Fuerzas y Cuerpos de Seguridad del Estado y Fuerzas Armadas.

CONCLUSIONES

El ciberespacio es una realidad diferente del espacio físico en el que había operado el derecho desde sus remotos orígenes con la aparición de las primeras normas dirigidas a garantizar una mínima coexistencia en sociedad. Pero es, además, una realidad que intersecta el mundo físico, alterando esa realidad previa, interactuando con ella y modificando tanto su naturaleza como la percepción de la misma. El derecho es, por su parte, un instrumento de ordenación de la vida social cuya eficacia es directamente proporcional a su capacidad de responder a las exigencias que impone la realidad que está llamado a ordenar.

Con este punto de partida, el modelo jurídico del ciberespacio no se puede construir mediante una mera o mecánica extrapolación de las reglas existentes en el espacio no virtual. Ese opción, que parece imponerse en la práctica, presenta una doble debilidad porque ese derecho difícilmente puede ser operativo en el marco ciberespacial que es esencialmente diferente y porque, posiblemente también, se haya minorado su efectividad en el mundo físico porque este ha cambiado significativamente con la aparición de la realidad virtual.

---

amenazas", *El ciberespacio. Nuevo escenario de confrontación*, Monografías del CESEDEN, nº 126, febrero 2012, 160-195, en concreto, pg. 180).

[36] ENRÍQUEZ GONZÁLEZ, C., "Estrategias internacionales para el ciberespacio", *El ciberespacio. Nuevo escenario de confrontación*, Monografías del CESEDEN, nº 126, febrero 2012, 66-116, en concreto, pg. 114.

[37] En efecto, «El ciberespacio rompe, de alguna manera, el monopolio estatal sobre la violencia. Digo de alguna manera, porque la sociedad —así, en abstracto— sí se va acomodando al significado de la globalización, por mucho que los Estados no lo hagan. Y la sociedad ya ha incorporado formas de violencia asimétrica que generan un impacto mucho más relevante del que corresponde a su potencia» (GÓMEZ DE ÁGREDA, A., "Ciberdespacio", *Boletín Electrónico del Instituto español de Estudios Estratégicos*, Documento de análisis 57/2013, 19 de junio de 2013, 1-9, en concreto, pg. 8).

El modelo jurídico del ciberespacio ha de construirse partiendo de esa premisa y otorgando, por esos mismos motivos, al ciberespacio la naturaleza de bien público global como fundamento de su articulación normativa en la que se habrían de asumir dos líneas de acción prioritaria: por una parte, reordenar las funciones y las relaciones entre lo público y lo privado para adaptarse a los parámetros específicos que impone el ciberespacio y, por otra, redireccionar el proceso de construcción normativa con el doble objetivo de reducir el papel protagónico del derecho penal y de los conflictos armados en este ámbito y de construir el auténtico ciberderecho como un conjunto normativo de naturaleza constitucional.

La responsabilidad principal en esa tarea corresponde a los Estados pero requiere un planteamiento capaz de reconocer la presencia de dos condicionantes: uno, la superación real del marco estatal que impone la existencia del ciberespacio, en particular, en el ejercicio de la soberanía y de las competencias estatales vinculadas al territorio del Estado; y, dos, el imperativo de la cooperación internacional para la ordenación jurídica del ciberespacio.

El ciberespacio impone al Estado un desafío mayor de lo que pudiera parecer. No solo afecta al alcance, contenido y modalidades de ejercicio de sus competencias, sino que también incide en su estructura y funcionamiento y en su defensa misma. El modelo de garantía de seguridad del Estado articulado tradicionalmente sobre la base de la diferenciación entre la amenaza externa y la interior que, siendo artificial, ha resultado eficaz a lo largo de la historia, quiebra absolutamente con el ciberespacio. Ni la «amenaza» admite ya esa categorización simplista, ni los mecanismos de respuesta pueden seguir funcionando con la misma dinámica. No se puede mantener la distinción entre seguridad ciudadana o pública y seguridad y defensa nacional, ni tampoco la distribución de funciones a esos efectos entre Fuerzas y Cuerpos de Seguridad del Estado y Fuerzas Armadas.

Después de dos décadas, no se han materializado las utopías del Manifiesto Barrow de 1996, pero es el momento de enfrentar una realidad en la que resulta obligado no solo adaptar las estructuras constitucionales estatales a los condicionantes que impone el ciberespacio sino, también y muy especialmente, articular un derecho constitucional del ciberespacio.

[i]

*Margarita Robles Carrillo**
Profesora Titular Derecho Internacional Público y RRII. UGR
Codirectora Centro Mixto UGR-MADOC