

*Margarita Robles Carrillo**

Gobernanza política versus
gobernanza tecnológica del
ciberespacio

Gobernanza política versus gobernanza tecnológica del ciberespacio

Resumen

La gobernanza del ciberespacio está siendo objeto de definición en el plano político y tecnológico siguiendo una evolución y asumiendo, en cada caso, un alcance y una naturaleza diferentes. El proceso de reforma de la ICANN se ha traducido en el establecimiento de unos objetivos y unos valores esenciales y en la constitución de una estructura orgánica que responden al modelo de organización *multistakeholder* con escasa representación de los Estados. El debate político internacional, en particular en el marco de Naciones Unidas, está conduciendo a la implantación de un modelo de gobernanza interestatal tradicional en el que no parece tener cabida la participación de la sociedad civil.

Abstract

The governance of cyberspace is being defined politically and technologically. The ICANN reform process has resulted in the establishment of essential objectives and values and the establishment of an organizational structure according to the multistakeholder model of organization with little representation of States. International political debate, particularly within the framework of the United Nations, is leading to the implementation of a model of traditional interstate governance without participation of civil society.

***NOTA:** Las ideas contenidas en los **Documentos de Opinión** son de responsabilidad de sus autores, sin que reflejen, necesariamente, el pensamiento del IEEE o del Ministerio de Defensa.

Palabras clave

Gobernanza política, gobernanza tecnológica, ICANN, Naciones Unidas.

Keywords

Political Governance, Technological Governance, ICANN, United Nations.

Introducción

La gobernanza del ciberespacio ha sido objeto de un amplio debate político y doctrinal desde sus inicios y, también, desde entonces, coexisten dos paradigmas sobre su organización y funcionamiento aparentemente enfrentados: el político y el tecnológico.

El discurso sobre la gobernanza política encuentra, en sus orígenes, propuestas realmente innovadoras como el *Manifiesto de Barlow*, que rechaza la aplicación del concepto de soberanía en este espacio y cuestiona cualquier extensión hacia el mismo de los poderes tradicionalmente reconocidos a los Estados. En la práctica, como cabía esperar, se ha impuesto el consenso claro y generalizado entre los diferentes Gobiernos sobre su protagonismo en la organización del ciberespacio. Ese principio básico es compartido por todos los países, pero hay un cierto desacuerdo en cuanto a su materialización efectiva porque se enfrentan dos grandes opciones políticas: por una parte, la defensa a ultranza de la aplicación del paradigma soberano al ciberespacio en términos similares a los del mundo físico; y, por otra, las propuestas de gobernanza *multistakeholder* que pretenden, en mayor o menor medida, según los casos, atemperar el modelo clásico de ejercicio de la soberanía implicando a diferentes interlocutores sociales en la gestión del ciberespacio¹. Es un debate abierto y complejo que se está reproduciendo en el marco universal y en distintas estructuras organizativas interregionales y regionales. En concreto, en el marco de Naciones Unidas y respecto de los aspectos fundamentales de su ordenación jurídico-política, parece estar decantándose hacia una fórmula intergubernamental clásica.

El discurso sobre la gobernanza tecnológica, por su parte, ha seguido una trayectoria significativamente distinta. Sin que haya faltado el componente de desacuerdo entre los Estados como telón de fondo, el proceso mismo de organización de esa gobernanza se ha sustraído en gran medida a la participación directa de los Gobiernos al haber pasado, sin apenas solución de continuidad, desde el control originario ejercido por EE.UU. a su privatización siguiendo un modelo de decisión *multistakeholder* y *bottom-up*. Este es, en resumen, el resultado de la reforma de la Corporación para la asignación de nombres y números de Internet (*Internet Corporation for Assigned Names and Numbers-ICANN*), culminada en octubre de 2016. Es una reforma que

¹ Sobre este concepto puede verse RAYMOND, M. y DeNARDIS, L. «Multistakeholderism: anatomy of an inchoate global institution». *International Theory*, vol. 7, 2015, pp. 572-616.

sacraliza el enorme y preocupante desajuste existente entre la dimensión político-jurídica y la dimensión técnica de la gobernanza del ciberespacio.

Gobernanza tecnológica

La seguridad, interoperabilidad, confiabilidad y, con ello, el correcto funcionamiento de las redes informáticas dependen de la identificación y localización del conjunto de los diferentes dispositivos integrados en ellas. La gestión de un sistema único de nombres de dominio y de direcciones de protocolo de Internet (IP) es el componente esencial de la gobernanza tecnológica del ciberespacio.

Desde los primeros trabajos de ARPANET, esa actividad de gestión, localizada de modo natural en EE.UU., es realizada por varias instituciones académicas y técnicas hasta que se centraliza en la IANA (Internet Assigned Numbers Authority), dependiente del Gobierno estadounidense. La IANA se ocupa de la administración de los parámetros de protocolo y de los recursos numéricos de Internet, así como de la gestión de la zona raíz del Sistema de nombres de dominio (DNS). En julio de 1997, la Administración Clinton decide la privatización de ese sistema con el objetivo de mejorar la competencia y la participación internacional creando, para ello, la ICANN.

La ICANN se constituye en 1998 como una entidad pública benéfica, sin ánimo de lucro, que tiene asignada la misión de garantizar el funcionamiento estable y seguro del sistema mundial de identificadores únicos de Internet². Desde entonces, se encarga principalmente de gestionar las funciones de la IANA sobre la base de un conjunto de acuerdos sucesivamente celebrados con el Departamento de Comercio de EE.UU.³. En esos denominados *Memorandum of Understanding* se reconoce a la National Telecommunications and Information Administration (NTIA)⁴ una capacidad de control general sobre la actividad de la ICANN que se manifiesta, en particular, en la gestión de la zona raíz del DNS.

A pesar de su explicación en clave histórica, esta situación de dependencia de la ICANN respecto del Gobierno estadounidense es objeto de numerosas críticas por parte de otros Estados y organismos internacionales. Entre ellas destacan, particularmente, las relativas a la falta de legitimidad de una corporación asentada en y

² <https://www.icann.org/resources/pages/articles-2012-02-25-en>.

³ <https://www.ntia.doc.gov/legacy/ntiahome/domainname/icann-memorandum.htm>.

⁴ Sobre este proceso, puede verse DeNARDIS, L. *The Emerging Field of Internet Governance*. Yale Information Society Project Working Paper Series, septiembre 2010.

tutelada por un único Estado, que conducen, finalmente, a la decisión de proceder a su reforma.

La reforma de la ICANN

El proceso de reforma se sitúa en un contexto marcado por la creciente impugnación del protagonismo asumido por EE.UU., en la gobernanza tecnológica del ciberespacio. En el marco de la Unión Internacional de Telecomunicaciones (UIT), en las Cumbres Mundiales de la Sociedad de la Información, en el Foro de Gobernanza de Internet (IGF) o en el seno de la NETmundial⁵ se reproducen los debates sobre la necesidad de modificar ese modelo⁶. Las propuestas en ese sentido oscilan desde la atribución de esas funciones a la propia UIT o la creación de una organización internacional *ad hoc*, hasta la defensa del mantenimiento del sistema *multistakeholder*, pero fuera del marco de control de EE.UU.

EE.UU. acepta la transición y la consiguiente pérdida de control sobre esa dimensión de la gobernanza del ciberespacio⁷, siempre que se cumplan unos criterios estructurales y operativos, en particular tres: el mantenimiento y mejora del modelo *multistakeholder* de la ICANN; la exclusión de cualquier opción que suponga su sustitución por un sistema público de control ya sea estatal o internacional; y el mantenimiento de la apertura de Internet. Los demás Estados, organizaciones y foros internacionales con competencias en la materia coinciden en la idea de situar a la ICANN fuera de la órbita de influencia de EE.UU., así como en establecer mecanismos de exigencia de control y responsabilidad de las actividades de esta corporación⁸. La legitimidad de la ICANN y, con ello, su autoridad misma se hace depender del cumplimiento de esas condiciones. Parece, entonces, más importante sustraerla al control de EE.UU., que someterla a un régimen jurídico negociado y aceptado entre la

⁵ En el NETmundial Multistakeholder Statement, adoptado el 24 de abril de 2014 se establecen, a partir de cerca de doscientas contribuciones y como recomendaciones dirigidas a otros foros y entidades competentes, una serie de principios para la gobernanza de Internet: «Multistakeholder; Open participative, consensus driven governance; transparent; Accountable; Inclusive and Equitable; Distributed; Collaborative; Enabling meaningful participation; Agility» (<http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf>).

⁶ NYE, J. S. *The Regime Complex For Managing Global Cyber Activities*. Harvard Kennedy School, Belfer Center for Science and International Affairs, noviembre 2014.

⁷ KRUGER, L. G. *Internet Governance and the Domain Name System: Issues for Congress*. CRS Report for Congress, noviembre 2016.

⁸ Sobre esta problemática, puede verse KOPPELL, J. G. S. «Pathologies of Accountability: ICANN and the Challenge of Multiple Accountabilities Disorder». *Public Administration Review*, vol. 65, n.º 1, 2005, pp. 95-96.

comunidad internacional de Estados, incluso, suponiendo esto la opción por su privatización.

Consecuentemente con ello, la reforma de la ICANN se realiza con el doble propósito de proceder a su internacionalización y privatización. El proceso de transición está presidido por dos objetivos marco conexos: reemplazar el papel de custodia de las funciones de la IANA desempeñado por la NTIA y mejorar los mecanismos de responsabilidad de la ICANN.

El proceso de reforma se desarrolla implicando al conjunto de la comunidad *multistakeholder* mediante convocatorias públicas solicitando comentarios sobre los resultados de la actividad de los dos grupos de trabajo y sobre la revisión de los Estatutos⁹. Es, precisamente, la NTIA quien solicita a la ICANN la organización de un debate inclusivo y global involucrando a todas las partes interesadas con la intención de diseñar un proyecto colectivo.

Después de poco más de dos años de trabajo, la transición culmina el 1 de octubre de 2016. En el proceso, el protagonismo asumido por la comunidad *multistakeholder* y por la Administración estadounidense contrasta con el escaso papel del resto de los Gobiernos y de las organizaciones internacionales. Esta dinámica tiene su reflejo en el resultado final, especialmente, en la definición de los objetivos y misiones de la ICANN y en su estructura orgánica, que muestran una clara opción por el sistema *multistakeholder* en el que la representación pública de los Estados se encuentra confinada a un papel asesor secundario.

Objetivos y valores esenciales de la ICANN

Tras la reforma de 2016, la ICANN mantiene su estatuto como corporación pública benéfica constituida de conformidad con la Nonprofit Public Benefit Corporation Law del Estado de California. En su actas constitutivas originarias, el artículo 3 dispone que la ICANN debe promover «el interés público mundial en la estabilidad operativa de Internet», como red de redes internacional que no pertenece individualmente a ningún Estado ni organización¹⁰. Esa filosofía se reproduce y confirma en las principales disposiciones de los Estatutos reformados de la ICANN sobre su misión, obligaciones y valores esenciales.

⁹ Puede consultarse el desarrollo de este proceso en: <https://www.icann.org/stewardship-implementation>.

¹⁰ <https://www.icann.org/resources/pages/articles-2012-02-25-en>.

El artículo 1, en su sección 1.1., apartado a), al tratar sobre su misión, estipula que las políticas de la ICANN se desarrollaran a través de un *bottom-up consensus-based multistakeholder process*¹¹. En el apartado c) se reconoce expresamente la naturaleza no intergubernamental, ni pública de esta corporación.

En el capítulo de obligaciones, que constituye una de la novedades más significativas de la reforma, el artículo 1, sección 1.2.a) establece textualmente la obligación de la ICANN de emplear «procesos de desarrollo de políticas abiertas, transparentes y de abajo hacia arriba, dirigidos por el sector privado (incluidos los actores empresariales, la sociedad civil, la comunidad tecnológica, el mundo académico y los usuarios finales), teniendo debidamente en cuenta el asesoramiento de los gobiernos y las autoridades públicas». En realidad, esta última referencia no genera un compromiso real en términos jurídicos y difícilmente se puede materializar si se tiene en cuenta que el órgano de representación de los Estados tiene competencias limitadas y una capacidad de decisión mínima, al carecer sus componentes de derecho a voto en el resto de los órganos decisorios.

Para terminar, entre los llamados valores esenciales que han de guiar sus acciones y decisiones recogidos en el artículo 1, sección 1.2.b), hay que destacar dos. Como primera providencia, la ICANN debe conseguir y apoyar una participación que refleje la diversidad cultural, geográfica y funcional de Internet en todos los niveles para asegurar que «se utiliza el proceso de desarrollo de la política de abajo hacia arriba y multisectorial para determinar el interés público mundial». A continuación, reconoce la responsabilidad de los Gobiernos y autoridades públicas en las políticas públicas y que tendrá en cuenta su asesoramiento en esos ámbitos pero, expresa y literalmente: «permanece enraizada en el sector privado (incluidos los agentes empresariales, la sociedad civil, la comunidad tecnológica, el mundo académico y los usuarios finales)». En cualquier caso, más allá de la definición de objetivos y misiones de la ICANN y de la referencia al papel de los Estados en cuestiones públicas, el auténtico alcance y naturaleza de la opción por el modelo *multistakeholder*, en detrimento de cualquier papel significativo de los Gobiernos, se aprecia en su estructura orgánica.

¹¹ <https://www.icann.org/resources/pages/governance/bylaws-en>.

La estructura orgánica

La ICANN cuenta con una estructura orgánica llamada a representar al conjunto de la comunidad *multistakeholder* que resulta extremadamente compleja no solo por el número de sus componentes sino, también, por las interacciones existentes entre ellos. Formal y estructuralmente, se presenta como un modelo abierto y participativo. Materialmente, ofrece poca claridad y transparencia en la definición de las respectivas responsabilidades.

La estructura orgánica es compleja. Junto con el presidente, el secretario y el director financiero, la ICANN cuenta con unos órganos principales, las organizaciones de apoyo y los comités asesores¹². Para explicar el sistema hay que empezar por estos últimos.

Las Organizaciones de Apoyo son tres: la Organización de Apoyo para Direcciones (ASO), marcadamente técnica, que tiene la misión de asesorar sobre las políticas relativas a la operación, asignación y administración de direcciones de Internet; la Organización de Apoyo para Nombres de Dominio con Código de País (ccNSO), que se ocupa de elaborar, fomentar el consenso y recomendar las políticas globales en esa materia; y la Organización de Apoyo para Nombres Genéricos (GNSO), que hace lo propio respecto de los dominios genéricos de nivel superior. La ASO representa a los Registros Regionales de Internet (RIR); la ccNSO está integrada por los administradores de los ccTLD; y la GNSO aglutina a los diferentes grupos *multistakeholder*. Cada una de ellas tiene su propia organización interna y funcionamiento y dispone de un órgano directivo en forma de Consejo. No obstante, a pesar de estar reunidas en una misma categoría como Organizaciones de Apoyo, no tienen asignadas unas funciones o una naturaleza homogéneas, salvo por el hecho de que son miembros de la llamada *Empowered Community* y participan en el nombramiento de los miembros de la Junta de Directores.

Los comités asesores son cuatro: el Comité Asesor Gubernamental (GAC) que, representando principalmente a los Estados, asesora sobre las actividades de ICANN que puedan afectarles o que conciernen a materias de interés público; el Comité Asesor At-Large (ALAC) se ocupa de aconsejar sobre las actividades que puedan afectar a los usuarios a quienes representa como colectivo; el Comité Asesor de Seguridad y Estabilidad (SSAC) es competente en los asuntos relativos a la seguridad e integridad de los sistemas de asignación de nombres y direcciones de Internet; y el

¹² <https://www.icann.org/community#groups>.

Comité Asesor de Sistema de Servidores Raíz (RSSAC) hace lo propio respecto del funcionamiento, administración, integridad y seguridad de dicho sistema. Los dos primeros responden a un perfil más político, mientras que los últimos son especialmente técnicos. Además del hecho de que todos ellos cumplen una función de asesoría, no tienen atribuciones comunes, ni un alcance o funcionamiento similares. En ese contexto, particularmente, no resulta fácil entender los motivos por los que la representación estatal merece un estatuto jurídico similar al del resto de los comités, en especial, los técnicos.

Los órganos principales son la *Empowered Community* (EC), la Junta de Directores y el Comité de Nominaciones.

La EC es, a su vez, una asociación sin ánimo de lucro constituida, como la propia ICANN, según la legislación del Estado de California. Está compuesta por la ASO, la ccNSO, la GNSO, el GAC y el ALC, esto es, las tres organizaciones de apoyo y los comités asesores de corte político. Entre sus funciones destacan el nombramiento y cese de los miembros de la Junta, distintos del presidente, y la propia destitución de la Junta, la aprobación de determinadas normas y la posibilidad de rechazar otras, incluidos los presupuestos, así como la legitimación para incoar los procedimientos de responsabilidad y para iniciar una acción ante cualquier tribunal con jurisdicción sobre la ICANN.

La Junta de Directores es el principal órgano operativo y funcional que ejerce, salvo disposición específica en contrario, los poderes de la ICANN. Está formada por dieciséis directores con derecho a voto y cuatro enlaces no votantes. Los enlaces son designados por el GAC, el SSAC, el RSSAC y el IETF (Internet Engineering Task Force). Los directores son propuestos siguiendo el siguiente reparto: ocho por el Comité de Nominaciones; dos por cada una de las organizaciones de apoyo (ASO, ccNSO y GNSO) y uno por el ALAC. El presidente de la ICANN ejerce como director completando el número. Llama la atención que el ALAC cuente con un director, mientras que el GAC solo merece un enlace sin derecho a voto.

El Comité de Nominaciones tiene la función principal de designar a los directores de la Junta que le corresponden, esto es, ocho. Está integrado por un presidente y un presidente electo, nombrados por la Junta, tres enlaces designados cada uno de ellos por el RSSAC, el SSAC y el GAC, cinco delegados votantes por el ALAC, siete delegados votantes por el GNSO, un delegado votante por parte del Consejo ccNSO,

otro por el Consejo ASO y un tercero por el IETF, así como un presidente asociado sin derecho a voto. En este caso, la situación del GAC con un enlace sin derecho a voto contrasta con la del ALAC con cinco delegados votantes.

En mi opinión, bajo la apariencia de un sistema amplio de representación con diez órganos de distinta naturaleza y diferente composición —la EC, la Junta de Directores, el Comité de Nominaciones, las tres organizaciones de apoyo y los cuatro comités asesores—, se esconde un entramado menos representativo y más complejo. Los tres primeros órganos, que son los principales, se nutren de los demás. Las reglas de designación de los miembros no son fácilmente comprensibles cuando, por ejemplo, ocho miembros de la Junta son propuestos por el Comité de Nominaciones, mientras que tres miembros del Comité de Nominaciones van a ser designados por la Junta. La naturaleza de los órganos no es homogénea, ni se encuentran en una situación de relativa paridad, como correspondería a un sistema básico de distribución de poderes. En lugar de ello, coexiste un órgano principal de decisión —la Junta— con una entidad como la EC, con una personalidad propia diferenciada, y con el resto que cumplen funciones de asesoramiento respecto de órganos en los que están representados en unos casos con capacidad de voto y en otros no. La aportación de cada órgano de apoyo o asesor se traduce en la posibilidad de contar, en cada caso, con miembros votantes o no votantes creando una desigualdad *de iure* y *de facto* que no va a estar exenta de problemas. Sin ir más lejos, el interés de los usuarios representado por el ALAC va a prevalecer sobre el interés público cuya defensa se encomienda al GAC ya que solo el primero tiene representación con voto en los demás órganos en los que participa. Con independencia de cualquier otro elemento sobre su autoridad, la representación pública que asumen los Estados cuenta, por el momento, con mayores garantías de legitimidad que la que proporciona el ALAC.

A la luz de estas consideraciones no es difícil tener la impresión de que la articulación del modelo *multistakeholder* para la gobernanza técnica del ciberespacio se ha forjado, en mayor medida, como una alternativa opuesta y enfrentada al modelo interestatal tradicional de relaciones que como una opción realmente abierta y participativa en la que todos los actores, incluidos los Estados, tienen el papel que les corresponde asumir. Hay una enorme diferencia entre superar el modelo intergubernamental clásico, articulando un sistema adaptado a la singularidad del ciberespacio, y organizarlo sin asumir el papel de los Estados como autoridades públicas que, también, han de tener

reconocida su función en la gobernanza técnica del ciberespacio. Existe una variedad de opciones intermedias que no pasan por mantener el sistema tradicional, ni tampoco por erradicarlo.

No es, sin embargo, un fenómeno aislado. Si la gobernanza tecnológica se ha organizado soslayando de la función del Estado, la gobernanza política está avanzando precisamente en sentido contrario eludiendo el papel de la comunidad *multistakeholder* en la gestión del ciberespacio.

Gobernanza política

La organización de la gobernanza política del ciberespacio está resultando ser, como cabía esperar, un proceso lento y complejo en el que los diversos intereses en presencia y, especialmente, las diferentes cosmovisiones de los Estados dificultan la elaboración del consenso mínimo necesario a esos efectos.

La necesidad de abordar la gestión del ciberespacio se manifiesta tempranamente en el seno de la Asamblea General de Naciones Unidas (AGNU) cuando, en 1998, decide solicitar las observaciones y comentarios de los Estados sobre los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional¹³. Desde entonces, el discurso sobre la gobernanza se reproduce por vías distintas, en particular, a través del procedimiento institucional puesto en marcha en el marco de la ONU gracias a los trabajos de los sucesivos Grupos de Expertos Gubernamentales (GEG). En paralelo al debate general, la actuación de algunas organizaciones y foros internacionales sirve para mostrar las diferentes aproximaciones existentes a propósito del gobierno del ciberespacio.

Las estrategias conjuntas

La disparidad de concepciones sobre la gobernanza del ciberespacio se aprecia en el marco de actividad de las organizaciones internacionales, así como en organismos y foros de otra naturaleza en los que se postula bien el principio tradicional de soberanía del Estado, bien el modelo *multistakeholder*. La Unión Europea (UE), el G-7 y la Organización de Cooperación de Shangai (OCS) son ejemplos ilustrativos de esas tendencias.

¹³ Resolución 53/70 de la Asamblea General de Naciones Unidas 4 de diciembre de 1998 (<http://www.un.org/es/comun/docs/?symbol=A/RES/53/70>).

La Estrategia de Ciberseguridad de la UE, adoptada en 2013, recoge la filosofía generalmente asumida por sus Estados miembros cuando defiende el principio de una gobernanza multilateral democrática y eficaz y la necesidad de promover una responsabilidad compartida con la implicación de todas las partes interesadas, ya sean las administraciones públicas, el sector privado o los ciudadanos¹⁴. La apuesta de la UE por el modelo *multistakeholder* de gobernanza no pretende cuestionar la autoridad de los Estados, ni el modelo tradicional de relaciones intergubernamentales. Simplemente asume que es necesario asociar, en mayor o menor medida, a los interlocutores sociales por tres razones básicas: el protagonismo que han alcanzado en el ciberespacio; las características singulares de este ámbito respecto del mundo físico; y la propia incapacidad de los Estados para gestionar eficazmente esta diferente realidad. En la gobernanza tecnológica, la idea es que un liderazgo del sector privado y una política pública eficaz no han de ser conceptos mutuamente excluyentes¹⁵.

Esa misma filosofía se encuentra en la Declaración de la Cumbre del G-7 celebrada en Ise-Shima, en mayo de 2016, donde se hace expreso el compromiso de los Estados participantes con un modelo de gobernanza *multistakeholder*¹⁶. Son dos los motivos principales que sustentan esa opción: por una parte, el convencimiento de que la seguridad y la resiliencia en el ciberespacio dependen de una estrecha cooperación nacional e internacional de todos los actores implicados, incluyendo el mundo empresarial y académico y la sociedad en su conjunto; y por otra parte, la voluntad de preservar la naturaleza global de Internet, promover el flujo de información y permitir a los usuarios acceder a la información, el conocimiento y los servicios a su elección. Un año después, sin embargo, la Declaración del G-7 sobre el comportamiento responsable de los Estados en el ciberespacio, adoptada en Lucca el 11 de abril de 2017¹⁷, constituye una convalidación política al más alto nivel de los trabajos realizados por los GEG, que se alejan de los paradigmas *multistakeholder*. Puede ser que, al haberse centrado en temas de paz y seguridad internacionales, esta opción se debilite. Puede ser, simplemente, que no se encuentre lo suficientemente articulada o madura. Pero podría ser, también, que se haya producido un acercamiento a las políticas defendidas por otros Estados, como los miembros de la OCS.

¹⁴ <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=JOIN:2013:0001:FIN:ES:PDF>.

¹⁵ <http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=URISERV%3Aasi0012>.

¹⁶ <http://www.mofa.go.jp/files/000160279.pdf>.

¹⁷ <http://www.mofa.go.jp/files/000246367.pdf>.

La OCS¹⁸ agrupa a Rusia, China, Kazajistán, Kirguistán, Tayikistán y Uzbekistán que adoptan, en 2009, el Convenio sobre Cooperación en el ámbito de la Seguridad Internacional de la Información que entra en vigor en 2011¹⁹. Los principios básicos que informan esta cooperación son la afirmación de la soberanía cibernética y de la necesidad de control gubernamental del ciberespacio, así como el rechazo a cualquier aproximación *multistakeholder* a la gobernanza del ciberespacio.

Estos países presentan en 2011 ante la AGNU una propuesta de elaboración de un Código internacional de conducta para la seguridad de la información que es reformulada en 2015. En ambas propuestas, el punto de partida es «el derecho soberano de los Estados, que tienen derechos y responsabilidades en lo que concierne a las cuestiones de política pública que suscita Internet en el plano internacional»²⁰. El principio de un control gubernamental independiente sobre las TIC se refuerza en 2015 afirmando el objetivo de «impedir que otros Estados exploten su posición dominante» con la intención de «socavar el derecho de los Estados de controlar de forma independiente los bienes y servicios relativos a las tecnologías de la información y las comunicaciones, o amenazar su seguridad política, económica y social»²¹.

La defensa del modelo de cooperación internacional clásico y la ausencia de referencias a cualquier modalidad de intervención *multistakeholder*, en este contexto, han tenido su efecto en la evolución de los trabajos dentro de los GEG en los que participan tanto Rusia como China.

Los informes de los GEG

Los trabajos de los sucesivos GEG han servido para ir decantando el consenso de los Estados sobre la aplicación de la normativa internacional al ciberespacio. Es importante destacar que, en su composición, que responde al principio de una distribución geográfica equitativa, siempre ha habido representación de los cinco miembros permanentes del Consejo de Seguridad. La función original asignada a los GEG consiste en examinar las amenazas existentes y potenciales en materia de seguridad de la información, así como las posibles vías de colaboración para hacer frente a las mismas. Pero, en la práctica, su actividad es considerablemente más amplia hasta el

¹⁸ <http://www.sectsco.org/EN123/>.

¹⁹ <http://cis-legislation.com/document.fwx?rgn=28340>.

²⁰ A/66/359, de 14 de septiembre de 2011, p. 3 y A/69/723, de 13 de enero de 2015, p. 3.

²¹ A/69/723, de 13 de enero de 2015, p. 5.

punto de haberse convertido en el foro intergubernamental donde se analiza el conjunto de la normativa internacional aplicable al ciberespacio en el contexto de la seguridad internacional, en particular, los principios estructurales de la Carta de Naciones Unidas. Tras el fracaso del primer grupo, en 2004, el GEG de 2010 consigue al menos identificar algunos riesgos, amenazas y vulnerabilidades reconociendo la necesidad de cooperar a nivel internacional²². Pero son los informes de los GEG de 2013 y, sobre todo, 2015 los que concluyen con avances significativos.

El informe del GEG de 2013 contiene un conjunto de recomendaciones divididas en tres secciones principales relativas a las normas, reglas y principios de comportamiento responsable de los Estados, junto con dos principios básicos desde entonces: la aplicación del derecho internacional en vigor al ciberespacio y la posibilidad de establecer normas adicionales, en caso necesario, atendiendo a sus características específicas²³.

El informe del GEG de 2015 constituye la confirmación y desarrollo de esas premisas que ahora se estructuran y desarrollan en cuatro categorías²⁴:

1) La normativa de derecho internacional de aplicación al uso de las TIC.

En este apartado se incluyen los principios de igualdad soberana, solución pacífica de controversias, prohibición del uso y de la amenaza de la fuerza, no intervención en los asuntos internos de otros Estados y respeto de los derechos humanos. Siguiendo los términos del informe, que expresamente reitera esta obligación, la soberanía y los principios que de ella se derivan se aplican a las actividades relacionadas con las TIC, así como su jurisdicción sobre la infraestructura de esas tecnologías en su territorio.

Junto a estos principios generales y básicos de la Carta de Naciones Unidas, se recogen asimismo dos conjuntos normativos específicos: por una parte, los principios de humanidad, necesidad, proporcionalidad y distinción, propios del Derecho Internacional de los Conflictos Armados (DICA); y, junto a ello, tres reglas en materia de responsabilidad. La primera, que podría parecer una obviedad en cualquier otro ámbito, es que los Estados no deben recurrir a terceros para cometer hechos internacionalmente ilícitos mediante las TIC. La segunda, que resulta frágil en exceso, es que «deberían» tratar de garantizar que su territorio no sea utilizado por agentes no

²² A/65/201, de 30 de julio de 2010.

²³ A/68/98, de 24 de junio de 2013.

²⁴ A/70/174, de 22 de julio de 2015.

estatales para la comisión de tales hechos. La tercera, en sintonía con la primera, establece que los Estados deben cumplir sus obligaciones internacionales en relación con los hechos internacionalmente ilícitos que se les puedan imputar en virtud del derecho internacional pero, en la medida en que la atribución no es tarea fácil, las acusaciones deberían estar fundamentadas. En definitiva, con los principios del DICA se limitan a reconocer lo existente —y, por ello, ya jurídicamente exigible—, sin atender al verdadero problema que es la dificultad de su aplicación en el entorno de un conflicto cibernético. Mientras, con las reglas sobre responsabilidad están interiorizando, más que cuestionando, las carencias en cuanto a su aplicación en el ciberespacio. Es obvio que los Estados están obligados a no cometer hechos internacionalmente ilícitos, ni por sí mismos, ni a través de terceros. Es también cierto que, en determinados supuestos, las reglas de responsabilidad permiten atribuir al Estado hechos ilícitos cometidos por particulares desde su territorio y que, en cualquier caso, la denominada obligación de diligencia debida les obliga a actuar para garantizar el respeto de la legalidad. Es, por último, evidente que cualquier acusación debe ser probada. La cuestión que hay que plantearse es el porqué de la necesidad de ponerse de acuerdo nuevamente sobre ello cuando se trata del ciberespacio.

2) Las normas, reglas y principios de comportamiento responsable de los Estados.

Estas normas son caracterizadas como voluntarias, no vinculantes, carentes de capacidad para limitar o prohibir acciones, que expresan las expectativas de la comunidad internacional y establecen criterios para determinar ese comportamiento responsable. Esta categoría, que se sitúa en la línea de las propuestas de un Código internacional de seguridad de la información liderada por Rusia y China, incluye recomendaciones de distinta naturaleza.

Básicamente, siguiendo este apartado del Informe del GEG, los Estados deberían colaborar, informarse, prestarse asistencia mutua y entablar acciones penales por el uso de las TIC con fines criminales y terroristas. Junto a estas recomendaciones generales, destacan otras específicas. Por una parte, se hace referencia expresamente al deber de los Estados de proteger las infraestructuras fundamentales y de atender los requerimientos de asistencia de que fueran objeto en relación con las mismas, así como, también, de garantizar la integridad de la cadena de suministro y de divulgar de modo responsable las vulnerabilidades relacionadas con las TIC. Por otra parte, se recomienda que los Estados no deberían realizar ni apoyar de forma deliberada

actividades en la esfera de las TIC contrarias a las obligaciones que les incumben en virtud del derecho internacional que puedan dañar infraestructuras críticas o sistemas de información de los equipos de respuesta de emergencias de otro Estado, ni deben utilizar esos equipos para participar en una actividad internacional malintencionada.

En realidad, tan preocupante es el hecho de que se haya recomendado que los Estados no realicen actividades contrarias a sus obligaciones internacionales, como la circunstancia misma de que esta previsión se localice en el apartado relativo a la normativa voluntaria. Ninguno de los aspectos singulares del uso de las TIC puede explicar —y menos aún justificar— que la «obligación» de los Estados de cumplir sus obligaciones internacionales se diluya dentro de esta categoría de normas no vinculantes sobre la gobernanza del ciberespacio.

3) Las medidas de fomento de la confianza.

Estas medidas de carácter voluntario están destinadas a fortalecer la paz y la seguridad internacionales y a incrementar la cooperación, la transparencia, la previsibilidad y la estabilidad entre los Estados. Entre ellas se encuentran la creación de puntos de contacto, mecanismos de consulta, cooperación a todos los niveles, incluido transfronterizo, el fomento de la transparencia o la creación de equipos de respuesta a las emergencias.

4) Las medidas de cooperación y asistencia internacionales.

Estas medidas están diseñadas con una doble intencionalidad para promover la seguridad y para contribuir a la creación de capacidades en la esfera de las TIC. Hay dos ideas básicas que sustentan este catálogo de propuestas de asistencia, promoción, cooperación y concienciación. Por una parte, la falta de capacitación de algunos Estados supone la existencia de vulnerabilidades tanto para ellos, como para la sociedad en su conjunto. Por otra parte, un enfoque regional en la creación de capacidades permite apreciar los aspectos específicos políticos, sociales, económicos o culturales, propiciando una aproximación adaptada a las necesidades de cada caso concreto.

Junto a la parte normativa, procedimentalmente, en las conclusiones del informe del GEG de 2015 se identifican los ejes fundamentales de evolución de este proceso de formación de un consenso sobre la gobernanza del ciberespacio. En primer lugar, en el plano institucional, Naciones Unidas están llamadas a desempeñar una función primordial en el desarrollo de un entendimiento común sobre la aplicación del derecho

internacional al ciberespacio. En segundo término, no en orden de importancia, los Estados tienen asignada la responsabilidad primordial de garantizar la paz, la seguridad y la estabilidad mediante su cooperación y en la gobernanza del ciberespacio. Para terminar, en este punto, se advierte que la eficacia de esa cooperación internacional mejoraría «si se establecieran mecanismos para la participación, según procediera, del sector privado, el mundo académico y las organizaciones de la sociedad civil»²⁵. Esta es la única referencia, lacónica y limitada, a una posible participación de la comunidad *multistakeholder* en la gobernanza política del ciberespacio.

La Resolución de la AGNU de 5 de diciembre de 2016 sobre los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional²⁶ constituye, respecto de sus predecesoras, un progreso significativo haciendo balance de los informes de los GEG de 2013 y 2015. La resolución acoge «con beneplácito» tres principios básicos. El primero es que el derecho internacional y, en particular, la Carta de Naciones Unidas son aplicables al ciberespacio y fundamentales para mantener la paz y la estabilidad y fomentar un entorno abierto, seguro, estable, accesible y pacífico. El segundo, que sintoniza con las propuestas lideradas por Rusia y China y asumidas en el Informe del GEG de 2015, reconoce que la aplicación de normas, reglas y principios de conducta estatal responsable de carácter voluntario y no vinculante «puede reducir los riesgos para la paz, la seguridad y la estabilidad internacionales». El tercero establece que, dadas las particularidades del ciberespacio, podrían elaborarse normas adicionales específicas con el transcurso del tiempo. Ello equivale, por una parte, a aceptar la insuficiencia de la normativa en vigor contemplada en el primer principio y, por otra, a preparar el camino para la conversión en obligatorias de las normas no vinculantes mencionadas en el segundo de esos principios. En ese sentido se interpreta el hecho de que la AGNU exhorte expresamente a los Estados miembros a guiarse por el informe de GEG de 2015 y promueva el examen a nivel multilateral tanto de las amenazas reales y potenciales, como de las estrategias y conceptos internacionales pertinentes encaminados a fortalecer la seguridad apoyando los trabajos del nuevo GEG creado por el secretario general en virtud de la Resolución 70/237.

²⁵ A/70/174, de 22 de julio de 2015, p. 17.

²⁶ A/RES/71/28, de 9 de diciembre de 2016.

La Declaración de Lucca del G-7 de 11 de abril de 2017 sobre el comportamiento responsable de los Estados en el ciberespacio es, como se apuntaba, la confirmación del consenso que se está gestando en la AGNU a través del informe del GEG de 2015, al que hace referencia expresamente y al que reproduce en la mayoría de sus contenidos. Habrá que esperar para ver si la preocupación por la paz y la seguridad internacionales que informa esta Declaración justifica la ausencia absoluta de referencias a la función de la comunidad *multistakeholder* o si también en este foro se está iniciando la deriva hacia fórmulas intergubernamentales clásicas de gestión del ciberespacio.

Conclusiones

La evolución, el contenido y la naturaleza de las gobernanzas política y tecnológica son completamente diferentes. La gobernanza política está siendo objeto de debate en diversos foros y dista mucho de estar mínimamente resuelta, mientras la tecnológica se ha completado en apenas dos años. La política se centra en la definición de las normas de derecho internacional obligatorias procedentes del mundo físico, las normas voluntarias, las medidas de confianza y de cooperación y asistencia mutua entre los Estados. La tecnológica se ocupa de garantizar el funcionamiento estable y seguro del sistema de identificadores únicos asumiendo la administración de los parámetros de protocolo, la asignación de los recursos numéricos de Internet y la gestión de la zona raíz del DNS. La política se está organizando siguiendo un modelo de gobernanza idéntico al existente en el mundo físico mediante la extensión al ciberespacio de esos mismos esquemas de funcionamiento, en particular, la soberanía y la jurisdicción de los Estados. La tecnológica constituye, hoy por hoy, la expresión más avanzada del modelo de organización y funcionamiento *multistakeholder*.

El modelo de gobernanza política, que se está gestando en el marco de los trabajos de los GEG y que está siendo avalado por la AGNU y por el propio G-7, no está reconociendo realmente la singularidad del ciberespacio, como sería deseable, para adaptarse a las necesidades y condicionantes particulares que requiere su efectiva ordenación jurídico-política. Esa especificidad se está usando en mayor medida como argumento para reinterpretar o limitar el alcance de la normativa internacional en vigor que, como debería ser, para justificar y construir un modelo jurídico-político capacitado para ordenar eficazmente el ciberespacio. Ni siquiera se debate en profundidad sobre

las modalidades específicas que requiere la aplicación del derecho vigente al ciberespacio. Ni tampoco se considera que es un ámbito en el que aparece sublimado el fenómeno de disminución del protagonismo de los Estados correlativo al aumento constante del papel y de las funciones de los agentes no estatales.

El modelo de gobernanza *multistakeholder* de la ICANN se ha visualizado, precisamente, como el paradigma de una nueva forma de organización capacitada para materializar ese cambio de posición en los actores que ha exacerbado el ciberespacio. Pero, queriendo llevarlo a su expresión máxima, acaba mostrando su propia debilidad estructural al no reconocer el estatuto cualificado que, de un modo u otro, han de seguir manteniendo los Estados, como corresponde a su naturaleza como principal autoridad pública. La presencia del GAC es más una apariencia que una realidad en ese sentido. Incluso, compartiendo o no la idea de que los Estados han de contar con una función en este contexto, podría entenderse el alcance limitado o residual de las atribuciones del GAC si no se pretendiese al mismo tiempo asignar la defensa de lo público a otros órganos con menor legitimidad.

El análisis de la reforma de la ICANN no permite llegar a conclusiones globalmente positivas sobre la organización y funcionamiento de este modelo de gobernanza y, además, plantea abiertamente el problema de fondo de su autoridad y legitimidad para la gestión del ciberespacio. La función de administración y coordinación de la infraestructura cibernética realizada por la ICANN no solo es importante desde una perspectiva técnica y práctica. Constituye realmente el ejercicio de un poder de naturaleza pública en la medida en que afecta a esferas cada vez más amplias de la vida política, social y económica que, precisamente por ello, ha de responder a unos principios básicos de legitimidad. Lejos de ser un presupuesto formalista o meramente teórico, la legitimación de las instituciones contribuye a su eficacia y eficiencia en términos funcionales, operativos y teleológicos, mientras que su ausencia ha alimentado, histórica y empíricamente, las amenazas y la inseguridad. La organización y el funcionamiento de la ICANN habrían de ajustarse a esos requerimientos como garantía para la seguridad de la información, la comunicación y las redes en su conjunto.

En esta situación se plantean varias cuestiones: ¿Pueden prescindir los Estados de la sociedad civil en la organización de la gobernanza política del ciberespacio? ¿Puede obviar la comunidad *multistakeholder* la función de los Estados en el marco de la

gobernanza tecnológica? ¿Cómo se podrían conciliar esas dinámicas que, por el momento, si no están enfrentadas, se están ignorando mutuamente? ¿Es la única opción posible o la mejor entre las posibles? Quizás, reconociendo al GAC un estatuto similar al del ALAC se podría haber cubierto, desde la parte tecnológica, la necesidad de una adecuada representación de los Estados.

Quizás, arbitrando alguna modalidad de participación de la sociedad civil en los trabajos de los GEG se podría haber iniciado el camino para asociar mínimamente a los actores no estatales en la gobernanza política del ciberespacio. La idea de una Fórmula Arria ampliada a interlocutores sociales, expertos y organizaciones podría ser una vía a explorar en ese sentido.

En la práctica, esta dialéctica político-tecnológica plantea serios interrogantes que van desde la viabilidad misma de la convivencia entre ambas modalidades de gobernanza —siendo, como son, diferentes por su naturaleza, objetivos y evolución—, hasta la capacidad del paradigma tecnológico de influir en la solución del dilema de la gobernanza política. La pretendida neutralidad de cada una de esas dimensiones del ciberespacio respecto de la otra no parece defendible.

La doctrina insiste en la impronta del aspecto tecnológico, rechazando su pretendida asepsia respecto del político. Desde esa perspectiva se defiende la necesidad de conciliar ambas modalidades de gobernanza²⁷ o, incluso, se reconoce que el concepto de *Governance of Internet* se ha visto superado por el de *Governance by Internet*²⁸.

En definitiva, esta situación se adivina difícilmente sostenible. Internet es generalmente reconocido como un recurso crítico de cuyo funcionamiento depende el conjunto de la sociedad y de los Estados. La seguridad y la estabilidad en la gobernanza tecnológica son necesarias para la gobernanza política del ciberespacio del mismo modo que la gestión de esta última es fundamental para el sostenimiento mismo de aquella otra.

El liderazgo privado, característico de la gobernanza tecnológica, no puede material y legítimamente sostenerse obviando la responsabilidad de los Estados en las políticas públicas. Pero tampoco la autoridad de los Estados podrá efectivamente imponerse

²⁷ De Nardis entiende que «The solution to long-term challenges in Internet governance requires bringing together the political and the technical, rather than dismissing the technical as not politically constructed or the political as not technologically constrained». DeNARDIS, L. «Five Destabilizing Trends in Internet Governance» *I-S: A Journal of Law and Policy*, vol. 12, 2015, p. 132.

²⁸ MUSIANI, F.; COGBURN, D. L.; DeNARDIS, L. y LEVINSON, N. S. *The Turn to Infrastructure in Internet Governance*. Nueva York: Palgrave MacMillan 2016.

soslayando el papel de la comunidad *multistakeholder* en la gobernanza del ciberespacio. En cualquiera de los casos, la ignorancia mutua no puede ser una opción.

*Margarita Robles Carrillo**
Profesora Titular Derecho Internacional Público y RRII
Grupo NESG (TIC-233)-UGR