SISTEMA ECONÓMICO LATINOAMERICANO Y DEL CARIBE

Universidad Pontificia de Salamanca
Institute of European Studies and Human Rights

EIIS EUROPEAN INSTITUTE OF INTERNATIONAL STUDIES

Informe de relatoría
Tercera edición de los cursos de Especialización en Ciberdiplomacia y La Diplomacia de las Monedas Digitales

Desarrollo Social

Tercera edición del Cursos de especialización en Ciberdiplomacia y La Diplomacia de las Monedas Digitales
Caracas, Venezuela
Del 11 al 14 de abril de 2023
SP/IIICECDMD/DT No. 1-23

C O N T E N I D O

I. RELATORÍA

En alianza con el Instituto Europeo de Estudios Internacionales (IEEI) y con la colaboración del de la Universidad Pontificia de Salamanca (España), la Secretaría Permanente del SELA realizó, del 11 al 14 de abril de 2023, vía digital, la Tercera edición de los cursos "Especialización en Ciberdiplomacia" y "La diplomacia de las Monedas Digitales".

En esta oportunidad, participaron 275 funcionarios públicos de la región, en su mayoría personal diplomático, personal de organismos regionales como la Comunidad Andina (CAN) y CAF-banco de desarrollo de América Latina, y docentes universitarios. Cada módulo de especialización contó con ocho horas académicas. Los contenidos sobre Ciberdiplomacia fueron impartidos los días 11 y 12 de abril, mientras que los de La Diplomacia de las Monedas Digitales lo fueron los días 13 y 14 del mismo mes. De nuevo, los facilitadores fueron los profesores Mario Torres Jarrin de la Universidad Pontifica de Salamanca y Shaun Riordan del IEEI.

En línea con su programación, ambos cursos fueron orientados a: i) desarrollar en los participantes capacidades negociadoras y obtener una mejor comprensión del desarrollo tecnológico y de las monedas digitales en el escenario internacional para afianzar los intereses de la región en la era digital; ii) analizar las diferentes agendas en una comunidad cibernética internacional, no exenta de conflictos interestatales, incluyendo el uso de las criptomonedas en actividades delictivas; iii) desarrollar habilidades en los futuros negociadores para interactuar con actores tecnológicos en la construcción de un acuerdo sobre normas de comportamiento en el ciberespacio, tanto en términos de gobernanza de Internet como de ciberseguridad y iv) explorar la forma de integrar los temas financieros en la política exterior con miras a la construcción de una diplomacia de las monedas digitales.

El Embajador Clarems Endara, Secretario Permanente del SELA y el Embajador Antonio Núñez García-Saúco, Director del IEEI, dieron las palabras de bienvenida a los participantes. El Embajador Endara expuso algunas ideas claves sobre la temática de los cursos y ponderó la importancia de desarrollar habilidades y capacidades en el dominio de las herramientas propias de la ciberdiplomacia y la techplomacia[1] en función de la necesidad de información que se requiere para "dirimir los problemas políticos y geopolíticos que surgen en el ciberespacio teniendo en cuenta que es un nuevo escenario en la vida de las personas para la difusión de información; un nuevo motor para el crecimiento económico; un nuevo vehículo para la prosperidad cultural; una nueva plataforma de gobernanza social; un nuevo puente para la comunicación y la cooperación, y un nuevo dominio de la soberanía estatal".

Señaló que las vulnerabilidades y riesgos potenciales de la infraestructura de la información obedecen en gran medida a la ausencia de reglas internacionales generales claras en el ciberespacio y, finalmente, expresó que la ciberdiplomacia "debe ser abordada como una política de Estado con definición de actores, objetivos, y metas a corto y largo plazo" y que ella demanda habilidades específicas para manejar las herramientas digitales con fines diplomáticos y actuar en la prevención, el abordaje y la solución de los problemas que tienen lugar en el ciberespacio. El texto de las palabras del Emb. Endara está disponible en:

Por su parte, el Embajador Núñez, expresó su coincidencia con las consideraciones hechas por el y ratificó la importancia de que los funcionarios involucrados se mantengan actualizados en el manejo de las herramientas digitales que necesitan para su trabajo vis a vis los retos asociados a la gobernanza de Internet y a la ciberseguridad que impactan tanto a la ciberdiplomacia como a la techplomacia.

[1] Concepto creado por el gobierno danés en 2017. Señala la importancia e impacto que tienen las *big tech companies* (GET, en español) en los asuntos internacionales, razón por la cual consideraron necesario repensar la diplomacia y enfocar parte de su acción exterior hacia las GET. El gobierno danés abrió la primera 'Tech Embajada' y nombraron a un 'Tech Embajador' ante los gigantes tecnológicos de los nuevos centros económicos y de poder: Silicon Valley, Copenhague y Beijing, por tanto, se brinda a las GET un estatus de actor internacional similar a las de los Estados. Mario Torres, en entrevista a la UPSA (https://www.upsa.es/actualidad).

II. CONCLUSIONES

A partir de las afirmaciones e ideas expresadas a lo largo de las dos sesiones de trabajo por los profesores Mario Torres y Shaun Riordan en sus presentaciones y en respuesta a las preguntas hechas por la audiencia, se derivaron las siguientes conclusiones y recomendaciones:

Ciberespacio

1. En el ciberespacio no existen fronteras, normas, ni gobernanza, de ahí la necesidad de crear normas internacionales que lo regulen.

2. El ciberespacio es un ámbito que requiere de la acción diplomática de los gobiernos en asuntos como la seguridad, la gobernanza de Internet y la regulación en materia de protección de datos o protección al consumidor, entre otros aspectos. El ciberespacio no responde a la lógica de soberanía territorial con la cual se rige el Estado moderno, al debate diario sobre el manejo de la información o a lo que debe ser la neutralidad de la red.

3. El ciberespacio constituye un nuevo escenario para la difusión de información; un nuevo motor para el crecimiento económico; un nuevo vehículo para la prosperidad cultural; una nueva plataforma para la gobernanza social; un nuevo puente para la comunicación y la cooperación y un nuevo dominio de la soberanía estatal.

4. Los Estados enfrentan algunos desafíos frente al ciberespacio de cuya estabilidad dependen la soberanía, la seguridad y el desarrollo de todos los países por lo que el desarrollo desequilibrado, las reglas inadecuadas y el orden inequitativo en el ciberespacio, así como la ampliación de la brecha digital entre países y regiones, constituyen una amenaza.

5. Las vulnerabilidades y riesgos potenciales de la infraestructura de la información obedecen, en gran medida, a la ausencia de reglas internacionales generales claras en el ciberespacio por lo que es necesario adaptar las normas legales a la era digital y a los avances en su regulación.

6. El uso de la ciberdiplomacia va más allá de la expansión de las redes diplomáticas a nivel digital y debe ser abordada como una política de Estado con definición de actores, objetivos y metas claramente definidas, lo que releva la necesidad de desarrollar habilidades para el uso de las herramientas digitales con fines diplomáticos para actuar en la prevención, el abordaje y la solución de los problemas propios del ciberespacio, es decir, en la ciberseguridad (acción para contrarrestar las amenazas y riesgos que surgen y se despliegan en el ciberespacio).

7. Hay una carencia de información no solamente de las posibilidades del ciberespacio sino que, en muchos países, incluso los parlamentarios, los tribunales, los fiscales, y los jueces, así como los ministerios que directa o indirectamente tienen que ver con el ciberespacio, y hasta los bancos centrales, están todos tratando de entender cómo funciona el ciberespacio.

8. Áreas como la gobernanza de Internet y la regulación económica y comercial del ciberespacio carecen de normas internacionales que regulen su comportamiento. Tampoco existen normas referidas a las distintas manifestaciones de la amenaza cibernética como la cibercriminalidad, la ciber(in)seguridad, el ciberespionaje y el ciberterrorismo.

9. La ciber(in)seguridad está afectando la paz internacional, el desarrollo sostenible, la cooperación digital, los derechos humanos y la privacidad, así como el entorno empresarial digital global.

10. La gobernanza del ciberespacio representa un desafío para el futuro del multilateralismo. El impacto de la Cuarta Revolución Industrial y la Globalización 4.0 en nuestro sistema internacional hace que sea necesario repensar el multilateralismo. Tal vez ha llegado el momento del Multilateralismo 4.0 (proceso de decisión 4 por 4 Helix y 0 para la Era Digital).

11. Hoy, la diferenciación entre los Estados viene dada por su capacidad tecnológica y su desarrollo digital y, dado que las *big tech companies* han alcanzado una presencia y un poder geopolítico igual o mayor que los Estados, y, como son ellas las que crean y administran el ciberespacio, cuando se trata de crear normas para la gobernanza en ese ámbito, los Estados van a la zaga de dichas empresas, hecho que abre la entrada de la diplomacia a esta materia dando lugar al surgimiento de la ciberdiplomacia.

12. La Unión Europea y América Latina y el Caribe son actores para la Gobernanza 4.0 la cual está destinada a reemplazar la visión de túnel y el enfoque descendente que primaron en el pasado. El actual, es un mundo muy complejo y ampliamente interconectado. Ello ha conducido a un cambio en los roles y en las responsabilidades de cada una de las partes interesadas de la sociedad de lo cual tanto las empresas como los gobiernos están plenamente conscientes.

13. Otro aspecto relevante asociado al ciberespacio es la fiscalidad (actualmente está siendo trabajada por la OCDE y la Unión Europea), es decir, todo lo relativo a los pagos tributarios (tributación transfronteriza) que deben realizar las empresas que actúan en este escenario que ya no es un terreno físico sino virtual, con todas sus implicaciones.

14. Las organizaciones regionales de integración tienen un escenario de actuación en el proceso de la elaboración de una normativa que gobierne el ciberespacio y deben actuar en coordinación con las empresas 4.0 y con los Estados, así como con el Grupo de Expertos Gubernamentales (GGE, en inglés) y el Grupo de Trabajo de Composición Abierta (OEWG, en inglés) de las Naciones Unidas.

15. Todos los actores que participan del ciberespacio: empresas internacionales, transnacionales y multinacionales de todo tipo; organismos internacionales, incluyendo los entes de integración regional los cuales deben actuar al amparo de Carta de las Naciones Unidas; las ONG; fundaciones de ámbito internacional o *Think Tanks;* las grandes empresas tecnológicas o *big tech companies*, convertidas ya en actores geopolíticos, y la Industria 4.0, requieren atención de parte de la diplomacia y de los Estados.

16. Actualmente, no existe una norma específica a nivel internacional que regule el comportamiento de los Estados y de otras entidades privadas y actores no estatales en el ciberespacio, debido, fundamentalmente, a su carácter difuso.

17. La ciberdiplomacia es la aplicación de la diplomacia a los problemas propios del ciberespacio y de esos problemas los más importantes no son de naturaleza técnica sino política y geopolítica, por lo que se ha dicho que "el ciberespacio es muy importante para dejárselo a los diplomáticos."

18. El problema de la atribución de responsabilidad en las ciber operaciones, en tanto que se producen en un espacio difuso, sin fronteras (el ciberespacio), y la ambigüedad de las operaciones cibernéticas aumentan los peligros crecientes.

19. En la actualidad, está planteado un dilema de la ciberseguridad en el que el país A teme al país B y penetra en sus sistemas informáticos para identificar sus capacidades e intenciones. El país B interpreta las

acciones del país A como una preparación agresiva para futuras operaciones cibernéticas y, consecuentemente, penetra en sus sistemas. El contacto diplomático tradicional contribuye a mitigar este dilema, lo que ha sido ratificado por algunos estudios de neurociencia cuyas conclusiones muestran que el contacto cara a cara ofrece mayor precisión en la identificación de intenciones.

20. Actualmente, las *big tech companies* no tienen interés en convertirse en un supra estado porque, fundamentalmente, su interés radica en la ampliación de sus mercados, al margen de las obligaciones características de un Estado. Asimismo, les interesan más las facilidades que los Estados puedan otorgarles como, por ejemplo, disposiciones que impidan la conformación de un mercado más equilibrado, facilitando así sus operaciones. Sin embargo, en alguna medida, constituyen un "superestado" en virtud de su inmenso poder económico y del alcance transfronterizo de su actuación.

21. La mayor capacidad de negociación con las *big tech companies* que tienen los Estados para los efectos de la regulación y la administración del ciberespacio, se deriva del hecho de que los sistemas de hardware, especialmente, los servidores están ubicados en los países y territorios soberanos, para los cuales es posible establecer normas que puedan controlar la acción de dichas empresas al interior de dichos países y territorios, pero solo en lo que concierne al hardware que utilizan.

22. El Derecho Internacional no está en capacidad de cubrir los delitos del ciberespacio. Cada vez más el delito cibernético se hace más sofisticado debido a la capacidad tecnológica de sus perpetradores por lo que, al menos, la mayoría de los Estados no tienen ni la fortaleza tecnológica ni los instrumentos legales para controlar el ciberdelito, razón por la cual todos los esfuerzos en función de la gobernanza del ciberespacio son de naturaleza multilateral bajo la égida de las Naciones Unidas.

23. La ciperdiplomacia o technoplomacia pueden servir de instrumentos para promover la creación de normas internacionales a la par que desarrollar relaciones formales con las *big tech companies*.

24. Un enfoque estratégico de la ciberseguridad contempla, entre otros, los siguientes aspectos: los problemas o desafíos de la ciberseguridad son de naturaleza tan social como técnica; cooperación internacional con aliados; compromisos con los rivales y la búsqueda de espacios comunes para la construcción de normas de conducta internacional.

25. La diplomacia del mundo digital no debe limitarse a la actuación de representantes de las empresas exclusivamente porque ellas no tienen la legitimidad ni la confiabilidad democrática. Se requieren representantes del gobierno porque, se espera que estén mejor capacitados para entender y gestionar los problemas políticos y geopolíticos asociados al ciberespacio, tan importantes como los problemas técnicos. Además, las empresas han mostrado un conocimiento muy deficiente de los elementos políticos.

Inteligencia artificial (IA)

1. Es un tema que debe ser debatido mucho más. Sorprende el muy reducido tiempo que se dedica a considerar las consecuencias sociales, políticas y geopolíticas de la IA en la educación, la política exterior, el mundo militar, entre otros. El diplomático debe preocuparse por entender la IA, preferiblemente, en sentido general, no técnico, de manera que pueda participar inteligentemente en los debates en torno a ella.

Internet

1. Desde la perspectiva de su gobernanza, Internet es visualizada como: i) un espacio libre de todo control gubernamental siguiendo un modelo *multistakeholder* (varias partes interesadas: organismos internacionales, gobiernos, profesionales de Internet, empresas y organizaciones de la sociedad civil) o de "soberanía ciber"; ii) ciberespacio como un dominio en el cual un Estado puede ejercer su soberanía; y iii) un escenario en el que tiene lugar "una nueva guerra fría" librada entre los partidarios de i) y de ii).

2. Hay una tendencia a aceptar la necesidad de controlar la red para frenar desviaciones de su uso como la pornografía infantil, el blanqueo de dinero y la desinformación, entre muchas otras.

3. La Internet Corporation for Assigned Names and Numbers, (ICANN) es una empresa privada sin fines de lucro, registrada en California y que tiene la responsabilidad de asignar los números de dominios en Internet. La Comisión Ejecutiva que decide sobre los dominios no tiene representación gubernamental y sus miembros se eligen a sí mismos.

4. En cuanto a la protección de los datos, la Unión Europea (UE) aboga por la creación de mecanismos que la hagan efectiva. Por su parte, Estados Unidos es más bien flexible al respecto y considera como un acto hostil contra las empresas estadounidenses, cualquier intento de la UE en materia de protección de datos.

La diplomacia de las monedas digitales

1. La criptomoneda se ha posicionado como un medio alternativo de la moneda tradicional, con la finalidad de ofrecer oportunidades de inversión, así como un manejo óptimo de los negocios a partir del dinero digital.
2. Las criptomonedas no cuentan con un soporte financiero que las respalde con lo que exponen los capitales invertidos en ellas y, al mismo tiempo, tienen la capacidad de generar grandes cambios en la economía de los países, como medio de pago o como posibilidad de inversión.
3. Las criptomonedas están provocando un cambio en el sistema internacional que afecta a la gobernanza global, a los flujos de comercio internacional y al sistema financiero.
4. La falta de regulación del ciberespacio está creando vacíos legales en diferentes sectores de la economía y en el conjunto de los ámbitos de la sociedad: jurídico, económico, político, social y cultural.
5. El mundo está asistiendo a una reconfiguración del sistema internacional a través del surgimiento de las *big tech companies* como nuevos actores geopolíticos.
6. Las criptomomonedas deben ser estudiadas y los posibles casos de blanqueamiento de dinero, participación de mafias y todo tipo de tráfico de personas, de drogas, etc., deben ser esclarecidos.
7. El Central Bank Digital Currency (CBDC) es el banco central de la moneda digital de un país.
8. Los CBDC manejan información sensible y privada de cada persona que podría ser utilizada por los gobiernos para monitorear y controlar a los ciudadanos.
9. A través de los CBDC se puede obtener información, en tiempo real, de las transacciones económicas lo que facilitaría una planificación de la economía.

III. RECOMENDACIONES

Ciberdiplomacia y La Diplomacia de las Monedas Digitales

1. Se necesita crear un regulador internacional que: i) identifique al actor principal en la gobernanza del ciberespacio; ii) promueva el debate entre las partes interesadas (actores públicos, privados, académicos y de la sociedad civil); iii) proporcione normas internacionales y iv) promueva la utilización de la ciberdiplomacia y la techplomacia.

2. Habida cuenta de su vinculación con los ministerios de relaciones exteriores en América Latina y el Caribe, el SELA podría convocar una conferencia internacional en la cual se plantee el diseño de una estrategia regional orientada a aminorar las brechas digitales en la región y a adoptar posiciones conjuntas para lograr tener un mayor poder de negociación con otras regiones y con las propias *big tech companies* (instancias que poseen la información más completa sobre el ciberespacio) con las cuales América Latina y el Caribe debe desarrollar relaciones, las cuales serán más equilibradas y provechosas en la medida en que la región se presente como un solo bloque.

Geopolítica y la diplomacia de las criptomonedas

1. Definir las características de los CBDC y velar para que garanticen los derechos fundamentales y los derechos humanos y no sean utilizados como un instrumento de control ciudadano.

2. Convocar a una conferencia internacional a nivel de bancos centrales para consensuar posiciones sobre las criptomonedas y el Central Bank Digital Currency (CBDC).