Versión original: inglés/francés - Traducción: Lic. Carina Galvalisi Kemayd
www.secretariagrulacuip.org

146ª Asamblea de la UIP
Manama (11–15 de marzo de 2023)

Los ciberdelitos: los nuevos riesgos a la seguridad mundial

Resolución adoptada por consenso [*] por la 146ª Asamblea de la UIP
(Manama, 15 de marzo de 2023)

La 146ª Asamblea de la Unión Interparlamentaria,

Condenando todas las formas de ciberdelincuencia y reafirmando la necesidad de combatir estos actos a través de la cooperación internacional,

Reafirmando el marco existente de las Naciones Unidas relativo al comportamiento responsable de los Estados en la utilización de las tecnologías de la información y la comunicación (TIC) y la necesidad de implementar este marco,

Reconociendo que existe la necesidad de generar confianza y entendimiento mutuo entre los países frente a la utilización maliciosa de las TIC por parte de actores estatales y no estatales, que no conocen fronteras ni límites,

Observando el uso y la dependencia cada vez mayores de las TIC en todo el mundo,

Consciente del aumento de las actividades de ciberdelincuencia vinculadas a la aceleración de la transformación digital, acentuada por la pandemia de COVID-19,

Tomando nota de la responsabilidad de los parlamentos de establecer un marco normativo que proteja a los ciudadanos en el ciberespacio utilizando nuevas infraestructuras y recursos, de la misma manera que en el mundo físico,

Recordando las siguientes resoluciones de la Asamblea General de las Naciones Unidas: 31/72 de 10 de diciembre de 1976 titulada *Convención sobre la prohibición del uso de técnicas de modificación ambiental con fines militares o cualquier otro propósito hostil*, 55/63 de 4 de diciembre de 2000 y 56/121 de 19 de diciembre de 2001 titulada *Lucha contra la explotación de las tecnologías de la información con fines delictivos*, 57/239 de 31 de enero de 2003 titulada *Creación de una cultura global de ciberseguridad*,

Recordando también las resoluciones anuales de la Asamblea General de las Naciones Unidas sobre el tema *Avances en informática y telecomunicaciones y seguridad internacional*, y en particular la resolución 69/28 de 2 de diciembre de 2014, la resolución 73/266 de 22 de diciembre de 2018 por la que se crea el Grupo de Expertos Gubernamentales para fomentar el comportamiento responsable de los Estados en el ciberespacio en el contexto de la seguridad internacional, así como la resolución 75/240 de 31 de diciembre de 2020 que establece

[*] La delegación de India expresó reservas sobre el párrafo operativo 25.
La delegación de la Federación de Rusia expresó reservas sobre el párrafo 11 del preámbulo y el párrafo operativo 1

el Grupo de Trabajo de composición abierta sobre la seguridad digital y su utilización (2021-2025), y *subrayando* las normas voluntarias y no
vinculantes relativas al comportamiento responsable de los Estados en la utilización de las TIC en el contexto de la seguridad internacional, elaboradas por el Grupo de Expertos Gubernamentales y aprobada por la resolución 70/237 de la Asamblea General de las Naciones Unidas de 23 de diciembre de 2015, que llama a los Estados Miembros de la ONU a ser guiados por estas normas, así como el establecimiento, mediante la resolución 77/37 de la Asamblea General de las Naciones Unidas de 7 de diciembre de 2022, de un programa de acción de las Naciones Unidas destinado a examinar las amenazas existentes y potenciales y a apoyar las capacidades y los esfuerzos de los Estados para implementar y promover los compromisos,

Recordando además la *Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional* de 15 de noviembre de 2000 y la *Convención de las Naciones Unidas contra la Corrupción* de 31 de octubre de 2003,

Subrayando la importancia de los convenios regionales sobre ciberdelincuencia, delincuencia organizada transnacional, intercambio de información y asistencia administrativa, en particular la *Convención del Consejo de Europa sobre ciberdelincuencia* de 23 de noviembre de 2001 y su *Protocolo adicional relativo a la tipificación como delito de los actos de carácter racista y xenófobo cometidos a través de sistemas informáticos* de 28 de enero de 2003, el *Acuerdo de Cooperación para Garantizar la Seguridad Internacional de la Información entre los Estados Miembros de la Organización de Cooperación de Shanghai* de 16 de junio de 2009 y la *Convención Árabe sobre la Lucha contra los Delitos Relacionados con la Tecnología de la Información* de 21 de diciembre de 2010, así como las Leyes Modelo del Parlamento Latinoamericano y Caribeño (PARLATINO) sobre Ciberdelincuencia (noviembre 2013) y sus versiones actualizadas, la prevención social de la violencia y del delito (noviembre 2015), los delitos informáticos (febrero 2021) y lucha contra el comercio ilícito y la delincuencia transnacional (febrero de 2021), el *Acuerdo de cooperación entre los Estados Miembros de la Comunidad de Estados Independientes para garantizar la seguridad de la información* de 20 de noviembre de 2013 y el *Acuerdo de cooperación entre los Estados Miembros de la Comunidad de Estados Independientes sobre la lucha contra la delincuencia en el ámbito de las tecnologías de la información* de 28 de septiembre de 2018, y la *Convención sobre ciberseguridad y protección de datos personales de la Unión Africana* de 27 de junio de 2014,

Subrayando también que la *Convención del Consejo de Europa sobre el Delito Cibernético*, que está abierta a la adhesión de todos los países, se ha convertido en un instrumento de importancia mundial que incluye a los Estados Partes de todas las regiones del mundo y tiene un impacto en estos,

Recordando el trabajo de la UIP sobre los diversos nuevos riesgos a los que están expuestas nuestras sociedades cada vez más digitalizadas, en particular las resoluciones de la UIP tituladas *La ciberguerra: una grave amenaza para la paz y la seguridad mundial* (adoptada el 1º de abril de 2015 en la 132ª Asamblea, en Hanói) y *La Legislación en todo el mundo para combatir la explotación y el abuso sexuales de niños en línea* (adoptada el 30 de noviembre de 2021 en la 143ª Asamblea, en Madrid), la cual recuerda también la Convención del Consejo de Europa titulada *La protección de los niños contra la explotación y el abuso sexuales* (Convención de Lanzarote) de 25 de octubre de 2007,

Acogiendo con beneplácito la labor de las Naciones Unidas para promover un comportamiento responsable de los Estados en el ciberespacio,

Acogiendo con satisfacción los esfuerzos realizados por las Naciones Unidas para adoptar, a través de la resolución 74/247 de la Asamblea General, de 27 de diciembre de 2019, una convención internacional sobre el delito cibernético, y *acogiendo también con satisfacción* la creación de un comité ad hoc encargado de elaborar esta convención,

Acogiendo con beneplácito el hecho de que la UIP esté participando en el proceso de consulta de múltiples partes interesadas de este comité especial para hacer escuchar la voz de los parlamentos,

Tomando nota de la necesidad de aplicar un enfoque global al problema del delito cibernético y sus graves consecuencias para los ciudadanos, así como de la necesidad de proteger la paz, la seguridad y la estabilidad económica mundiales, respetando al mismo tiempo los principios fundamentales de los derechos humanos, incluida la libertad de expresión ,

Reconociendo que los legisladores, los gobiernos y todas las partes interesadas deben tomar urgentemente medidas más enérgicas a nivel nacional para combatir el delito cibernético, dada su multiplicación y rápida evolución,

Reconociendo también que todas las medidas adoptadas en esta área deben garantizar el respeto de los derechos humanos y los derechos fundamentales,

Observando la evolución desigual de las capacidades delos países en el área de las TIC y de su capacidad para proteger la infraestructura de las TIC, y *subrayando* la necesidad de una mayor asistencia técnica y colaboración, en particular para los países en desarrollo,

Observando también que los Estados deben actuar de conformidad con sus obligaciones en virtud del derecho internacional de los derechos humanos, incluido el *Pacto Internacional de Derechos Civiles y Políticos*, la *Convención sobre los Derechos del Niño*, la *Convención contra la tortura y otros tratos o penas crueles, inhumanos o degradantes* , la *Convención sobre la eliminación de todas las formas de discriminación contra la mujer*, así como sus protocolos adicionales y otros instrumentos internacionales de derechos humanos pertinentes,

Reconociendo que es necesaria una acción parlamentaria conjunta de alcance internacional para difundir e implementar las normas voluntarias y no vinculantes de comportamiento responsable de los Estados en la utilización de las TIC,

Observando que la ciberdelincuencia puede suponer una grave amenaza para los procesos democráticos, en particular en lo que respecta a la interferencia en las elecciones mediante el uso de lagunas en la ciberseguridad o cuentas falsas de redes sociales,

Reconociendo que las mujeres, los jóvenes, los niños, los ancianos, las personas con discapacidad y las poblaciones racializadas son particularmente vulnerables a la ciberdelincuencia,

Reconociendo también la necesidad de promover la igualdad de género y el empoderamiento de las mujeres y las niñas en toda su diversidad, incluso mediante la incorporación de la perspectiva de género y en el diseño, implementación y aplicación de las políticas, los programas y la legislación sobre estos temas,

Tomando nota de la naturaleza de las amenazas y los riesgos del ciberdelito transnacional para la paz y la seguridad internacionales, así como del rápido desarrollo del ciberespacio, lo que significa que los métodos utilizados por los ciberdelincuentes son cada vez más sofisticados,

Tomando nota también que el delito cibernético incluye, entre otros, ataques a sistemas informáticos, violaciones de la privacidad, la creación y despliegue de software malicioso y, cada vez más, ataques a infraestructura civil estratégica, así como otros actos que pueden ocurrir fuera de línea y ser facilitados por los sistemas informáticos, incluido el fraude en línea, el tráfico de drogas, el blanqueo de capitales, los delitos de odio, la trata de personas y la violencia de género facilitada por la tecnología, como el acoso sexual, las amenazas, el acoso, la intimidación, la incitación al odio por motivos de género y la explotación sexual de mujeres y niños a través de Internet, todo lo cual tiene un impacto negativo en la seguridad global y la estabilidad económica,

Considerando que la mayoría de las leyes nacionales fueron adoptadas antes de la aparición del delito cibernético y, por lo tanto, no siempre permiten responder de manera efectiva a estas amenazas,

1. *Alienta* a los parlamentos a tomar las medidas necesarias para que su país se adhiera, si aún no lo ha hecho, a los instrumentos internacionales existentes que abordan la utilización de las TIC con fines delictivos, en particular, la *Convención sobre Ciberdelincuencia* del Consejo de Europa, que constituye el tratado multilateral

más completo sobre ciberdelincuencia actualmente en vigor y que está abierto a la adhesión de todos los Estados;

2. *Pide* a los parlamentos que aseguren que la legislación sobre los ciberdelitos esté actualizada y sea pertinente, de conformidad con el derecho internacional, incluidos los instrumentos internacionales de derechos humanos, para asignar los medios necesarios y movilizar a todas las partes interesadas, incluidos el sector privado, el mundo académico, la sociedad civil y la comunidad técnica, dada la escala, el alcance, la velocidad, la complejidad y la frecuencia cada vez mayores de estas actividades y sus consecuencias para la seguridad nacional, la paz y la seguridad internacionales y la estabilidad económica mundial, así como prever en estas leyes la jurisdicción extraterritorial para permitir el enjuiciamiento de autores de actos delictivos, independientemente del lugar donde se hayan cometido estos actos y de si constituyen o no un delito en la jurisdicción extranjera correspondiente;

3. *Insta* a los parlamentos a asegurar que las evaluaciones de impacto sobre los derechos humanos se integren en todos los procesos legislativos relacionados con la ciberdelincuencia;

4. *Pide* a los parlamentos que fortalezcan las capacidades de los funcionarios encargados de hacer cumplir la ley, incluidos los servicios de investigación, los fiscales y los jueces, en el ámbito de la ciberdelincuencia, y que los capaciten para investigar, enjuiciar a los autores de estos delitos y juzgar de manera eficaz los casos de ciberdelincuencia;

5. *Alienta* a los parlamentos a hacer pleno uso de su función de supervisión para garantizar que los gobiernos cuenten con las herramientas necesarias, incluidos los recursos y capacidades apropiados, para prevenir y combatir el rápido aumento de la ciberdelincuencia y proteger la ciberseguridad, la identidad, la privacidad y los datos de los ciudadanos, garantizando al mismo tiempo el respeto por los derechos humanos y las libertades;

6. *Recomienda firmemente* a los parlamentos a garantizar que los marcos legislativos nacionales relacionados con la protección de la infraestructura nacional crítica, incluida la infraestructura de Internet, estén actualizados, o que establezcan dichos marcos según sea necesario;

7. *Alienta* a los parlamentos a promover un ciberespacio abierto, libre y seguro instando a su gobierno a cumplir con las normas de las Naciones Unidas sobre el comportamiento responsable de los Estados en el ciberespacio, cooperar en la lucha contra el ciberdelito y evitar que los ciberdelincuentes y los actores maliciosos actúen, respondan a las solicitudes de asistencia y desarrollo de capacidades, cuando sea posible en tiempo real, de acuerdo con el estado de derecho y respetando plenamente el derecho internacional de los derechos humanos y los derechos fundamentales, para asegurar la cadena de suministro de las empresas en su país, para informar espontáneamente a terceros sobre posibles vulnerabilidades para ayudarlos a prevenir incidentes futuros, y en particular para apoyar y proteger a todos los equipos de respuesta en caso de un incidente cibernético dentro y fuera de las fronteras de su país;

8. *Alienta también* a los parlamentos a desarrollar legislación sensible al género que promueva servicios transversales de seguridad cibernética centrados en la prevención (concientización, auditoría y capacitación) y detección de incidentes (24/7) y que permitan una respuesta inmediata y efectiva a las amenazas cibernéticas, a través de un enfoque centrado en la víctima;

9. *Recomienda* que los parlamentos promuevan el establecimiento de instituciones y órganos apropiados, por ejemplo, centros nacionales de ciberseguridad, equipos de respuesta rápida informática, equipos de respuesta a incidentes de seguridad informática y centros de operaciones de seguridad, cuando aún no existan en su país;

10. *Recomienda también* que todos los parlamentos se aseguren de que estas instituciones y órganos cuenten con suficientes recursos presupuestarios y personal especializado, incluidas mujeres expertas en ciberseguridad, para poder responder de manera flexible, rápida y eficaz al ciberdelito y para proteger la infraestructura civil, las instituciones públicas, las empresas y los ciudadanos sin infringir la privacidad, teniendo en cuenta que la creciente digitalización de los servicios públicos y colectivos puede dar lugar a una exposición significativa a los riesgos digitales;

11. *Insta* a los parlamentos a que promuevan la coordinación internacional entre estas instituciones y organismos para monitorear, prevenir, detectar, investigar y combatir las ciberamenazas;

12. *Invita* a los parlamentos a alentar a su gobierno a brindar capacitación específica en seguridad cibernética para aumentar el número de especialistas en seguridad cibernética y desarrollar su capacidad;

13. *Reafirma* que un entorno de las TIC abierto, seguro, estable, accesible y pacífico es esencial para todos y requiere una cooperación eficaz entre los Estados para reducir los riesgos para la paz y la seguridad internacionales, y pide a la comunidad internacional que promueva el pleno respeto de los derechos humanos y libertades fundamentales;

14. *Pide* a los parlamentos que fomenten la inversión en investigación y desarrollo, incluyendo disposiciones específicas sobre ciberseguridad en proyectos de ley y propuestas legislativas y proporcionando suficientes créditos presupuestarios, para anticipar posibles ciberamenazas emergentes y protegerse de ellas;

15. *Alienta* a los parlamentos a asociarse con empresas, instituciones académicas y todas las demás partes interesadas, incluida la sociedad civil, encargando a su gobierno que desempeñe el papel de facilitador, a fin de desarrollar un ecosistema de ciberseguridad sólido y colaborativo que respete plenamente los principios de derechos humanos y las obligaciones internacionales pertinentes;

16. *Pide* a los parlamentos y parlamentarios que trabajen activamente para desarrollar, a nivel nacional, una comprensión común y actualizada de la naturaleza del delito cibernético tal como lo experimentan los ciudadanos, las organizaciones y las instituciones;

17. *Insta* a los parlamentos a ayudar a desarrollar una verdadera "cultura de ciberseguridad" mediante el desarrollo de programas educativos destinados a formar a las generaciones futuras, desde la infancia, en el aprendizaje digital y el conocimiento tecnológico, tanto en términos de las amplias posibilidades que ofrecen las tecnologías como de los importantes riesgos asociados con las mismas;

18. *Recomienda* que los parlamentos fortalezcan la protección de las mujeres, los jóvenes, los niños, los ancianos, las personas con discapacidad y las poblaciones racializadas en el ciberespacio, garantizando el respeto de los derechos humanos y proporcionando en las políticas materiales educativos sobre el uso de los dispositivos de redes sociales para prevenir la violencia basada en el género;

19. *Insta* a los parlamentos a que tomen las medidas necesarias para proteger los momentos cruciales de la democracia, en particular los períodos en que los ciudadanos ejercen su derecho al voto, a fin de evitar ataques e injerencias encaminadas a influir, modificar o violar la libre formación de la opinión de los ciudadanos durante los procesos electorales;

20. *Pide* a la comunidad internacional que tome medidas para proteger la democracia garantizando que todos los parlamentos del mundo, como instituciones que

representan la voluntad del pueblo, gocen de una protección especial mediante su inclusión en las listas de infraestructura civil crítica nacional y servicios esenciales;

21. *Resalta* la necesidad de seguir reforzando la cooperación y la asistencia internacionales en el área de la seguridad de las TIC y el desarrollo de capacidades, a fin de reducir la brecha digital y fortalecer la lucha contra las ciberamenazas en todo el mundo;

22. *Pide* a los parlamentos que adquieran una comprensión más profunda de la naturaleza compleja y en rápida evolución del delito cibernético facilitando el libre intercambio de conocimientos, experiencias y conocimientos, y organizando seminarios, talleres y conferencias especializados en este tema;

23. *Invita* a la Secretaría de la UIP, junto con las organizaciones concernidas, a promover esta nueva visión de la ciberseguridad apoyando a los parlamentos en sus esfuerzos de creación de capacidades;

24. *Recomienda* que la UIP, como la organización mundial de los parlamentos, desempeñe un papel de liderazgo en la prevención y la lucha contra el delito cibernético y la promoción de la resiliencia cibernética participando en todos los foros internacionales pertinentes, incluidos los organizados por las Naciones Unidas, para hacer oír la voz de los parlamentos;

25. *Promueve* la creación de un grupo de trabajo sobre ciberdelincuencia, subsidiario del Consejo Directivo de la UIP, con la misión de cumplir con los mandatos y objetivos establecidos en esta resolución, y que se encargará de apoyar el proceso de promoción de una Convención Internacional sobre Ciberdelincuencia en el marco del sistema de las Naciones Unidas y fortalecer las capacidades de los parlamentos Miembros de la UIP en la elaboración de leyes, la supervisión y la elaboración de presupuestos.

26. *Recomienda* que la UIP sensibilice a los parlamentos sobre la realización de los Objetivos de Desarrollo Sostenible destacando, ante todo, sus compromisos universales de seguridad digital.