ORGANIZACIÓN MUNDIAL DEL COMERCIO

G/TBT/GEN/357

20 de julio de 2023

(23-4958) Página: 1/7

Comité de Obstáculos Técnicos al Comercio

SESIÓN TEMÁTICA SOBRE LA COOPERACIÓN ENTRE LOS MIEMBROS EN MATERIA DE REGLAMENTACIÓN DE LA CIBERSEGURIDAD

20 DE JUNIO DE 2023, 15 - 18 H

Informe del Moderador[1]

En el noveno examen trienal, los Miembros acordaron seguir celebrando sesiones temáticas en paralelo a las reuniones ordinarias del Comité en el período de 2022 a 2024, con miras a profundizar aún más en los intercambios de experiencias del Comité sobre temas específicos. Sobre esta base, el Comité acordó celebrar una sesión temática sobre la cooperación en materia de reglamentación de la ciberseguridad.[2] La sesión temática brindó la oportunidad de examinar la contribución de los reglamentos técnicos, las normas y los procedimientos de evaluación de la conformidad a las políticas de los Miembros para hacer frente a las amenazas a la ciberseguridad. Los Miembros examinaron los enfoques actuales para gestionar los riesgos de ciberseguridad y las oportunidades de cooperación en materia de reglamentación. La información sobre los oradores, las exposiciones y los materiales conexos puede consultarse en el sitio web de la OMC.[3]

1 OBSERVACIONES INTRODUCTORIAS DEL MODERADOR

1.1. La sesión temática fue oportuna, en particular en vista del creciente debate entre los Miembros sobre las políticas y los reglamentos de ciberseguridad en el Comité OTC.

1.2. En primer lugar, como dato ilustrativo, los Miembros han notificado al Comité OTC alrededor de 80 medidas relacionadas con la ciberseguridad (al 31 de mayo de 2023). Se trata claramente de una nueva tendencia, ya que la gran mayoría de esas medidas (más del 60%) se notificaron a partir de 2020. Esas notificaciones se referían a una amplia gama de productos y situaciones, por ejemplo: la ciberseguridad de la Internet de las cosas (IdC), la tecnología 5G, las telecomunicaciones, los vehículos y el equipo radioeléctrico y los productos basados en programas informáticos y conectados a la red. En aproximadamente la mitad de esas medidas se indicaba que se habían propuesto o adoptado para la protección de los intereses de seguridad nacional.

1.3. En segundo lugar, en los últimos años, los Miembros de la OMC han utilizado cada vez más el Comité OTC para plantear y debatir preocupaciones comerciales específicas relativas a diversas medidas relacionadas con la ciberseguridad. Las medidas objeto de esas preocupaciones regulan, por ejemplo, los productos de las TIC y los equipos de red, los vehículos, la aviación civil, la banca y los seguros. Hasta la fecha, los Miembros han planteado al menos 26 preocupaciones comerciales específicas de este tipo, la mayoría de ellas (el 60%) en los seis últimos años (2017-mayo de 2023). Estos debates son importantes habida cuenta de la naturaleza del tema, así como del valor cuantitativo de las preocupaciones en cuestión. Según las estimaciones de la Secretaría de la OMC, el valor medio de las importaciones por preocupación comercial específica relacionada con la ciberseguridad asciende a casi USD 160.000 millones. De hecho, en comparación con el resto de preocupaciones comerciales específicas relativas a los otros "temas", las medidas relacionadas con la ciberseguridad son el tipo de preocupaciones comerciales específicas más importante por lo que respecta al valor.

[1] Sr. Wei Guo Tang (Singapur). Este informe se distribuye bajo la responsabilidad del moderador.
[2] G/TBT/46, párrafo 2.11.
[3] OMC | Sesión temática sobre la cooperación entre los Miembros en materia de reglamentación de la ciberseguridad.

2 DEBATE

2.1 Preguntas orientativas

- ¿Cuáles son los desafíos y las oportunidades que se plantean en el ámbito del comercio y la reglamentación de la ciberseguridad?

- ¿Cómo contribuyen las disciplinas y los principios del Acuerdo OTC de la OMC a la formulación de políticas comerciales eficaces para garantizar la ciberseguridad? ¿Qué función puede desempeñar el Comité OTC en ese proceso?

- ¿Qué mejores prácticas deberían orientar la elaboración y aplicación de reglamentos en esta esfera? ¿Qué función pueden desempeñar las normas internacionales a este respecto?

3 INTERVENCIONES

3.1. El **Sr. Mike Mullane** (CEI)[4] presentó la labor de la CEI en materia de normas de ciberseguridad, centrándose en el enfoque ecosistémico de la organización con respecto a la elaboración de normas en esta esfera. La CEI elabora normas horizontales de ciberseguridad centradas en la seguridad de la información y las operaciones y normas verticales relativas a sectores específicos (por ejemplo, la IEC 63154 o la ISO/IEC 29128-1). El Sr. Mullane también mencionó algunos de los principales beneficios de utilizar normas y evaluaciones de la conformidad en la esfera de la ciberseguridad, por ejemplo, que crean seguridad y confianza con los interlocutores comerciales, permiten garantizar la coherencia gracias a la armonización y aumentan el acceso a los mercados y el reconocimiento mundial. También explicó el enfoque basado en el riesgo de las normas de la CEI, que alienta a las empresas a clasificar sus activos con arreglo al nivel de seguridad requerido. Para concluir, el Sr. Mullane destacó la importancia de la colaboración mundial para hacer frente a las amenazas a la ciberseguridad y alentó a los Miembros a adoptar el marco común de normas de la CEI.

3.2. La **Sra. Nandini Jolly** (Canadá)[5] explicó que, en el contexto posterior a la pandemia de COVID-19 y el clima geopolítico actual, cada vez es más importante la seguridad centrada en los datos (frente a la que se centra únicamente en las redes). La oradora presentó el enfoque de confianza cero de CryptoMill en materia de ciberseguridad, cuyo objetivo es pasar a una seguridad centrada en los datos, y destacó la importancia de ser conscientes de que existen riesgos tanto dentro como fuera de una red.

3.3. Los servicios de CryptoMill están especializados en resolver problemas vinculados a la ciberdelincuencia externa, filtraciones de datos internos, programas maliciosos secuestradores, vulnerabilidades de la cadena de suministro, correos electrónicos enviados a direcciones erróneas, datos residuales y dispositivos robados. La Sra. Jolly presentó también el paquete informático "Circles of Trust" de la empresa, una plataforma de seguridad que permite a las empresas, el sector militar y los gobiernos tener el control del acceso a todos los datos sensibles y de su utilización, por ejemplo para que los datos compartidos con asociados comerciales también estén protegidos. La oradora concluyó expresando su preocupación por los riesgos de ciberseguridad asociados a la creciente popularidad del trabajo híbrido. La Sra. Jolly reiteró la importante necesidad de reforzar la colaboración y la cooperación, también en la esfera de las normas, para identificar y resolver esos riesgos. La colaboración puede ayudar a mejorar el intercambio de información a fin de acelerar el desarrollo tecnológico necesario para hacer frente a estas amenazas.

3.4. El **Sr. Jonathan McHale** (Estados Unidos)[6] centró su exposición en la necesidad de cooperación y de soluciones mundiales para hacer frente a las amenazas a la ciberseguridad. Explicó que las medidas nacionales destinadas al mundo digital, como las prescripciones nacionales en materia de encriptación o seguridad de los servicios wifi, distorsionaban claramente el comercio y no tenían beneficios evidentes, y que algunas medidas, como las de localización de los datos, podían a veces comprometer la ciberseguridad mundial al limitar la visibilidad global de las amenazas existentes. En su opinión, se necesitaba una respuesta mundial basada en la normalización para

[4] Oficial de Promoción, Comisión Electrotécnica Internacional (CEI).
[5] Directora Ejecutiva de Crypto Mill Cybersecurity Solutions, Canadá.
[6] Vicepresidente de Comercio Digital, Asociación de la Industria de la Informática y las Comunicaciones (CCIA), Estados Unidos.

hacer frente a las amenazas a la ciberseguridad, en un entorno digital que, tal como estaba diseñado, también tenía un alcance mundial. El Sr. McHale subrayó que es necesario cooperar para alcanzar un consenso mundial sobre cuáles son las amenazas más importantes a la ciberseguridad, a fin de utilizar de manera eficiente los recursos para hacerles frente. El orador concluyó recordando a los asistentes los principales factores que debían tenerse en cuenta al elaborar normas sobre ciberseguridad, como los requisitos de conformidad conexos, la participación de las partes interesadas en el proceso de elaboración y los efectos sobre el comercio.

3.5. La **Sra. Jacqueline Fick** (Sudáfrica)[7] subrayó la importancia de la cooperación internacional y la armonización al elaborar legislación en materia de ciberseguridad, a fin de mejorar las estrategias de ciberseguridad y la privacidad de los datos. La Sra. Fick explicó que la ciberseguridad y la ciberdelincuencia son cuestiones interrelacionadas que deben abordarse conjuntamente. A tal fin, propuso un enfoque colaborativo transfronterizo para afrontar el hecho de que la ciberdelincuencia no sabe de fronteras: mecanismos eficientes y eficaces para lidiar con problemas que ocurren muy rápidamente. Contar con legislación en materia de ciberseguridad es fundamental porque es básica para asegurar un comercio electrónico eficaz, aumenta la confianza entre los países, mejora la respuesta ante los incidentes y refuerza la capacidad de obligar a los ciberdelincuentes a rendir cuentas cuando es necesario. Así pues, la Sra. Fick subrayó que la armonización, la cooperación internacional y la normalización son necesarias no solo para crear instrumentos internacionales eficaces, sino también para aumentar la certidumbre con respecto a las prácticas de ciberseguridad aceptadas a nivel mundial, intensificar las medidas de lucha contra la ciberdelincuencia y facilitar el intercambio de pruebas electrónicas entre los países que sean admisibles en un tribunal de justicia. No es necesario "reinventar la rueda". Ninguno de estos esfuerzos debe considerarse un intento de interferir en la soberanía de los países, sino más bien de impulsar un entorno cibernético mundial seguro. La Sra. Fick señaló que las medidas de ciberseguridad eran una prioridad para el Gobierno de Sudáfrica y describió el enfoque legislativo que habían adoptado al respecto. También hizo un llamamiento en favor del aumento de la formación y la sensibilización en materia de ciberseguridad y de la asistencia judicial recíproca y el intercambio de información.

3.6. En su exposición, el **Sr. Jiefu Gan** (China)[8] defendió la necesidad de promover una cooperación multilateral más inclusiva en lo que respecta a la normalización y las evaluaciones de la conformidad en el ámbito de la ciberseguridad y enumeró algunas de las oportunidades y desafíos a este respecto. Según el Sr. Gan, hay oportunidades en las esferas de la economía digital, los datos y los productos digitales, así como en las de la ciberseguridad y la seguridad de los datos. Entre los desafíos más notables cabe mencionar el déficit de gobernanza digital a nivel mundial y, en consecuencia, el riesgo de división y fragmentación de dicha gobernanza.

3.7. El Sr. Gan planteó varias propuestas, a saber: mantener los mercados abiertos y libres de discriminación, fomentar la unidad y la cooperación mundiales mediante la creación de normas interoperables y comunes, establecer un equilibrio entre desarrollo y seguridad, asegurar el compromiso con la equidad y la justicia y promover una cooperación más inclusiva en lo que respecta a las normas y las evaluaciones de la conformidad en el ámbito de la ciberseguridad. Por último, proporcionó ejemplos de prácticas de China, donde se habían adoptado varias medidas como la utilización de procedimientos de evaluación de la conformidad como instrumento de apoyo técnico para la gestión de la ciberseguridad y la aplicación de legislación para promover la certificación y las normas.

3.8. La **Sra. Huirong Tian** (China)[9] presentó las actividades de normalización llevadas a cabo en China en materia de ciberseguridad y protección de datos en el ámbito de las TIC. La oradora describió los cuatro principales tipos de normas en estas esferas y sus distintos ámbitos de aplicación: i) normas nacionales, ii) normas industriales, iii) normas de asociaciones y iv) normas empresariales. Hay varios comités técnicos de normalización (TC) para cada esfera. Por ejemplo, las normas nacionales de seguridad se organizan principalmente en el marco del TC260. En concreto, la organización de las normas de seguridad industriales recae en la Asociación de Normas de Comunicaciones de China (CCSA), y el principal comité técnico encargado de los aspectos de seguridad es el TC8, un comité técnico que se ocupa de la seguridad de las redes y los datos. La

[7] Directora Ejecutiva, VizStrat Solutions, Sudáfrica.

[8] Subdirector de Departamento, Centro Tecnológico y de Certificación de China para el Examen de la Ciberseguridad, China.

[9] Ingeniera Jefe del Instituto de Investigación sobre Seguridad, Academia de Tecnología de la Información y las Comunicaciones de China (CAICT), China.

labor relacionada con la seguridad en el marco de la CCSA abarca, entre otras, las normas relativas a la seguridad de las redes, los datos, las tecnologías emergentes y las aplicaciones integradas. La cooperación internacional y las organizaciones internacionales de normalización también son importantes para la labor de la CCSA, por ejemplo, la cooperación con el Grupo de Tareas sobre Ingeniería de Internet (IETF) y la Open Mobile Alliance (OMA) y las asociaciones con la Global Standards Collaboration (GSC) y el Proyecto de Asociación de Tercera Generación (3GPP), entre otros.

3.9. La **Sra. Amy Mahn** (Estados Unidos)[10] presentó su organización y describió el arraigado papel que esta desempeña en el ámbito de la ciberseguridad desde que el NIST elaboró la norma de cifrado de datos en la década de 1970. También presentó el marco de ciberseguridad del NIST, que ayuda a las organizaciones a reducir sus riesgos de ciberseguridad y, además de en los Estados Unidos, ya ha sido adoptado por numerosos Gobiernos de todo el mundo, entre ellos el del Uruguay, el Japón e Italia. El marco de ciberseguridad está basado en puntos de vista muy diversos, tanto del sector privado como del mundo académico y el sector público, y actualmente se está revisando sobre la base de las observaciones de las partes interesadas. La Sra. Mahn también reiteró las observaciones formuladas por los oradores anteriores sobre el papel fundamental que pueden desempeñar unas normas ampliamente aceptadas en la creación de mercados competitivos y seguros y la facilitación del comercio internacional.

3.10. El **Sr. Hideyasu Tamura** (Japón)[11] comenzó expresando su preocupación por las medidas de ciberseguridad que se estaban adoptando de manera recurrente, que podrían restringir el comercio. Estas incluyen, por ejemplo, la obligación de utilizar componentes o programas informáticos de origen nacional en infraestructuras críticas, por motivos de seguridad. El orador recordó al público la importancia de elaborar medidas de ciberseguridad que estén en consonancia con el Acuerdo OTC y que restrinjan el comercio lo mínimo posible. Al igual que otros oradores, el Sr. Tamura hizo hincapié en la necesidad de adoptar un enfoque de cooperación para abordar la cuestión de la ciberseguridad y destacó en particular el ambicioso enfoque de normalización del Tratado Integral y Progresista de Asociación Transpacífico (CPTPP). Para concluir, se refirió a la necesidad de instaurar sistemas de etiquetado en materia de ciberseguridad, así como de asegurar la armonización o la interoperabilidad entre ellos.

3.11. El **Sr. Mohamad Endhy Aziz** (Indonesia)[12] describió la evolución de la ciberseguridad en Asia Sudoriental en los últimos años y destacó la creciente importancia de la economía digital para la región. En Indonesia, el panorama digital gira en torno al comercio electrónico y los servicios digitales, sectores que se espera que contribuyan al PIB de la economía en al menos un 14% de aquí a 2027. Sin embargo, el Sr. Endhy Aziz también advirtió de que Indonesia está cada vez más expuesta a las amenazas cibernéticas, pues el número de ataques cibernéticos se ha multiplicado por siete en los últimos cuatro años. Por consiguiente, el aumento de la cooperación internacional en asuntos de ciberseguridad es especialmente importante para Indonesia, así como para otros asociados de la ASEAN. Según el Sr. Endhy Aziz, la comunidad comercial puede tomar mayores medidas para aumentar la cooperación en materia de ciberseguridad, en particular trabajando para llegar a un entendimiento común sobre las amenazas cibernéticas y su alcance y conviniendo en adoptar un enfoque de ciberseguridad basado en el riesgo. Para concluir, el orador recordó al público la importancia de garantizar también el cumplimiento de las normas de ciberseguridad comunes y de seguir elaborando esas normas de forma que restrinjan el comercio lo mínimo posible.

3.12. La **Sra. Veena Dholiwar** (Reino Unido)[13] describió en líneas generales el régimen de seguridad de los productos del Reino Unido, que forma parte de la estrategia nacional de ciberseguridad del Gobierno. Esta estrategia estaba motivada por su compromiso de proteger los intereses de los ciudadanos y evitarles perjuicios. Uno de los principales elementos del régimen es la Ley de Seguridad de los Productos e Infraestructura de las Telecomunicaciones de 2022. Con esta Ley, el régimen de seguridad del Reino Unido sería el primero del mundo en exigir requisitos mínimos

[10] Especialista en Política Internacional, Instituto Nacional de Normas (NIST), Estados Unidos.
[11] Director Superior de la Oficina de Política Comercial Internacional, Ministerio de Economía, Comercio e Industria (METI), Japón.
[12] Especialista Superior en Ciberseguridad, Organismo Nacional de Ciberseguridad y Criptografía, Indonesia.
[13] Jefa de Observancia y Pruebas, Seguridad de los Productos de la IdC, Departamento de Ciencia, Innovación y Tecnología (DSIT), Reino Unido.

de ciberseguridad antes de poder vender productos de consumo de la IdC o "inteligentes" a los consumidores del Reino Unido.[14]

3.13. La Sra. Dholiwar también resumió la labor llevada a cabo en el Reino Unido para elaborar un código voluntario de prácticas, normas internacionales y las bases para la adopción de legislación. Puso de relieve el ejercicio de colaboración, que incluyó la participación de las partes interesadas, consultas públicas, llamamientos para presentar opiniones y actividades de investigación con las ramas de producción y los consumidores. La oradora subrayó que el régimen estaba de conformidad con las obligaciones de transparencia en materia de OTC y los principios de apertura y colaboración. Por último, destacó el compromiso del Reino Unido con la colaboración internacional y su voluntad de compartir su experiencia con otros países Miembros.

3.14. El **Sr. Fabio Polverino** (Unión Europea)[15] y el **Sr. Luis Miguel Vega Fidalgo** (Unión Europea)[16] hicieron una exposición acerca del valioso papel de la reglamentación en materia de ciberseguridad en el comercio. Para ilustrar la importancia de la reglamentación, los oradores detallaron los elevados costos asociados a los incidentes de ciberseguridad. Un ejemplo claro provenía de Alemania, donde en 2020 el costo global de los incidentes de seguridad sufridos por las empresas ascendió a EUR 220.000 millones. Para abordar la cuestión de la ciberseguridad de los productos, la UE reguló primero los dispositivos inalámbricos con el Reglamento Delegado de la Directiva sobre los Equipos Radioeléctricos (RED DA) y, con la propuesta de Ley de Ciberresiliencia, ahora está evolucionando para abarcar todos los productos con elementos digitales y todo su ciclo de vida. Este enfoque jurídico por niveles ha permitido reevaluar, detectar y rectificar cualquier deficiencia encontrada en la legislación anterior.

3.15. Los ponentes pusieron de relieve reglamentos actuales y futuros, a saber: i) el Reglamento Delegado de la Directiva sobre los Equipos Radioeléctricos (RED DA) y ii) la Ley de Ciberresiliencia. El RED DA introducido en 2022 es un instrumento legislativo que se centra en los requisitos de ciberseguridad de los dispositivos inalámbricos. Colma una laguna de la legislación anterior sobre productos y por primera vez impone obligaciones a los fabricantes de productos en materia de ciberseguridad. La Ley de Ciberresiliencia, propuesta en septiembre de 2022 y pendiente de adopción definitiva, se basa en la legislación vigente (incluido el RED DA) y colma una laguna legislativa al introducir requisitos de ciberseguridad obligatorios para todos los productos con elementos digitales, incluidos los productos consistentes en equipos informáticos (*hardware*) y en programas informáticos (*software*). El principal objetivo de esta Ley es que los fabricantes velen por la adecuada ciberseguridad de los productos con elementos digitales que se introducen en el mercado de la UE, desde la fase de diseño y desarrollo y a lo largo de todo el ciclo de vida de los productos. También trata de garantizar un marco de ciberseguridad coherente mediante el establecimiento de requisitos horizontales de ciberseguridad y fomentará la confianza de los consumidores al mejorar la transparencia de las características de seguridad. Tanto el RED DA como la Ley de Ciberresiliencia se aplicarán por medio de normas sobre productos y/o procesos, sobre la base de las normas europeas e internacionales existentes. Esto demuestra la función que desempeñan las normas y las ventajas que ofrecen a la hora de aportar seguridad jurídica, reducir los costos de cumplimiento y evitar obstáculos al comercio, entre otras.

4 DEBATE

4.1. El debate dio lugar a un diálogo abierto entre el sector privado, representantes de los organismos de reglamentación y delegados sobre sus perspectivas y enfoques acerca del tema de la ciberseguridad. Los participantes del sector privado destacaron unánimemente la importancia de que las autoridades de reglamentación promovieran la interoperabilidad, la celebración de consultas con las partes interesadas y los debates técnicos al elaborar normas y reglamentos en materia de ciberseguridad. Los participantes también manifestaron su apoyo a las medidas y enfoques prácticos presentados por los organismos de reglamentación que habían intervenido.

[14] El régimen establece tres requisitos de seguridad que los fabricantes deben cumplir antes de vender productos a los consumidores del Reino Unido.

[15] Responsable de Políticas, Unidad de Política de Ciberseguridad y Privacidad Digital, Dirección General de Redes de Comunicación, Contenido y Tecnologías (DG CONNECT), Comisión Europea.

[16] Responsable de Políticas, Unidad de Maquinaria y Equipo, Dirección General de Mercado Interior, Industria, Emprendimiento y Pymes (DG GROW), Comisión Europea.

4.2. Se preguntó a los ponentes si consideraban que la solidez de las normas de ciberseguridad dependía del país de origen de los productores o los proveedores de productos digitales. En respuesta, diversos ponentes aludieron a normas internacionales existentes que acabarían aplicándose a todos los países sin distinción.

4.3. También hubo un debate más amplio sobre la participación de las partes interesadas externas, incluidas las empresas, en las iniciativas de colaboración que se estaban llevando a cabo a nivel nacional y regional en materia de ciberseguridad. En vista de las numerosas leyes y medidas presentadas durante las exposiciones, se pidió a los Miembros de la OMC en cuestión que notificaran oficialmente todos los reglamentos, normas y procedimientos de evaluación de la conformidad nuevos y propuestos, de conformidad con lo estipulado en el Acuerdo OTC.

5 OBSERVACIONES DEL MODERADOR

5.1. Esta sesión, que contó con aportaciones de 12 oradores, fue muy enriquecedora. Las principales conclusiones de la sesión temática sobre la cooperación entre los Miembros en materia de reglamentación de la ciberseguridad son las siguientes:

- Los Miembros recurren cada vez más a la adopción de medidas reglamentarias en el marco de sus iniciativas para abordar la ciberseguridad. Algunos oradores advirtieron de que esas medidas reglamentarias a veces tenían el efecto opuesto de socavar los esfuerzos mundiales en materia de ciberseguridad si se adoptaban unilateralmente o a nivel nacional. Los oradores también manifestaron preocupación por los posibles obstáculos al comercio que podían plantear las medidas nacionales sobre ciberseguridad. A este respecto, varios oradores destacaron la necesidad de llegar a un entendimiento común de los riesgos de ciberseguridad actuales y futuros, lo que también permitiría a los Miembros hacer frente a los problemas de ciberseguridad de manera más eficiente.

- Como se constató en la sesión, los esfuerzos por elaborar normas internacionales ambiciosas, equitativas e inclusivas en el ámbito de la ciberseguridad van por buen camino. Todos los oradores coincidieron en que las normas internacionales eran fundamentales para luchar contra las amenazas a la ciberseguridad. Muchos (si no todos) mencionaron iniciativas internacionales, incluida la labor de organismos de normalización como la CEI y la ISO.

- La mayoría de los oradores (tanto de la industria como del sector público) subrayaron la necesidad de que los poderes públicos y el sector privado trabajaran de manera más coordinada y colaborativa con los organismos de normalización. Esto es esencial para hacer frente a la creciente fragmentación y divergencia de la reglamentación destinada a abordar las preocupaciones relativas a la ciberseguridad y la cuestión de la gobernanza digital. Esta colaboración también es importante para luchar contra el aumento de la ciberdelincuencia y de los incidentes cibernéticos. A este respecto, los oradores señalaron que los organismos de reglamentación debían colaborar con las partes interesadas al redactar y adoptar medidas en materia de ciberseguridad. Esto se extiende a las distintas ramas de producción y a los consumidores del mercado.

- Los Miembros desarrollados y en desarrollo informaron sobre sus experiencias de formulación, adopción y aplicación de medidas reglamentarias y normas en materia de ciberseguridad encaminadas a proteger a sus ciudadanos. Los organismos internacionales de normalización también presentaron su enfoque ecosistémico para la elaboración de normas sobre ciberseguridad, que englobaba tanto normas horizontales centradas en la seguridad de la información y las operaciones como normas verticales relativas a sectores específicos.

- Del sector privado, escuchamos ejemplos de empresas de ciberseguridad que se dedican a luchar contra una serie de amenazas a la ciberseguridad. También escuchamos los problemas comunes ligados a la reglamentación de la ciberseguridad a los que se enfrentan las pymes, como el riesgo de verse excluidas de un mercado a causa de los precios cuando la reglamentación se vuelve demasiado estricta y fragmentada.

5.2. En general, los debates fueron enriquecedores y esclarecedores. El moderador desea expresar su agradecimiento por las estimulantes aportaciones de los oradores y confía en que el Comité OTC siga aprovechando los debates temáticos sobre la cooperación en materia de reglamentación de la ciberseguridad.