FORO DE GOBERNANZA DE INTERNET 2022

Addis Abeba IGF Mensajes

Este documento es un resumen de los puntos planteados durante los 17 Reunión Anual del Foro de Gobernanza de Internet celebrada en Addis Abeba del 28 de noviembre al 2 de diciembre de 2022.

Los puntos de vista y opiniones expresados en este documento no reflejan necesariamente los de la Secretaría de las Naciones Unidas. Las denominaciones y la terminología empleadas pueden no ajustarse a la práctica de las Naciones Unidas y no implican la expresión de opinión alguna por parte de la Organización.

Las discusiones en el IGF 2022 se centraron en cinco temas clave que se han identificado para el Pacto Mundial Digital (GDC) que se propuso en el informe de 2021 del Secretario General de las Naciones Unidas sobre el 75 aniversario de las Naciones Unidas, *Nuestra agenda común*, y será considerado por la Asamblea General de la ONU en 2023. Esto formará parte del desarrollo de la Cumbre del Futuro que está prevista para 2024.

Los temas considerados por el IGF fueron:

- **Conectar a todas las personas y salvaguardar los Derechos Humanos**
- **Evitar la fragmentación de Internet**
- **Regulación de los datos y protección de la privacidad**
- **Potenciar la seguridad, la protección y la responsabilidad**
- **Abordar tecnologías avanzadas, incluida la Inteligencia Artificial (IA)**

La comunidad de múltiples partes interesadas del IGF expresó su apoyo a la propuesta del Secretario General para un Pacto Digital Global. Los mensajes establecidos en este documento representan contribuciones del IGF hacia el desarrollo del Pacto. Las Coaliciones Dinámicas del IGF, que ya están abordando desafíos y oportunidades específicos que son relevantes para las áreas temáticas propuestas para la GDC, también han expresado su intención de contribuir a las fases de preparación e implementación del proceso de la GDC de la ONU.

[1] **Los mensajes surgieron durante el 17el reunión anual del IGF. estaban sujetos a consultas publicas a través del cual se recopilaron e integraron los comentarios en este borrador final.**

Conectar a todas las personas y salvaguardando los derechos humanos

Tema

El Pacto Mundial Digital (GDC) propuesto por el Secretario General de las Naciones Unidas tiene como primer principio "Conectar a todas las personas a Internet, incluidas todas las escuelas". Esto implica que la conectividad y el acceso a Internet se han convertido en requisitos básicos para garantizar los medios de vida, la seguridad y la educación de las personas en todo el mundo, y que Internet en las escuelas proporciona puntos de acceso cruciales, pone los recursos de información a disposición de todos los estudiantes y construye la alfabetización digital desde las primeras etapas de la vida. Sin embargo, 2700 millones de personas siguen desconectadas en la actualidad, siendo las de los países menos desarrollados y las comunidades rurales las más desfavorecidas.

El acceso efectivo va más allá de la mera conectividad y es inseparable de la salvaguardia de los derechos humanos en línea. El acceso que contribuye al bienestar de las sociedades debe tener los Derechos Humanos en su centro. Esto incluye, entre muchos otros, la capacidad de los usuarios para expresarse libremente, para el ejercicio sin restricciones de la participación democrática y política, para que personas de todos los orígenes experimenten Internet sin temor a sufrir acoso o discriminación, y para que los niños disfruten de los mismos derechos y protecciones en línea que tienen fuera de línea. Internet es un habilitador de derechos y debe incorporar sin problemas los derechos humanos establecidos, a medida que aumentamos nuestra dependencia digital para funciones rutinarias y que los límites entre la vida "en línea" y "fuera de línea" se vuelven menos significativos.

Mensajes

Brechas digitales

- **Las brechas digitales entre diferentes países y regiones siguen siendo factores importantes que afectan el desarrollo nacional e internacional**, incluido el progreso hacia los Objetivos de Desarrollo Sostenible (ODS). De particular focalización son los países menos desarrollados y los pequeños estados insulares en desarrollo (SIDS). Las brechas digitales son mucho más que brechas de conectividad. El acceso afectividad incluye cuestiones de accesibilidad, asequibilidad, contenido, servicios, alfabetización digital y otras capacidades, así como conectividad. La asequibilidad es un problema particular para muchas personas, especialmente en el Sur Global.
- **La pandemia de COVID-19 demostró el papel de Internet para permitir la resiliencia individual y económica, pero también ilustró hasta qué punto están en desventaja aquellos que carecen de conectividad o acceso efectivo,** lo que podría exacerbar otras desigualdades. Tomará tiempo comprender el impacto total y las implicaciones de las intervenciones relacionadas con COVID en relación con el acceso, el uso y los Derechos Humanos.
- **Algunos grupos dentro de todas las sociedades experimentan brechas digitales más profundas o tienen un acceso menos eficiente que otros.** Las mujeres en muchas sociedades están menos conectadas que los hombres y hacen menos uso de la conectividad. La desventaja digital es mayor entre las comunidades vulnerables y marginadas, y muchas personas experimentan múltiples desventajas debido a la combinación de factores relacionados con la edad, el género, la etnia, el idioma, la clase social y otros factores. Iniciativas específicas en infraestructura, dispositivos y servicios pueden ayudar a mejorar las tasas de acceso para los grupos sociales menos conectados, pero deben ir acompañados de medidas para abordar otras deficiencias en el acceso significativo y deben asociarse con otras medidas para abordar las desventajas y la discriminación.

- Una **infraestructura digital resistente y segura es crucial para la inclusión digital. Los gobiernos deben proteger y promover la infraestructura requerida, incluida la red eléctrica interconectada y autónoma, así como las redes de comunicaciones**. En partes de África y otros continentes, las grandes distancias entre las comunidades rurales y remotas, incluidas las de los Pequeños Estados Insulares en Desarrollo, hacen que la conectividad de última milla sea comercialmente poco atractiva para el sector privado. La conectividad, la velocidad y la confiabilidad son aspectos importantes de la provisión de infraestructura. Se necesitará tiempo e inversión para mejorar la capacidad de la infraestructura y abordar los desequilibrios regionales, especialmente en las zonas rurales.
- **La cooperación entre los grupos de partes interesadas es importante para garantizar y permitir el acceso. Los gobiernos y los socios de múltiples partes interesadas deben apoyar el establecimiento y el trabajo de agencias y marcos regulatorios efectivos, abordar los desafíos en áreas comercialmente poco atractivas y alentar enfoques innovadores para la conectividad,** incluidas las redes comunitarias, la asignación adecuada del espectro, el acceso proporcionado por satélites de órbita terrestre baja y la disponibilidad de contenido local, incluido el contenido en los idiomas locales.

La brecha digital de género y los derechos de las mujeres

- **Los hombres tienen significativamente más probabilidades de estar en línea o tener conectividad móvil que las mujeres.** La brecha digital de género es particularmente amplia en los países menos adelantados. La meta 9c de los ODS, que busca lograr un acceso universal y asequible a Internet, no se puede cumplir hasta que se cierre esta brecha.
- **La amenaza de violencia y acoso es un impedimento para la participación de las mujeres en línea**. La violencia de género en línea es un factor importante que impulsa y refuerza la desigualdad de género en el acceso y uso de Internet, lo que lleva a algunas mujeres a abandonar los espacios en línea. Debe reconocerse y abordarse el papel de los servicios y plataformas tecnológicos en la propagación de la violencia de género. Las mujeres deben recibir orientación para resistir y reparar la violencia de género en línea, incluso a través de líneas de ayuda dirigidas por la comunidad. Los recursos, las pautas de la comunidad y los informes en las plataformas deben estar disponibles en los idiomas locales.
- **Los conceptos de igualdad de género, inclusión y derechos y protección de las mujeres deben incorporarse al Pacto Mundial Digital (GDC),** como ha sido propuesto por ONU Mujeres.

Derechos Humanos y desarrollo digital

- **El acceso universal debe respetar los derechos humanos, para garantizar que Internet sea accesible y seguro para todos.** Estos incluyen la libertad de expresión y asociación, el derecho a la privacidad y otros derechos civiles, políticos, económicos, sociales y culturales establecidos en los acuerdos internacionales de derechos. Las estructuras de gobernanza de Internet y el diseño de las tecnologías digitales deben respetar estos derechos. Las organizaciones de desarrollo de estándares deberían, en su trabajo, considerar invitar a la participación de expertos en derechos humanos en línea de todas las comunidades de partes interesadas.
- **La transparencia, la responsabilidad y la debida diligencia con respecto a los Derechos Humanos son responsabilidades de todos los grupos de partes interesadas, incluidas las organizaciones intergubernamentales e internacionales, los gobiernos, el sector privado, la comunidad técnica y la sociedad civil.** Esto requerirá la alineación de las prácticas de negocio con los derechos digitales, así como la cooperación entre las partes interesadas para abordar cuestiones como la desinformación, la discriminación y el discurso de odio, especialmente en momentos de inestabilidad política, elecciones y transferencias de poder.

- **El acceso a Internet proporciona una oportunidad crucial para el acceso a la información y la expresión**. Los gobiernos deben evitar recurrir a los cierres de Internet debido a su impacto negativo tanto en los derechos humanos como en el bienestar económico. Las empresas de tecnología y redes sociales deben apoyar a los ciudadanos en sus esfuerzos con respecto a los cierres.
- **Es importante mejorar el seguimiento y la implementación de los derechos digitales**. Se han hecho una serie de sugerencias para establecer arreglos de monitoreo internacional dentro del sistema de la ONU, con la participación de múltiples partes interesadas. Estos podrían complementar y aprovechar los mecanismos existentes, incluidos tanto los relacionados con el desarrollo digital y los derechos como los de otras esferas, como el cambio climático.
- **Internet ofrece oportunidades para mejorar el derecho a la educación,** como parte de políticas más amplias para la mejora educativa. La calidad de la educación en el Sur Global, particularmente durante la pandemia, ha sufrido debido a la falta de conectividad. Si bien las TIC pueden permitir un acceso significativo para los estudiantes, las diferencias en las tasas de adopción globales y locales han exacerbado las desigualdades previas a la pandemia. La experiencia durante la pandemia se puede utilizar para mejorar el uso de los recursos digitales en el futuro.
- **Se deben realizar esfuerzos para ayudar a las empresas más pequeñas y locales a aprovechar al máximo Internet**. El uso de herramientas digitales por parte de las pequeñas y medianas empresas ha aumentado considerablemente desde 2020, pero las microempresas aún enfrentan desafíos importantes en su capacidad para digitalizar sus negocios.
- **Los cambios en el mercado laboral creados en torno a las plataformas en línea presentan tanto oportunidades como desafíos para la creación y la calidad del empleo,** especialmente para las mujeres que desempeñan un papel más importante que los hombres en el sector informal en la mayoría de los países. La falta de formación sigue siendo un obstáculo para que muchas personas maximicen su potencial de empleo.
- **Es necesario mejorar las competencias digitales y adaptar las metodologías de enseñanza, aprendizaje y formación para adaptarse a los nuevos paradigmas** tanto en la educación como en el empleo. Es importante identificar y cerrar la brecha entre las necesidades de la industria y la educación terciaria.

Evitar la fragmentación de Internet

Tema

El mantenimiento de una Internet global, abierta e interoperable es un valor central del IGF. Esto implica que se sigan desplegando estándares y protocolos técnicos comunes para lograr una red de redes interconectadas entre países y regiones, y que los estándares de contenido y servicios sean compatibles con los derechos humanos y el estado de derecho. El llamado a esto, aplicar un marco a Internet que priorice los derechos y libertades de los usuarios, así como, ya través de, la coherencia infraestructural de extremo a extremo, se ha hecho eco en los planes para el GDC.

El riesgo de fragmentación es real y creciente. Si bien es necesario abordar la fragmentación técnica y comercial, donde el funcionamiento de Internet se ve afectado por una combinación de condiciones y prácticas comerciales voluntarias e involuntarias, también es motivo de preocupación la fragmentación por política gubernamental que afecta el carácter abierto e interoperable de Internet.

Mensajes

Comprender los problemas

- **El Pacto Mundial Digital brinda la oportunidad de reafirmar el valor de una Internet abierta e interconectada para la realización de la Carta de las Naciones Unidas, el logro de los Objetivos de Desarrollo Sostenible y el ejercicio de los Derechos Humanos.** Existe un acuerdo generalizado dentro de la comunidad de Internet sobre el valor de una Internet global y no fragmentada como plataforma para la actividad humana.

- **Los temas planteados en los debates sobre la fragmentación de Internet tienen varios niveles, y diferentes partes interesadas dan una variedad de significados e interpretaciones al término**. Algunos están más preocupados por los aspectos técnicos y de infraestructura de Internet, mientras que otros se centran en cuestiones de política pública, incluido el acceso, los derechos y los impactos en la experiencia del usuario. Estos se exploran en un borrador de marco preparado por la Red de Políticas de Fragmentación de Internet del IGF. El respeto y la comprensión de las percepciones y experiencias de fragmentación de las diferentes personas son esenciales si queremos alcanzar respuestas eficaces y coordinadas.

- **Una amplia gama de factores políticos, económicos y técnicos pueden impulsar potencialmente la fragmentación.** Sin embargo, la diversidad y la descentralización no deben confundirse con la fragmentación. Estos son aspectos fundamentalmente positivos de la arquitectura y las operaciones de Internet.

Abordar el riesgo de fragmentación

- **Los mecanismos efectivos de gobernanza de múltiples partes interesadas son esenciales para la gobernanza de una Internet global no fragmentada**. Es necesario reforzar la confianza en estos mecanismos, para garantizar que sean sólidos y sostenibles, y para fomentar la coherencia entre las estructuras de gobernanza a medida que evolucionan para enfrentar nuevos desafíos.

- **Es necesario estar atentos a los riesgos de fragmentación nuevos o en desarrollo**. La cooperación y la coordinación globales serán esenciales para identificar señales de alerta temprana, mapear el impacto de las políticas y otros desarrollos, y prepararse para abordar las implicaciones de estos cambios. Un enfoque de múltiples partes interesadas es el más adecuado para valorar, evaluar y monitorizar las posibles consecuencias no deseadas de las medidas que afectan a Internet y para sugerir alternativas efectivas que eviten o mitiguen los riesgos de fragmentación. La Red de Políticas sobre Fragmentación de Internet del IGF es un ejemplo positivo de este enfoque.

- **La apertura de Internet es fundamental para fomentar el disfrute de los Derechos Humanos de los usuarios de Internet, promover la competencia y la igualdad de oportunidades, y salvaguardar la capacidad generadora de la naturaleza colaborativa de Internet.** Los debates sobre la neutralidad de la red y la gestión no discriminatoria del tráfico son solo una parte de discusiones más amplias en este contexto. La neutralidad de la red es necesaria pero no suficiente para garantizar la apertura de Internet. También son necesarias la interoperabilidad de infraestructuras y datos, y la neutralidad de plataformas y dispositivos.

- **Si bien los enfoques legales, regulatorios y de políticas diferirán en todo el mundo, la coordinación activa a través de las fronteras internacionales es vital para garantizar que los enfoques fragmentados no amenacen el alcance global y la interoperabilidad de Internet.** Mantener la integridad de la red global requiere colaboración regulatoria internacional y consenso sobre principios básicos.

- **Muchos factores diferentes afectan la experiencia de Internet en diferentes jurisdicciones, incluidos diferentes contextos sociales, demográficos, económicos, culturales y políticos, así como cuestiones técnicas y de infraestructura. La búsqueda de algunos formas de gobernanza digital a nivel nacional pueden aumentar el riesgo de fragmentación a nivel técnico de Internet. Sin embargo, los marcos regulatorios también deben considerar diferentes requisitos en diferentes contextos y seguir el ritmo de los rápidos cambios en tecnología y servicios.**

- **Existe la necesidad de un mayor intercambio de conocimientos e información entre las partes interesadas,** profundizar el debate sobre la diplomacia cibernética como un fenómeno en evolución y considerar el alcance de las intervenciones apropiadas. Los organismos de elaboración de normas deben continuar mejorando la divulgación y el compromiso con las partes interesadas y mejorar la comprensión entre las comunidades políticas y técnicas. Las decisiones técnicas que tienen implicaciones políticas deben ser discutidas por los organismos de normalización a través de la participación directa de todas las partes interesadas afectadas.

Regulación de los datos y protección de la privacidad

Tema

Los datos son el recurso clave de la era digital globalizada. El movimiento de datos impulsa las economías, mientras que el análisis de datos, incluido el análisis de big data, ha sido la base de innovaciones notables en todas las disciplinas, desde finanzas hasta salud o gestión policial.

Pero el uso generalizado, el flujo rutinario a través de las fronteras y la permanencia de los datos siguen siendo temas delicados y sin resolver. Como activo comercial transnacional, los flujos de datos operan en un entorno en el que existe poca coherencia entre los regímenes jurídicos nacionales y en el que existen importantes desafíos de aplicación. La privacidad de los datos personales se sacrifica con demasiada frecuencia en el transcurso de los intercambios de datos, desde el punto de recopilación hasta la aplicación y el almacenamiento, con profundas consecuencias para la confianza y la seguridad.

Para aprovechar la importante promesa de los datos, económicamente y con fines de investigación, es necesario relanzar los debates sobre la gobernanza, la integridad y la protección de la privacidad de las personas.

Mensajes

La centralidad de los datos

- **Los datos se han convertido en un recurso crítico en una era cada vez más digital.** Los flujos de datos son cruciales para la cooperación internacional en muchos campos, incluida la investigación científica, la aplicación de la ley y la seguridad nacional y mundial. Los datos, la seguridad de los datos y la protección de los datos son facilitadores críticos del desarrollo sostenible. El uso efectivo y el intercambio de datos a escala global pueden ayudar a superar los desafíos compartidos y las amenazas que plantean las crisis en cascada, como las pandemias y el cambio climático.

- **Los datos pueden generar ganancias y un valor social significativo.** Sin embargo, los beneficios de la economía basada en datos hasta ahora se han distribuido de manera desigual. Muchas personas están preocupadas de que pueden convertirse principalmente en proveedores de datos en lugar de beneficiarios.

- **La relación entre quienes generan y quienes utilizan los datos es importante.** La pobreza de datos es un problema importante, especialmente en las comunidades locales y entre los segmentos vulnerables de la población. La falta de privacidad de los datos y la protección inadecuada de los datos socavan la confianza en la gestión de datos. Es importante desarrollar la alfabetización de datos y las capacidades de datos en todos los niveles de gobierno, en los currículos educativos y para el público en general.

- **La gestión de datos y la gobernanza son cuestiones complejas tanto en la gobernanza nacional como internacional.** El desarrollo en los datos, incluidos el análisis de big data, las innovaciones en inteligencia artificial y aprendizaje automático, y las innovaciones en las dimensiones de las políticas públicas y los ODS, demuestran la necesidad de una consideración adecuada de los impactos políticos, económicos y sociales así como de los matices en las interventiones sobre las políticas.

Las instituciones gubernamentales y reguladoras necesitan la infraestructura y la capacidad necesarias para implementar marcos de gobernanza de datos nacionales integrados y efectivos. Los desarrolladores de aplicaciones tienen la responsabilidad de garantizar un diseño ético y seguro.

Privacidad y justicia de datos

- **La privacidad de los datos no es una cuestión de conveniencia o buenas prácticas sino de derechos humanos.** Además de los derechos a la intimidad, la igualdad de trato y la no discriminación, afecta el acceso a otros derechos humanos como la sanidad, la educación y los servicios públicos, así como derechos democráticos como la libertad de expresión y asociación. Las leyes de privacidad deben ser sustanciales, basadas en evidencia y susceptibles de una aplicación clara. Aquellos afectados por ellos deberían ser capaces de comprender claramente sus implicaciones.

- **Los flujos de datos y el intercambio de datos deben tener lugar sin comprometer la privacidad de los datos.** La privacidad de los datos personales a menudo se ha sacrificado en los procesos de intercambio de datos, entre la recopilación de información y su aplicación, con riesgos intencionales y no intencionales para la confianza y la seguridad. El acceso y uso de Internet no debe depender del seguimiento de datos: los usuarios deben tener derecho a elegir en qué medida se comparte su información, incluida la información derivada de su actividad en línea. Los datos personales no deben exportarse a jurisdicciones que no ofrezcan las garantías adecuadas.

- **Las políticas deben ir más allá de la protección de datos a la justicia de datos en la que las personas tienen opciones sobre cómo se utilizan los datos personales y dónde pueden compartir los beneficios y beneficios de la innovación.** aportados por conjuntos de datos derivados de sus propios datos. Por lo tanto, las protecciones de la privacidad deberían contribuir a una economía digital más segura y próspera.

- **Los gobiernos y los reguladores deben garantizar que los datos personales estén protegidos**, identificando las responsabilidades diferenciadas de las diferentes partes interesadas y sin imponer cargas o responsabilidades indebidas a los usuarios individuales. Las políticas de gobernanza de datos deben desarrollarse con aportes de múltiples partes interesadas para garantizar que se comprendan los desafíos de implementación.

- **La privacidad y la protección de datos son particularmente importantes para la gobernanza de la inteligencia artificial y el aprendizaje automático.** Todas las partes interesadas en la cadena de suministro de IA tienen un papel que desempeñar en la defensa de los derechos de privacidad.

- **Se necesitan órganos de supervisión independientes equipados con los recursos apropiados.** Las oficinas de protección de datos deben tener el mandato de gestionar el registro de datos, brindar orientación, implementar investigaciones y resolver quejas de los interesados.

Gobernanza de datos

- **Los problemas relacionados con el gobierno de datos no deben tratarse en silos o de forma aislada de sus impactos.** El panorama actual de la gobernanza de datos es un mosaico fragmentado de normas nacionales, regionales e internacionales que implican responsabilidades para los gobiernos nacionales, las empresas del sector privado y las personas.

- **Se necesita una mayor coherencia a nivel global para lograr un enfoque equilibrado en el que los datos trabajen para las personas y el planeta.** La legislación y los marcos regulatorios existentes a nivel nacional, regional e internacional a menudo son insuficientes y no logran mantenerse al día con el ritmo de cambio en tecnología y aplicaciones. Deben buscar garantizar altos estándares de seguridad por parte de las empresas y otras organizaciones responsables de almacenar datos.

- **Diferentes contextos y desafíos, historias, culturas, tradiciones legales y estructuras regulatorias significan que no puede haber un conjunto rígido de reglas para todos.** Diferentes individuos y organizaciones también interpretan enfoques similares en términos generales de diferentes maneras. Sin embargo, si bien los países y regiones deben desarrollar sus propios enfoques personalizados para la gobernanza de datos, debe haber coherencia e interoperabilidad para facilitar los flujos de datos y garantizar la igualdad de condiciones.

- **La transparencia, la participación y la rendición de cuentas son aspectos importantes de la buena gobernanza de datos.** Las consideraciones importantes en el gobierno de los datos incluyen (pero no se limitan a): estándares y clasificación de datos; compartir, intercambiar e interoperabilidad de datos; seguridad de datos y privacidad de datos; infraestructura de datos; datos e identidad digital; justicia y equidad de datos; trazabilidad, transparencia y explicabilidad de los datos; minimización y limitación de datos; precisión y calidad de los datos; sesgo de datos, marginación y discriminación; el ciclo de vida de los datos, la especificidad y la retención del uso de los datos; responsabilidad de datos y ética de datos; daños a los datos, seguridad de datos y protección de datos

- **Muchas partes interesadas tienen roles dentro de este contexto y deben ejercer su poder e influencia para promover una gobernanza de datos efectiva,** incluidos reguladores, investigadores, organizaciones de normalización, organizaciones de consumidores y usuarios finales. Las políticas para el gobierno de datos deben desarrollarse con el aporte de esta comunidad de múltiples partes interesadas que tiene experiencia tanto en debates legales sobre privacidad como en los desafíos del "mundo real" de implementar soluciones efectivas de privacidad de datos.

- **Las economías en desarrollo necesitan mejorar sus capacidades institucionales para gobernar, usar y gestionar datos de manera integral, objetiva y basada en evidencia, incluso a través de la cooperación regional y global.** Esto requiere una mejor comprensión de las capacidades institucionales de los funcionarios gubernamentales y las partes interesadas.

Flujos de datos transfronterizos

- **Los flujos de datos transfronterizos son esenciales para muchos aspectos del comercio electrónico y el comercio digital.** La gestión eficiente del comercio intrarregional y de la cadena de suministro se basa en el flujo fluido de datos, así como de bienes, servicios y capital. Sin embargo, todos estos requieren consideraciones transversales complejas para la convergencia regulatoria, la armonización de los marcos legales, la gobernanza de Internet, la reforma de políticas de tecnología de la información y las comunicaciones y la implementación de infraestructura regional estratégica.

- **Los actuales acuerdos comerciales multilaterales, regionales y bilaterales son insuficientes para los flujos de datos transfronterizos actuales y futuros.** Estos operan en un entorno en gran parte no regulado con poca coherencia entre los regímenes legales nacionales. Los enfoques difieren y son contextuales, lo que genera barreras al comercio, mientras que muchos países actualmente no cuentan con una legislación adecuada o capacidad de aplicación. Existe una necesidad creciente de desarrollar y armonizar medidas para gestionar los flujos transfronterizos que faciliten desarrollo y generación de valor económico, en diferentes contextos, respetando la soberanía nacional y la privacidad de los usuarios.

Habilitación de la seguridad, la protección y la rendición de cuentas

Tema

La seguridad de Internet está amenazada de varias maneras. La ciberseguridad tradicional se ocupa de la protección de redes, dispositivos y datos contra el acceso no autorizado o el uso delictivo. Esto abarca el problema actual de los ataques cibernéticos, ya sean perpetrados por individuos o sancionados por el estado, y ya sea que los objetivos sean cívicos, comerciales o gubernamentales. Factores como la ausencia de acuerdos de seguridad cibernética amplios y vinculantes y redes insuficientemente seguras contribuyen a la pérdida de oportunidades para capitalizar plenamente los beneficios económicos de las tecnologías digitales, particularmente para los países en desarrollo.

Los problemas de seguridad, protección y responsabilidad son multifacéticos, incluidos distintos problemas relacionados con la infraestructura, los servicios, el contenido y otros aspectos de Internet. Nuestra comprensión de la seguridad y la protección, por ejemplo, ahora incluye desafíos persistentes de información errónea y desinformación en línea. En los últimos años, estos han sido factores que han agravado los efectos de la pandemia de COVID-19 y que han planteado riesgos significativos para los procesos electorales en todo el mundo. Esto ha enfatizado la necesidad de responsabilidad y criterios claros para el contenido engañoso.

El concepto de 'seguridad' puede ampliarse aún más para incluir la seguridad ambiental, considerando los esfuerzos para 'verde' Internet y reducir las emisiones de carbono asociadas con el consumo digital. La necesidad de abordar el impacto ambiental de la digitalización es un tema cada vez más importante en las discusiones del IGF.

Mensajes

El papel de los políticos

- **La ciberseguridad debe verse como un desafío central para la política de Internet.** Las consideraciones de confianza y seguridad deben ser parte integral del desarrollo de un acceso seguro y protegido, incluido el respeto por los derechos humanos, la apertura y la transparencia en la formulación de políticas, y un enfoque de múltiples partes interesadas que sirva a los intereses de los usuarios finales.

- **Garantizar la seguridad cibernética y prevenir el delito cibernético son áreas importantes de la política que requieren una atención seria y el desarrollo de experiencia**. Sin embargo, difieren en su propósito y el enfoque requerido para cada uno es diferente. Un enfoque que es efectivo en uno no será efectivo en el otro sin adaptación y reformulación.

- **Los problemas de ciberseguridad y ciberdelincuencia tienen dimensiones transfronterizas y organizacionales. Abordar estos requiere:**

a) enfoques de todo el gobierno y de toda la Sociedad que incluyan alianzas sólidas y esfuerzos coordinados, que involucren a parlamentos, reguladores y otras autoridades y agencias gubernamentales relevantes, el sector privado, la comunidad técnica, la academia y la sociedad civil; y

b) cooperación regional e internacional eficiente y eficaz, es decir, intergubernamental, multilateral y de múltiples partes interesadas.

- **Los gobiernos, el sector privado y la comunidad técnica deben tener cuidado de evitar la adopción de leyes sobre delitos cibernéticos y el establecimiento de estándares que afecten negativamente el trabajo de los defensores de la seguridad cibernética**. Deben invitar a todas las partes interesadas a participar en el desarrollo de políticas y facilitar la interacción y el intercambio de experiencias y conocimientos entre sus diferentes comunidades.

- **La sociedad civil debe participar en los debates sobre ciberdelincuencia y ciberseguridad.** Para hacerlo de manera efectiva, las partes interesadas de la sociedad civil deben informarse sobre los diferentes enfoques y temas involucrados, y trabajar con otras partes interesadas para recopilar la información y los recursos necesarios para participar plenamente en la formulación de políticas.

La seguridad cibernética

- **La comunidad internacional debe explorar formas prácticas de incorporar la creación de capacidad en seguridad cibernética en esfuerzos más amplios de desarrollo digital.** Las tensiones entre el deseo de avanzar en la transformación digital y la necesidad de habilitar una ciberseguridad efectiva plantean desafíos para habilitar un entorno en línea seguro y protegido y lograr los Objetivos de Desarrollo Sostenible. Si bien es necesario hacer más para aumentar la resiliencia de la infraestructura digital, no es suficiente. La traducción de los acuerdos internacionales existentes en acciones factibles está muy retrasada.
- **Los estándares que permiten la ciberseguridad son esenciales para una Internet abierta, segura y resiliente que permita el progreso social y el crecimiento económico, y son particularmente importantes para proteger a quienes aún no están conectados.** Dichos estándares han sido desarrollados, pero su uso necesita crecer significativamente para que sean completamente efectivos. Las Naciones Unidas podrían ayudar a acelerar la adopción global de estándares clave al incluir su promoción en el Pacto Mundial Digital, al apoyar la promoción y el desarrollo de capacidades y al alentar iniciativas para probar y monitorear la implementación. La concientización temprana y el desarrollo de capacidades en estándares no deben olvidarse como prioridades en áreas donde muchos todavía tienen que conectarse e Internet está creciendo.
- **Es necesario hacer más para mejorar la conciencia de los responsables políticos nacionales y otras partes interesadas sobre los desafíos de la seguridad cibernética y las normas y principios internacionales.** Esto debería incluir la concientización y el desarrollo de capacidades sobre los vínculos entre el desarrollo sostenible y la seguridad cibernética, reuniendo a diversas partes interesadas para movilizar una administración eficaz, sostenible e inclusiva de la cooperación internacional para la resiliencia cibernética. Se han establecido una serie de iniciativas internacionales para apoyar esto. Las agencias de financiamiento y otras partes interesadas también deben abordar las oportunidades para financiar la resiliencia cibernética.
- **Las normas de ciberseguridad deben marcar la diferencia en las experiencias personales de los usuarios de Internet del pasado, presente y futuro.** Escuchar las experiencias de las víctimas individuales y organizacionales de los ataques de seguridad cibernética, y las de los primeros en responder, es importante en este contexto, particularmente cuando se desarrollan nuevas normas.

Ciberdelincuencia

- **El cibercrimen representa una amenaza creciente para muchos usuarios de Internet.** Las regulaciones contra el ciberdelito deben tener en cuenta el tamaño, la capacidad y los recursos de las plataformas. Las obligaciones legales deben considerar la diversidad del sector técnico y reconocer las necesidades y circunstancias de las pequeñas empresas para cumplir con sus obligaciones legales, por ejemplo, para contrarrestar la explotación terrorista y de violencia extremista de sus servicios.

- **Los gobiernos y los formuladores de políticas deben garantizar que las respuestas legales al uso criminal y terrorista de Internet salvaguarden tanto el estado de derecho como los Derechos Humanos**, teniendo plenamente en cuenta la libertad de expresión y garantizando la transparencia y la rendición de cuentas en la aplicación de medidas contra la ciberdelincuencia.

Contenido y desinformación

- **La desinformación puede y debe abordarse a través de mecanismos que aborden los riesgos que enfrentan las personas y las sociedades al tiempo que protegen la libertad de expresión, el pluralismo y el proceso democrático.** El apoyo al periodismo y los medios profesionales juega un papel importante en los esfuerzos para abordar la desinformación, incluido el compromiso con las normas periodísticas establecidas.

- **Las habilidades de alfabetización mediática y digital permiten a los ciudadanos tener una visión más crítica del contenido o la información que encuentran, lo que ayuda a identificar la desinformación y la información errónea y fortalece la participación democrática.** La alfabetización digital puede ayudar a aumentar la conciencia sobre la seguridad en línea, especialmente para las personas y comunidades más vulnerables. Las iniciativas deben ser sensibles a las necesidades y riesgos asociados con los diferentes grupos demográficos. Los diferentes enfoques para los jóvenes y las generaciones mayores, por ejemplo, deben responder a diferentes patrones de uso.

- **Los planes de estudios educativos deben incluir habilidades de alfabetización digital que ayuden a los niños a estar seguros en línea.** Las iniciativas deben involucrar a los padres, maestros y tutores. Los legisladores y las plataformas digitales deben asumir la responsabilidad de garantizar la seguridad de los niños dentro de un marco de derechos de los niños en línea coherente con los acuerdos internacionales de derechos, incluida la Convención de las Naciones Unidas sobre los Derechos del Niño.

- **El sistema de nombres de dominio tiene una capacidad técnica limitada en este contexto.** El diálogo continuo con las partes interesadas debe aclarar cuándo y cómo se puede utilizar para remediar problemas de contenido específicos y debe fortalecer las normas del proceso debido.

- **El cifrado juega un papel importante en la construcción de una Internet abierta, segura y democrática** y ayuda a los usuarios a lograr seguridad, privacidad y libertad de expresión. Deben abordarse los problemas relacionados con la aplicación de la ley y la capacidad del usuario para administrar el acceso en áreas como la protección infantil.

- **Los problemas de traducción presentan barreras significativas que pueden inhibir el compromiso significativo de los usuarios finales con los estándares y pautas de la comunidad de las plataformas.** Los términos clave a veces están mal traducidos, lo que da lugar a interpretaciones ambiguas. El compromiso con diferentes comunidades lingüísticas para mejorar la precisión y relevancia de la traducción, incluida la comunicación de conceptos sin equivalentes en diferentes idiomas, es una parte importante para permitir que las plataformas y los usuarios entiendan lo que se espera de ellos.

Abordar las tecnologías avanzadas, incluid la Inteligencia Artificial (IA)

Tema

Las tecnologías digitales avanzadas dan forma cada vez más a nuestra economía y sociedad, incluidos los sistemas de inteligencia artificial (IA) que guían nuestras experiencias en línea, potencian los dispositivos inteligentes e influyen en nuestras propias decisiones y las que otros toman sobre nosotros, así como la robótica y las aplicaciones de Internet de las cosas que se implementan en áreas tan diversas como la fabricación, la atención médica y la agricultura. Aún siendo prometedoras, estas tecnologías no vienen sin escollos. La toma de decisiones algorítmica, por ejemplo, puede dar lugar a sesgos, discriminación, estereotipos y una mayor desigualdad social, mientras que los sistemas basados en IA pueden plantear riesgos para la seguridad humana y los derechos humanos. Los dispositivos de Internet de las cosas llegan con desafíos de privacidad y ciberseguridad. La realidad aumentada y virtual plantea problemas de seguridad pública, protección de datos y protección del consumidor.

Aprovechar las oportunidades que ofrecen las tecnologías avanzadas, mientras se abordan los desafíos y riesgos relacionados, es una tarea que ningún actor puede asumir por sí solo. Se requiere el diálogo y la cooperación de múltiples partes interesadas (gobiernos, organizaciones intergubernamentales, empresas de tecnología, sociedad civil y otros) para garantizar que estas tecnologías se desarrollen y desplieguen de una manera centrada en el ser humano y respetuosa de los derechos humanos.

Mensajes

Gobernanza

- **Las tecnologías avanzadas, incluida la inteligencia artificial, deben diseñarse de manera que respeten el estado de derecho, los derechos humanos, los valores democráticos y la diversidad, e incluyan las salvaguardias adecuadas.** Deben beneficiar a las personas y al planeta impulsando el crecimiento inclusivo, el desarrollo sostenible y el bienestar. Los mecanismos de supervisión y cumplimiento deben seguir principios y reglas, y los actores de IA deben rendir cuentas por cualquier daño causado.

- **La suposición de que la tecnología necesariamente mejora la igualdad es errónea.** Aquellos que diseñan tecnologías de aprendizaje automático y los datos utilizados para entrenar aplicaciones de IA a menudo no son representativos de sus sociedades. Las tecnologías pueden amplificar las desigualdades y causar daños, en particular a los grupos vulnerables y marginados.

- **Las sociedades deben adaptarse a la transformación que traerá la IA a través de cambios en su marco de cooperación y modelo de gobernanza.** La construcción de una sociedad inteligente centrada en el ser humano requiere la plena cooperación del gobierno, las empresas, las organizaciones sociales y la academia. El control humano continuo sigue siendo esencial para garantizar que los algoritmos no conduzcan a resultados que son indeseable o descontrolado. Romper los silos entre ingenieros y expertos en políticas es fundamental para lograr esto.

- **El acuerdo global sobre las normas de IA no se puede lograr en un proceso sencillo.** Si bien existen algunas normas, en su mayoría son leyes blandas en lugar de principios vinculantes. El desarrollo de estándares globales significativos requerirá la participación efectiva de todos los países, incluidos los países en desarrollo y desarrollados, y los aportes de las iniciativas regionales, así como el compromiso de todas las partes interesadas.

- **La creación de capacidad es importante en los esfuerzos por abordar las tecnologías avanzadas.** Se necesitan políticas para la alfabetización en IA, el desarrollo de habilidades y los recursos lingüísticos para los idiomas minoritarios a fin de formular un enfoque verdaderamente global de las tecnologías avanzadas.

Confianza, seguridad y privacidad

- **Los marcos regulatorios deben incluir principios para ayudar a las redes sociales y otras plataformas a cumplir con las obligaciones de debida diligencia para la gestión de contenido que podría dañar la democracia y los derechos humanos.** Los marcos deben contribuir a la conversación global sobre la moderación de contenido en línea para empoderar a los usuarios, incluidos los grupos más vulnerables y los usuarios de idiomas minoritarios. Las tecnologías emergentes, como la computación afectiva, que considera cómo las computadoras pueden reconocer, interpretar y simular las emociones humanas, requieren una evaluación ética sustantiva.

- **La transparencia en la operación y el reporte de los sistemas algorítmicos es esencial para los derechos humanos.** La IA facilita la observación y el análisis constantes de los datos para personalizar y orientar el contenido y la publicidad. Las experiencias en línea personalizadas resultantes corren el riesgo de desagregar los espacios de información en línea y limitar la exposición de las personas a la diversidad de información. La falta de pluralismo de información puede fomentar la manipulación y el engaño, fomentando las desigualdades, socavando los debates democráticos y potencialmente permitiendo el autoritarismo digital, el odio y la violencia.

- **Las partes interesadas de las comunidades técnicas y no técnicas deben compartir su experiencia y trabajar juntas para desarrollar principios, directrices y estándares.**que sean lo suficientemente flexibles para su aplicación en diversos contextos y que fomenten la confianza en los sistemas de IA.

- **Es importante reconocer y respetar los diferentes antecedentes institucionales y culturales de los diversos países y comunidades**., además de promover la inclusión y permitir la cooperación internacional en IA.

Derechos y moderación de contenidos

- **Es esencial que las políticas para la gobernanza de contenido de las plataformas en línea y su aplicación estén en línea con los estándares internacionales de derechos humanos.** Las tecnologías de inteligencia artificial y aprendizaje automático ya se están utilizando para decidir si el contenido debe publicarse o eliminarse, qué contenido se prioriza y a quién se difunde. Estas herramientas juegan un papel importante en la configuración del discurso político y público de maneras que afectan los derechos humanos tanto individuales como colectivos, incluyendo los derechos sociales, económicos y culturales y los derechos a la paz y la seguridad mundiales. A menudo se implementan con poca o ninguna transparencia, presentación de responsabilidad o supervisión pública. Esto debe ser rectificado.

.

- **Las mismas tecnologías que se pueden usar para promover los derechos humanos también se pueden usar para la vigilancia, para promover agendas violentas y de otras formas que infrinjan esos derechos** Las consecuencias no deseadas de la gestión automatizada de contenido pueden ser especialmente perjudiciales en tiempos de conflicto o crisis, cuando pueden silenciar las voces críticas en el momento en que son más cruciales.

- **Los estándares técnicos juegan un papel importante para permitir el desarrollo y mejorar el valor de las tecnologías digitales y las infraestructuras, servicios, protocolos, aplicaciones y dispositivos relacionados. También pueden tener impactos poderosos en los derechos humanos.** Sin embargo, los procesos técnicos de establecimiento de estándares dentro de las organizaciones de desarrollo de estándares no tienen plenamente en cuenta las preocupaciones de derechos humanos. Estos procesos suelen ser opacos, complejos y requieren muchos recursos para que la sociedad civil y otras partes interesadas puedan acceder a ellos y seguirlos sistemáticamente. Esto debe ser abordado.