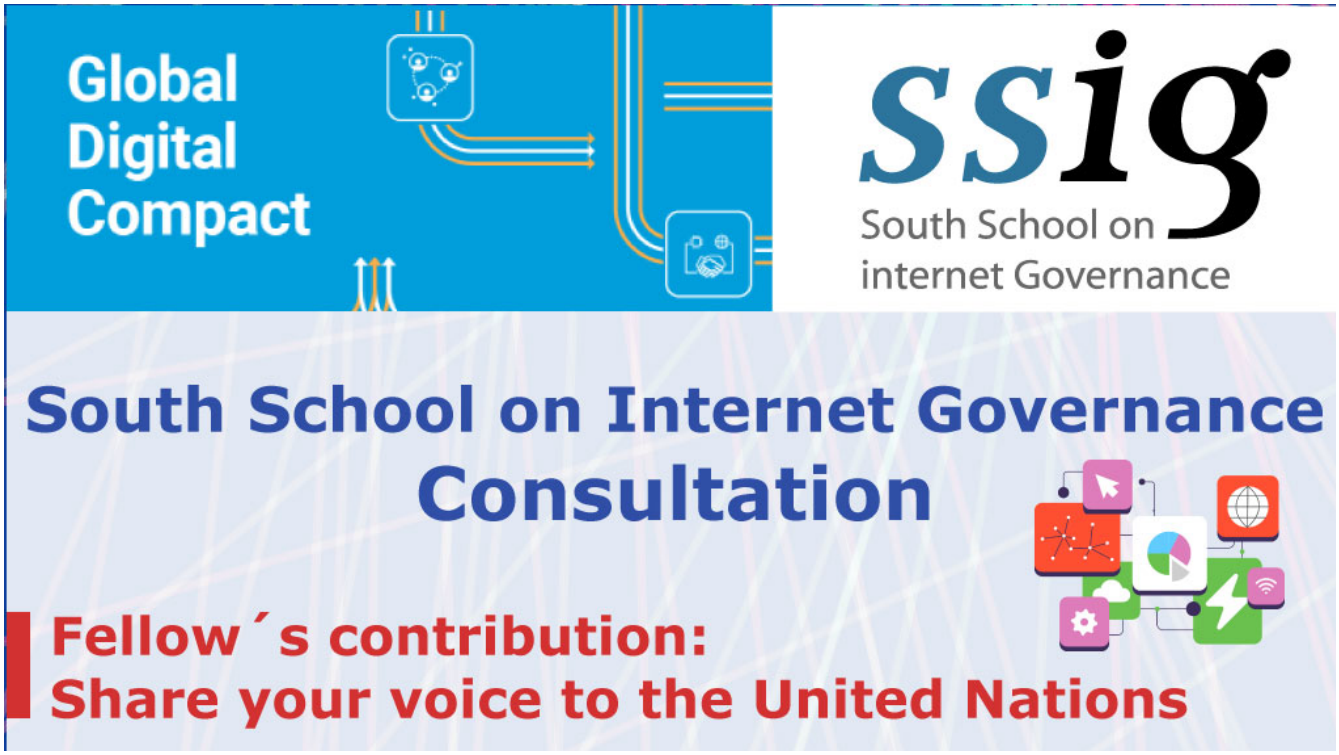


South School on Internet Governance
SSIG fellow´s contribution to the Global Digital Compact

The South School on Internet Governance has joined efforts with its participants to contribute to the Global Digital Compact consultation organized by the United Nations.

Contributions were received from 65 fellows from 22 countries of the five continents, their names, country of residence and stakeholder group are detailed in this document, coordinated by the SSIG academic team. The consultation and elaboration of the final document was made in three languages: English, Spanish and Portuguese.

This contribution was prepared through an online process of consultation and community drafting, which includes the 7 key digital issues that the Common Agenda report suggests for the Digital Global Compact, these are the following:

1- Connect everyone to the Internet, including all schools
2- Avoid Internet fragmentation
3- Protect data
4- Apply human rights online
5- Introduce accountability criteria for discrimination and misleading content
6- Promote the regulation of artificial intelligence
7- Digital commons as a global public good

The South School on Internet Governance and all its community of fellows from all over the world makes this contribution hoping that it will be helpful and valuable for this process.

Olga Cavalli
Academic Director
South School on Internet Governance
olga@gobernanzainternet.org

Adrián Carballo
Director Institutional Relations
South School on Internet Governance
adrian@gobernanzainternet.org

SSIG fellow contributors to the Global Digital Compact		
In alphabetical order by country of residence		
Name	**Country of residence**	**Stakeholder**
Olga Cavalli	Argentina	Academia
Camila Aldana	Argentina	Technical community
Edith Sztychmasjter	Argentina	Private sector
Emiliano Leonel Aguirre Vila	Argentina	Civil Society
Claudia Gabriela Gasol Varela	Argentina	Academia
Oscar Gabriel Cervella	Argentina	Private sector
María Gilda Carballo	Argentina	Academia
Stella Maris Moreira	Argentina	Academia
Ezequiel Gonzalez	Argentina	Government
Sebastian Thüer	Argentina	Academia
Marcela Alejandra Travé	Argentina	Academia
Eva Maricel Wamba Ortiz	Argentina	Government
AHM Bazlur Rahman	Bangladesh	Civil Society
Iqbal Ahmed	Bangladesh	Private sector
Andy Alvaro Saavedra Guevara	Bolivia	Private sector
Karina Ingrid Medinaceli Díaz	Bolivia	Academia
Mariana Ottich	Bolivia	Government
Miguel Herman	Brazil	Academia
Cristiane Jacqueline Felinto	Brazil	Government
Ricardo Alan Kardec Loiola	Brazil	Technical community
Larissa Galdino de Magalhães Santos	Brazil	Academia
Marvin Correia	Brazil	Civil Society
Carolina Sancho Hirane	Chile	Academia
Carolina Valenzuela	Chile	Technical community
Juan Sebastián Gonzalez Sanabria	Colombia	Academia
Paula Otalora Heredia	Colombia	Academia
Víctor Alfonso Bedoya Mancera	Colombia	Academia
Roberto Lemaitre Picado	Costa Rica	Academia
Alfredo Velazco	Ecuador	Civil Society
Francisco Montesdeoca	Ecuador	Civil Society
Sandra Verónica Rodriguez Dominguez	El Salvador	Academia

Alberto Barbero Merás	España	Academia
Kervens St Sauveur	Haïti	Academia
Christian Rameau	Haïti	Academia
Henry Javier Pinto Flores	Honduras	Private sector
Sandy Karyna Palma Rodríguez	Honduras	Government
Kapil Goyal	India	Academia
Kapil Goyal	India	Academia
Valentina Grazia Sapuppo	Italy	Civil Society
Bonface Witaba	Kenya	Civil Society
Lorena Maldonado	México	Private sector
Gerardo Martínez Hernández	México	Civil Society
Hilda Saray Gómez González	México	Civil Society
Javier Velázquez Camargo	México	Academia
Adolfo Jesús Toledo Fraginals	México	Academia
Erika-Yamel Munive-Cortés	México	Civil Society
Juan Antonio Ramírez Márquez	México	Private sector
Anahiby Becerril	México	Academia
Sergio Reynoso	México	Private sector
Alicia Edith Trejo Jiménez	México	Private sector
Denisse Lelis	México	Private sector
Alma Romero Casales	México	Government
Joel Robinson	Panamá	Government
Isabel Fiafilio Rodríguez	Perú	Civil Society
Wilmer Caról Azurza Neyra	Perú	Government
Judith Murungi	Uganda	Academia
Felix Uribe	United States of America	Academia
Gustavo Ortega Alvarado	United States of America	Civil Society
Federico Rodríguez Hormaechea	Uruguay	Private sector
Nicolas Fiumarelli	Uruguay	Technical community
Diego Cajade	Uruguay	Civil Society
Alfredo vaneskahian	Uruguay	Government
Patricia Flores	Venezuela	Government

About the South School on Internet Governance

The main objective of the South School on Internet Governance is to involve young students and professionals from Latin America and the Caribbean, trained in different disciplines, to become involved in the Internet Governance debate and to understand its importance in the future of the Internet.

Their active involvement is relevant to address issues that are important for the development of the region and its insertion in a globalized world.

The mission of the South School on Internet Governance is:

- Increase the representativeness of the Latin American and Caribbean region in spaces where Internet Governance is debated and defined
- Create a training space for new generations of professionals who actively participate in meetings where the future of the Internet is shaped
- Train new leaders of opinion on topics related with Internet Governance in each of the countries of the region

In the 14 consecutive editions of the South School on Internet Governance, more than 7,000 fellowships have been awarded to face-to-face and remote participants from countries from the five continents. Thousands of remote participants from around the world were also involved through remote / hybrid participation. All the 14 editions have simultaneous translation in English/Spanish and when organized in Brazil also in Portuguese.

Onsite fellows receive a complete fellowship that includes training, hotel, and meals. All activities of the SSIG are free for the community.

SSIG offers free fellowships for a six-month training program in three stages:

- Stage 1 Eight-week preparatory course based on podcasts, videos and reading material, with exclusive material prepared by SSIG team in Spanish and English, including 30 learning hours.
- Stage 2 One-week face-to-face / hybrid event of intensive training with simultaneous translation by interpreters, with 40 hours of learning.
- Stage 3 Research phase with supervision and tutoring by University of Mendoza, Argentina, to obtain a Diploma in Internet Governance for those fellows with a university degree who successfully complete the three learning stages.

The South School on Internet Governance rotates between countries and has been organized with great success in:

1) 2009 - Buenos Aires, Argentina
2) 2010 - San Pablo, Brazil
3) 2011 - Ciudad de México, México
4) 2012 - Bogotá, Colombia
5) 2013 - Panamá, Panamá
6) 2014 - Port of Spain, Trinidad & Tobago
7) 2015 - San José de Costa Rica

8) 2016 – OAS Venue, Washington DC, USA
9) 2017 - FGV - Río de Janeiro, Brazil
10) 2018 – OAS Venue CYBER SSIG, Washington DC, USA
11) 2019 - Secretaría de Economía, Ciudad de México
12) 2020 – Virtual Edition – Host:University of Buenos Aires
13) 2021 – Virtual Edition – Host: MINTIC Colombia
14) 2022 - Hybrid Edition - Buenos Aires, Argentina

The SSIG LAC YouTube channel contains videos of all editions of SSIG. Each session can be viewed independently in Spanish or English.

SSIG has received the “WSIS Champion” award from the United Nations in recognition of its impact on Internet training.

SSIG is a founding member of the “Dynamic Coalition of Schools on Internet Governance” at the United Nations Internet Governance Forum.

In 2018 the book "Internet Governance and Regulations in Latin America'' was published in honor of the tenth anniversary of the South School on Internet Governance. The book is available in Spanish, English and Portuguese free for the community visiting www.gobernanzainternet.org.

Website: www.gobernanzainternet.org

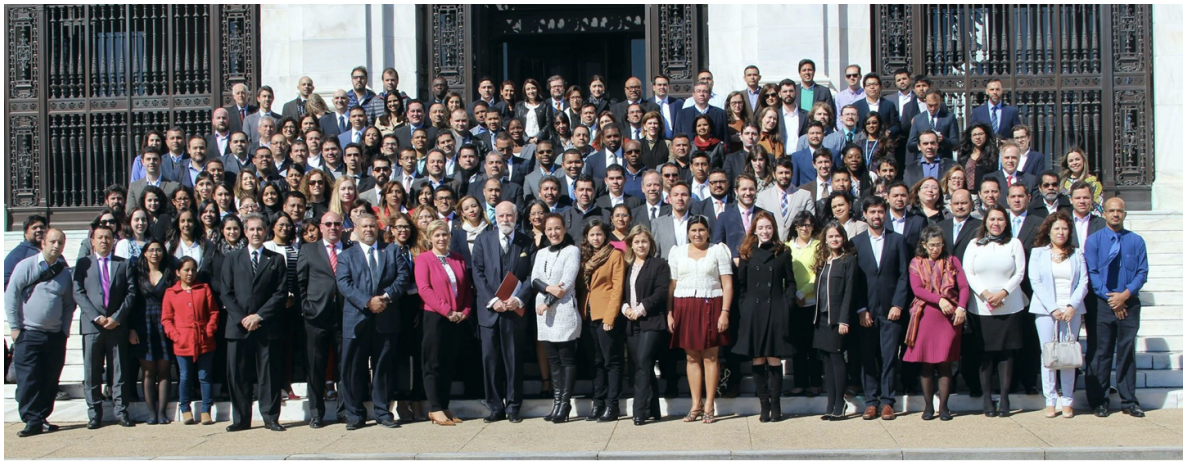
Twitter: @SSIGLAC

YouTube channel: SSIG LAC

Facebook / Linkedin: South Scholl on Internet Governance

Instagram: SSIGLAC

Contact: info@gobernanzainternet.org



English version
South School on Internet Governance fellow´s contribution to the Global Digital Compact

The South School on Internet Governance has joined efforts with its participants to contribute to the Global Digital Compact consultation organized by the United Nations.

Fellows from different countries have contributed this document to the Global Digital Compact process. The contribution to the Digital Global Compact has been made through an online survey that includes the 7 key digital issues that the Common Agenda report suggests for the Digital Global Compact, these are the following:

1- Connect everyone to the Internet, including all schools
2- Avoid Internet fragmentation
3- Protect data
4- Apply human rights online
5- Introduce accountability criteria for discrimination and misleading content
6- Promote the regulation of artificial intelligence
7- Digital commons as a global public good

Here are the contributions made by fellows at the South School on Internet Governance:

1- Connect everyone to the Internet, including all schools

Making all people literate in the use of ICTs is a fundamental principle.
The Internet is a human right, therefore it must be accessible, affordable, taking into account universal accessibility for all.
Access to knowledge must be universal, which is why it is necessary to guarantee Internet access in schools regardless of their location.
All people must have access to the infrastructure necessary to access the Internet and must receive training in the safe use of the Internet.
States must make the necessary and verifiable efforts to guarantee Internet access throughout their territory.
Public administrations must ensure the health and well-being of digital human beings.
States must work to build digital trust.
States must commit themselves to breaking down the digital divide by providing schools with the necessary infrastructure and equipment for the education of the youngest human beings.
Public administrations must guarantee digital operators, digital users and digital learners the Right to Disconnect.
The Internet must be the widest network in the world, it must cover the whole world and it must be for everyone.
Digital education and digital training must be a priority so that people can learn how the Internet really works, its advantages and disadvantages, so that they can assert their rights and duties and propose solutions for better Internet management. This could reduce the impact of digital technology on global warming, reduce cyber attacks, and decrease the dehumanization of users towards technology.

Digital education and digital training must be one of the priorities of national governments to create a culture of Internet use that will combat crimes against children and the most vulnerable people.
Behavioral ethics must find a central role among the teachings of the Digital School.

1.2 - Key commitment to this principle

All human beings have the right to be digital human beings.
Fundamental personal rights must be guaranteed on the Internet.
Regulations must be created to protect freedom of expression, neurorights and data protection.
Digital access is a fundamental right.
Digital learners have the right to realize themselves and their digital identity on the World Wide Web.
States must guarantee universal Internet access to the entire population, particularly the most vulnerable, monitoring the availability of the Internet for all, including rules that oblige Internet service providers to provide Internet service to schools.
Incentives and alliances must be developed to deploy the necessary infrastructure, constantly working to improve and develop its Internet infrastructure.
All public officials and political leaders must understand the benefit of the internet.
States must adopt transparent regulations that guarantee remuneration to human beings when their services are impacted by cybersecurity failures caused by third parties as a result of omissions and negligence.
The governments of the global South will have to work in partnership with the countries of the North to have the best infrastructure and so that the Internet connection in the North is similar to that of the South. Each country must work on a digital letter adapted to their customs, their tradition, their population and their internal laws so that they can protect themselves and the rights of their respective population. Digital education will have to be taught in primary and secondary schools in each country because as language, biology and history are basic goods to integrate well into society, digital education is vital so that they can know how not to be addicted, Learn about the impact of digital technologies on global warming, the importance of protecting your data on the Internet and your digital rights and duties.

2- Avoid Internet fragmentation

Interconnection must be guaranteed in all regions of the planet, promoting digital integration and inclusion, without restricting Internet access.
The internet must be homogeneous and standard, it must be a tool to guarantee access to adequate and truthful information.
The power of the internet lies in its reach and must be taken care of, taking care of net neutrality.
The Internet must remain an open network, without restrictions and with common protocols. The stronger the Internet, the better its benefits will be for everyone. A strong Internet is inclusive and resilient.
States must offer public open data services and the adoption of open protocols.
Avoiding the fragmentation of the Internet is an important goal to ensure that the Internet remains a global, open and interoperable platform that fosters innovation, communication and access to information for all users.
Countries must commit to an Internet that is globally compatible and interoperable.

2.1 - Key commitment to this principle

Risk management must be done preemptively to ensure continuous interconnection.
Freedom of expression and access to information must be guaranteed and Internet interoperability standards must be regulated.
It is important to establish sanction agreements for fragmentation detections promoted by government entities
The population must be educated and the development of clear policies on net neutrality encouraged, in which all interested parties must participate.
The Internet must be an open place where freedom prevails and with minimal government interference.
Just as domain name administration has an Enforcement Authority which is ICANN, the Multistakeholder community should create an entity that acts as an Enforcement Authority to prevent fragmentation events.
Training should be created to identify the factors that lead to the fragmentation of the Internet.
States should monitor the monopolization of data services and the massive promulgation of third parties in the adoption of proprietary protocols.
Avoiding the fragmentation of the Internet requires a collaborative and multifaceted approach that involves all stakeholders from all sectors of society.

3- Protect data

States must guarantee the right to be alone.
The protection of personal data is a right that must be exercised on the Internet.
It is of great importance to safeguard the use of personal data: my information is my property, without my permission no one can use my data and information.
Data protection must be guaranteed from the States in all areas by design and by default.
A fundamental principle for the use of data is that the citizen must be the sole owner of their data and have the freedom to withdraw them when they consider it necessary.
It is urgent to raise awareness of the use of data on the Internet since data protection is a human right and a fundamental right.
Conscious, voluntary consent to transparent data processing, given by data subjects, is essential and its collection must be demonstrated by data controllers, public and private.
States must constantly verify that all companies operating in their territory and/or under their jurisdiction do not design their business model based on the personal data of users.
It is of crucial importance that each State provides itself with an infrastructure that guarantees the rights of data subjects.
Data subjects must be guaranteed the right of access to their data.
Data subjects must be guaranteed the right to rectification of their data.
Data subject must have the right to obtain the erasure of personal data.
Data subjects must have the right to restriction of processing of personal data.
Data subject must have the right to erase personal data.
Data subject must have the right to object to processing of personal data.
The data subject must have the right to not be subject to a decision based exclusively on automated processing of personal data.
Data subjects must have the right to appeal to the courts for compensation claims arising from illegal processing of their data.

3.1 - Key commitment to this principle

Data regulation requires respecting international conventions, protecting the individual from misuse of data and respecting the data of others.
It is important to educate and make users aware of the risks of the information they share on the Internet and make the impact of privacy visible. Sanctions should be established for the misuse of personal data.
There should be a global data protection regulation applicable anywhere in the world regardless of location.
The regulations must allow a point of contact to be able to exercise the right against technology companies.
Greater controls must be implemented in the processing of personal data and information must be provided to human beings to protect themselves.
Political leaders must be aware of data governance and States must adopt regulations and standards that monitor data protection for all human beings and especially the most vulnerable.
Data protection will also require a multi-layered approach involving technical, administrative and physical security measures, as well as regular monitoring and testing to ensure that data remains secure over time.

4- Apply human rights online

Anonymity in the network must be avoided, as well as raising awareness among the population about the risks of cybercrime.
Governments must be guarantors of ensuring the rights of human beings, regardless of their physical or digital location.
Freedom of expression online is a fundamental principle for a democratic society.
Human rights must be applied in all interactions of the subjects.
States must adopt mandatory and optional national and international measures to promote a culture of respect for human rights.
Digital life is an extension of human life: human beings in any field require respect and defense of their human rights.
Human beings have the right to informed consent, which must be established when their communication is mediated through Artificial Intelligence.
It is of great importance to consider that human rights are extrapolated to cyberspace, to establish their scope, manifestation and impact.

4.1 - Key commitment to this principle

Network security can be achieved through preventive measures, campaigns must be created to help raise awareness of actions that may affect the rights of users.
Mechanisms must be established to prevent rights protection measures (copyright and personal data) from being means of censorship. We must work, educate, and legislate together to achieve it.
The necessary tools for the application of human rights must be made available to people.
At the international level, a "Scoring" system should be created where companies "voluntarily" adhere and on a common basis of certain points, an Enforcement Authority, monitors and points are taken out in case of verifying non-compliance or acknowledging their work in accordance with human rights, as an incentive. These recognitions, for the companies, would operate as a capital and a good letter of introduction for their businesses.

States must regulate and regulate the implications of the interaction of Artificial Intelligence with human beings according to the risks and impacts of these relationships.
Recognize and protect freedom of expression, combating hate speech and discrimination online.

5- Introduce accountability criteria for discrimination and misleading content

Put an end to digital functional illiteracy by educating people about the rights on the Internet and the responsibility of its use.
Regulate and prosecute illegal activities carried out through the Internet, protecting the user from the use of misleading content.
Promote the validation of publication and dissemination of content by applications when there is a mass reproduction of some text or image.
You must educate yourself to be able to discern false or misleading news or content.
Every citizen has the right to receive accurate information and not be subject to subversion and ambiguity of content.
Recognize vulnerability to erroneous information, that which is deliberately false and that which is manipulated, aiming to confuse what is true with what is distorted, leading to equivocal conclusions, particularly when this can affect collective decision-making processes.

5.1 - Key commitment to this principle

States must train and generate dissemination campaigns that explain the danger of misleading or false content being disseminated on the Internet.
Use Artificial Intelligence to detect misleading content by creating tools or firewalls for misleading content.
Make the population aware of misleading content.
The right to digital non-discrimination and to receive truthful information must be guaranteed.
Establish sanctions and corrective actions for people who generate misleading content, including the impossibility of connecting to technological means to avoid repetition.
Develop criteria to respond to misleading content by avoiding censorship.
Make tools available to penalize operators that offer misleading content online, using artificial intelligence to prevent false news from going viral and thus deceiving people.
States must create and promote official observatories of public content and promote actions that seek transparency of the actors involved.

6- Promote the regulation of artificial intelligence

The regulation of AI must be in favor of humanity, allow its use in an open manner, protect the rights of people, and use it as a development tool in different communities.
More education must be achieved to understand the scope of Artificial Intelligence and train more people to access it.
The objective of artificial intelligence must be evaluated and its impact on job losses seen.
human beings must have the right to informed consent when mediating the use of artificial intelligence in their communications.

6.1 - Key commitment to this principle

States must regulate AI at the international level and, on this basis, establish national policies.

Create a partnership between government regulators and end-users, including other related parties, to discuss how to alleviate the impact on those harmed by the advancement of artificial intelligence and build understanding of the scope of AI.
Implement AI as a "living" element of society, regulating its use and scope of application and creating AI programs with quality data.
It must be respected and controlled that the results of the AI application do not contain biases, working with the aim of using it in as many tasks as possible, including the usual activities of daily life of human beings.
Just as the Internet Governance Forum was created at WSIS, a space must be created at the UN level for the creation of an AI Governance Forum that promotes standards and regulations that foster innovation and technological advancement, without neglecting the protection of human rights.

7- Digital commons as a global public good

Digital common goods are the cultural heritage of humanity and their correct use and benefits to the community must be ensured.
Digital commons should help promote innovation and knowledge.
The Internet must be a universal good.
Digital commons are a public good in itself.
Taking care of the digital commons is similar to taking care of the planet where we all live. Let's not look for a problem like climate change to get us to act in favor of the digital commons.
human beings have the right to donate the content they produce for the good of humanity without harming third parties.
Digital commons are shared resources that are collectively managed and maintained by a community, rather than by a single owner or entity.
As a global public good, the digital commons should be available for use and reuse by anyone who needs it, without restrictions or barriers such as patents, copyrights, or other forms of intellectual property protection. This enables people and communities around the world to benefit from shared knowledge and resources, and to collaborate and innovate more effectively.

7.1 - Key commitment to this principle

It is important to define the concept of a public good by creating a common understanding of its use and protection.
The designation of public goods should be continually reviewed because technological progress is fast, and in this review an active participation of the community is necessary.
It is important to achieve the globalization of access to research content and its immediate impact in the regions, as well as to raise awareness about the concept of "global public good", what they are, what implications they have in daily life and emphasizing the need for the law is in charge of protecting them, without impeding innovation.
States must adopt policies that promote innovation and free dissemination of content for human beings.
The creation and sharing of digital resources should be encouraged: promotion of open source software, open data and open educational resources, as well as support for the creation and dissemination of scientific research and cultural works.

Fostering community collaboration and engagement: This involves promoting community collaboration and engagement in the management and maintenance of the digital commons, and ensuring that the benefits of these resources are widely and equitably shared.

Spanish version
South School on Internet Governance fellow´s contribution to the Global Digital Compact

La South School on Internet Governance ha sumado esfuerzos con sus participantes para contribuir a la consulta del Global Digital Compact organizada por Naciones Unidas.

Becarios de distintos países han contribuido con este documento al proceso de Global Digital Compact. La contribución al Pacto Mundial Digital se ha realizado a través de una encuesta en línea que incluye los 7 temas digitales clave que el informe de la Agenda Común sugiere para el Pacto Mundial Digital, estos son los siguientes:

1- Conectar a todas las personas a Internet, incluidas todas las escuelas
2- Evite la fragmentación de Internet
3- Proteger datos
4- Aplicar los derechos humanos en línea
5- Introducir criterios de rendición de cuentas para la discriminación y el contenido engañoso
6- Promover la regulación de la inteligencia artificial
7- Bienes comunes digitales como un bien público global

Aquí se detallan las contribuciones realizadas por los becarios de la South School on Internet Governance:

1- Conectar a todas las personas a Internet, incluidas todas las escuelas

Alfabetizar en el uso de las TIC´s a todas las personas es un principio fundamental.
Internet es un derecho humano por lo tanto debe ser genuinamente accesible, asequible, teniendo en cuenta la accesibilidad universal para todos.
El acceso al conocimiento debe ser universal, por lo que se requiere garantizar el acceso a Internet en las escuelas independientemente de su ubicación y/o cantidad de habitantes donde se encuentre.
Todas las personas deben tener acceso a la infraestructura necesaria para tener acceso a Internet y deben recibir capacitación para el uso seguro de internet.
Los Estados, deben realizar los esfuerzos necesarios y comprobables, para garantizar el acceso a Internet en todo su territorio, lo cual incluye zonas rurales y alejadas de los grandes centros urbanos.
Internet debe ser la más amplia red en el mundo, debe cobijar a todo el mundo y debe ser para todos.
La educación y formación digital debe ser una prioridad para que las personas puedan conocer cómo funciona realmente internet, sus ventajas y desventajas, que puedan hacer valer su derecho

y su deber y proponer soluciones para una mejor gestión de Internet. Esto podría reducir el impacto de la tecnología digital en el calentamiento global, reducir los ciberataques, disminuyendo la deshumanización de los usuarios hacia la tecnología.

1.2 - Compromiso clave para este principio

Se deben crear regulaciones para proteger la libertad de expresión y la protección de datos.
Los estados deben garantizar el acceso universal a toda la población, particularmente a los más vulnerables, vigilando la disponibilidad del Internet para todos, incluyendo reglas que obliguen a los oferentes de servicios de internet a otorgar servicio de Internet a las escuelas.
Se deben desarrollar incentivos y alianzas para desplegar la infraestructura necesaria en todo su territorio, trabajando constantemente en mejorar su infraestructura de Internet y desarrollarla.
Todos los funcionarios públicos y líderes políticos deben comprender el beneficio del internet.
Los Estados deben adoptar una normativa transparente que garantice la remuneración a los ciudadanos cuando sus servicios sean impactados por fallas de ciberseguridad ocasionadas por terceros a consecuencia de omisiones y negligencias.
Los gobiernos del Sur global tendrán que trabajar en sociedad con los países del Norte para tener la mejor infraestructura y para que la conexión a Internet en el Norte sea similar a la del Sur.
Cada país deberá trabajar en una carta digital adaptada a sus costumbres, su tradición, su población y sus leyes internas para que puedan protegerse a sí mismos y a los derechos de su respectiva población. La educación digital se tendrá que enseñar en la escuela primaria y secundaria de cada país porque como el idioma, la biología y la historia son bienes básicos para integrarse bien en la sociedad, la educación digital es vital para que puedan saber cómo no ser adictos, conocer el impacto de tecnologías digitales sobre el calentamiento global, la importancia de proteger sus datos en Internet y sus derechos y deberes digitales.

2- Evitar la fragmentación de Internet

La interconexión debe garantizarse en todas las regiones del planeta, promoviendo la integración digital y la inclusión, sin restringir el acceso a Internet.
El internet debe ser homogéneo y estándar, debe ser un herramienta para garantizar el acceso a la información adecuada y con veracidad.
El poder de internet reside en su alcance y se debe cuidar, cuidando la neutralidad de la red.
Internet debe seguir siendo una red abierta, sin restricciones y con protocolos comunes, mientras más fuerte sea Internet, mejor serán sus beneficios para todos. Una Internet fuerte es incluyente y resiliente.
Los Estados deberán ofrecer servicios públicos de datos abiertos y la adopción de protocolos abiertos.
Se debe evitar la fragmentación de Internet es un objetivo importante para garantizar que Internet siga siendo una plataforma global, abierta e interoperable que fomente la innovación, la comunicación y el acceso a la información para todos los usuarios.
Los países deben comprometerse a contar con una Internet que sea compatible a nivel mundial, e interoperable.

2.1 - Compromiso clave para este principio

La gestión de riesgos debe realizarse de manera preventiva para asegurar una interconexión continua.
Se debe garantizar libertad de expresión y acceso a la información y regular los estándares de interoperabilidad del Internet.
Es importante establecer acuerdos sancionatorios a detecciones de fragmentación propiciados desde entes gubernamentales
Se debe educar a la población y fomentar el desarrollo de políticas claras sobre la neutralidad de la red, en la que deben participar todos los actores interesados.
Internet debe de ser un lugar abierto donde prime la libertad y con la mínima interferencia de los gobiernos
Así como la administración de nombres de dominios tiene una Autoridad de Aplicación que es ICANN, la comunidad de Multistakeholder debería crear una entidad que actúe como Autoridad de Aplicación para prevenir eventos de fragmentación.
Se deben crear capacitaciones para identificar los factores que suponen la fragmentación del internet.
Los Estados deberán monitorear la monopolización de servicios de datos y la promulgación masiva de terceros en la adopción de protocolos propietarios.
Evitar la fragmentación de Internet requiere un enfoque colaborativo y multifacético que involucre a todas las partes interesadas de todos los sectores de la sociedad.

3- Proteger los datos

La protección de datos debe de ser garantizada desde los Estados en todos los ámbitos por defecto.
Es de gran importancia salvaguardar el uso de datos personales: mi información es mi propiedad, sin mi permiso nadie puede usar mis datos y mi información.
Un principio fundamental para el uso de datos es que el ciudadano debe ser el único propietario de sus datos y tener la libertad de retirarlos cuando considere necesario.
La protección de datos personales es un derecho que se debe poder ejercer en Internet.
Es urgente la concientización del uso de los datos en internet ya que la protección de datos es un derecho humano y un derecho fundamental.
Los Estados deben verificar constantemente que todas las empresas que actúen en su territorio y/o bajo su jurisdicción, no diseñen su modelo de negocio basado en los datos personales de los usuarios.
El propio Estado debe realizar un uso razonable y criterioso de los datos personales de los ciudadanos limitando su uso al mínimo indispensable.

3.1 - Compromiso clave para este principio

La regulación de datos requiere respetar convenciones internacionales, protegiendo al individuo de uso indebido de los datos y respetando los datos de otros.
Es importante educar y concientizar a los usuarios sobre los riesgos de la información que comparten en internet y hacer visible el impacto de la privacidad. Se deben establecer sanciones por el uso indebido de los datos personales.

Debería existir una normativa global de protección de datos aplicable en cualquier parte del mundo sin importar la localización.
Las regulaciones deben permitir un punto de contacto para poder ejercer el derecho contra empresas de tecnología.
Se deben de implementar mayores controles en los tratamientos de datos personales y facilitar al ciudadano información para protegerse.
Los líderes políticos deben conocer la gobernanza de datos y los Estados deberán adoptar regulaciones y normas que vigilen la protección de datos para todos los ciudadanos y en especial los más vulnerables.
La protección de datos también requerirá un enfoque de múltiples niveles que involucre medidas de seguridad técnicas, administrativas y físicas, así como monitoreo y pruebas regulares para garantizar que los datos permanezcan seguros a lo largo del tiempo.
El propio Estado deberá tener una política de protección de datos personales clara, transparente y que informe a los ciudadanos cómo será procesada su información.

4- Aplicar los derechos humanos online

Se debe evitar el anonimato en la red, también concientizar a la población sobre los riesgos de los ciberdelitos.
Los Gobiernos deben ser garantes de velar por los derechos de los ciudadanos, independientemente de su lugar físico o digital.
La libertad de expresión en línea es un principio fundamental para una sociedad democrática.
Los derechos humanos se deben aplicar en todas las interacciones de los sujetos.
Los Estados deben adoptar medidas nacionales e internacionales, obligatorias y facultativas para promover una cultura de respeto a los derechos humanos.
La vida digital es una extensión de la vida humana: el ser humano en cualquier ámbito requiere respeto y defensa de sus derechos humanos.
Los ciudadanos tienen derecho al consentimiento informado, el que debe establecerse cuando sus comunicación está mediada por medio de Inteligencia Artificial.
Es de gran importancia considerar que los derechos humanos se extrapolan al ciberespacio, establecer su alcance, manifestación e impacto.

4.1 - Compromiso clave para este principio

La seguridad en la red se podrá conseguir a través de medidas preventivas, se deben crear campañas que ayuden a concientizar de las acciones que pueden afectar los derechos de los usuarios.
Se deben establecer mecanismos para evitar que medidas de protección de derechos (derechos de autor y datos personales) sean medios de censura. Debemos trabajar, educar, legislar juntos para lograrlo.
Se deben poner a disposición de las personas las herramientas necesarias para la aplicación de los derechos humanos.
A nivel internacional debería crearse un sistema de "Scoring" donde las empresas "voluntariamente" se adhieran y sobre una base en común de determinados puntos, una Autoridad de Aplicación, haga un monitoreo y se le saque puntos en caso de verificarse incumplimientos o reconocer su labor acorde a los Derechos Humanos (DDHH), a modo de

incentivo. Esos reconocimientos, para las empresas, operaría como un capital y una buena carta de presentación para sus negocios.
Los Estados deben de regular y normar las implicaciones de la interacción de la Inteligencia Artificial con la ciudadanía según los riesgos e impactos de estas relaciones.
Reconocer y proteger la libertad de expresión, combatiendo el discurso de odio y la discriminación en línea.

5- Introducir criterios de rendición de cuentas para la discriminación y el contenido engañoso

Acabar con el analfabetismo funcional digital educando a las personas sobre los derechos en Internet y la responsabilidad de su uso.
Regular y perseguir actividades ilícitas realizadas mediante Internet, protegiendo al usuario por el uso de contenido engañoso.
Promover la validación de publicación y difusión de contenidos por aplicaciones cuando se presente reproducción en masa de algún texto o imagen.
Se debe educar para poder discernir noticias o contenidos falsos o engañosos.
Todo ciudadano tiene el derecho a recibir información precisa y no sujeta a la subversión y ambigüedad de contenido.
Reconocer la vulnerabilidad ante información errónea, la que es deliberadamente falsa y aquella que es manipulada, orientándose a confundir entre lo que es cierto, lo distorsionado induciendo a conclusiones equívocas, particularmente cuando ello puede incidir en procesos decisionales colectivos.

5.1 - Compromiso clave para este principio

Los Estados deben capacitar y generar campañas de difusión que expliquen el peligro de que el contenido engañoso o falso se difunda por Internet.
Utilizar a la Inteligencia Artificial para detectar contenido engañoso creando herramientas o cortafuegos para esos contenidos engañosos.
Concientizar a la población acerca del contenido engañoso.
Se debe garantizar el derecho a la no discriminación digital y a recibir información veraz.
Establecer sanciones y acciones correctivas para personas que generen contenido engañoso, incluyendo la imposibilidad de conectarse a medios tecnológicos para evitar su repetición.
Desarrollar criterios para responder ante contenido engañoso evitando la censura.
Poner a disposición herramientas para la sanción de los operadores que ofrezcan contenidos engañosos en la red, usando inteligencia artificial para evitar que noticias que son falsas puedan hacerse virales y de esta forma engañar a la personas.
Los Estados deberán crear y fomentar observatorios oficiales del contenido público y propiciar acciones que procuren la transparencia de los actores involucrados.

6- Promover la regulación de la Inteligencia artificial

La regulación de la IA debe ser en favor de la humanidad, permitir su uso de manera abierta, protegiendo los derechos de las personas, utilizándose como herramienta de desarrollo en las distintas comunidades.

Se debe lograr mayor educación para comprender los alcances de la Inteligencia Artificial y capacitar a más población para su acceso.
Se debe evaluar el objetivo de la inteligencia artificial y ver su impacto en la pérdida de puestos laborales.
Los ciudadanos deben tener derecho al consentimiento informado cuando medie el uso de inteligencia artificial en sus comunicaciones.

6.1 - Compromiso clave para este principio

Los Estados deben regular a nivel internacional la IA y, sobre esta base, establecer políticas nacionales.
Crear una asociación entre los organismos reguladores gubernamentales y los usuarios finales, incluidas otras partes relacionadas a fin de analizar de qué manera aliviar el impacto a los perjudicados por el avance de la inteligencia artificial y generar entendimiento del alcance de AI.
Implementar la IA como un elemento "vivo" de la sociedad, regulando su uso y ámbito de aplicación y creando programas de IA con datos de calidad.
Se debe respetar y controlar que los resultados de la aplicación de IA no contengan sesgos trabajando con el objetivo de utilizarla en la mayor parte de tareas posibles incluyendo actividades habituales de la vida diaria de los ciudadanos.
Así como se creó el Foro de Gobernanza de Internet en la CMSI, se debe crear un espacio en el ámbito de la ONU para la creación de un Foro de Gobernanza de IA que promueva estándares y regulaciones que fomenten la innovación y el avance tecnológico, sin descuidar la protección de los DDHH .

7- Bienes comunes digitales como bien público global

Los bienes comunes digitales son patrimonio cultural de la humanidad y se debe asegurar el libre acceso y su correcto uso y beneficios a la comunidad.
Los bienes comunes digitales deben ayudar a promover la innovación y el conocimiento.
Internet debe ser un bien universal.
Los bienes comunes digitales, son un bien público en sí mismo.
Cuidar de los bienes comunes digitales es semejante a cuidar el planeta donde todos habitamos. No busquemos un problema como el cambio climático para ponernos a favor de los bienes comunes digitales.
La ciudadanía tiene derecho a donar para bien de la humanidad el contenido que produzcan sin perjudicar a terceros.
Los bienes comunes digitales son recursos compartidos que son administrados y mantenidos colectivamente por una comunidad, en lugar de por un solo propietario o entidad.
Como bien público mundial, los bienes comunes digitales deben estar disponibles para su uso y reutilización por parte de cualquier persona que los necesite, sin restricciones ni barreras como patentes, derechos de autor u otras formas de protección de la propiedad intelectual. Esto permite que las personas y las comunidades de todo el mundo se beneficien del conocimiento y los recursos compartidos, y colaboren e innoven de manera más eficaz.

7.1.- Compromiso clave para este principio

Es importante definir el concepto de bien público creando un entendimiento común de su uso y protección.
La designación de bienes públicos debe revisarse continuamente pues el avance tecnológico es veloz, y en esta revisión es necesario una activa participación de la comunidad.
Es importante lograr la globalización del acceso a los contenidos investigativos y a su impacto inmediato en las regiones, así como crear conciencia sobre el concepto de "bien público global", cuáles son, qué implicancias tienen en la vida cotidiana y enfatizando en la necesidad de que el derecho se encargue de tutelarlos, sin impedir la innovación.
Los Estados deben de adoptar políticas que promulguen la innovación y difusión libre de contenidos pro la ciudadanía.
Se debe fomentar la creación y el intercambio de recursos digitales: promoción de software de código abierto, datos abiertos y recursos educativos abiertos, así como el apoyo a la creación y difusión de investigaciones científicas y obras culturales.
Fomentar la colaboración y el compromiso de la comunidad: esto implica promover la colaboración y el compromiso de la comunidad en la gestión y el mantenimiento de los bienes comunes digitales, y garantizar que los beneficios de estos recursos se compartan de manera amplia y equitativa.

Portuguese version

South School on Internet Governance fellow´s contribution to the Global Digital Compact

A South School on Internet Governance uniu esforços com seus participantes para contribuir com a consulta Global Digital Compact organizada pelas Nações Unidas.

Bolsistas de diferentes países contribuíram com este documento para o processo do Global Digital Compact. A contribuição para o Digital Global Compact foi feita através de uma pesquisa online que inclui as 7 principais questões digitais que o relatório da Agenda Comum sugere para o Digital Global Compact, são elas:

1- Conecte todos à Internet, incluindo todas as escolas
2- Evite a fragmentação da Internet
3- Proteja os dados
4- Aplicar os direitos humanos online
5- Introduzir critérios de responsabilidade para discriminação e conteúdo enganoso
6- Promover a regulamentação da inteligência artificial
7- Bens comuns digitais como um bem público global

Aqui estão as contribuições feitas pelos membros da South School on Internet Governance:

1- Conecte todos à Internet, incluindo todas as escolas

A alfabetização de todas as pessoas no uso das TIC é um princípio fundamental.

A Internet é um direito humano, portanto deve ser acessível, acessível, levando em consideração a acessibilidade universal para todos.
O acesso ao conhecimento deve ser universal, por isso é necessário garantir o acesso à Internet nas escolas, independentemente da sua localização.
Todas as pessoas devem ter acesso à infraestrutura necessária para acessar a Internet e devem receber treinamento no uso seguro da Internet.
Os Estados devem fazer os esforços necessários e verificáveis para garantir o acesso à Internet em todo o seu território.
A Internet deve ser a rede mais ampla do mundo, deve abranger todo o mundo e deve ser para todos.
A educação digital e a formação digital devem ser uma prioridade para que as pessoas aprendam como a Internet realmente funciona, as suas vantagens e desvantagens, para que possam fazer valer os seus direitos e deveres e propor soluções para uma melhor gestão da Internet. Isso poderia reduzir o impacto da tecnologia digital no aquecimento global, reduzir os ataques cibernéticos, diminuindo a desumanização dos usuários em relação à tecnologia.

1.2 - Compromisso fundamental com este princípio

Os Estados devem garantir o acesso universal a toda a população, especialmente aos mais vulneráveis, monitorando a disponibilidade da Internet para todos, incluindo regras que obriguem os provedores de serviços de Internet a fornecer serviço de Internet para as escolas.
Incentivos e alianças devem ser desenvolvidos para implantar a infraestrutura necessária, trabalhando constantemente para melhorar e desenvolver sua infraestrutura de Internet.
Todos os funcionários públicos e líderes políticos devem compreender os benefícios da Internet.
Os Estados devem adotar normas transparentes que garantam a remuneração dos cidadãos quando seus serviços forem afetados por falhas de segurança cibernética causadas por terceiros como resultado de omissões e negligências.
Os governos do Sul global terão que trabalhar em parceria com os países do Norte para ter a melhor infraestrutura e para que a conexão à Internet no Norte seja semelhante à do Sul. Cada país deve trabalhar em uma carta digital adaptada aos seus costumes, sua tradição, sua população e suas leis internas para que possam proteger a si mesmos e aos direitos de sua respectiva população. A educação digital terá que ser ensinada nas escolas primárias e secundárias de cada país porque como a língua, a biologia e a história são bens básicos para se integrar bem na sociedade, a educação digital é vital para que saibam como não se viciar, Conheça o impacto das tecnologias digitais sobre aquecimento global, a importância de proteger seus dados na Internet e seus direitos e deveres digitais.

2- Evite a fragmentação da Internet

A interconexão deve ser garantida em todas as regiões do planeta, promovendo a integração e inclusão digital, sem restringir o acesso à Internet.
A internet deve ser homogênea e padronizada, deve ser uma ferramenta para garantir o acesso à informação adequada e verdadeira.
O poder da internet está ao seu alcance e deve ser cuidado, zelando pela neutralidade da rede.
A Internet deve permanecer uma rede aberta, sem restrições e com protocolos comuns.Quanto mais forte a Internet, melhores serão seus benefícios para todos. Uma Internet forte é inclusiva e resiliente.
Os Estados devem oferecer serviços públicos de dados abertos e a adoção de protocolos abertos.

Evitar a fragmentação da Internet é um objetivo importante para garantir que a Internet continue sendo uma plataforma global, aberta e interoperável que promove inovação, comunicação e acesso à informação para todos os usuários.
Os países devem se comprometer com uma Internet que seja globalmente compatível e interoperável.

2.1 - Compromisso fundamental com este princípio

O gerenciamento de riscos deve ser feito preventivamente para garantir a interconexão contínua.
A liberdade de expressão e o acesso à informação devem ser garantidos e os padrões de interoperabilidade da Internet devem ser regulamentados.
É importante estabelecer acordos de sanção para detecção de fragmentação promovidas por entidades governamentais
A população deve ser educada e o desenvolvimento de políticas claras de neutralidade da rede, nas quais todos os interessados devem participar.
A Internet deve ser um lugar aberto onde a liberdade prevaleça e com o mínimo de interferência do governo.
Assim como a administração de nomes de domínio tem uma Autoridade de Execução que é a ICANN, a comunidade Multissetorial deve criar uma entidade que atue como uma Autoridade de Execução para evitar eventos de fragmentação.
Deve-se criar treinamento para identificar os fatores que levam à fragmentação da Internet.
Os Estados devem monitorar a monopolização dos serviços de dados e a promulgação massiva de terceiros na adoção de protocolos proprietários.
Evitar a fragmentação da Internet requer uma abordagem colaborativa e multifacetada que envolve todas as partes interessadas de todos os setores da sociedade.

3- Proteja os dados

A proteção de dados deve ser garantida pelos Estados em todas as áreas por padrão.
É de grande importância salvaguardar a utilização dos dados pessoais: as minhas informações são propriedade minha, sem a minha autorização ninguém pode utilizar os meus dados e informações.
Um princípio fundamental para o uso de dados é que o cidadão deve ser o único proprietário de seus dados e ter a liberdade de retirá-los quando julgar necessário.
A proteção de dados pessoais é um direito que deve ser exercido na Internet.
É urgente sensibilizar para a utilização de dados na Internet uma vez que a proteção de dados é um direito humano e um direito fundamental.
Os Estados devem verificar constantemente se todas as empresas que operam em seu território e/ou sob sua jurisdição não desenham seu modelo de negócios com base nos dados pessoais dos usuários.

3.1 - Compromisso fundamental com este princípio

A regulamentação de dados exige respeitar as convenções internacionais, protegendo o indivíduo do uso indevido de dados e respeitando os dados de terceiros.
É importante educar e conscientizar os usuários sobre os riscos das informações que compartilham na Internet e tornar visível o impacto da privacidade. Devem ser estabelecidas sanções para o uso indevido de dados pessoais.

Deve haver um regulamento global de proteção de dados aplicável em qualquer lugar do mundo, independentemente da localização.
Os regulamentos devem permitir que um ponto de contato possa exercer o direito contra empresas de tecnologia.
Maiores controles devem ser implementados no processamento de dados pessoais e informações devem ser fornecidas aos cidadãos para se protegerem.
Os líderes políticos devem estar cientes da governança de dados e os Estados devem adotar regulamentos e padrões que monitorem a proteção de dados para todos os cidadãos e especialmente para os mais vulneráveis.
A proteção de dados também exigirá uma abordagem em várias camadas envolvendo medidas de segurança técnica, administrativa e física, bem como monitoramento e testes regulares para garantir que os dados permaneçam seguros ao longo do tempo.

4- Aplicar os direitos humanos online

O anonimato na rede deve ser evitado, assim como a conscientização da população sobre os riscos do cibercrime.
Os governos devem ser os garantes da garantia dos direitos dos cidadãos, independentemente da sua localização física ou digital.
A liberdade de expressão online é um princípio fundamental para uma sociedade democrática.
Os direitos humanos devem ser aplicados em todas as interações dos sujeitos.
Os Estados devem adotar medidas nacionais e internacionais obrigatórias e facultativas para promover uma cultura de respeito aos direitos humanos.
A vida digital é uma extensão da vida humana: o ser humano em qualquer área exige respeito e defesa de seus direitos humanos.
Os cidadãos têm direito ao consentimento informado, que deve ser estabelecido quando sua comunicação é mediada por Inteligência Artificial.
É de grande importância considerar que os direitos humanos são extrapolados para o ciberespaço, para estabelecer seu alcance, manifestação e impacto.

4.1 - Compromisso fundamental com este princípio

A segurança da rede pode ser alcançada por meio de medidas preventivas, devendo ser criadas campanhas que ajudem a conscientizar sobre ações que possam afetar os direitos dos usuários.
Devem ser estabelecidos mecanismos para evitar que medidas de proteção de direitos (direitos autorais e dados pessoais) sejam meios de censura. Devemos trabalhar, educar, legislar juntos para alcançá-lo.
As ferramentas necessárias para a aplicação dos direitos humanos devem ser disponibilizadas às pessoas.
A nível internacional, deve ser criado um sistema de "Scoring" onde as empresas adiram "voluntariamente" e numa base comum de determinados pontos, uma Enforcement Authority, monitores e pontos são retirados em caso de verificação de incumprimento ou reconhecimento do seu trabalho em de acordo com os direitos humanos, como um incentivo. Esses reconhecimentos, para as empresas, funcionariam como um capital e uma boa carta de apresentação para seus negócios.
Os Estados devem regulamentar e regulamentar as implicações da interação da Inteligência Artificial com os cidadãos de acordo com os riscos e impactos dessas relações.

Reconhecer e proteger a liberdade de expressão, combatendo o discurso de ódio e a discriminação online.

5- Introduzir critérios de responsabilidade para discriminação e conteúdo enganoso

Acabar com o analfabetismo funcional digital, educando as pessoas sobre os direitos na Internet e a responsabilidade de seu uso.
Regular e processar as atividades ilegais realizadas através da Internet, protegendo o usuário do uso de conteúdo enganoso.
Promover a validação de publicação e divulgação de conteúdo por aplicativos quando houver reprodução em massa de algum texto ou imagem.
Você deve educar-se para ser capaz de discernir notícias ou conteúdos falsos ou enganosos.
Todo cidadão tem o direito de receber informações precisas e não sujeitas a subversão e ambigüidade de conteúdo.
Reconhecer a vulnerabilidade a informações erróneas, deliberadamente falsas e manipuladas, procurando confundir o que é verdadeiro com o que é distorcido, conduzindo a conclusões equívocas, sobretudo quando esta pode afetar os processos de decisão coletiva.

5.1 - Compromisso fundamental com este princípio

Os Estados devem treinar e gerar campanhas de divulgação que expliquem o perigo de conteúdos enganosos ou falsos serem divulgados na Internet.
Use Inteligência Artificial para detectar conteúdo enganoso criando ferramentas ou firewalls para conteúdo enganoso.
Conscientizar a população sobre conteúdos enganosos.
O direito à não discriminação digital e ao recebimento de informações verídicas deve ser garantido.
Estabelecer sanções e ações corretivas para pessoas que geram conteúdo enganoso, incluindo a impossibilidade de conexão com meios tecnológicos para evitar a repetição.
Desenvolva critérios para responder a conteúdos enganosos evitando a censura.
Disponibilizar ferramentas para penalizar os operadores que oferecem conteúdo enganoso online, usando inteligência artificial para evitar que notícias falsas se tornem virais e, assim, engane as pessoas.
Os Estados devem criar e promover observatórios oficiais de conteúdo público e promover ações que busquem a transparência dos atores envolvidos.

6- Promover a regulamentação da inteligência artificial

A regulamentação da IA deve ser a favor da humanidade, permitindo seu uso de forma aberta, protegendo os direitos das pessoas, utilizando-a como ferramenta de desenvolvimento em diferentes comunidades.
Mais educação deve ser alcançada para entender o alcance da Inteligência Artificial e treinar mais pessoas para acessá-la.
O objetivo da inteligência artificial deve ser avaliado e seu impacto na perda de empregos deve ser visto.
Os cidadãos devem ter o direito ao consentimento informado ao mediar o uso de inteligência artificial em suas comunicações.

6.1 - Compromisso fundamental com este princípio

Os Estados devem regular a IA em nível internacional e, com base nisso, estabelecer políticas nacionais.
Crie uma parceria entre reguladores governamentais e usuários finais, incluindo outras partes relacionadas, para discutir como aliviar o impacto sobre os prejudicados pelo avanço da inteligência artificial e desenvolver a compreensão do escopo da IA.
Implementar a IA como elemento “vivo” da sociedade, regulamentando seu uso e escopo de aplicação e criando programas de IA com dados de qualidade.
Deve-se respeitar e controlar que os resultados da aplicação da IA não contenham vieses, trabalhando-se com o objetivo de utilizá-la no maior número de tarefas possíveis, incluindo as atividades habituais do cotidiano dos cidadãos.
Assim como o Fórum de Governança da Internet foi criado na WSIS, deve ser criado um espaço no nível da ONU para a criação de um Fórum de Governança de IA que promova padrões e regulamentos que fomentem a inovação e o avanço tecnológico, sem descuidar da proteção dos direitos humanos.

7- Bens comuns digitais como um bem público global

Os bens comuns digitais são patrimônio cultural da humanidade e seu uso correto e benefícios para a comunidade devem ser assegurados.
Os bens comuns digitais devem ajudar a promover a inovação e o conhecimento.
A Internet deve ser um bem universal.
Os bens comuns digitais são um bem público em si.
Cuidar dos bens comuns digitais é como cuidar do planeta onde todos vivemos. Não vamos procurar um problema como a mudança climática para nos levar a agir em favor dos bens comuns digitais.
Os cidadãos têm o direito de doar o conteúdo que produzem para o bem da humanidade sem prejudicar terceiros.
Os bens comuns digitais são recursos compartilhados que são gerenciados e mantidos coletivamente por uma comunidade, e não por um único proprietário ou entidade.
Como um bem público global, o bem comum digital deve estar disponível para uso e reutilização por qualquer pessoa que dele necessite, sem restrições ou barreiras como patentes, direitos autorais ou outras formas de proteção à propriedade intelectual. Isso permite que pessoas e comunidades em todo o mundo se beneficiem de conhecimento e recursos compartilhados e colaborem e inovem de forma mais eficaz.

71. - Compromisso fundamental com este princípio

É importante definir o conceito de bem público criando um entendimento comum de seu uso e proteção.
A designação de bens públicos deve ser continuamente revista porque o progresso tecnológico é rápido, e nessa revisão é necessária uma participação ativa da comunidade.
É importante conseguir a globalização do acesso aos conteúdos de investigação e o seu impacto imediato nas regiões, bem como sensibilizar para o conceito de "bem público global", o que são, que implicações têm na vida quotidiana e enfatizar a a necessidade, pois a lei se encarrega de protegê-los, sem impedir a inovação.

Os Estados devem adotar políticas que promovam a inovação e a divulgação gratuita de conteúdos para os cidadãos.
Deve ser incentivada a criação e partilha de recursos digitais: promoção de software de código aberto, dados abertos e recursos educativos abertos, bem como apoio à criação e divulgação de investigação científica e obras culturais.
Promover a colaboração e o envolvimento da comunidade: envolve promover a colaboração e o envolvimento da comunidade na gestão e manutenção dos bens comuns digitais e garantir que os benefícios desses recursos sejam compartilhados de forma ampla e equitativa.