INTERNET GOVERNANCE FORUM 2022

Addis Ababa IGF Messages

This document[1] is a summary of points raised during the 17th annual Internet Governance Forum meeting hosted in Addis Ababa on 28 November - 2 December 2022.

The views and opinions expressed herein do not necessarily reflect those of the United Nations Secretariat. The designations and terminology employed may not conform to United Nations practice and do not imply the expression of any opinion whatsoever on the part of the Organization.

Discussions at the 2022 IGF focused on five key themes that have been identified for the Global Digital Compact (GDC) which was proposed in the United Nations Secretary-General's 2021 report on the 75th anniversary of the United Nations, *Our Common Agenda*, and will be considered by the UN General Assembly in 2023. This will form part of the development of the Summit of the Future which is scheduled for 2024.

The themes considered by the IGF were:

- **Connecting All People and Safeguarding Human Rights**
- **Avoiding Internet Fragmentation**
- **Governing Data and Protecting Privacy**
- **Enabling Safety, Security and Accountability**
- **Addressing Advanced Technologies including Artificial Intelligence (AI)**

The IGF's multistakeholder community expressed support for the Secretary-General's proposal for a Global Digital Compact. The messages set out in this document represent contributions from the IGF towards development of the Compact. IGF Dynamic Coalitions which are already addressing specific challenges and opportunities that are relevant to the thematic areas proposed for the GDC have also expressed their intention to contribute to the UN's preparatory and implementation phases of the GDC process.

[1] The messages emerged during the 17th annual IGF meeting. They were subject for public consultations through which feedback was collected and integrated in this final draft.

Connecting All People and Safeguarding Human Rights

Theme

The UN Secretary-General's proposed Global Digital Compact (GDC) has as its first principle to "Connect all people to the Internet, including all schools." This recognizes that Internet connectivity and access have become prerequisites for ensuring the livelihoods, safety and education of people all around the world – and that Internet in schools provides crucial points of access, makes informational resources available to all students, and builds digital literacy from the earliest stages of life. Yet 2.7 billion people remain unconnected today, with those in least developed countries and rural communities most disadvantaged.

Meaningful access reaches beyond mere connectivity and is inextricable from the safeguarding of human rights online. Access that contributes to the wellbeing of societies must have human rights at its centre. This includes, among many others, the ability for users to express themselves freely, for the unfettered exercise of democratic and political participation, for persons of all backgrounds to experience the Internet without fear of harassment or discrimination, and for children to enjoy the same rights and protections online as they do offline. The Internet is both an enabler of rights and must seamlessly incorporate established human rights, as we increase our digital dependence for routine functions, and as boundaries between life "online" and "offline" are becoming less significant.

Messages

Digital Divides

- **The digital divides between different countries and regions remain powerful factors affecting national and international development**, including progress towards the Sustainable Development Goals (SDGs). Of particular concern are least developed countries and small island developing states (SIDS). Digital divides are much more than connectivity divides. Meaningful access includes issues of accessibility, affordability, content, services, digital literacy and other capabilities as well as connectivity. Affordability is a particular problem for many people, especially in the Global South.
- **The COVID-19 pandemic demonstrated the Internet's role in enabling individual and economic resilience, but also illustrated the extent to which those who lack connectivity or meaningful access are disadvantaged**, potentially exacerbating other inequalities. It will take time to understand the full impact and implications of COVID-related interventions concerning access, use and human rights.
- **Some groups within all societies experience deeper digital divides or have less meaningful access than others.** Women in many societies are less connected than men and make less use of connectivity. Digital disadvantage is greater among vulnerable and marginalised communities, and many people experience multiple disadvantages through the combination of factors related to age, gender, ethnicity, language, social class and other factors. Targeted initiatives in infrastructure,

devices and services can help to improve the access rates for less-connected social groups, but need to be accompanied by measures to address other deficiencies in meaningful access and should be associated with other measures to address disadvantage and discrimination.

- **Resilient and secure digital infrastructure is crucial for digital inclusion. Governments should protect and promote required infrastructure, including grid and off-grid power as well as communications networks.** In parts of Africa and other continents, large distances between rural and remote communities, including those in SIDS, make last-mile connectivity commercially unattractive to the private sector. Connectivity, speed and reliability are important aspects of infrastructure provision. It will take time and investment to improve the capacity of infrastructure and address regional imbalances, especially in rural areas.
- **Cooperation amongst stakeholder groups is important in ensuring and enabling access. Governments, and multistakeholder partners, should support the establishment and work of effective regulatory agencies and frameworks, address challenges in commercially unattractive areas, and encourage innovative approaches to connectivity** including community networks, appropriate spectrum allocation, access delivered by low earth orbit satellites and the availability of local content, including content in local languages.

The Gender Digital Divide and women's rights

- **Men are significantly more likely to be online or have mobile connectivity than women.** The gender digital gap is particularly wide in Least Developed Countries. SDG target 9c, which seeks to achieve universal, affordable Internet access, cannot be met until this gap is closed.
- **The threat of violence and harassment is a deterrent to women's online participation.** Online gender-based violence is an important factor driving and reinforcing gender inequality in Internet access and usage, leading to some women leaving online spaces. The role of technology services and platforms in propagating gender-based violence should be acknowledged and addressed. Women should be supported by guidance to resist and redress online gender-based violence, including through community-led helplines. Resources, community guidelines and reporting on platforms should be made available in local languages.
- **Concepts of gender equality, inclusion, and women's rights and protection should be incorporated into the Global Digital Compact** (GDC), as has been proposed by UN Women.

Human Rights and digital development

- **Universal access should respect human rights, to ensure the Internet is both accessible and safe for all.** These include freedom of expression and association, the right to privacy and other civil and political and economic, social and cultural rights set out in international rights agreements. Internet governance structures and the design of digital technologies should respect these rights. Standards development organisations should consider inviting participation by experts in online human rights, from all stakeholder communities, in their work.
- **Transparency, accountability and due diligence regarding human rights are the responsibilities of all stakeholder groups, including intergovernmental and international organisations, governments, the private sector, the technical community and civil society.** This will require alignment of business

practices with digital rights and cooperation between stakeholders to address issues such as disinformation, discrimination and hate speech, especially at times of political unrest, elections and transfers of power.

- **Access to the Internet provides a crucial opportunity for access to information and expression.** Governments should avoid recourse to Internet shutdowns because of their negative impact on both human rights and economic welfare. Social media and technology companies should support citizens in their advocacy efforts concerning shutdowns.
- **It is important to improve the monitoring and implementation of digital rights.** A number of suggestions have been made to establish international monitoring arrangements within the UN system, with multistakeholder engagement. These could complement and build on existing mechanisms, including both those concerned with digital development and rights and those in other spheres such as climate change.
- **The internet provides opportunities for enhancing rights to education**, as part of broader policies for educational improvement**.** The quality of education in the Global South, particularly during the pandemic, has suffered due to a lack of connectivity. While ICTs can enable meaningful access for students, differences in global and local adoption rates have exacerbated pre-pandemic inequalities. Experience during the pandemic can be used to improve the use of digital resources in the future.
- **Efforts should be made to help smaller and local businesses take maximum advantage of the Internet.** Use of digital tools by small and medium-sized enterprises has increased greatly since 2020, but micro-enterprises still face significant challenges in their ability to digitalise their businesses.
- **Labour market changes built around online platforms present both opportunities and challenges for job creation and job quality**, especially for women who play a greater part than men in the informal sector in most countries. Lack of training remains a barrier for many people in maximising their employment potential.
- **Digital competencies must be improved, and adaptations in teaching, learning and training methodologies are needed to adapt to new paradigms** in both education and employment. It is important to identify and close the gap between the needs of the industry and tertiary education.

Avoiding Internet Fragmentation

Theme

The maintenance of a global, open and interoperable Internet is a core value of the IGF. This implies that common technical standards and protocols continue to be deployed to achieve a network of interconnected networks across countries and regions, and that standards for content and services are consistent with human rights and with the rule of law. The call for this – applying a framework to the Internet that prioritises the rights and freedoms of users as well as, and through, infrastructural, end-to-end coherence – has been echoed in plans for the GDC.

The risk of fragmentation is real and mounting. While technical and commercial fragmentation – where the functioning of the Internet is impacted by a mix of voluntary and involuntary conditions and business practices – needs to be addressed, fragmentation by government policy that affects the open and interoperable character of the Internet is also of concern.

Messages

Understanding the issues

- **The Global Digital Compact provides an opportunity to reassert the value of an open interconnected internet for the realisation of the UN Charter, achievement of the Sustainable Development Goals and exercise of human rights.** There is widespread agreement within the Internet community about the value of a global, unfragmented Internet as a platform for human activity.

- **The issues raised in discussions of Internet fragmentation are multi-layered, and different stakeholders give a variety of meanings and interpretations to the term.** Some are most concerned with technical and infrastructural aspects of the Internet, while others focus on public policy issues including access, rights and impacts on user experience. These are explored in a draft framework prepared by the IGF Policy Network on Internet Fragmentation. Respect and understanding for different people's perceptions and experience of fragmentation is essential if we are to reach effective and coordinated responses.

- **A wide range of political, economic, and technical factors can potentially drive fragmentation.** However, diversity and decentralisation should not be mistaken for fragmentation. These are fundamentally positive aspects of the Internet's architecture and operations.

Addressing the risk of fragmentation

- **Effective multistakeholder governance mechanisms are essential for the governance of a global unfragmented Internet.** There is a need to reinforce trust in these mechanisms, to ensure that they are robust and sustainable, and to foster coherence across governance structures as they evolve to meet new challenges.

- **There is a need for vigilance concerning new or developing risks of fragmentation.** Global cooperation and coordination will be essential in identifying early warning signs, mapping the impact of policies and other developments, and preparing to address the implications of these changes. A multistakeholder approach is best suited to assess, evaluate and monitor the potential unintended consequences of measures that affect the Internet and to suggest effective alternatives that avoid or mitigate the risks of fragmentation. The IGF Policy Network on Internet Fragmentation is a positive example of this approach.

- **Internet openness is instrumental in fostering the enjoyment of Internet users' human rights, promoting competition and equality of opportunity, and safeguarding the generative peer-to-peer nature of the Internet.** Debates about net neutrality and non-discriminatory traffic management are only part of broader discussions in this context. Net neutrality is necessary but not sufficient to guarantee Internet openness. Infrastructural and data interoperability, and platform and device neutrality, are also necessary.

- **While legal, regulatory and policy approaches will differ around the world, active coordination across international boundaries is vital to ensuring that fragmented approaches do not threaten the global reach and interoperability of the Internet.** Maintaining the integrity of the global network requires international regulatory collaboration and consensus on basic principles.

- **Many different factors affect the experience of the Internet in different jurisdictions, including different social, demographic, economic, cultural and political contexts as well as technical and infrastructure issues.** The pursuit of some forms of digital governance at national level can increase the risk of fragmentation at the technical level of the Internet. However, regulatory frameworks must also consider different requirements in different contexts and keep pace with rapid change in technology and services.

- **There is a need for greater knowledge- and information-sharing among stakeholders**, to further discussion of cyber-diplomacy as an evolving phenomenon, and to consider the scope for appropriate interventions. Standard-making bodies should continue to improve outreach and engagement with stakeholders and to improve understanding between policy and technical communities. Technical decisions that bear policy implications should be discussed by standardisation bodies through the direct involvement of all affected stakeholders.

Governing Data and Protecting Privacy

Theme

Data are the key resource of the globalised digital age. The movement of data drives economies, while data analysis, including big data analytics, has been the basis for remarkable innovations across disciplines, from finance, to health and law enforcement.

But the widespread use, routine flow across borders and fungibility of data remain sensitive and unresolved topics. As a transnational, commercial asset, data flows operate in an environment in which there is little consistency between national legal regimes and where there are significant enforcement challenges. The privacy of personal data is too often sacrificed over the course of data exchanges, from the point of collection to application and storage, with deep consequences for trust and security.

To harness the significant promise of data, economically and for research purposes, discussions need to be relaunched around governance, integrity and the protection of peoples' privacy.

Messages

The centrality of data

- **Data have become a critical resource in an increasingly digital age.** Data flows are crucial to international cooperation in many fields including scientific research, law enforcement, and national and global security. Data, data security and data protection are critical enablers of sustainable development. The effective use and sharing of data on a global scale can help overcome shared challenges and the threats posed by cascading crises such as pandemics and climate change.

- **Data can generate both profit and significant social value.** The benefits of the data-driven economy, however, have so far been unevenly distributed. Many people are concerned that they may become primarily providers of data rather than beneficiaries.

- **The relationship between those who generate and those who use data is important.** Data poverty is a significant problem, especially in local communities and among vulnerable segments of populations. Lack of data privacy and inadequate data protection undermine trust in data management. It is important to build data literacy and data capacities across levels of government, in educational curricula and for the general public.

- **Data management and governance are complex issues in both national and international governance.** Developments in data – including big data analytics, innovations in artificial intelligence and machine learning, and innovations across public policy dimensions and the SDGs – demonstrate the need for appropriate consideration of political, economic and social impacts and for nuanced

policy interventions. Government and regulatory institutions need the infrastructure and capacity required to implement effective, integrated national data governance frameworks. Application developers have a responsibility to ensure ethical and safe design.

Data privacy and data justice

- **Data privacy is not a matter of convenience or good practice but of human rights**. As well as the rights to privacy, equal treatment and non-discrimination it affects access to other human rights such as those to healthcare, education and public services, as well as democratic rights such as free expression and association. Privacy laws should be substantial, evidence-based and capable of clear enforcement. Those affected by them should be able to understand their implications clearly.

- **Data flows and data exchange should take place without compromising data privacy**. The privacy of personal data has often been sacrificed in the processes of data exchange, between the gathering of information and its application, with intentional and unintentional risks to trust and security. Internet access and use should not be dependent on data-tracking: users should have the right to choose the extent to which their information is shared, including information derived from their online activity. Personal data should not be exported into jurisdictions which do not provide adequate guarantees.

- **Policies should reach beyond data protection to data justice in which people have choices over how personal data are used and where they can share the returns and benefits of innovation** brought by datasets derived from their data. Privacy protections should thereby contribute to a safer and more prosperous digital economy.

- **Governments and regulators should ensure that personal data are protected**, identifying the differentiated responsibilities of different stakeholders and without imposing undue burdens or responsibilities on individual users. Data governance policies should be developed with multistakeholder input to ensure that implementation challenges are understood.

- **Privacy and data protection are particularly significant for the governance of artificial intelligence and machine learning.** All stakeholders in the AI supply chain have a role to play in upholding privacy rights.

- **There is a need for independent oversight bodies equipped with appropriate resources.** Data protection offices should have a mandate to manage data registration, provide guidance, implement investigations and resolve complaints from data subjects.

Data governance

- **Issues concerning data governance should not be treated in silos or in isolation from their impacts.** The current data governance landscape is a fragmented patchwork of national, regional, and international rules involving responsibilities for national governments, private sector businesses and individuals.

- **Greater coherence is needed on a global level to achieve a balanced approach in which data work for people and the planet.** Existing legislation and regulatory frameworks at national, regional, and international levels are often insufficient and fail to keep up with the pace of change in technology and applications. They should seek to ensure high security standards by businesses and other organisations responsible for holding data.

- **Different contexts and challenges, histories, cultures, legal traditions, and regulatory structures mean that there cannot be one rigid set of rules for all.** Different individuals and organisations also interpret broadly similar approaches in different ways. However, while countries and regions must develop their own tailored approaches to data governance there should be consistency and interoperability to facilitate data flows and ensure a level playing field.

- **Transparency, participation and accountability are important aspects of good data governance.** Important considerations in governing data include (but are not limited to): data standards and classification; data sharing, exchange and interoperability; data security and data privacy; data infrastructure; data and digital identity; data justice and fairness; data traceability, transparency and explicability; data minimization and data limitation; data accuracy and quality; data bias, marginalization and discrimination; the data life cycle, specificity and retention of data use; data accountability and data ethics; data harms, data security and data protection

- **Many stakeholders have roles within this context and should exercise their power and influence to promote effective data governance**, including regulators, researchers, standards organizations, consumer organisations and end users. Policies for data governance should be developed with input from this multistakeholder community which has expertise in both legal debates around privacy and the "real world" challenges of implementing effective data privacy solutions.

- **Developing economies need to enhance their institutional capacities to govern, use and manage data in a comprehensive, objective and evidence-based manner, including through regional and global cooperation.** This requires improved understanding of the institutional capacities of government officials and stakeholders.

Cross-border data flows

- **Cross-border data flows are essential to many aspects of e-commerce and digital trade.** Efficient intra-regional trade and supply chain management relies on the smooth flow of data as well as goods, services and capital. However, all of these require complex cross-cutting considerations for regulatory convergence, harmonisation of legal frameworks, Internet governance, information and communications technology policy reform and strategic regional infrastructure implementation.

- **Current multilateral, regional and bilateral trade agreements are insufficient for current and future cross-border data flows.** These operate in a largely unregulated environment with little consistency between national legal regimes. Approaches differ and are contextual, generating barriers to trade, while many countries do not currently have adequate legislation or enforcement capacity. There is a growing need to develop and harmonise measures to manage cross-border flows that facilitate

development and economic value generation, in different contexts, while respecting national sovereignty and user privacy.

Enabling Safety, Security and Accountability

Theme

The security of the Internet is under threat in several ways. Traditional cybersecurity deals with the protection of networks, devices and data from unauthorised access or criminal use. This encompasses the ongoing problem of cyber-attacks, whether they are perpetrated by individuals or state-sanctioned, and whether the targets are civic, commercial or governmental. Factors such as the absence of broad and binding cybersecurity agreements and insufficiently secure networks contribute to the loss of opportunities to capitalise fully on the economic benefits of digital technologies, particularly for developing countries.

Issues of safety, security and accountability are multifaceted, including distinct issues concerning infrastructure, services, content and other aspects of the Internet. Our understanding of safety and security, for instance, now includes persistent challenges of online misinformation and disinformation. In recent years, these have been factors in aggravating the effects of the COVID-19 pandemic as well as posing significant risks to electoral processes around the world. This has emphasised the need for accountability and clear criteria for misleading content.

The concept of 'safety' may be further widened to include environmental safety, considering efforts to 'green' the Internet and reduce carbon emissions associated with digital consumption. The need to address the environmental impact of digitalisation is an increasingly important theme in IGF discussions.

Messages

The role of policymakers

- **Cybersecurity should be seen as a central challenge for Internet policy.** Considerations of trust and security should be integral to the development of safe, secure access, including respect for human rights, openness and transparency in policymaking, and a multistakeholder approach that serves the interests of end-users.

- **Ensuring cybersecurity and preventing cybercrime are both important areas of policy that require serious attention and the development of expertise.** They differ in purpose, however, and the approach required for each is different. An approach that is effective in one will not be effective in the other without adaptation and reformulation.

- **Cybersecurity and cybercrime issues have cross-organisational and cross-border dimensions. Tackling these requires:**

a) **whole-of-government and whole-of-society approaches** that include strong partnerships and coordinated efforts, involving parliaments, regulators and other relevant government authorities and agencies, the private sector, the technical community, academia, and civil society; and
b) **efficient and effective regional and international cooperation** that is intergovernmental, multilateral and multistakeholder.

- **Governments, the private sector and the technical community should take care to avoid adopting cybercrime laws and establishing standards that negatively affect the work of cybersecurity defenders.** They should invite all stakeholders to engage in policy development and facilitate interaction and sharing of experience and expertise between their different communities.

- **Civil society should participate in both cybercrime and cybersecurity discussions.** To do so effectively, civil society stakeholders should educate themselves on the different approaches and issues involved, and work with other stakeholders to gather the information and resources required to participate fully in making policy.

Cybersecurity

- **The international community should explore practical ways to mainstream cybersecurity capacity-building into broader digital development efforts.** Tensions between the desire to advance digital transformation and the need to enable effective cybersecurity pose challenges in enabling a safe, secure online environment and achieving the Sustainable Development Goals. While doing more to increase the resilience of digital infrastructure is necessary, it is not sufficient. Translating existing international agreements into feasible actions is long overdue.
- **Standards that enable cybersecurity are essential for an open, secure and resilient Internet that enables social progress and economic growth, and are particularly important in protecting those who are not yet connected.** Such standards have been developed, but their use needs to grow significantly to make them fully effective. The United Nations could help accelerate the global adoption of key standards by including their promotion in the Global Digital Compact, by supporting advocacy and capacity building and by encouraging initiatives to test and monitor deployment. Early awareness raising and capacity building on standards should not be forgotten as priorities in areas where many still have to get connected and the internet is growing.
- **More needs to be done to improve national policymakers' and other stakeholders' awareness of the challenges of cybersecurity and of international norms and principles.** This should include awareness and capacity-building concerning the links between sustainable development and cybersecurity, bringing diverse stakeholders together to mobilise effective, sustainable and inclusive stewardship of international cooperation for cyber-resilience. A number of international initiatives have been established to support this. Opportunities to finance cyber resilience also need to be addressed by funding agencies and other stakeholders.
- **Cybersecurity norms must make a difference to the personal experiences of Internet users past, present and future.** Listening to the experiences of individual and organisational victims of cybersecurity attacks, and those of first responders, is important in this context, particularly when developing new norms.

Cybercrime

- **Cybercrime poses an increasing threat to many Internet users.** Regulations countering cybercrime should be sensitive to the size, capacity and resources of platforms. Legal obligations should consider the diversity of the technical sector, and acknowledge the needs and circumstances of smaller businesses in adhering to their legal obligations, for instance in countering terrorist and violent extremist exploitation of their services.

- **Governments and policymakers should ensure that legal responses to criminal and terrorist use of the Internet safeguard both the rule of law and human rights**, taking freedom of expression fully into account and ensuring transparency and accountability in the implementation of measures against cybercrime.

Content and disinformation

- **Disinformation can and should be addressed through mechanisms that address the risks faced by individuals and societies while protecting freedom of expression, pluralism and democratic process.** Support for professional journalism and media plays an important part in efforts to address disinformation, including commitment to established journalistic norms.

- **Media and digital literacy skills empower citizens to take a more critical view of the content or information they encounter, helping to identify disinformation and misinformation and strengthen democratic participation.** Digital literacy education can help to increase online safety awareness, especially for more vulnerable individuals and communities. Initiatives need to be sensitive to the needs and risks associated with different demographic groups. Different approaches for young people and older generations, for example, must respond to different usage patterns.

- **Educational curricula should include digital literacy skills that help children to be safe online.** Initiatives should involve parents, teachers and guardians. Lawmakers and digital platforms should take responsibility to ensure children's safety within a framework of children's rights online consistent with international rights agreements including the UN Convention on the Rights of the Child.

- **The domain name system has limited technical capacity in this context.** Continued stakeholder dialogue should clarify when and how it may be used to remedy specific content problems, and should strengthen due-process norms.

- **Encryption plays an important role in building an open, safe and democratic Internet** and helps users to achieve safety, privacy and freedom of speech. Issues concerning law enforcement and user's ability to manage access in areas such as child protection need to be addressed.

- **Translation issues present significant barriers that can inhibit end-users' meaningful engagement with platforms' community standards and guidelines**. Key terms are sometimes poorly translated, resulting in ambiguous interpretations. Engagement with different language communities to improve the accuracy and relevance of translation, including the communication of concepts without direct

equivalents in different languages, is an important part of enabling platforms and users to understand what is expected of them.

Addressing Advanced Technologies, including Artificial Intelligence (AI)

Theme

Advanced digital technologies increasingly shape our economy and society, including artificial intelligence (AI) systems which guide our online experiences, power smart devices, and influence our own decisions and those that others take about us, as well as robotics and Internet of Things applications that are deployed in areas as diverse as manufacturing, healthcare, and agriculture. Beyond their promises, these technologies come with pitfalls. Algorithmic decision-making, for instance, can result in bias, discrimination, stereotyping and wider social inequality, while AI-based systems can pose risks to human safety and human rights. Internet of Things devices come with privacy and cybersecurity challenges. Augmented and virtual reality raises issues of public safety, data protection, and consumer protection.

Taking advantage of the opportunities offered by advanced technologies, while addressing related challenges and risks is a task that no one actor can take up on its own. Multistakeholder dialogue and cooperation – involving governments, intergovernmental organisations, technology companies, civil society, and other stakeholders – are required to ensure that these technologies are developed and deployed in a manner that is human-centred and respectful of human rights.

Messages

Governance

- **Advanced technologies, including artificial intelligence, should be designed in a way that respects the rule of law, human rights, democratic values and diversity, and includes appropriate safeguards.** They should benefit people and the planet by driving inclusive growth, sustainable development and well-being. Oversight and enforcement mechanisms should follow principles and rules, with AI actors being held accountable for any damage caused.
- **The assumption that technology necessarily enhances equality is flawed.** Those who design machine learning technologies and the data used to train AI applications are often unrepresentative of their societies. Technologies can amplify inequalities and cause harm, particularly to vulnerable and marginalised groups.
- **Societies need to adjust to the transformation that AI will bring about through changes to their cooperation framework and governance model.** Building a human-centred intelligent society requires the full cooperation of government, enterprises, social organisations and academia. Ongoing human control remains essential, to ensure that algorithms do not lead to outcomes that are

undesired or uncontrolled. Breaking down silos between engineers and policy experts is critical to achieving this.

- **Global agreement on AI norms cannot be achieved in one straightforward process.** While there are some existing norms, these are mostly soft laws rather than binding principles. The development of meaningful global standards will require effective participation from all countries, including developing and developed countries, and inputs from regional initiatives, as well as the engagement of all stakeholders.
- **Capacity-building is important in efforts to address advanced technologies.** Policies for AI literacy, skills development and language resources for minority languages are needed in order to formulate a truly global approach to advanced technologies.

Trust, security and privacy

- **Regulatory frameworks should include principles to help social media and other platforms fulfil due diligence obligations for the management of content that could damage democracy and human rights.** Frameworks should contribute to the global conversation on online content moderation to empower users, including the most vulnerable groups and users of minority languages. Emerging technologies such as affective computing, which consider how computers may recognise, interpret and simulate human emotions, require substantive ethical assessment.

- **Transparency in the operation and reporting of algorithmic systems is essential for human rights.** AI facilitates the constant observation and analysis of data to personalise and target content and advertising. The resulting personalised online experiences run the risk of disaggregating online information spaces and limiting individuals' exposure to diversity of information. Lack of information pluralism can foster manipulation and deception – furthering inequalities, undermining democratic debates, and potentially enabling digital authoritarianism, hatred and violence.

- **Stakeholders from technical and non-technical communities should share expertise and work together to develop principles, guidelines and standards** that are sufficiently flexible for application in diverse contexts and that foster trust in AI systems.

- **It is important to recognise and respect the different institutional and cultural backgrounds of diverse countries and communities**, as well as promoting inclusivity and enabling international cooperation in AI.

Rights and content moderation

- **It is essential that policies for content governance by online platforms, and their enforcement, are in line with international human rights standards.** Artificial intelligence and machine-learning technologies are already being used to decide whether content should be posted or removed, what content is prioritised and to whom it is disseminated. These tools play a significant role in shaping political and public discourse in ways that affect both individual and collective human rights, including

social, economic and cultural rights and rights to global peace and security. They are often deployed with little or no transparency, accountability, or public oversight. This should be rectified.

- **The same technologies that can be used to promote human rights can also be used for surveillance, to promote violent agendas and in other ways that infringe those rights.** Unintended consequences of automated content management can be particularly detrimental in times of conflict or crisis when they may silence critical voices at a time when they are most crucial.

- **Technical standards play an important role in enabling the development and enhancing the value of digital technologies and related infrastructures, services, protocols, applications, and devices. They may also have powerful impacts on human rights.** Yet the technical standard-setting processes within standards development organisations do not take human rights concerns fully into consideration. These processes are often opaque, complex, and resource-heavy for civil society and other stakeholders to access and follow systematically. This should be addressed.

منتدى حوكمة الإنترنت 2022

أديس أبابا رسائل منتدى حوكمة الإنترنت

تعد هذه الوثيقة ملخص للمنتدى السنوي لحوكمة الإنترنت الاجتماع والذي استضافته العاصمة الأثيوبية أديس أبابا في الفترة من 28 نوفمبر إلى 2 ديسمبر 2022.

الآراء ووجهات النظر المعبر عنها هنا لا تعبر بالضرورة عن آراء ووجهات نظر أمانة الأمم المتحدة. وقد لا تتوافق التسميات والمصطلحات المستخدمة مع ممارسة الأمم المتحدة ولا تنطوي على التعبير عن أي رأي كان من جانب المنظمة.

ركزت المناقشات في منتدى حوكمة الإنترنت 2022 على خمسة مواضيع رئيسية تم تحديدها للمحتوى الرقمي العالمي (GDC) الذي تم اقتراحه في تقرير الأمين العام للأمم المتحدة لعام 2021 في الذكرى 75 للأمم المتحدة بعنوان جدول *أعمالنا المشترك*، وستنظر فيه الجمعية العامة للأمم المتحدة في عام 2023. وسيشكل ذلك جزءا من القمة المقرر لها الانعقاد في عام 2024.

المواضيع التي نظر فيها منتدى حوكمة الإنترنت (IGF) هي:

- ربط جميع الناس وحماية حقوق الإنسان
- تجنب تجزئة الإنترنت
- إدارة البيانات وحماية الخصوصية
- تمكين السلامة والأمن والمساءلة
- معالجة التقنيات المتقدمة بما في ذلك الذكاء الاصطناعي (AI)

أعرب مجتمع أصحاب المصلحة المتعددين في منتدى حوكمة الإنترنت عن دعمه لاقتراح الأمين العام بشأن الاتفاق الرقمي العالمي. وتمثل الرسائل الواردة في هذه الوثيقة مساهمات من منتدى حوكمة الإنترنت نحو تطوير ذلك الاتفاق. ان التحالفات الديناميكية لمنتدى حوكمة الإنترنت تعالج بالفعل تلك المحددات كما أعربت عن التحديات والفرص ذات الصلة بالمواضيع المقترحة للاتفاق وعن عزمها على المساهمة مع الأمم المتحدة في المراحل التحضيرية والتنفيذية للاتفاق الرقمي العالمي.

ربط جميع الناس وحماية حقوق الإنسان

الموضوع

يتمثل المبدأ الأول للاتفاق الرقمي العالمي (GDC) الذي اقترحه الأمين العام للأمم المتحدة في "اربط جميع الناس على شبكة الإنترنت، بما في ذلك جميع المدارس ". هذا يعترف بأن الاتصال بالإنترنت والوصول إليها قد أصبح شرطا من الشروط أساسية لضمان سبل العيش والسلامة والتعليم للناس في جميع أنحاء العالم - وأن الإنترنت في المدارس يوفر نقاط وصول أساسية لذلك، كما يجعل الموارد المعلوماتية متاحة لجميع الطلاب، ويعمل على محو الأمية الرقمية من المراحل الأولى من الحياة. ومع ذلك، لا يزال هناك 2.7 مليار اليوم غير متصلين بالإنترنت، من ضمنهم أولئك الموجودين في البلدان الاقل نموا والمجتمعات الريفية الأكثر حرمانا.

ان معنى الوصول والاستفادة من الانترنت يتجاوز مجرد الاتصال ولا ينفصل عن حماية حقوق الإنسان عبر الإنترنت. يجب أن يساهم الوصول للإنترنت في رفاه المجتمعات وتدخل حقوق الإنسان في صميم ذلك. وهذا يشمل، من بين أمور أخرى كثيرة، قدرة المستخدمين على التعبير عن أنفسهم بحرية، ممارسة المشاركة الديمقراطية والسياسية للأفراد من جميع الخلفيات بدون قيد لتجربة الإنترنت دون خوف من المضايقة أو التمييز، وأن يتمتع الأطفال بنفس الحقوق والحماية عبر الإنترنت كما يفعلون في وضع عدم الاتصال بالشبكة. ان الإنترنت هو عامل تمكين للحقوق ويجب أن يكون سلسا في دمج حقوق الإنسان الراسخة، حيث اصحنا نزيد من اعتمادنا الرقمي في الاعمال الروتينية، بحيث اصبحت الحدود الفاصلة لدينا بين الحياة "عبر اتصالنا بالإنترنت" و " عدم اتصالنا بالإنترنت " أقل أهمية.

الرسائل

الفجوات الرقمية

- **لا تزال الفجوات الرقمية بين مختلف البلدان والمناطق عوامل قوية تؤثر على التنمية الوطنية والدولية،** بما في ذلك التقدم المحرز نحو تحقيق التنمية المستدامة الأهداف (SDGs). ومما يثير القلق بوجه خاص البلدان الأقل نموا والدول الجزرية الصغيرة النامية (SIDS). ان الفجوات الرقمية هي أكثر بكثير من مجرد فجوات في الاتصال بالإنترنت. ان الوصول الهادف يتضمن مشكلات تتعدى إمكانية الوصول للإنترنت ويضمن ذلك القدرة على تحمل التكاليف، والمحتوى، والخدمات، ومحو الأمية الرقمية وغيرها من القدرات. ان القدرة على تحمل التكاليف الاتصال بالإنترنت هي مشكلة خاصة لكثير من الناس، وخاصة في الجنوب العالمي.

- أظهرت جائحة COVID-19 دور الإنترنت في تمكين الفرد وتوفير المرونة الاقتصاد، ولكنها اوضحت كذلك حجم أولئك المحرومين من الاتصال بالإنترنت أو الوصول الهادف، مما قد يؤدي إلى تفاقم أوجه عدم المساواة. سوف يستغرق الأمر بعض الوقت لفهم التأثير الكامل والآثار المترتبة على التدخلات المتعلقة بكوفيد فيما يتعلق بالوصول والاستخدام وحقوق الإنسان.

- **تعاني بعض المجموعات داخل جميع المجتمعات من فجوات رقمية أعمق أو لديها وصول أقل جدوى من غيرها.** النساء في العديد من المجتمعات أقل ارتباطا بالإنترنت من الرجال وأقل استخداما لها. ان الحرمان الرقمي أكبر بين المجتمعات الضعيفة والمهمشة، وكثير من الناس يعانون من الحرمان من خلال مجموعة من العوامل المتعددة المتعلقة بالعمر، الجنس والعرق واللغة والطبقة الاجتماعية وعوامل أخرى. يمكن أن تساعد المبادرات المستهدفة في البنية التحتية والأجهزة والخدمات في تحسين معدلات الوصول للفئات الاجتماعية الأقل اتصالا بالإنترنت، ولكنها تحتاج إلى أن تكون مصحوبة بتدابير لمعالجة أوجه القصور الأخرى في الوصول المجدي وينبغي أن تكون مرتبطة بتدابير أخرى لمعالجة الحرمان والتمييز.

- **تعد البنية التحتية الرقمية المرنة والآمنة أمرا بالغ الأهمية للإدراج الرقمي. ينبغي على الحكومات حماية وتعزيز البنية التحتية المطلوبة، بما في ذلك الشبكة والطاقة خارج الشبكة وكذلك شبكات الاتصالات.** في أجزاء من أفريقيا وقارات أخرى، هنالك مسافات كبيرة من المناطق الريفية والمجتمعات النائية، بما في ذلك تلك الدول الجزرية الصغيرة، مما يجعل توصيلية الميل الأخير غير جذابة تجاريا للقطاع الخاص. ان الاتصال والسرعة والموثوقية هي جوانب مهمة من توفير البنية التحتية. وسيستغرق الأمر وقتا واستثمارا لتحسين قدرة البنية التحتية ومعالجة الاختلالات الإقليمية، لا سيما في المناطق الريفية.

- **التعاون بين مجموعات أصحاب المصلحة مهم لضمان وتمكين الوصول للإنترنت. وينبغي على الحكومات والشركاء من أصحاب المصلحة المتعددين أن يدعموا إنشاء وعمل الوكالات والأطر التنظيمية الفعالة ، والتصدي للتحديات غير الجذابة تجاريا وتشجيع المناهج المبتكرة للتوصيلية** بما في ذلك الشبكات المجتمعية ، التوزيع المناسب للطيف والنفاذ الذي توفره الأقمار الصناعية ذات المدار الأرضي المنخفض وتوفير المحتوى المحلي، بما في ذلك المحتوى باللغات المحلية.

الفجوة الرقمية بين الجنسين وحقوق المرأة

- **من المرجح أن يكون الرجال متصلين بالإنترنت أو لديهم اتصال عن طريق الأجهزة المحمولة أكثر من النساء.** ان الفجوة الرقيمة بين الرجال والنساء واسعة وبشكل خاص في البلدان الأقل نموا. ان تحقيق الهدف 9ج من أهداف التنمية المستدامة، والتي تسعى الى تحقيق الوصول الشامل والميسور التكلفة للإنترنت لا يمكن تلبيته ما لم يتم سد هذه الفجوة.

- **يشكل التهديد بالعنف والتحرش عائقا أمام مشاركة المرأة على الإنترنت.** يعد العنف القائم عبر الإنترنت على النوع الاجتماعي هو عامل مهم يدفع ويعزز من عدم المساواة بين الجنسين في الوصول والاستخدام للإنترنت، مما يؤدي إلى مغادرة بعض النساء للمساحات عبر الإنترنت. وينبغي الاعتراف بدور الخدمات وينبغي الاعتراف بدور الخدمات والمنصات التكنولوجية في نشر العنف القائم على نوع الجنس ومعالجته. والمنصات في نشر العنف القائم على نوع الجنس ومعالجته. يجب دعم النساء بإرشادات لمقاومة العنف القائم على النوع الاجتماعي عبر الإنترنت ومعالجته، من خلال خطوط المساعدة التي يقودها المجتمع. الموارد وإرشادات المجتمع وإعداد التقارير على المنصات باللغات المحلية.

- **يجب دمج مفاهيم المساواة بين الجنسين وحقوق المرأة وحمايتها في الاتفاق الرقمي العالمي (GDC)** ، كما اقترحته هيئة الأمم المتحدة للمرأة.

حقوق الإنسان والتنمية الرقمية

- **يجب أن يحترم الوصول الشامل للإنترنت حقوق الإنسان، لضمان إمكانية الوصول للإنترنت للجميع والامان فيها.** وتشمل هذه حرية التعبير وتكوين الجمعيات، والحق في الخصوصية وغيرها من الحقوق المدنية والحقوق السياسية والاقتصادية والاجتماعية والثقافية المنصوص عليها في اتفاقيات الحقوق الدولية. وينبغي أن تحترم هياكل إدارة الإنترنت ومصممي التكنولوجيات الرقمية هذه الحقوق ويجب على منظمات وضع المعايير النظر في دعوة الخبراء في مجال حقوق الإنسان على الإنترنت، من جميع مجتمعات أصحاب المصلحة، للمشاركة في عملهم.

- **الشفافية والمساءلة والعناية الواجبة فيما يتعلق بحقوق الإنسان هي مسؤوليات جميع مجموعات أصحاب المصلحة، بما في ذلك المنظمات الحكومية الدولية والمنظمات الدولية، والحكومات، القطاع الخاص والمجتمع التقني والمجتمع المدني.** سيتطلب ذلك مواءمة ممارسات الأعمال مع الحقوق الرقمية والتعاون بين أصحاب المصلحة لمعالجة قضايا مثل المعلومات المضللة والتمييز وخطاب الكراهية، خاصة في أوقات الاضطرابات السياسية والانتخابات وانتقال السلطة.

- **يوفر الوصول إلى الإنترنت فرصة حاسمة للوصول إلى المعلومات والتعبير عن الرأي.** يجب على الحكومات تجنب اللجوء إلى إغلاق الإنترنت بسبب تأثيره السلبي على حقوق الإنسان والرفاه الاقتصادي. يجب على وسائل التواصل الاجتماعي وشركات التكنولوجيا دعم المواطنين في جهود الدعوة الخاصة بهم فيما يتعلق بعدم اغلاق الانترنت.

- **من المهم تحسين رصد الحقوق الرقمية وتنفيذها.** وهناك عدد الاقتراحات التي قدمت لوضع ترتيبات مراقبة دولية داخل الأمم المتحدة.، مع مشاركة أصحاب المصلحة المتعددين. ويمكن أن تكمل هذه التدابير القائمة وتبني عليها الآليات، بما في ذلك الآليات المعنية بالتنمية والحقوق الرقمية وتلك المتعلقة بغيرها من مجالات مثل تغير المناخ.

- **توفر شبكة الإنترنت فرصا لتعزيز الحق في التعليم،** كجزء من سياسات أوسع نطاقا لتحسين التعليم. ان جودة التعليم في الجنوب العالمي، ولا سيما خلال الوباء، عانى بسبب نقص الاتصال بالإنترنت. في حين أن تكنولوجيا المعلومات والاتصالات يمكن أن تمكن من الوصول المجدي إلى الطلاب، أدت الاختلافات في معدلات التبني العالمية والمحلية لذلك إلى تفاقم عدم المساواة قبل الجائحة. ويمكن استخدام الخبرة خلال فترة الوباء لتحسين استخدام الموارد الرقمية في المستقبل.

- **ينبغي بذل الجهود لمساعدة الشركات الصغيرة والمحلية على الاستفادة القصوى من الإنترنت.** زاد استخدام الأدوات الرقمية من قبل الشركات الصغيرة والمتوسطة بشكل كبير منذ عام 2020، لكن الشركات الصغيرة لا تزال تواجه تحديات كبيرة في قدرتها على رقمنه أعمالها.

- **تمثل التغيرات في سوق العمل المبنية على المنصات الإلكترونية فرصا وتحديات لخلق فرص العمل وجودة الوظائف،** خاصة بالنسبة للنساء اللواتي يلعبن دورا أكبر من الرجال في القطاع غير الرسمي في معظم البلدان. لا يزال نقص التدريب يشكل عائقا أمام العديد من الأشخاص في تعظيم إمكاناتهم الوظيفية.

- **يجب تحسين قدرات الكفاءات الرقمية وتكييفها في التدريس والتعلم والتدريب. وهناك حاجة إلى منهجيات للتكيف مع النماذج الجديدة** في كل من التعليم والعمالة. من المهم تحديد وسد الفجوة بين احتياجات الصناعة والتعليم العالي.

تجنب تجزئة الإنترنت

الموضوع

يعد الحفاظ على إنترنت عالمي ومفتوح وقابل للتشغيل البيني قيمة أساسية لمنتدى إدارة الإنترنت. هذا يعني أن يتواصل نشر المعايير والبروتوكولات التقنية المشتركة لتحقيق شبكة واحدة تتكون من الشبكات المترابطة عبر البلدان والمناطق، وأن تكون معايير المحتوى والخدمات متسقة مع حقوق الإنسان ومع سيادة القانون وقد ترددت الدعوة إلى ذلك - تطبيق إطار عمل على الإنترنت يعطي الأولوية لحقوق وحريات المستخدمين ومن خلال البنية التحتية، والاتساق الشامل في الخطط في الاتفاق الرقمي العالم

إن خطر التجزؤ هو حقيقي ويتصاعد. بينما التجزئة الفنية والتجارية – حيث يتأثر أداء الإنترنت بمزيج من الظروف الطوعية وغير الطوعية والممارسات التجارية - يحتاج إلى معالجة، كما أن التجزئة بسبب سياسة الحكومة تؤثر على الطابع المفتوح والقابل للتشغيل المتبادل للإنترنت هي أيضا مصدر قلق.

الرسائل

فهم القضايا

- **يوفر الاتفاق الرقمي العالمي فرصة لإعادة التأكيد على قيمة الترابط المفتوح للإنترنت من أجل تحقيق ميثاق الأمم المتحدة وتحقيق أهداف التنمية المستدامة وممارسة حقوق الإنسان.** هناك اتفاق واسع النطاق داخل مجتمع الإنترنت حول قيمة الإنترنت العالمية غير المجزأة كمنصة للنشاط البشري.

- **القضايا التي أثيرت في المناقشات حول تجزئة الإنترنت متعددة الطبقات ومختلفة يعطى أصحاب المصلحة مجموعة متنوعة من المعاني والتفسيرات للمصطلح..** البعض أكثر قلقا للجوانب التقنية والبنية التحتية للإنترنت، بينما يركز البعض الآخر على قضايا السياسة العامة بما في ذلك الوصول والحقوق والتأثيرات على تجربة المستخدم. يتم حاليا استكشاف تجزئة الإنترنت في إطار مشروع أعدته شبكة سياسة منتدى حوكمة الانترنت. إن احترام وتفهم تصورات الناس المختلفة وتجربتهم للتجزؤ أمر ضروري إذا أردنا التوصل إلى استجابات فعالة ومنسقة

- **يمكن لمجموعة واسعة من العوامل السياسية والاقتصادية والتقنية أن تؤدي إلى التفتت.** ومع ذلك، لا ينبغي الخلط بين التنوع واللامركزية والتشرذم. هذه هي الجوانب الإيجابية بشكل أساسي لبنية الإنترنت وعملياتها.

معالجة مخاطر التجزؤ

- **تعد آليات الحوكمة الفعالة لأصحاب المصلحة المتعددين ضرورية لإدارة شبكة إنترنت عالمية غير مجزأة.** وثمة حاجة إلى تعزيز الثقة في هذه الآليات، وضمان أن تكون قوية ومستدامة، وتعزيز الاتساق عبر هياكل الحوكمة أثناء تطورها إلى مواجهة التحديات الجديدة.

- ثمة حاجة إلى توخي اليقظة فيما يتعلق بمخاطر الجزءات الجديدة أو الناشئة. وسيكون التعاون والتنسيق العالميين أساسيين في تحديد علامات الإنذار المبكر، ورسم خرائط لأثر السياسات وغيرها من التطورات، والاستعداد لمعالجة الآثار المترتبة على هذه التغييرات. إن نهج أصحاب المصلحة المتعددين هو الأنسب لتقييم ورصد العواقب المحتملة غير المقصودة للتدابير التي تؤثر على الإنترنت واقتراح بدائل فعالة تتجنب أو تخفف من مخاطر التجزئة. وتعد شبكة سياسة منتدى حوكمة الإنترنت حول تجزئة الإنترنت مثالا إيجابيا على هذا النهج.

- **يعد انفتاح الإنترنت مفيدا في تعزيز تمتع مستخدمي الإنترنت بحقوق الإنسان، وتعزيز المنافسة وتكافؤ الفرص، وتحمى طبيعة الترابط الشبكي peer to peer للإنترنت.** المناقشات حول حيادية الإنترنت وإدارة حركة المرور غير التمييزية ليست سوى جزء من مناقشات أوسع في هذا السياق. حيادية الإنترنت ضرورية ولكنها ليست كافية لضمان انفتاح الإنترنت. البنية التحتية وقابلية التشغيل البيني للبيانات، وحيادية النظام الأساسي والمنصات، ضرورية أيضا.

- **في حين أن المناهج القانونية والتنظيمية والسياسية ستختلف في جميع أنحاء العالم، الا ان التنسيق النشط عبر الحدود الدولية أمر حيوي لضمان عدم تأثير تهديد نهج التجزئة من الوصول العالمي وقابلية التشغيل البيني للإنترنت.** يتطلب الحفاظ على سلامة الشبكة العالمية التعاون التنظيمي الدولي والتوافق على المبادئ الأساسية. ويمكن أن يؤدي السعي وراء بعض أشكال الحوكمة الرقمية على المستوى الوطني إلى زيادة خطر التجزئة على المستوى التقني للإنترنت. ومع ذلك، يجب أن تراعي الأطر التنظيمية أيضا المتطلبات المختلفة في سياقات مختلفة ومواكبة التغيير السريع في التكنولوجيا والخدمات.

- **ثمة حاجة إلى مزيد من تبادل المعارف والمعلومات بين أصحاب المصلحة،** ومواصلة مناقشة الدبلوماسية السيبرانية كظاهرة متطورة، والنظر في نطاق التدخلات. وينبغي لهيئات وضع المعايير أن تواصل تحسين التوعية والمشاركة مع أصحاب المصلحة وتحسين التفاهم بين الأوساط المعنية بالسياسات والأوساط التقنية. وينبغي أن تناقش هيئات المقاييس كذلك القرارات التقنية التي تترتب عليها آثار سياسية من خلال المشاركة المباشرة لجميع أصحاب المصلحة المتأثرين.

إدارة البيانات وحماية الخصوصية

الموضوع

البيانات هي المورد الرئيسي للعصر الرقمي المعولم. تقود حركة البيانات الاقتصادات، في حين أن تحليل البيانات، بما في ذلك تحليلات البيانات الضخمة، كان الأساس لابتكارات ملحوظة عبر التخصصات، من التمويل، إلى الصحة الى إنفاذ القانون.

لكن الاستخدام الواسع النطاق والتدفق الروتيني عبر الحدود وقابلية استبدال البيانات لا تزال مواضيع حساسة ولم يتم حلها. وباعتبارها أصلا تجاريا عابرا للحدود الوطنية، تعمل تدفقات البيانات في بيئة لا يوجد فيها اتساق يذكر بين النظم القانونية الوطنية وحيث توجد تحديات كبيرة في الإنفاذ. لتسخير الكم الكبير للبيانات، اقتصاديا ولأغراض البحث، يجب إعادة إطلاق المناقشات حول الحوكمة والنزاهة وحماية خصوصية الناس. غالبا ما يتم التضحية بخصوصية البيانات الشخصية على مدار عمليات تبادل البيانات، من نقطة الجمع إلى التطبيق والبرمجيات ومرحلة التخزين، مع عواقب وخيمة على الثقة والأمان.

لتسخير الكم الكبير للبيانات، اقتصاديا ولأغراض البحث، يجب إعادة إطلاق المناقشات حول الحوكمة والنزاهة وحماية خصوصية الناس.

الرسائل

مركزية البيانات

- **أصبحت البيانات موردا مهما في عصر متزايد رقميا.** تعد تدفقات البيانات أمرا بالغ الأهمية للتعاون الدولي في العديد من المجالات بما في ذلك البحث العلمي وإنفاذ القانون والأمن الوطني و العالمي. البيانات وأمن البيانات وحماية البيانات هي عوامل تمكين حاسمة للتنمية المستدامة. يمكن أن يساعد الاستخدام الفعال للبيانات وتبادلها على نطاق عالمي في التغلب على التحديات المشتركة والتهديدات التي تشكلها الأزمات المتتالية مثل الأوبئة وتغير المناخ.

- **يمكن للبيانات أن تولد ربحا وقيمة اجتماعية كبيرة.** ومع ذلك، تم توزيع فوائد الاقتصاد القائم على البيانات حتى الآن بشكل غير متساو. كثير من الناس قلقون من أنهم قد يصبحون في المقام الأول مقدمي البيانات بدلا من مستفيدين.

- **العلاقة بين أولئك الذين يولدون البيانات وأولئك الذين يستخدمون البيانات مهمة.** يمثل فقر البيانات مشكلة كبيرة، لاسيما في المجتمعات المحلية وبين الشرائح الضعيفة من السكان. ويؤدي افتقار خصوصية البيانات وعدم كفاية حمايتها إلى تقويض الثقة في إدارة البيانات. ومن المهم بناء الإلمام بالبيانات والقدرات المتعلقة بالبيانات عبر مستويات الحكومة وفي المناهج التعليمية ولعامة الناس.

- **تعد إدارة البيانات والحوكمة من القضايا المعقدة في كل من الحوكمة الوطنية والدولية.** تظهر التطورات في البيانات - بما في ذلك تحليلات البيانات الضخمة، والابتكارات في الذكاء الاصطناعي والتعلم الآلي، والابتكارات عبر أبعاد السياسة العامة وأهداف التنمية المستدامة - الحاجة إلى النظر المناسب في الآثار السياسية والاقتصادية والاجتماعية والتدخلات السياسية الدقيقة. تحتاج المؤسسات الحكومية والتنظيمية إلى البنية التحتية والقدرات اللازمة لتنفيذ أطر عمل وطنية فعالة ومتكاملة لإدارة البيانات. يتحمل مطورو التطبيقات مسؤولية ضمان التصميم الأخلاقي والآمن.

خصوصية البيانات وعدالة البيانات

- **خصوصية البيانات ليست مسألة ملاءمة أو ممارسة جيدة ولكنها تدخل ضمن حقوق الإنسان.** فبالإضافة إلى الحق في الخصوصية والمساواة في المعاملة وعدم التمييز، فإنه يؤثر على الوصول إلى حقوق الإنسان الأخرى مثل تلك المتعلقة بالرعاية الصحية والتعليم والخدمات العامة، فضلا عن الحقوق الديمقراطية مثل حرية التعبير وتكوين الجمعيات. يجب أن تكون قوانين الخصوصية جوهرية وقائمة على الأدلة وقادرة على الإنفاذ الواضح. ويجب أن يكون المتضررون منها قادرين على فهم آثارها بوضوح.

- **يجب أن يتم تدفق البيانات وتبادل البيانات دون المساس بخصوصيتها.** غالبا ما يتم التضحية بخصوصية البيانات الشخصية في عمليات تبادل البيانات، خلال عمليتي الجمع والتطبيق، مع وجود مخاطر سواء ان كانت متعمدة او غير متعمدة على الثقة والأمن. يجب ألا يعتمد الوصول إلى الإنترنت واستخدامها على تتبع البيانات. يجب أن يكون للمستخدمين الحق في اختيار مدى مشاركة معلوماتهم، بما في ذلك المعلومات المستمدة من النشاط عبر الإنترنت. ولا ينبغي تصدير البيانات الشخصية إلى الولايات القضائية التي لا تقدم ضمانات كافية على ذلك.

- **على السياسات ان تصل الى ما هو ابعد من مجرد حماية البيانات إلى عدالة البيانات التي يكون فيها للناس خيارات بشأن كيفية استخدام البيانات الشخصية وحيث يمكنهم مشاركة عوائد وفوائد الابتكار** الذي تجلبه مجموعات البيانات المستمدة من بياناتها. وبالتالي يجب أن تساهم حماية الخصوصية في اقتصاد رقمي أكثر أمانا وازدهارا.

- **يجب على الحكومات والهيئات التنظيمية ضمان حماية البيانات الشخصية،** وتحديد المسؤوليات المتباينة لمختلف أصحاب المصلحة ودون فرض أعباء لا داعي لها أو المسؤوليات على المستخدمين الفرديين. يجب تطوير سياسات إدارة البيانات باستخدام مدخلات أصحاب المصلحة المتعددين لضمان فهم تحديات التنفيذ.

- **الخصوصية وحماية البيانات ذات أهمية خاصة لحوكمة الذكاء الاصطناعي والتعلم الآلي.** جميع أصحاب المصلحة في سلسلة التوريد الذكاء الاصطناعي لهم دور يلعبونه في الحفاظ على حقوق الخصوصية

- **ثمة حاجة إلى هيئات رقابة مستقلة مجهزة بالموارد الملائمة.** يجب أن يكون لمكاتب حماية البيانات ولاية لإدارة تسجيل البيانات وتقديم التوجيه والتنفيذ للتحقيقات وحل الشكاوى من أصحاب البيانات.

حوكمة البيانات

- **لا ينبغي التعامل مع القضايا المتعلقة بإدارة البيانات في عزلة أو بمعزل عن آثارها.** المشهد الحالي لحوكمة البيانات هو خليط مجزأ من القواعد الوطنية والإقليمية والدولية التي تنطوي على مسؤوليات للحكومات الوطنية وشركات القطاع الخاص والافراد.

- **هناك حاجة إلى مزيد من الاتساق على المستوى العالمي لتحقيق نهج متوازن تعمل فيه البيانات لصالح الناس وكوكب الارض.** التشريعات والأطر التنظيمية القائمة على الصعيد الوطني والإقليمي غالبا ما تكون المستويات الدولية فيها غير كافية وتفشل في مواكبة وتيرة التغيير في التكنولوجيا والتطبيقات. يجب أن تسعى إلى ضمان معايير أمنية عالية من قبل الشركات وغيرها من المنظمات المسؤولة عن الاحتفاظ بالبيانات.

- **إن السياقات والتحديات المختلفة من تاريخيه وثقافية والتقاليد القانونية والهياكل التنظيمية تعني أنه لا يمكن أن تكون هناك مجموعة واحدة صارمة من القواعد للجميع.** يفسر الأفراد والمنظمات المختلفة أيضا المناهج المتشابهة أيضا بطرق مختلفة. وعلى أي حال ، ففي حين يجب على البلدان والمناطق تطوير مناهجها المصممة خصيصا لها لإدارة البيانات ، يجب أن يكون هناك اتساق و قابلية التشغيل البيني لتسهيل تدفق البيانات وضمان تكافؤ الفرص.

- **الشفافية والمشاركة والمساءلة هي جوانب مهمة من جوانب الإدارة الجيدة للبيانات.** تشمل الاعتبارات المهمة في إدارة البيانات (على سبيل المثال لا الحصر): معايير البيانات وتصنيفها. تقسيم البيانات وتبادلها وقابلية التشغيل البيني؛ أمن البيانات وخصوصية البيانات؛ بيانات البنية التحتية; البيانات والهوية الرقمية؛ عدالة البيانات وإنصافها ؛ إمكانية تتبع البيانات والشفافية و قابلية التفسير؛ تقليل البيانات والحد منها ؛ دقة البيانات وجودتها ؛ تحيز البيانات ، التهميش والتمييز؛ دورة حياة البيانات وخصوصيتها والاحتفاظ باستخدام البيانات ؛ بيانات المساءلة وأخلاقيات البيانات؛ أضرار البيانات وأمن البيانات وحماية البيانات

- **العديد من أصحاب المصلحة لديهم أدوار في هذا السياق ويجب أن يمارسوا سلطتهم ونفوذهم لتعزيز الحوكمة الفعالة للبيانات،** بما في ذلك المنظمين والباحثين ومنظمات المعايير، منظمات المستهلكين والمستخدمين النهائيين. يجب تطوير سياسات إدارة البيانات مع المدخلات من مجتمع أصحاب المصلحة المتعددين ممن يتمتعون بخبرة في كل من المناقشات القانونية حول الخصوصية وتحديات "العالم الحقيقي" لتنفيذ حلول فعالة لخصوصية البيانات.

- **تحتاج الاقتصادات النامية إلى تعزيز قدراتها المؤسسية على تنظيم البيانات واستخدامها وإدارتها بطريقة شاملة وموضوعية وقائمة على الأدلة**، بما في ذلك من خلال المناطق الإقليمية والاقتصادية. التعاون العالمي. وهذا يتطلب فهما أفضل للقدرات المؤسسية للمسؤولين الحكوميون وأصحاب المصلحة.

تدفقات البيانات عبر الحدود

- **تعد تدفقات البيانات عبر الحدود ضرورية للعديد من جوانب التجارة الإلكترونية والتجارة الرقمية.** تعتمد التجارة البينية الفعالة وإدارة سلسلة التوريد على التدفق السلس للبيانات وكذلك السلع، الخدمات ورأس المال. ومع ذلك، فإن كل هذه الأمور تتطلب اعتبارات شاملة معقدة للتقارب التنظيمي، ومواءمة الأطر القانونية، وإدارة الإنترنت، والمعلومات وإصلاح سياسات تكنولوجيا الاتصالات وتنفيذ البنية التحتية الإقليمية الاستراتيجية

- **الاتفاقات التجارية الحالية المتعددة الأطراف والإقليمية والثنائية غير كافية لتدفقات البيانات الحالية والمستقبلية عبر الحدود.** وتعمل هذه الهيئات في بيئة غير منظمة إلى حد كبير مع قدر ضئيل من الاتساق بين النظم القانونية الوطنية. وتختلف النهج وتكون سياقية مما يولد حواجز أمام التجارة، في حين أن العديد من البلدان ليس لديها حاليا تشريعات كافية أو ذات قدرة على الإنفاذ. هناك حاجة متزايدة إلى وضع وتنسيق تدابير لإدارة التدفقات عبر الحدود التي تيسر التنمية وتوليد القيمة الاقتصادية، في سياقات مختلفة، مع احترام السيادة الوطنية وخصوصية المستخدم.

تمكين السلامة والأمن والمساءلة

الموضوع

يتعرض أمن الإنترنت للتهديد بعدة طرق. يتعامل الأمن السيبراني التقليدي مع حماية الشبكات والأجهزة والبيانات من الوصول غير المصرح به أو الاستخدام الإجرامي. وهذا يشمل المشكلة المستمرة للهجمات السيبرانية، سواء ارتكبها أفراد أو أقرتها الدولة، وإذا ما كانت الأهداف مدنية أو تجارية أو حكومية. تساهم عوامل مثل عدم وجود اتفاقيات واسعة وملزمة للأمن السيبراني والشبكات غير الآمنة بشكل كاف في فقدان فرص الاستفادة الكاملة من الفوائد الاقتصادية للتكنولوجيات الرقمية، لا سيما من للبلدان النامية.

وقضايا السلامة والأمن والمساءلة متعددة الأوجه، بما في ذلك قضايا متميزة تتعلق بالبنية التحتية والخدمات والمحتوى والجوانب الأخرى للإنترنت. فهمنا للسلامة والأمن، على سبيل المثال، يشمل الآن التحديات المستمرة المتمثلة في المعلومات المضللة والمعلومات المضللة عبر الإنترنت. وفي السنوات الأخيرة، ساهمت هذه عوامل في تفاقم آثار جائحة COVID-19 وهي

تشكل مخاطر كبيرة على العمليات الانتخابية في جميع أنحاء العالم. كل ذلك أكد على الحاجة إلى المساءلة والمعايير الواضحة لماهية المحتوى المضلل.

كذلك يمكن توسيع مفهوم "السلامة" ليشمل السلامة البيئية، مع الأخذ في الاعتبار الجهود المبذولة "لتخضير" الإنترنت وتقليل انبعاثات الكربون المرتبطة بالاستهلاك الرقمي. تعد الحاجة إلى معالجة التأثير البيئي للرقمنة موضوعا متزايد الأهمية في مناقشات منتدى حوكمة الإنترنت.

الرسائل

دور واضعي السياسات

- **يجب النظر إلى الأمن السيبراني على أنه تحد رئيسي لسياسة الإنترنت.** وينبغي أن تكون اعتبارات الثقة والأمن جزءا لا يتجزأ من تطوير الوصول الآمن والمأمون، بما في ذلك احترام حقوق الإنسان، والانفتاح والشفافية في صنع السياسات، واتباع نهج لأصحاب المصلحة المتعددين يخدم مصالح المستخدمين النهائيين.

- **إن ضمان الأمن السيبراني ومنع الجريمة السيبرانية هما مجالان مهمان من مجالات السياسة التي تتطلب اهتماما جادا وتنمية الخبرة.** ومع ذلك، فهي تختلف في الغرض والنهج المطلوب لكل منها. فالنهج الفعال في أحدهما لن يكون فعالا في الآخر دون تكييفه وإعادة صياغته.

- **لقضايا الأمن السيبراني والجريمة السيبرانية أبعاد عابرة للمنظمة وعبر الحدود**. تتطلب معالجة هذه الأمور ما يلي:

1. **نهج يشمل الحكومة بأكملها والمجتمع بأسره** يؤدى الى شراكات قوية وجهودا منسقة، تشمل البرلمانات والهيئات التنظيمية والسلطات الحكومية الأخرى ذات الصلة والوكالات، والقطاع الخاص، والمجتمع التقني، والأوساط الأكاديمية، والمجتمع المدني؛ و
2. **التعاون الإقليمي والدولي الكفء والفعال الذي يتسم بالكفاءة والفعالية**، متعددة الأطراف ومتعددة أصحاب المصلحة.

- **وينبغي للحكومات والقطاع الخاص والأوساط التقنية أن تحرص على تجنب اعتماد قوانين الجرائم الإلكترونية ووضع المعايير التي تؤثر سلبا على عمل المدافعين عن الأمن السيبراني**. وينبغي لها أن تدعو جميع أصحاب المصلحة إلى المشاركة في وضع السياسات وتيسيرها بالإضافة للتفاعل وتبادل التجارب والخبرات بين مجتمعاتهم المختلفة.

- **وينبغي للمجتمع المدني أن يشارك في المناقشات المتعلقة بالجريمة السيبرانية والأمن السيبراني على حد سواء**. وللقيام بذلك بفعالية، ينبغي لأصحاب المصلحة في المجتمع المدني تثقيف أنفسهم بشأن مختلف النهج والقضايا المعنية، والعمل مع أصحاب المصلحة الآخرين لجمع المعلومات والموارد اللازمة للمشاركة الكاملة في صنع السياسات.

الأمن السيبراني

- **ينبغي للمجتمع الدولي أن يستكشف سبلا عملية لتعميم بناء القدرات في مجال الأمن السيبراني على نطاق أوسع وبزل جهود في مجال التنمية الرقمية.** تشكل التوترات بين الرغبة في تعزيز التحول الرقمي والحاجة إلى تمكين الأمن السيبراني الفعال تحديات في تمكين آمن، وبيئة آمنة على الإنترنت لتحقيق أهداف التنمية المستدامة. في حين أن بذل المزيد من الجهد لزيادة مرونة البنية التحتية الرقمية ضروري، إلا أنه ليس كافيا. لقد طال انتظار ترجمة الاتفاقات الدولية القائمة إلى إجراءات مجدية.

- **تعد المعايير التي تمكن الأمن السيبراني ضرورية لإنترنت مفتوح وآمن ومرن يمكن التقدم الاجتماعي والنمو الاقتصادي، وهي مهمة بشكل خاص في حماية هؤلاء الذين لم يتصلوا بعد.** وقد تم ضع هذه المعايير، ولكن استخدامها يحتاج إلى اضافات كبيرة لجعلها فعالة تماما. يمكن للأمم المتحدة أن تساعد في تسريع اعتماد المعايير الرئيسية على الصعيد العالمي من خلال إدراج الترويج لها في الاتفاق الرقمي العالمي، من خلال دعم الدعوة وبناء القدرات وتشجيع المبادرات لاختبار ومراقبة النشر. لا ينبغي إغفال زيادة الوعي المبكر وبناء القدرات بشأن المعايير كأولويات في المناطق التي لا يزال يتعين على الكثيرين فيها الاتصال بالإنترنت الاخذ في النمو.

- **لا بد من بذل المزيد من الجهود لتحسين وعي واضعي السياسات الوطنية وغيرهم من أصحاب المصلحة بتحديات الأمن السيبراني والمعايير والمبادئ الدولية.** يجب أن يشمل ذلك الوعي وبناء القدرات فيما يتعلق بالصلات بين التنمية المستدامة والقدرات والأمن السيبراني، الذي يجمع مختلف أصحاب المصلحة معا لتعبئة الإشراف الفعال والمستدام والشامل للتعاون الدولي من أجل المرونة السيبرانية. وقد اتخذت عدد من المبادرات الدولية لدعم ذلك. كذلك يحب تناول الفرص الخاصة بتمويل المرونة السيبرانية التي تعالجها وكالات التمويل وأصحاب المصلحة الآخرون.

الجرائم الإلكترونية

- **تشكل الجرائم الإلكترونية تهديدا متزايدا للعديد من مستخدمي الإنترنت.** لوائح مكافحة الجرائم الإلكترونية يجب أن تكون حساسة لحجم وقدرة وموارد المنصات. وينبغي أن تراعي الالتزامات القانونية تنوع القطاع التقني، وأن تعترف باحتياجات وظروف الشركات الصغيرة في التقيد بالتزاماتها القانونية، على سبيل المثال في مكافحة الاستغلال الإرهابي والمتطرف العنيف لخدماتها.

- **ينبغي للحكومات وواضعي السياسات أن يكفلوا أن تضمن الاستجابات القانونية للاستخدام الإجرامي والإرهابي للإنترنت سيادة القانون وحقوق الإنسان على حد سواء،** مع مراعاة حرية التعبير مراعاة تامة وضمان الشفافية والمساءلة في تنفيذ تدابير مكافحة جرائم الفضاء الحاسوبي.

المحتوى والمعلومات المضللة

- **يمكن ويجب معالجة المعلومات المضللة من خلال آليات تعالج المخاطر التي تواجه الأفراد والمجتمعات مع حماية حرية التعبير والتعددية والعملية الديمقراطية.** يلعب دعم الصحافة المهنية ووسائل الإعلام دورا مهما في الجهود المبذولة لمعالجة المعلومات المضللة، بما في ذلك الالتزام بالمعايير الصحفية الراسخة.

- **تمكن مهارات محو الأمية الإعلامية والرقمية المواطنين من إلقاء نظرة أكثر انتقادا للمحتوى أو المعلومات التي يواجهونها،** مما يساعد على تحديد المعلومات المضللة والمعلومات الخاطئة وتعزيز المشاركة الديمقراطية. يمكن أن يساعد تعليم محو الأمية الرقمية في زيادة الوعي بالسلامة على الإنترنت، خاصة للأفراد والمجتمعات الأكثر ضعفا. كذلك يجب أن تكون المبادرات حساسة للاحتياجات والمخاطر المرتبطة بالمجموعات الديموغرافية المختلفة. فعلى سبيل المثال، يجب أن تستجيب المناهج لأنماط الاستخدام المختلفة للشباب والأجيال الأكبر سنا.

- **يجب أن تتضمن المناهج التعليمية مهارات محو الأمية الرقمية التي تساعد الأطفال على أن يكونوا آمنين على الإنترنت.** وينبغي أن تشمل المبادرات الآباء والمعلمين والأوصياء. كذلك يجب على المشرعين والمنصات الرقمية تحمل مسؤولية ضمان سلامة الأطفال في إطار حقوق الطفل على الإنترنت بما يتفق مع اتفاقيات الحقوق الدولية بما في ذلك اتفاقية الأمم المتحدة لحقوق الطفل.

- **ويتسم نظام أسماء الحقول بقدرة تقنية محدودة في هذا السياق.** الحوار المستمر أصحاب المصلحة ينبغي أن يوضح امتى وكيف يمكن استخدامه لمعالجة المشاكل المتعلقة بالمحتوى، كما وينبغي أن يعزز ذلك الحوار معايير الإجراءات القانونية الواجبة.

- **يلعب التشفير دورا مهما في بناء إنترنت مفتوح وآمن وديمقراطي ويساعد المستخدمين على تحقيق الأمان والخصوصية وحرية التعبير.** يجب معالجة القضايا المتعلقة بإنفاذ القانون المستخدم كما يجب معالجة القدرة على إدارة الوصول في مجالات مثل حماية الطفل.

- **تمثل مشكلات الترجمة حواجز كبيرة يمكن أن تمنع مشاركة المستخدمين النهائيين بشكل هادف مع معايير وإرشادات مجتمع المنصات**. في بعض الأحيان يتم ترجمة المصطلحات الرئيسية بشكل سيئ، مما يؤدي إلى تفسيرات غامضة. ويعد التعامل مع المجتمعات اللغوية المختلفة لتحسين دقة الترجمة وملاءمتها امر ضروري، يشمل ذلك توصيل المفاهيم دون معادلات مباشرة بلغات مختلفة، وهو جزءا مهم من تمكين أصحاب المنصات والمستخدمين من فهم ما هو متوقع منهم.

معالجة التقنيات المتقدمة، بما في ذلك الذكاء الاصطناعي (AI)

الموضوع

تعمل التقنيات الرقمية المتقدمة على تشكيل اقتصادنا ومجتمعنا بشكل متزايد، بما في ذلك أنظمة الذكاء الاصطناعي والتي توجه تجاربنا عبر الإنترنت، وتشغيل أجهزتنا الذكية، كما تؤثر على قراراتنا وتلك التي يتخذها الآخرون عنا، بالإضافة إلى تطبيقات الروبوتات وإنترنت الأشياء التي يتم نشرها في مجالات متنوعة مثل التصنيع والرعاية الصحية والزراعة. وعلى الرغم من وعودهم، تأتي هذه التقنيات مع مزالق. فصنع القرار الخوارزمي على سبيل المثال، يمكن أن يؤدي إلى التحيز والتمييز والقوالب النمطية وعدم المساواة الاجتماعية الأوسع نطاقا، في حين أن النظم القائمة على الذكاء الاصطناعي يمكن أن تشكل مخاطر على سلامة الإنسان وحقوق الإنسان. كذلك تأتي أجهزة إنترنت الأشياء مع تحديات مرتبطة بالخصوصية والأمن السيبراني. كما يثير الواقع المعزز والافتراضي قضايا السلامة العامة وحماية البيانات وحماية المستهلك.

ان الاستفادة من الفرص التي توفرها التقنيات المتقدمة، مع معالجة التحديات والمخاطر مهمة ضخمة لا يمكن لأي جهة فاعلة أن تضطلع بها بمفردها. إن الحوار والتعاون بين أصحاب المصلحة المتعددين - بما في ذلك الحكومات والمنظمات الحكومية الدولية وشركات التكنولوجيا والمجتمع المدني وأصحاب المصلحة الآخرين - مطلوبان لضمان تطوير هذه التقنيات ونشرها بطريقة يكون محورها الإنسان واحترام حقوقه.

الرسائل

الحوكمة

- **ينبغي تصميم التكنولوجيات المتقدمة، بما في ذلك الذكاء الاصطناعي، بطريقة تحترم سيادة القانون وحقوق الإنسان والقيم الديمقراطية والتنوع، مع ضرورة ان تشمل الضمانات المناسبة لذلك.** وينبغي لها أن تفيد الناس والكوكب من خلال دفع عجلة النمو الشامل والتنمية المستدامة والرفاه. كما ينبغي أن تتبع آليات الرقابة والإنفاذ المبادئ والقواعد، مع مساءلة الجهات الفاعلة الذكاء الاصطناعي عن أي ضرر ناجم.

- **إن الافتراض بأن التكنولوجيا تعزز المساواة بالضرورة هو افتراض خاطئ.** أولئك الذين يصممون الآلة غالبا ما تكون تقنيات التعلم والبيانات المستخدمة لتدريب تطبيقات الذكاء الاصطناعي غير ممثلة لها في المجتمعات. وبهذا يمكن للتكنولوجيات أن تزيد من أوجه عدم المساواة وتسبب الضرر، لا سيما للفئات الضعيفة والمهمشة.

- **تحتاج المجتمعات إلى التكيف مع التحول الذي سيحدثه الذكاء الاصطناعي من خلال التغييرات في إطار التعاون ونموذج الحوكمة الخاص بها.** يتطلب بناء مجتمع ذكي محوره الإنسان التعاون الكامل من الحكومات والشركات والمنظمات الاجتماعية والأوساط الأكاديمية. تظل السيطرة البشرية المستمرة ضرورية لضمان أن الخوارزميات لا تؤدي إلى نتائج غير مرغوب فيها أو غير خاضعة للرقابة. يعد كسر العزلة القائمة بين المهندسين وخبراء السياسة أمرا بالغ الأهمية تحقيق هذا.

- **ولا يمكن التوصل إلى اتفاق عالمي بشأن معايير الذكاء الاصطناعي في عملية واحدة مباشرة.** وفي حين أن هناك بعض المعايير القائمة، إلا أنها في الغالب قوانين غير ومبادئ غير ملزمة. وسيتطلب وضع معايير عالمية ذات مغزى مشاركة فعالة من جميع البلدان، بما فيها البلدان النامية والبلدان المتقدمة، ومدخلات من المبادرات الإقليمية، فضلا عن المشاركة. من جميع أصحاب المصلحة.

- **بناء القدرات مهم في الجهود الرامية إلى معالجة التكنولوجيات المتقدمة.** وهناك حاجة إلى سياسات لمحو امية الذكاء الاصطناعي وتنمية المهارات والموارد اللغوية للغات الأقليات من أجل صياغة نهج عالمي حقيقي للتكنولوجيات المتقدمة.

الثقة والأمان والخصوصية

- **يجب أن تتضمن الأطر التنظيمية مبادئ لمساعدة وسائل التواصل الاجتماعي وغيرها من المنصات على الوفاء بالتزامات العناية الواجبة لإدارة المحتوى الذي يمكن أن يضر بالديمقراطية وحقوق الإنسان.** يجب أن تساهم الأطر في المحادثات العالمية حول الإشراف على المحتوى عبر الإنترنت من أجل تمكين المستخدمين، بما في ذلك الفئات الأكثر ضعفا ومستخدمي لغات الأقليات. تتطلب التقنيات الناشئة مثل الحوسبة العاطفية، التي تنظر في كيفية التعرف على أجهزة الكمبيوتر وتفسيرها ومحاكاة المشاعر البشرية، تقييما أخلاقيا موضوعيا.

- **الشفافية في تشغيل النظم الخوارزمية والإبلاغ عنها ضرورية لحقوق الإنسان.** الذكاء الاصطناعي يسهل المراقبة والتحليل المستمرين للبيانات لتخصيص واستهداف المحتوى والإعلانات. تتعرض التجارب الشخصية عبر الإنترنت الناتجة عن ذلك لخطر تصنيف مساحات المعلومات عبر الإنترنت والحد من تعرض الأفراد لتنوع المعلومات. نقص المعلومات يمكن للتعددية من أن تعزز التلاعب والخداع - مما يزيد من عدم المساواة ويقوض الديمقراطية ، وربما تمكين الاستبداد الرقمي والكراهية والعنف.

- **يجب على أصحاب المصلحة من الأوساط التقنية وغير التقنية تبادل الخبرات والعمل معا لوضع مبادئ ومبادئ توجيهية ومعايير مرنة بما فيه الكفاية** للتطبيق في سياقات متنوعة والتي تعزز الثقة في أنظمة الذكاء الاصطناعي.

- **من المهم الاعتراف بالخلفيات المؤسسية والثقافية المختلفة للبلدان والمجتمعات المتنوعة واحترامها،** فضلا عن تعزيز وتمكين التعاون الدولي في مجال الذكاء الاصطناعي.

الإشراف على الحقوق والمحتوى

- **من الضروري أن تتماشى سياسات حوكمة المحتوى من قبل المنصات الإلكترونية، وإنفاذها، مع المعايير الدولية لحقوق الإنسان.** الذكاء الاصطناعي والتعلم الآلي يتم بالفعل باستخدام التقنيات لتحديد ما إذا كان ينبغي نشر المحتوى أو إزالته ، وما هو المحتوى الذي يتم إعطاؤه الأولوية ولمن يتم نشره. وتؤدي هذه الأدوات دورا هاما في تشكيل الخطاب السياسي والعام بطرق تؤثر على حقوق الإنسان الفردية والجماعية على حد سواء، بما في ذلك الحقوق الاجتماعية والاقتصادية والثقافية والحقوق في السلام والأمن العالميين. وغالبا ما يتم نشرها مع القليل من الشفافية أو المساءلة أو الرقابة العامة أو انعدامها. وهذا ما يجب تصحيح.

- **كما يمكن أيضا استخدام نفس التكنولوجيات التي يمكن استخدامها لتعزيز حقوق الإنسان في المراقبة، والترويج لجداول أعمال العنف، وبطرق أخرى تنتهك تلك الحقوق.** العواقب الغير مقصودة في إدارة المحتوى الآلي يمكن أن تكون ضارة بشكل خاص في أوقات الصراع أو الأزمات وذلك عندما تسكت الأصوات الناقدة في وقت تكون فيه تلك الاصوات أكثر أهمية.

- **تلعب المعايير الفنية دورا مهما في تمكين تطوير وتعزيز قيمة التقنيات الرقمية والبنى التحتية والخدمات والبروتوكولات والتطبيقات والأجهزة ذات الصلة. وقد يكون لها أيضا آثار قوية على حقوق الإنسان.** ومع ذلك، فإن عمليات وضع المعايير التقنية داخل المنظمات المختصة بوضع المعايير لا تأخذ شواغل حقوق الإنسان في الاعتبار بالكامل. غالبا ما تكون هذه العمليات مبهمة ومعقدة وكثيفة الموارد بحيث يتعذر على المجتمع المدني وأصحاب المصلحة الآخرين الوصول إليها ومتابعتها بشكل منهجي. وينبغي معالجة هذا الأمر.

注意：感谢杨晓波和李娜的自愿贡献，因此可以提供此翻译。 IGF 对他们表示感谢。

2022 年联合国互联网治理论坛

亚的斯亚贝巴 IGF 关键信息

本文件[1]是 2022 年 11 月 28 日至 12 月 2 日在亚的斯亚贝巴举行的第十七届联合国互联网治理论坛年会期间提出的要点摘要。

本文所表达的观点和意见并不代表联合国秘书处。文中所使用的名称和术语可能不符合联合国的惯例，也不意味着本组织的任何立场。

2022 年 IGF 集中讨论了全球数字契约（GDC）中确认的五个关键主题。GDC 是联合国秘书长在关于联合国成立 75 周年的报告《我们的共同议程》中提出来的，将在 2023 年的联合国大会上进行审议。这也将成为计划于 2024 年举行的未来峰会发展的组成部分。

IGF 讨论的主题包括：

- **连接所有人并保障人权**
- **避免互联网碎片化**
- **数据治理和隐私保护**
- **实现安全、安保和问责制**
- **处理包括人工智能（AI）在内的前沿技术问题**

IGF 的多利益相关方社群对秘书长关于全球数字契约的提议表示支持。本文件所载信息代表了 IGF 对该契约发展的贡献。IGF 动态联盟已经在处理与全球数字契约主题相关的具体挑战和机遇，同时也表示愿意在联合国关于全球数字契约的筹备和执行阶段中做出贡献。

[1] 这些信息来自第十七届联合国互联网治理论坛年会。文件曾公开征求意见，并将收集到的公众反馈内容纳入到本最终版本中。

连接所有人并保障人权

主题

联合国秘书长提出全球数字契约（GDC）的首要原则是“让所有人连接到互联网，包括所有学校”。此契约承认互联网连接和接入已成为确保世界各地人民的生计、安全和教育的先决条件,同时也承认学校互联网提供了关键的接入点，使所有学生都能获得信息资源，并能从小开始培养数字素养。然而目前全球仍有 27 亿人无法上网。这对处于最不发达国家和农村社群的人们尤其不利。

有意义的连接不仅仅是互联互通，而且与保障网络人权密不可分。促进社会福祉的网络接入必须将人权置于中心地位。这包括用户自由表达自我的能力；不受限制地践行民主和参与政治；任何背景的人都能在不恐惧被骚扰或歧视的情况下体验互联网；以及儿童能在网上享有与在线下相同的权利和保护。随着我们的日常生活日益依赖互联网，线上和线下的界限正变得越来越不明显，互联网既是权利的推动者，也必须无缝地纳入到既定的人权内涵中。

关键信息

数字鸿沟

- **不同国家和地区之间的数字鸿沟仍然是影响国家和国际发展的强大因素**，包括影响可持续发展目标（SDGs）的进展，尤其是最不发达国家和小岛屿发展中国家（SIDS）。数字鸿沟远不止是互联互通方面的鸿沟。有意义的接入包括可访问性、可负担性、内容、服务、数字素养和其他能力以及连通性等问题。对许多人来说，负担能力是一个特别的问题，特别是在全球南方。

- **COVID-19 大流行展示了互联网在增强个人和经济韧性方面的作用，但也表明了那些尚未连接至互联网及未进行有意义连接的人在很大程度上处于不利地位。**这可能加剧其他不平等。理解与 COVID-19 相关的干预措施在互联网的获取，使用以及人权的全面影响尚需要时间。

- **在所有社会中，有些群体比其他群体的数字鸿沟更大，或更缺乏有意义的接入。**在许多社会中，女性的网络连接比男性少，对连接的利用也较少。弱势和被边缘化社群的数字劣势更大。许多人由于年龄、性别、族裔、语言、社会阶层等其他因素而经历多重劣势。在基础设施、设备和服务方面采取有针对性的措施可以帮助提高连接较少社会群体的接入率，但同时需要采取方法来解决有意义的接入方面的其他问题，并应与其他举措相结合以解决劣势和歧视。

- **有弹性和安全的数字基础设施对数字包容至关重要。各国政府应保护和促进所需的基础设施，包括电网、离网电力以及通信网络。**在非洲和其他大陆的部分地区，农村和偏远社区之间的距离遥远，这也包括小岛屿发展中国家的社区。这使得最后一英里的连接在商业上对私营部门缺少吸引力。连接、速度和可靠性是基础设施供应的重要方面。提高基础设施能力和解决区域失衡问题需要时间和投资，尤其是在农村地区。

- **利益相关方群体之间的合作对于确保和促进接入十分重要。各国政府和多利益相关方伙伴应支持建立有效的监管机构和工作框架，解决因商业上缺乏吸引力的领域所带来的挑战，以及鼓励以创新方式实现互联互通，**包括社区网络、适当的频谱分配、近地轨道卫星提供的接入和本地内容（包括本地语言内容）的可用性。

性别数字鸿沟与女性权利

- **男性上网或拥有移动网络连接的可能性明显高于女性。**在最不发达国家，性别数字差距尤其大。在消除这一差距之前，旨在实现普遍、负担得起的互联网接入的可持续发展目标 9c 无法实现。

- **暴力和骚扰的威胁阻碍了女性的在线参与。**网络性别暴力是推动和加剧互联网接入和使用方面性别不平等的重要因素，导致一些女性离开网络空间。技术服务和平台在宣传基于性别的暴力方面的角色应得到承认和解决。应指导女性抵制和纠正基于性别的在线暴力，包括通过社区组织的求助热线等。应以本地语言提供有关平台的资源、社区准则和报告。

- 按照联合国妇女署的建议，**应将性别平等、包容以及女性权利和保护的概念纳入全球数字契约（GDC）。**

人权和数字发展

- **普遍接入应尊重人权，以确保互联网对所有人而言都是可接入和安全的。**数字权利包括言论和结社自由、隐私权以及国际权利协定规定的其他公民权利、政治权利、经济权利、社会权利和文化权利。互联网治理架构和数字技术设计应尊重这些权利。标准制定组织应该考虑邀请来自所有利益相关方社群的线上人权专家参与他们的工作。

- **人权方面的透明度、问责制和尽职调查是所有利益相关方群体的责任，包括政府间和国际性组织、政府、私营部门、技术社群和公民社会。**这将要求商业实践与数字权利结合起来，并要求利益相关方开展合作，以解决虚假信息、歧视和仇恨言论等问题，特别是在政治动荡、选举和权力转移时期。

- **接入互联网为获取信息和表达途径提供了一个关键的机会。**政府应避免关闭互联网，因为这对人权和经济福利都有负面影响。社交媒体和技术公司应该支持公民就关闭互联网问题所建立的倡议工作。

- **加强对数字权利的监督和实施尤其重要。**关于在联合国系统内建立多利益相关方参与的国际监督安排，一些建议已被提出。这些建议可以补充和发展现有机制，包括与数字发展和权利有关的机制，以及气候变化等其他领域的机制。

- 作为更广泛的改善教育政策的一部分，**互联网为加强受教育权提供了机会。**由于缺乏网络连接，全球南方的教育质量受到影响，特别是在疫情大流行期间。尽管信息通信技术可以使学生获得有意义的接入，但全球和本地采用率的差异加剧了大流行前的不平等。大流行期间的经验可用于改进未来数字资源的使用。

- **应努力帮助规模较小的本地企业最大限度地利用互联网。**自 2020 年以来，中小企业对数字化工具的使用大幅增加，但微型企业在业务数字化能力方面仍面临重大挑战。

- **在线平台所带来的劳动力市场变化为创造就业和提高就业质量带来了机遇和挑战，**特别是对于大多数国家非正规部门中比男性发挥更大作用的女性而言。缺乏培训仍然是许多人最大限度发挥其就业潜力的障碍。

- **必须提高数字化能力，教学、学习和培训方法也需要调整，以适应教育和就业的新范式。**重要的是要找出并缩小行业需求与高等教育之间的差距。

避免互联网碎片化

主题

维护一个全球开放和可互操作的互联网是 IGF 的核心价值之一。这意味着整个互联网继续采用共同的技术标准和协议，以实现跨国家和地区网络间的互联互通；以及内容和服务的标准符合人权和法规。应用一个框架于互联网——其优先考虑用户的权利和自由，以及基础设施和端到端的一致性——这些呼吁都已经在全球数字契约的计划中得到了响应。

互联网碎片化的风险是真实存在的，而且还在不断增加。尽管技术和商业碎片化——互联网的运作受到各种自愿和非自愿条件以及商业实践的综合影响——需要加以解决，但是影响互联网开放性和互操作性的政府政策造成的碎片化也值得关注。

关键信息

对问题的理解

- **全球数字契约为重申一个开放连接的互联网的价值提供了机会，这有助于实现《联合国宪章》、实现可持续发展目标和行使人权。**互联网社群就一个全球完整的互联网作为人类活动平台的价值达成了广泛的共识。

- **在互联网碎片化的讨论中提出的问题是多层次的，不同的利益相关者对这个术语给出了各种不同的含义和解释。**一些人最关心互联网的技术和基础设施，而另一些人则关注公共政策问题，包括接入、权利和对用户体验的影响。IGF 政策网络所编写的关于互联网碎片化的框架草案对这些问题进行了探讨。如果我们要达成有效和协调一致的应对措施，尊重和理解不同人对碎片化的看法和体验至关重要。

- **广泛的政治、经济和技术因素都可能潜在地推动碎片化。**然而，多样性和去中心化不应被误认为碎片化。这些从根本上来说都是互联网架构和运营的积极方面。

处理碎片化的风险

- **有效的多利益相关方治理机制对于治理一个全球完整的互联网至关重要。**有必要加强对这些机制的信任，确保它们是强有力和可持续的，并在治理结构不断发展以迎接新挑战的同时促进这些结构之间的一致性。

- **有必要对新的或正在形成的碎片化风险保持警惕。**全球合作和协调对于查明早期预警迹象、了解政策和其他事态发展的影响以及准备应对这些变化至关重要。多利益相关方模式最适合于评估、评价和监督影响互联网措施的潜在意外后果，并提出有效的替代办法，以避免或减轻碎片化的风险。IGF 政策网络在针对互联网碎片化的方面就是一个积极示范。

- **互联网开放有助于促进互联网用户享有人权，促进竞争和机会平等，并保护互联网生成的对等天性。**关于网络中立和非歧视性流量管理的辩论仅仅属于这方面广泛讨论的一部分。网络中立对于保障互联网开放是必要但不足够充分的条件。基础设施和数据互操作性以及平台和设备的中立性也是必要的。

- **尽管世界各地的法律、监管和政策模式不同，但跨国际边界的积极协调对于确保碎片化措施不会威胁到互联网的全球覆盖和互操作性至关重要。**维持全球网络的完整性需要国际监管合作，并就基本原则达成共识。

- **许多不同的因素影响着不同法域的互联网体验，包括不同的社会、人口、经济、文化和政治环境以及技术和基础设施问题。**在国家层面追求某些形式的数字治理会增加互联网技术层面的碎片化风险。然而，监管框架还必须考虑不同情况下的不同要求，并跟上技术和服务的快速变化。

- **有必要加强利益相关方之间的知识和信息共享，**进一步讨论网络外交这一不断演变的现象，并考虑适当干预的范围。标准制定机构应继续加强与利益相关方的接触和互动，并增进政策和技术社群之间的理解。标准化组织应通过所有受影响的利益相关方的直接参与，讨论具有政策影响力的技术层面的决定。

数据治理和隐私保护

主题

数据是全球化数字时代的关键资源。数据流动促进经济增长，同时数据分析，包括大数据分析，也一直是金融、健康、执法等各领域取得突破性创新的基础。

但数据的广泛使用、常规性跨境流动和可替代性仍然是十分敏感且亟待解决的问题。作为一种跨国商业资产，数据流动在缺乏各国间法律制度一致性的环境下运行，会给执法带来重大挑战。从数据收集到应用和存储，数据交换常会牺牲个人隐私。这会对信任和安全造成严重影响。

若想发挥数据在经济和研究方面的巨大潜力，需要围绕治理、诚信和个人隐私保护展开重新讨论。

关键信息

数据的中心性

- **在日益数字化的时代，数据已成为关键资源。**数据流动对许多领域的跨国合作至关重要，包括科学研究、执法以及国家和全球安全。数据、数据安全和数据保护是可持续发展的重要保障。在全球范围内有效使用和共享数据，有助于应对共同的挑战，如疫情、气候变化等连锁危机带来的威胁。

- **数据可以产生利润和显著的社会价值。**然而，到目前为止，数据驱动的经济利益分配不均。许多人担忧他们可能成为主要数据提供者，而非受益者。

- **数据生成者和使用者之间的关系十分重要。**数据贫困是一个重大问题，特别是在本地社区和弱势群体中。缺乏数据隐私和保护会破坏对数据管理的信任。在各级政府、教育课程和公众中建立数据素养和数据能力，是重要的解决方式。

- **数据管理和治理是国家和国际治理中的复杂问题。**数据开发利用——包括大数据分析、人工智能和机器学习的创新，以及公共政策层面和可持续发展目标的创新——需要适当考虑政治、经济和社会影响，并结合细致的政策干预。政府和监管机构需要一定的基础设施和能力，以构建有效、综合的国家数据治理框架。应用程序开发人员有责任确保设计的安全性并符合道德规范。

数据隐私和数据正义

- **数据隐私并非便利或良好实践问题，而是关乎人权。**除了隐私权、平等待遇和非歧视之外，数据还影响其他方面的人权，如获得医疗、教育和公共服务的权利，以及言论自由、结社自由等民主权利。隐私法应该是实质性的、有理有据的，并且能够明确执行。受到这些影响的人应该可以清楚地理解其影响。

- **数据流动和数据交换应在不损害数据隐私的情况下进行。**在数据交换、信息收集和使用过程中，个人数据隐私经常受到侵害，对信任和安全造成有意/无意的风险。互联网接入和使用不应依赖数据跟踪：用户应该有权选择信息分享范围，包括由其在线行为产生的信息。个人数据不应被引入没有充足保证的法域。

- **政策应从数据保护延伸到数据正义，让人们可以选择如何使用个人数据，以及在何处分享由其数据集产生的创新收益和好处。**因此，隐私保护应促进更安全、更繁荣的数字经济。

- **政府和监管机构应确保个人数据得到保护**，确定不同利益相关方的不同责任，而不给个人用户施加过度的负担或责任。数据治理政策应参考多利益相关方的意见，以确保实施过程中的挑战能够被充分吸收理解。

- **隐私和数据保护对于人工智能和机器学习的治理尤为重要。**人工智能供应链中的所有利益相关方都能在维护隐私权方面发挥作用。

- **需要配备拥有适当资源的独立监督机构。**数据保护办公室应授权管理数据登记、提供指导、实施调查和解决数据主体的投诉。

数据治理

- **与数据治理有关的问题及其影响不应被孤立看待。**当前的数据治理格局是由碎片化的国家、区域和国际规则拼凑而成，涉及各国政府、私营部门和个人的责任。

- **全球要加强一致性，实现数据为人类和地球服务的平衡之道。**国家、区域和国际层面现有的立法和监管框架不足，无法跟上技术和应用的变化步伐。这些框架应确保拥有数据的企业和其他组织采用高水平的安全标准。

- **不同的背景和挑战、历史、文化、法律传统、监管架构意味着不可能形成一套针对所有人的刚性规则。**不同的个人和组织也以不同的方式诠释着大致相似的模式。尽管各国和地区必须制定符合自己的数据治理模式，但也应保持一致性和互操作性，以促进数据流动、确保公平竞争。

- **透明度、参与度和问责制是良好数据治理的重要方面。**数据治理的重要考虑因素包括（但不限于）：数据标准和分类；数据共享、交换和互操作性；数据安全和数据隐私；数据基础设施；数据和数字身份；数据正义与公平；数据可追溯性、透明度和可解释性；数据最小化和数据限制；数据准确性和质量；数据偏见、边缘化和歧视；数据生命周期、数据使用的明确性和保存时间；数据问责制和数据伦理；数据危害、数据安全和数据保护。

- 包括监管机构、研究人员、标准化组织、消费者组织和终端用户等在内的**多个多利益相关方扮演着一定角色，应行使其权利且发挥影响力，促进有效的数据治理。**数据治理政策的制定应基于多方利益相关方社群的意见。他们在围绕隐私的法律辩论和实施有效数据隐私解决方案的“现实世界”挑战的方面具有一定的专业知识。

- **发展中经济体需要加强其制度能力的建设，以全面、客观和循证的方式治理、使用和管理数据，包括通过区域和全球合作。**这需要进一步了解政府官员和其他利益相关方的制度能力。

跨境数据流动

- **跨境数据流动对电子商务和数字贸易的许多方面至关重要。**有效的区域内贸易和供应链管理依赖于数据以及货物、服务和资本的顺畅流动。然而，这些需要考虑复杂的交叉因素：监管的趋同性，法律框架的协调，互联网治理，信息和通信技术政策改革，以及战略性区域基础设施实施。

- **目前的多边、区域和双边贸易协定不能完全适用于当前和未来的跨境数据流动。**这些都是在基本上不受监管的环境中运作，国家法律制度之间几乎没有一致性。各国采用的方式不同，且各有背景，因此造成贸易壁垒，许多国家目前没有足够的立法或执法能力。制定和协调管理跨境数据流动的措施愈发必要，以促进不同背景下的发展和经济价值创造，同时尊重国家主权和用户隐私。

实现安全、安保和问责制

主题

互联网面临的安全威胁主要有几个方面。传统的网络安全涉及保护网络、设备和数据免受未经授权的访问或被犯罪使用。持续存在的网络攻击问题也包括在内，无论这些攻击来自个人还是国家制裁，目标是公民、商业还是政府。缺乏广泛和具有约束力的网络安全协定、网络安全性不足等因素导致充分利用数字技术带来的经济效益的机会流失，特别是对发展中国家而言。

安全、安保和问责制的问题应该从多方面考虑，包括基础设施、服务、内容和互联网的其他方面。例如，现在我们对安全和安保的理解包括在线虚假信息和错误信息的持续挑战。近年来，这些因素加剧了新冠肺炎疫情的影响，并对世界各地的选举进程构成重大风险。这强调了对误导性内容建立责任制并明确标准的必要性。

考虑到“绿色”互联网和减少与数字消费相关的碳排放，“安全”的概念可能会进一步扩大到包括环境安全。解决数字化对环境的影响是 IGF 讨论中日益重要的主题。

关键信息

政策制定者的作用

- **网络安全应被视为互联网政策的核心挑战。**信任和安全方面的考虑对安全、可靠接入的发展不可或缺，包括尊重人权、政策制定的公开和透明，以及服务终端用户利益的多利益相关方模式。

- **确保网络安全和预防网络犯罪是同等重要的政策领域，需要高度重视和发展专业能力。**然而，它们目标不同，所需的方法也不同。针对一个方面有效的方法不适用于其他方面，需要进行调整和重新制定。

- **网络安全和网络犯罪问题具有跨组织、跨境等多层性质。解决这些问题需要：**
  a）**全政府和全社会通力合作**，包括强有力的伙伴关系和协调努力，涉及议会、监管机构、其他有关政府主管部门和机构、私营部门、技术社群、学术界和公民社会；以及
  b）**政府间、多边和多方利益相关方的高效和有效的区域和国际合作。**

- **各国政府、私营部门和技术社群应注意避免通过的网络犯罪法和建立的有关标准对网络安全维护者的工作产生负面影响。**他们应邀请所有利益相关方共同参与政策制定，并促进不同社群之间的互动及经验和专门知识的交流。

- **公民社会应参与网络犯罪和网络安全讨论。**为确保进行有效讨论，公民社会利益相关方应就所涉及的不同方法和问题进行自我教育，并与其他利益相关方合作，收集充分参与决策所需的信息和资源。

网络安全

- **国际社会应探索切实可行的方式，将网络安全能力建设纳入到更广泛的数字发展主流中。**数字化转型的愿望与实现有效网络安全的需求之间的紧张关系，对实现安全、可靠的在线环境和实现可持续发展目标构成了挑战。提高数字基础设施的弹性十分重要，但这还不够。将现有的国际协定转化为可行的行动势在必行。

- **实现网络安全的标准对于构建开放、安全和有弹性的互联网至关重要，这有利于促进社会进步和经济增长，特别是对保护尚未联网人们的安全也很关键。**此类标准已经制定，但大量的使用需求才能促成其充分有效地发挥作用。联合国可以通过将关键标准的推广纳入全球数字契约、支持倡议和能力建设，鼓励测试和监督部署等举措，加速关键标准在全球范围的采纳。在联网需求大且互联网仍处发展期的地区，尽早提高认识、加强标准能力建设是优先事项。

- **仍需加大力度提高国家政策制定者和其他利益相关方对网络安全、国际规范和原则带来挑战的认识。**这应包括认识可持续发展与网络安全之间的联系，加强相关能力建设，将不同的利益相关方聚集在一起，组织促成有效、可持续和包容性的国际合作以提高网络弹性。现已有许多国际举措对此进行支撑。资助机构和其他利益相关方也需要把握为网络弹性提供资金的机会。

- **网络安全规范必须影响互联网用户过去、现在和未来的体验。**在这种情况下，倾听遭受网络安全攻击的个人和组织以及第一响应者的经历非常重要，特别是当制定新规范的背景之时。

网络犯罪

- **网络犯罪对许多互联网用户构成越来越大的威胁。**打击网络犯罪的法规应当对平台规模、能力和资源足够敏感。法律义务应考虑技术部门的多样性，并认识到小企业在遵守其法律义务方面的需求和情况，例如打击恐怖和暴力极端主义分子对其服务的滥用。

- **各国政府和政策制定者应确保对犯罪和恐怖分子使用互联网的法律回应既保障法治又保障人权，**充分考虑到言论自由，并在打击网络犯罪的同时确保透明度和问责制。

内容和虚假信息

- **可以并且应该通过解决个人和社会所面临风险的机制来应对虚假信息，同时保护言论自由、多元化和民主进程。**对专业新闻和媒体的支持在解决虚假信息方面发挥着重要作用，包括对既定新闻规范的承诺。

- **媒体和数字素养技能赋权公民对所遇到的内容或信息持更具批判性的态度，这有助于识别虚假信息和错误信息，提高民主参与度。**数字素养教育有助于提高在线安全意识，尤其是对弱势的个人和社群。针对不同人口群体的需求和风险所采取的各项举措需要保持敏感度。例如，针对年轻人和老年人采取的不同方法，须对应不同的使用模式。

- **教育课程应包含帮助儿童安全上网的数字素养技能。**措施应涉及父母、教师和监护人。立法者和数字平台应承担相应责任，在儿童在线权利框架内确保儿童安全。这一框架应与包括《联合国儿童权利公约》在内的国际权利协定保持一致。

- **域名系统在这方面的技术能力有限。**持续的利益相关方对话应澄清何时以及采用何种方式来补救具体的在线内容问题，同时应加强正当程序规范。

- **加密对于构建一个开放、安全和民主的互联网至关重要，**并能帮助用户实现安全、隐私和言论自由。仍有一些问题需要解决，如执法、用户对儿童保护等领域接入的管理能力。

- **翻译造成的严重障碍会阻碍终端用户有效参与平台社区标准和准则的制定。**关键术语有时翻译不到位，导致解释不明确。与不同语言社群互动以提高翻译的准确性和关联性，包括与其交流有关概念但避免采用在不同语言中直接对等的名称，对增进平台和用户的理解至关重要。

处理包括人工智能（AI）在内的前沿技术问题

主题

先进的数字技术不断塑造我们的经济和社会，包括引领在线体验、为智能设备提供动力，同时影响我们自己的决定和他人对我们作出决定的人工智能（AI）系统，以及在制造业、医疗保健和农业等不同领域部署的机器人技术和物联网应用程序。这些技术提供了发展机遇，也带来了挑战。例如，算法决策可导致偏见、歧视、刻板印象和更广泛的社会不平等，而基于人工智能的系统会对人类安全和人权构成风险。物联网设备带来隐私和网络安全挑战。增强现实和虚拟现实技术引发了公共安全、数据保护和消费保护等问题。

把握先进技术带来的机遇，同时应对相关的挑战和风险是一项任何一方都无法独自承担的任务，需要包括政府、政府间组织、技术公司、公民社会和其他利益相关方在内的多利益相关方对话和合作，以确保技术的开发和部署以人为本、尊重人权。

关键信息

治理

- **包括人工智能在内的前沿技术的设计应尊重法治、人权、民主价值和多样性，并包括适当的保障措施。**前沿技术应该通过推动包容性增长、可持续发展和福祉来造福人类和地球。监督和执行机制应遵循一定的原则和规则，人工智能参与者应对造成的任何损害负责。

- **技术必然促进平等的假设存在缺陷。**设计机器学习技术的人和训练人工智能应用程序的数据往往在其所在社会并没有代表性。技术会加剧不平等现象，并对弱势群体以及边缘化群体造成伤害。

- **社会需要适应人工智能对合作框架和治理模式带来的变革。**构建以人为本的智能社会需要政府、企业、社会组织和学术届通力合作。为防止算法带来不受控或不想要的结果，持续的人为控制仍然必不可少。打破工程师和政策专家之间的孤岛对于实现这一目标至关重要。

- **单一进程不能促使全球就人工智能规范达成共识。**现有规范大多是软性法律，而不是具有约束力的原则。有意义的全球标准制定需要所有国家的参与，包括发展中国家和发达国家。同时，区域性倡议的反映和所有利益相关方的参与也十分重要。

- **能力建设对于前沿技术发展很重要。**需要制定人工智能素养、技能开发和提供少数民族语言资源的政策，以便就前沿技术制定真正的全球方案。

信任、安全和隐私

- **监管框架应包括帮助社交媒体和其他平台履行勤勉尽责义务的原则，管理可能损害民主和人权的内容。**这一框架应促进在线内容审核的全球对话，以赋权用户，包括最弱势群体和少数民族语言用户。新兴技术，例如考虑计算机如何识别、理解和模拟人类情感的情感计算技术，需要进行实质性的伦理评估。

- **算法系统运行和报告的透明度对于人权至关重要。**人工智能有助于持续观察和分析数据，以个性化和定向推送内容和广告。由此产生的个性化在线体验会产生在线信息空间碎片化的风险，限制个人接触多样化的信息。信息多样性缺乏会助长操纵和欺骗——加剧不平等，破坏民主辩论，并可能加剧数字权威主义、仇恨和暴力。

- **来自技术和非技术社群的利益相关方需要交流专业知识并共同制定通用原则，这些原则和标准在**多种环境中需要足够灵活，并能促进对人工智能系统的信任。

- **承认和尊重不同国家和社群的不同制度和文化背景很重要，**促进包容性、加强人工智能领域的国际合作也是如此。

权利和内容审核

- **在线平台的内容治理政策及其执行需要符合国际人权标准。**人工智能和机器学习技术已经被用于决定内容的发布和删除、内容的优先级和传播对象。这些工具通过影响个体和集体人权的方式明显塑造政治和公共话语，包括社会、经济和文化权利以及全球和平和安全的权利。这些工具很少或根本没有透明度、问责制或公众监督。这种现象理应得到纠正。

- **用于促进人权的技术同样可以被用于实施监视、宣扬暴力意图以及侵犯这些权利的其他行为。**在冲突和危机时期，自动化内容管理产生的意外后果尤其有害，因为它们可能压制在这一时期最关键的批评声音。

- **技术标准能够促进发展，推动数字技术及相关基础设施、服务、协议、应用程序和设备的价值，同时也可能对人权产生重大影响。**然而，标准制定组织内的技术标准制定过程没有充分考虑到人权问题。这些流程通常隐晦、复杂，而且公民社会和其他利益相关方需要大量的资源才能系统性地访问和遵循。这个问题应该要解决。

Cette traduction est disponible grâce à la contribution volontaire de Mme. Muriel Alapini, Mme. Hariniombonana Andriamampionona, Mme. Melanie Nedelec et M. Arsène Tungali. L'IGF leur en est reconnaissant.

FORUM SUR LA GOUVERNANCE DE L'INTERNET 2022

Messages IGF d'Addis Abeba

Ce document est le résumé des points soulevés lors de la 17e réunion annuelle du Forum sur la gouvernance de l'Internet qui s'est tenue à Addis- Abeba du 28 novembre au 2 décembre 2022.

Les points de vue et les opinions exprimés ici ne reflètent pas nécessairement ceux du Secrétariat des Nations Unies. Les appellations et la terminologie employées peuvent ne pas être conformes à la pratique des Nations Unies et n'impliquent pas l'expression d'une quelconque opinion de la part de l'Organisation.

Les discussions lors de l'IGF 2022 se sont concentrées sur cinq thèmes clés identifiés pour le Pacte numérique mondial (GDC). Ce dernier a été lui-même proposé dans le rapport 2021 du Secrétaire général des Nations Unies lors du 75e anniversaire des Nations Unies, notre Programme Commun, et sera examiné par l'Assemblée générale des Nations Unies en 2023. Il s'inscrira dans le cadre de l'élaboration du Sommet du Futur prévu en 2024

Les thèmes considérés par l'IGF étaient :

- Connecter toutes les personnes et protéger les droits de l'homme
- Éviter la fragmentation d'Internet
- Gouverner les données et protéger la vie privée
- Assurer la sûreté, la sécurité et la responsabilité
- Aborder les technologies avancées, y compris l'intelligence artificielle (IA)

La communauté multipartite de l'IGF a exprimé son soutien à la proposition du Secrétaire général pour un Pacte numérique mondial. Les messages présentés dans ce document représentent les contributions de l'IGF à l'élaboration du Pacte. Les Coalitions Dynamiques de l'IGF qui traitent déjà les défis et les opportunités spécifiques en rapport avec les domaines thématiques proposés pour le GDC, ont également exprimé leur intention de contribuer aux phases préparatoires et au processus de mise en œuvre par les Nations Unies.

Connecter toutes les personnes et protéger les droits de l'homme

Thème

Le Pacte numérique mondial (GDC) proposé par le Secrétaire général des Nations Unies a pour premier principe de « Connecter tous les individus à Internet, y compris toutes les écoles ». Ce principe reconnaît que la connectivité et l'accès à Internet sont devenus des conditions préalables pour garantir les moyens de subsistance, la sécurité et l'éducation des personnes partout dans le monde, - et que la présence d'Internet dans les écoles fournit des points d'accès cruciaux, met des ressources d'information à la disposition de tous les élèves et permet l'acquisition de la culture numérique dès la petite enfance.

Pourtant, aujourd'hui, 2.7 milliards de personnes ne sont toujours pas connectées dont les plus défavorisées proviennent des pays les moins avancés et des communautés rurales Un accès significatif va au--delà de la simple connectivité et est indissociable de la protection des droits de l'homme en ligne. Un accès qui contribue au bien--être de la société doit être axé sur les droits de l'homme.

Il s'agit, entre autres,de la possibilité pour les utilisateurs de s'exprimer librement, de l'exercice sans entrave à la participation démocratique et politique, de la possibilité pour les personnes de tous horizons de faire l'expérience d'Internet sans crainte de harcèlement ou de discrimination, et de la possibilité pour les enfants de jouir des mêmes droits et protections en ligne comme hors ligne. Internet est à la fois un catalyseur de droits et doit intégrer de manière transparente les droits de l'homme établis, puisque nous augmentons notre dépendance numérique pour les fonctions de routine, et que les frontières entre la vie « en ligne » et « hors ligne » deviennent de moins en moins importantes.

Messages

Fracture numérique

- Les fractures numériques entre les différents pays et régions restent un facteur important qui affecte le développement national et international, y compris les progrès vers les objectifs de développement durable (ODD). Les pays les moins avancés et les petits États insulaires en développement (SIDS) sont particulièrement concernés. Les fractures numériques sont bien plus que des fractures de connectivité. Un accès significatif comprend les questions d'accessibilité, de prix, de contenu, de services, de culture numérique et d'autres capacités ainsi que de connectivité. L'accessibilité financière est un problème particulier pour de nombreuses personnes, notamment dans les pays du Sud.
- La pandémie de COVID-19 a démontré le rôle que joue l'Internet dans la résilience individuelle et économique, mais a aussi illustré à quel point ceux qui ne sont pas connectés ou n'ont pas un accès significatif sont désavantagés, exacerbant potentiellement d'autres inégalités. Il faudra du temps pour comprendre tout l'impact et les implications des interventions liées au COVID concernant l'accès, l'utilisation et les droits de l'homme.

- Dans toutes les sociétés, certains groupes connaissent des fractures numériques plus profondes ou ont un accès moins significatif que d'autres. Dans de nombreuses sociétés, les femmes sont moins connectées que les hommes et utilisent moins la connectivité. Le désavantage numérique est plus important dans les communautés vulnérables et marginalisées, et de nombreuses personnes subissent de multiples désavantages en raison de la combinaison de facteurs liés à l'âge, au sexe, à l'origine ethnique, à la langue, à la classe sociale et à d'autres facteurs. Des initiatives ciblées dans les infrastructures, dispositifs et services peuvent contribuer à améliorer les taux d'accès pour les groupes sociaux moins connectés, mais elles doivent être accompagnés de mesures visant à remédier à d'autres lacunes en matière d'accès significatif et doivent être associés à d'autres mesures visant à lutter contre les désavantages et la discrimination.

- Une infrastructure numérique résiliente et sécurisée est essentielle à l'inclusion numérique. Les gouvernements doivent protéger et promouvoir les infrastructures nécessaires, notamment l'électricité en réseau et hors réseau ainsi que les réseaux de communication. Dans certaines régions d' Afrique et d'autres continents, l'éloignement des communautés rurales et leur enclavement, y compris celles des SIDS, rendent la connectivité du dernier kilomètre commercialement peu attrayante pour le secteur privé. La connectivité, la rapidité et la fiabilité sont des aspects importants de la fourniture d'infrastructures. Il faudra du temps et des investissements pour améliorer la capacité des infrastructures et remédier aux déséquilibres régionaux, en particulier dans les zones rurales.

- La coopération entre les groupes de parties prenantes est importante pour garantir et permettre l'accès. Les gouvernements et les partenaires multipartites devraient soutenir la mise en place et le travail des organismes de régulation et de cadres réglementaires efficaces, relever les défis dans les zones commercialement peu attrayantes et encourager des approches innovantes en matière de connectivité, y compris les réseaux communautaires, l'attribution appropriée du spectre, l'accès fourni par les satellites en orbite terrestre basse et la disponibilité de contenu local, y compris le contenu dans les langues locales.

La fracture numérique entre les sexes et les droits des femmes

- Les hommes sont nettement plus susceptibles d'être en ligne ou d'avoir une connexion mobile que les femmes. La fracture numérique entre les sexes est particulièrement important dans les pays les moins avancés. La cible 9c des ODD, qui vise à parvenir à un accès Internet universel et abordable, ne pourra être atteinte tant que cet écart ne sera pas comblé.

- La menace de violence et de harcèlement a un effet dissuasif pour la participation des femmes en ligne. La violence sexiste en ligne est un facteur important qui entraîne et renforce l'inégalité entre les sexes en matière d'accès et d'utilisation d'Internet, ce qui conduit certaines femmes à quitter les espaces en ligne. Le rôle des services et plateformes technologiques dans la propagation de la violence sexiste doit être reconnu et traité. Les femmes devraient bénéficier de conseils pour résister à la violence sexiste en ligne et y remédier, y compris par le biais de lignes d'assistance communautaires. Les ressources, les directives communautaires et les rapports sur les plateformes doivent être disponibles dans les langues locales.

- Les concepts d'égalité des sexes, d'inclusion et de droits et de protection des femmes doivent être intégrés dans le Pacte Numérique Mondial (GDC), comme cela a été proposé par ONU Femmes.

Droits de l'homme et développement numérique

- L'accès universel doit respecter les droits de l'homme, afin de garantir qu'Internet est à la fois accessible et sûr pour tous. Il s'agit notamment de la liberté d'expression et d'association, du droit à la vie privée et d'autres droits civils, politiques, économiques, sociaux et culturels énoncés dans les accords internationaux sur les droits. Les structures de gouvernance de l'internet et la conception des technologies numériques doivent respecter ces droits. Les organismes d'élaboration de normes devraient envisager d'inviter des experts en droit de l'homme en ligne, issus de toutes les communautés de parties prenantes, afin de participer à leurs travaux.

- La transparence, la responsabilité et la diligence raisonnable en matière de droits de l'homme incombent à tous les groupes de parties prenantes, y compris les organisations intergouvernementales et internationales, les gouvernements, le secteur privé, la communauté technique et la société civile. Cela nécessitera un alignement des pratiques commerciales avec les droits numériques et la coopération entre les parties prenantes pour traiter des questions telles que la désinformation, la discrimination et les discours de haine, en particulier en période de troubles politiques, d'élections et de transferts de pouvoir.

- L'accès à Internet offre une opportunité cruciale d'accès à l'information et à l'expression. Les gouvernements devraient éviter de recourir aux coupures d'Internet en raison de leur impact négatif tant sur les droits de l'homme que sur le bien-être

économique. Les médias sociaux et les entreprises de technologie devraient soutenir les citoyens dans leurs efforts de plaidoyer concernant les coupures.

*Il est important d'améliorer le suivi et la mise en œuvre des droits numériques. Un certain nombre de suggestions ont été faites pour mettre en place des dispositifs de suivi internationaux au sein du système des Nations Unies, avec un engagement multipartite. Ces dispositifs pourraient compléter et s'appuyer sur les mécanismes existants, y compris ceux qui concernent le développement et les droits numériques et ceux qui concernent d'autres domaines tels que le changement climatique.

- Internet offre des possibilités de renforcer les droits à l'éducation, dans le cadre de politiques plus larges d'amélioration de l'éducation. La qualité de l'éducation dans les pays du Sud, en particulier pendant la pandémie, a souffert d'un manque de connectivité. Alors que les TIC peuvent permettre un accès significatif pour les étudiants, les différences dans les taux d'adoption mondiaux et locaux ont exacerbé les inégalités pré-pandémiques. L'expérience acquise pendant la pandémie peut être utilisée pour améliorer l'utilisation des ressources numériques à l'avenir.

- Des efforts doivent être faits pour aider les entreprises plus petites et locales à tirer le meilleur parti d'Internet. L'utilisation des outils numériques par les petites et moyennes entreprises a considérablement augmenté depuis 2020, mais les micro-entreprises sont toujours confrontées à des défis importants dans leur capacité à numériser leurs activités.

L'évolution du marché du travail autour des plateformes en ligne présente à la fois des opportunités et des défis pour la création d'emplois et la qualité des emplois, en particulier pour les femmes qui jouent un rôle plus important que les hommes dans le secteur informel dans la plupart des pays. Le manque de formation reste, pour beaucoup, un obstacle à la maximisation de leur potentiel d'emploi.

Les compétences numériques doivent être améliorées et des adaptations des méthodologies d'enseignement, d'apprentissage et de formation sont nécessaires pour s'adapter aux nouveaux paradigmes de l'éducation et de l'emploi. Il est important d'identifier et de combler l'écart entre les besoins de l'industrie et l'enseignement supérieur.

Éviter la fragmentation d'Internet

Thème

Le maintien d'un Internet mondial, ouvert et interopérable est une valeur fondamentale de l'IGF. Cela implique que des normes et protocoles techniques communs continuent d'être déployés pour créer un réseau de réseaux interconnectés entre les pays et les régions, et que les normes relatives au contenu et aux services soient conformes aux droits de l'homme et à l'État de droit. L'appel en ce sens, appliquer un cadre à Internet qui donne la priorité aux droits et libertés des utilisateurs ainsi qu'à la cohérence infrastructurelle de bout en bout, -a été repris dans les plans de la GDC.

Le risque de fragmentation est réel et croissant. Si la fragmentation technique et commerciale -- où le fonctionnement d'Internet est affecté par un mélange de conditions volontaires et involontaires et de pratiques commerciales - -doit être abordée, la fragmentation par la politique gouvernementale affectant le caractère ouvert et interopérable d'Internet est également préoccupante.

Messages

Comprendre les enjeux

Le Pacte numérique mondial est l'occasion de réaffirmer la valeur d'un Internet interconnecté ouvert pour la réalisation de la Charte des Nations Unies, la réalisation des objectifs de développement durable et l'exercice des droits de l'homme. Il existe un large consensus au sein de la communauté Internet sur la valeur d'un Internet mondial non fragmenté en tant que plate-forme pour l'activité humaine.

Les questions soulevées dans les discussions sur la fragmentation d'Internet sont multiples et les différentes parties prenantes donnent une variété de significations et d'interprétations au terme. Certains sont plus concernés par les aspects techniques et infrastructurels d'Internet, tandis que d'autres se concentrent sur les questions de politique publique, y compris l'accès, les droits et les impacts sur l'expérience de l'utilisateur. Ces questions sont examinées dans un projet de cadre préparé par le Réseau politique du FGI sur la fragmentation d'Internet. Le respect et la compréhension des perceptions et de l'expérience de la fragmentation des différentes personnes sont essentiels si nous voulons parvenir à des réponses efficaces et coordonnées.

Un large éventail de facteurs politiques, économiques et techniques peuvent potentiellement favoriser la fragmentation. Cependant, il ne faut pas confondre la diversité et la décentralisation avec la fragmentation. Ce sont des aspects fondamentalement positifs de l'architecture et du fonctionnement d'Internet.

Faire face au risque de fragmentation

Des mécanismes de gouvernance multipartite efficaces sont essentiels à la gouvernance de l'Internet mondial non fragmenté. Il est nécessaire de renforcer la confiance dans ces mécanismes, de veiller à ce qu'ils soient solides et durables, et de favoriser la cohérence entre les structures de gouvernance à mesure qu'elles évoluent pour relever de nouveaux défis.

Il convient d'être vigilant face aux risques de fragmentation nouveaux ou en développement. La coopération et la coordination à l'échelle mondiale seront essentielles pour identifier les signes avant-coureurs, cartographier l'impact des politiques et autres développements, et se préparer à faire face aux implications de ces changements. Une approche multipartite est la mieux adaptée pour évaluer et surveiller les conséquences involontaires potentielles des mesures qui affectent Internet et pour proposer des alternatives efficaces qui évitent ou atténuent les risques de fragmentation. Le Réseau politique IGF sur la fragmentation d'Internet est un exemple positif de cette approche.

L'ouverture d'Internet permet de favoriser l'exercice des droits de l'homme des internautes, de promouvoir la concurrence et l'égalité des chances et de préserver la nature générative d'internet de pair à pair. Les débats sur la neutralité du réseau et la gestion non discriminatoire du trafic ne sont qu'une partie des discussions plus larges dans ce contexte. La neutralité du réseau est nécessaire mais pas suffisante pour garantir l'ouverture d'Internet. L'interopérabilité des infrastructures et des données, ainsi que la neutralité des plateformes et des appareils, sont également nécessaires.

Si les approches juridiques, réglementaires et politiques diffèrent dans le monde, une coordination active au-delà des frontières internationales est essentielle pour garantir que les approches fragmentées ne menacent pas la portée mondiale et l'interopérabilité d'Internet. Le maintien de l'intégrité du réseau mondial nécessite une collaboration réglementaire internationale et un consensus sur les principes de base.

De nombreux facteurs différents affectent l'expérience d'Internet dans différentes juridictions, notamment des contextes sociaux, démographiques, économiques, culturels et politiques différents, ainsi que des questions techniques et d'infrastructure. La poursuite de certaines formes de gouvernance numérique au niveau national peut accroître le risque de fragmentation au niveau technique de l'Internet. Toutefois, les cadres réglementaires doivent également tenir compte des exigences différentes selon les contextes et suivre le rythme de l'évolution rapide des technologies et des services.

Il est nécessaire de renforcer le partage des connaissances et des informations entre les parties prenantes, d'approfondir le débat sur la cyber-diplomatie en tant que phénomène évolutif et d'examiner les possibilités d'interventions appropriées. Les organismes de normalisation devraient continuer à améliorer la sensibilisation et l'engagement avec les parties prenantes et à améliorer la compréhension entre les communautés politiques et techniques. Les décisions techniques qui ont des implications politiques devraient être discutées par les organismes de normalisation avec la participation directe de toutes les parties prenantes concernées.

Gouvernance des données et protection de la vie privée

Thème

Les données sont la ressource clé de l'ère numérique mondialisée. Le mouvement des données stimule les économies, tandis que l'analyse des données, y compris l'analyse des mégadonnées, a été à la base d'innovations remarquables dans toutes les disciplines, de la finance à la santé en passant par l'application de la loi.

Mais l'utilisation généralisée, le flux routinier à travers les frontières et la fongibilité des données restent des sujets sensibles et non résolus. En tant qu'actif commercial transnational, les flux de données s'effectuent dans un environnement où il existe peu de cohérence entre les régimes juridiques nationaux où les défis en matière d'application sont importants. La confidentialité des données personnelles est trop souvent sacrifiée au cours des échanges de données, du point de collecte à l'application et au stockage, avec de graves conséquences pour la confiance et la sécurité.

Pour exploiter la promesse importante des données, économiquement et à des fins de recherche, il faut relancer les discussions autour de la gouvernance, de l'intégrité et de la protection de la vie privée des personnes.

Messages

La centralité des données

Les données sont devenues une ressource essentielle dans une ère de plus en plus numérique. Les flux de données sont cruciaux pour la coopération internationale dans de nombreux domaines, notamment la recherche scientifique, l'application de la loi et la sécurité nationale et mondiale. Les données, la sécurité des données et la protection des données sont des catalyseurs essentiels du développement durable. L'utilisation et le partage efficaces des données à l'échelle mondiale peuvent aider à surmonter les défis communs et les menaces posées par les crises en cascade telles que les pandémies et le changement climatique.

Les données peuvent générer à la fois des bénéfices et une importante valeur sociale. Toutefois, les avantages de l'économie fondée sur les données ont jusqu'à présent été inégalement répartis. De nombreuses personnes craignent de devenir principalement des fournisseurs de données plutôt que des bénéficiaires.

La relation entre ceux qui génèrent et ceux qui utilisent les données est importante. La pauvreté des données est un problème important, en particulier dans les communautés locales et parmi les segments vulnérables de la population. Le manque de confidentialité des données et leur protection inadéquate sapent la confiance dans la gestion des données. Il est important de développer la culture et les capacités en matière de données à tous les niveaux de gouvernement dans les programmes d'enseignement et pour le grand public.

La gestion et la gouvernance des données sont des questions complexes dans la gouvernance nationale et internationale. L'évolution des données - y compris l'analyse des mégadonnées, les innovations dans l'intelligence artificielle et l'apprentissage automatique, et les innovations dans les dimensions des politiques publiques et les ODD - démontrent la nécessité d'une prise en compte appropriée des impacts politiques, économiques et sociaux et d'une approche nuancée des interventions politiques.

Les institutions gouvernementales et réglementaires ont besoin de l'infrastructure et des capacités nécessaires pour mettre en œuvre des cadres nationaux de gouvernance des données efficaces et intégrés. Les développeurs d'applications ont la responsabilité d'assurer une conception éthique et sûre.

Confidentialité des données et justice des données

La confidentialité des données n'est pas une question de commodité ou de bonnes pratiques, mais des droits de l'homme. Outre les droits à la vie privée, à l'égalité de traitement et à la non--discrimination, elle affecte l'accès à d'autres droits de l'homme tels que ceux à la santé, à l'éducation et aux services publics, ainsi qu'aux droits démocratiques tels que la liberté d'expression et d'association. Les lois sur la protection de la vie privée doivent être substantielles, fondées sur des preuves claires. Les personnes concernées doivent être en mesure de comprendre clairement leurs implications.

Les flux et l'échange de données doivent se faire sans compromettre la confidentialité des données. La confidentialité des données personnelles a souvent été sacrifiée dans les processus d'échange entre la collecte d'informations et leur application, avec des risques intentionnels et non intentionnels pour la confiance et la sécurité.

L'accès et l'utilisation d'Internet ne devraient pas dépendre du suivi des données : les utilisateurs devraient avoir le droit de choisir la mesure dans laquelle leurs informations sont partagées, y compris les informations dérivées de leur activité en ligne. Les données personnelles ne doivent pas être exportées vers des juridictions qui n'offrent pas les garanties adéquates.

Les politiques doivent aller au delà de la protection des données pour aboutir à une justice des données, dans laquelle les personnes ont le choix de l'utilisation de leurs données personnelles et peuvent partager les retours et les avantages de l'innovation apportés par les ensembles de données dérivés de leurs données. Les protections de la vie privée devraient ainsi contribuer à une économie numérique plus sûre et plus prospère.

Les gouvernements et les régulateurs devraient veiller à ce que les données personnelles soient protégées, en identifiant les responsabilités différenciées des différentes parties prenantes et sans imposer de charges ou de responsabilités excessives aux utilisateurs individuels. Les politiques de gouvernance des données doivent être élaborées avec la

contribution de plusieurs parties prenantes pour garantir que les défis de mise en œuvre sont compris.

La confidentialité et la protection des données sont particulièrement essentielles à la gouvernance de l'intelligence artificielle et de l'apprentissage automatique. Toutes les parties prenantes de la chaîne d'approvisionnement de l'IA ont un rôle à jouer dans le respect des droits à la vie privée.

Il est nécessaire de disposer d'organes de contrôle indépendants dotés de ressources appropriées. Les bureaux de protection des données devraient avoir pour mandat de gérer l'enregistrement des données, de fournir des conseils, de mener des enquêtes et de résoudre les plaintes des personnes concernées.

Gouvernance des données

Les questions relatives à la gouvernance des données ne doivent pas être traitées en silos ou isolément de leurs impacts.

Le paysage actuel de la gouvernance des données est un patchwork fragmenté de règles nationales, régionales et internationales impliquant des responsabilités pour les gouvernements nationaux, les entreprises du secteur privé et les particuliers.

Une plus grande cohérence est nécessaire au niveau mondial pour parvenir à une approche équilibrée dans laquelle les données sont au service des personnes et de la planète. La législation et les cadres réglementaires existants aux niveaux national, régional et international sont souvent insuffisants et ne parviennent pas à suivre le rythme de l'évolution des technologies et des applications. Ils doivent viser à garantir des normes de sécurité élevées pour les entreprises et autres organisations responsables de la détention de données.

En raison de la diversité des contextes et des défis, des histoires, des cultures, des traditions juridiques et des structures réglementaires, il ne peut y avoir un ensemble rigide de règles pour tous. Différentes personnes et organisations interprètent également des approches largement similaires de différentes manières. Cependant, si les pays et les régions doivent développer leurs approches personnalisées de la gouvernance des données, il doit y avoir cohérence et interopérabilité pour faciliter les flux de données et garantir des conditions de concurrence équitables.

La transparence, la participation et la responsabilité sont des aspects importants d'une bonne gouvernance des données.

Les éléments importants à porendre en compte dans la gouvernance des données sont notamment les suivants (liste non exhaustive) : les normes et la classification des données ; partage, échange et interopérabilité des données ; la sécurité des données et la confidentialité des données ; infrastructures de données ; données et identité numérique ; la justice et l'équité des données ; traçabilité, transparence et explicabilité des données ; minimisation et limitation

des données ; exactitude et qualité des données ; biais de données, marginalisation et discrimination ; le cycle de vie des données, la spécificité et la conservation de l'utilisation des données ; la responsabilité des données et l'éthique des données ; dommages aux données, sécurité des données et protection des données.

Dans ce contexte, de nombreuses parties prenantes ont un rôle à jouer et devraient exercer leur pouvoir et influence pour promouvoir une gouvernance des données efficace, notamment les régulateurs, les chercheurs, les organismes de normalisation, les organisations de consommateurs et les utilisateurs finaux. Des politiques de gouvernance des données devraient être élaborées avec la contribution de cette communauté multipartite qui possède une expertise à la fois dans les débats juridiques sur la confidentialité et les défis du « monde réel » de la mise en œuvre de solutions efficaces de confidentialité des données.

Les économies en développement doivent renforcer leurs capacités institutionnelles pour gouverner, utiliser et gérer les données de manière globale, objective et fondée sur des données probantes, notamment par le biais de la coopération régionale et mondiale. Pour ce faire, il faut mieux comprendre les capacités institutionnelles des responsables gouvernementaux et des parties prenantes.

Flux de données transfrontaliers

Les flux de données transfrontaliers sont essentiels à de nombreux aspects du commerce électronique et du commerce numérique. Une gestion efficace du commerce intra-régional et de la chaîne d'approvisionnement repose sur la fluidité des flux de données ainsi que des biens, des services et des capitaux. Cependant, tous ces éléments nécessitent des considérations transversales complexes en matière de réglementation, de convergence, d'harmonisation des cadres juridiques, la gouvernance de l'internet, la réforme de la politique en matière de technologies de l'information et de la communication et l'infrastructure régionale stratégique

Les accords commerciaux multilatéraux, régionaux et bilatéraux actuels sont insuffisants pour les flux de données transfrontaliers actuels et futurs. Ceux-ci opèrent dans un environnement largement non réglementé avec peu de cohérence entre les régimes juridiques nationaux. Les approches diffèrent et sont contextuelles, générant des obstacles au commerce, alors que de nombreux pays ne disposent pas actuellement d'une législation ou d'une capacité d'application adéquates. Il y a un besoin croissant de développer et d'harmoniser des mesures de gestion des flux transfrontaliers qui facilitent le développement et la création de valeur économique, dans différents contextes, tout en respectant la souveraineté nationale et la vie privée des utilisateurs.

Permettre la sûreté, la sécurité et la responsabilité

Thème

La sécurité d'Internet est menacée à plusieurs égards. La cybersécurité traditionnelle concerne la protection des réseaux, des appareils et des données contre les accès non autorisés ou les utilisations criminelles. Elle englobe le problème permanent des cyberattaques, qu'elles soient perpétrées par des individus ou sanctionnées par l'État, et que les cibles soient civiles, commerciales ou gouvernementales. Des facteurs tels que l'absence d'accords de cybersécurité larges et contraignants et des réseaux insuffisamment sécurisés contribuent à la perte de possibilités de tirer pleinement parti des avantages économiques des technologies numériques, en particulier pour les pays en développement.

Les questions de sûreté, de sécurité et de responsabilité sont multiples, et comprennent des problèmes distincts concernant l'infrastructure, les services, le contenu et d'autres aspects d'Internet. Notre compréhension de la sûreté et de la sécurité, par exemple, inclut désormais les défis persistants de la mauvaise information et de la désinformation en ligne. Ces dernières années, ces facteurs ont aggravé les effets de la pandémie de COVID-19 et ont fait poser des risques importants sur les processus électoraux dans le monde. Cela a souligné la nécessité d'une responsabilité et de critères clairs pour les contenus trompeurs.

Le concept de « sécurité » peut être encore élargi à la sécurité environnementale, compte tenu des efforts visant à « écologiser » l'Internet et à réduire les émissions de carbone liées à la consommation numérique. La nécessité de traiter l'impact environnemental de la numérisation est un thème de plus en plus important dans les discussions de l'IGF.

Messages

Le rôle des décideurs politiques

La cybersécurité doit être considérée comme un défi central pour la politique Internet. Les considérations de confiance et de sécurité devraient faire partie intégrante du développement d'un accès sûr et sécurisé, y compris le respect des droits de l'homme, l'ouverture et la transparence dans l'élaboration des politiques, et une approche multipartite qui sert les intérêts des utilisateurs finaux.

La garantie de la cybersécurité et la prévention de la cybercriminalité sont deux domaines politiques importants qui nécessitent une attention sérieuse et le développement d'une expertise. Leur objectif diffère toutefois, et l'approche requise pour chacun est différente. Une approche efficace dans l'un ne le sera pas dans l'autre sans adaptation et reformulation.

Les problèmes de cybersécurité et de cybercriminalité ont des dimensions inter organisationnelles et transfrontalières. Pour y faire face, il faut :

a) des approches pangouvernementales et pansociétales qui incluent des partenariats solides et des efforts coordonnés, impliquant les parlements, les régulateurs et autres autorités et agences gouvernementales compétentes, le secteur privé, la communauté technique, les universités et la société civile ; et

b) une coopération régionale et internationale efficiente et efficace qui soit intergouvernementale, multilatérale et multipartite.

Les gouvernements, le secteur privé et la communauté technique doivent veiller à éviter d'adopter des lois sur la cybercriminalité et d'établir des normes qui affectent négativement le travail des défenseurs de la cybersécurité. Ils devraient inviter toutes les parties prenantes à participer à l'élaboration des politiques et faciliter l'interaction et le partage d'expérience et d'expertise entre leurs différentes.groupes

La société civile devrait participer aux discussions sur la cybercriminalité et la cybersécurité. Pour le faire efficacement, les parties prenantes de la société civile doivent se former aux différentes approches et questions en jeu, et travailler avec d'autres parties prenantes pour rassembler les informations et les ressources nécessaires pour participer pleinement à l'élaboration des politiques.

La cyber-sécurité

La communauté internationale devrait explorer des moyens pratiques d'intégrer le renforcement des capacités en matière de cybersécurité dans les efforts de développement numérique plus larges. Les tensions entre le désir de faire progresser la transformation numérique et la nécessité de permettre une cybersécurité efficace posent des problèmes pour permettre un environnement en ligne sûr et sécurisé et atteindre les objectifs de développement durable. S'il est nécessaire d'en faire plus pour accroître la résilience de l'infrastructure numérique, ce n’est pas suffisant. Il est grand temps de traduire les accords internationaux existants en actions réalisables.

Les normes permettant d’assurer la cybersécurité sont essentielles pour un Internet ouvert, sûr et résilient qui permet le progrès social et la croissance économique, et sont particulièrement importantes pour protéger ceux qui ne sont pas encore connectés. De telles normes ont été élaborées, mais leur utilisation doit se développer de manière significative pour qu'elles soient pleinement efficaces. Les Nations Unies pourraient aider à accélérer l'adoption mondiale des normes clés en incluant leur promotion dans le Pacte numérique mondial, en soutenant le plaidoyer et le renforcement des capacités et en encourageant les initiatives pour tester et surveiller le déploiement. La sensibilisation précoce et le renforcement des capacités sur les normes ne doivent pas être oubliés en tant que priorités dans des domaines où beaucoup doivent encore se connecter et où Internet se développe.

Il faut faire davantage pour améliorer la sensibilisation des décideurs politiques nationaux et des autres parties prenantes aux défis de la cybersécurité et aux normes et principes internationaux. Il s'agit notamment de sensibiliser et de renforcer les capacités concernant les liens entre le développement durable et la cybersécurité, en réunissant diverses parties prenantes pour mobiliser une gestion efficace, durable et inclusive de la coopération

internationale pour la cyber résilience. Un certain nombre d'initiatives internationales ont été mises en place pour soutenir cela. Les opportunités de financement de la cyber résilience doivent également être abordées par les agences de financement et les autres parties prenantes.

Les normes de cybersécurité doivent faire une différence dans les expériences personnelles passées, présentes et futures des internautes. Dans ce contexte, l'écoute des expériences des victimes individuelles et organisationnelles d'attaques de cybersécurité, et celles des premiers intervenants, est importante, en particulier pour l'élaboration de nouvelles normes.

Cybercriminalité

La cybercriminalité représente une menace croissante pour de nombreux internautes. Les réglementations de lutte contre la cybercriminalité doivent tenir compte de la taille, de la capacité et des ressources des plateformes. Les obligations légales doivent tenir compte de la diversité du secteur technique et reconnaître les besoins et les circonstances des petites entreprises dans le respect de leurs obligations légales, par exemple dans la lutte contre l'exploitation de leurs services par des terroristes et extrémistes violents.

Les gouvernements et les décideurs politiques doivent veiller à ce que les réponses juridiques à l'utilisation criminelle et terroriste d'Internet préservent à la fois l'État de droit et les droits de l'homme, en tenant pleinement compte de la liberté d'expression et en garantissant la transparence et la responsabilité dans la mise en œuvre des mesures contre la cybercriminalité.

Contenu et désinformation

La désinformation peut et doit être traitée par des mécanismes qui répondent aux risques encourus par les individus et les sociétés tout en protégeant la liberté d'expression, le pluralisme et le processus démocratique. Le soutien au journalisme et aux médias professionnels joue un rôle important dans les efforts de lutte contre la désinformation, y compris l'engagement envers les normes journalistiques établies.

Les compétences en matière de médias et d'éducation numérique permettent aux citoyens d'avoir une vision plus critique du contenu ou des informations qu'ils rencontrent, aidant à identifier la désinformation et la mésinformation et à renforcer la participation démocratique. L'éducation à la culture numérique peut contribuer à accroître la sensibilisation à la sécurité en ligne, en particulier pour les personnes et les communautés les plus vulnérables. Les initiatives doivent être sensibles aux besoins et aux risques associés aux différents groupes démographiques. Différentes approches pour les jeunes et les générations plus âgées, par exemple, doivent répondre à différents modes d'utilisation.

Les programmes d'enseignement devraient inclure des compétences en matière de culture numérique aidant les enfants à être en sécurité en ligne. Les initiatives doivent impliquer les parents, les enseignants et les tuteurs. Les législateurs et les plateformes numériques

devraient assumer la responsabilité d'assurer la sécurité des enfants dans un cadre des droits de l'enfant en ligne conforme aux accords internationaux sur les droits, y compris la Convention des Nations Unies relative aux droits de l'enfant.

Le système des noms de domaine a une capacité technique limitée dans ce contexte. Un dialogue continu avec les parties prenantes devrait clarifier quand et comment il peut être utilisé pour remédier à des problèmes de contenu spécifiques, et devrait renforcer les normes de procédure régulière.

Le cryptage joue un rôle important dans la construction d'un Internet ouvert, sûr et démocratique et aide les utilisateurs à assurer leur sécurité, leur confidentialité et leur liberté d'expression. Les questions relatives à l'application de la loi et à la capacité de l'utilisateur à gérer l'accès dans des domaines tels que la protection de l'enfance doivent être abordées.

Les problèmes de traduction constituent des obstacles importants qui peuvent empêcher les utilisateurs finaux de s’engager de manière significative après les normes et directives communautaires des plateformes. Les termes clés sont parfois mal traduits, ce qui entraîne des interprétations ambiguës.

Pour permettre aux plateformes et aux utilisateurs de comprendre ce que l'on attend d'eux, il est important de s'engager auprès des différentes communautés linguistiques afin d'améliorer la précision et la pertinence des traductions, y compris la communication de concepts sans équivalents directs dans différentes langues

Aborder les technologies avancées, y compris les Intelligences Artificielles (IA)

Thème

Les technologies numériques avancées façonnent de plus en plus notre économie et notre société, y compris les systèmes d'intelligence artificielle (IA) qui guident nos expériences en ligne, alimentent les appareils intelligents et influencent nos propres décisions et celles que les autres prennent à notre sujet, ainsi que les applications de la robotique et d'internet des objets qui sont déployés dans des domaines aussi divers que la fabrication, la santé et l'agriculture. Au-delà de leurs promesses, ces technologies comportent des écueils. La prise de décision algorithmique, par exemple, peut entraîner des préjugés, de la discrimination, des stéréotypes et des inégalités sociales plus larges, tandis que les systèmes basés sur l'IA peuvent présenter des risques pour la sécurité humaine et les droits de l'homme. Les dispositifs de l'internet des objets présentent des défis en matière de confidentialité et de cybersécurité.La réalité augmentée et virtuelle soulève des questions de sécurité publique, de protection des données et de protection des consommateurs.

Tirer parti des opportunités offertes par les technologies de pointe, tout en relevant les défis et les risques qui y sont liés, est une tâche qu'aucun acteur ne peut assumer seul. Le dialogue et la coopération multipartites - impliquant les gouvernements, les organisations intergouvernementales, les entreprises technologiques, la société civile et d'autres parties prenantes - sont nécessaires pour garantir que ces technologies soient développées et déployées d'une manière centrée sur l'humain et respectueuse des droits de l'homme.

Messages

Gouvernance

Les technologies avancées, y compris l'intelligence artificielle, doivent être conçues de manière à respecter l'état de droit, les droits de l'homme, les valeurs démocratiques et la diversité, et comporter des garanties appropriées.

Elles devraient profiter aux personnes et à la planète en stimulant la croissance inclusive, le développement durable et le bien-être. Les mécanismes de surveillance et d'application doivent suivre des principes et des règles, les acteurs de l'IA étant tenus responsables de tout dommage causé.

L'hypothèse selon laquelle la technologie améliore nécessairement l'égalité est erronée. Ceux qui conçoivent les technologies d'apprentissage automatique et les données utilisées pour former les applications d'IA ne sont souvent pas représentatifs de leurs sociétés. Les technologies peuvent amplifier les inégalités et nuire, en particulier aux groupes vulnérables et marginalisés.

Les sociétés doivent s'adapter à la transformation qu'entraîne l'IA en modifiant leur cadre de coopération et leur modèle de gouvernance.

La construction d'une société intelligente centrée sur l'humain nécessite la pleine coopération du gouvernement, des entreprises, des organisations sociales et des universités. Un contrôle humain continu reste essentiel pour s'assurer que les algorithmes n'aboutissent pas à des résultats indésirables ou incontrôlés. Pour y parvenir, il est essentiel de briser les silos entre les ingénieurs et les experts en politiques.

Un accord mondial sur les normes d'IA ne peut être obtenu par un processus simple. Bien qu'il existe certaines normes, il s'agit principalement de lois souples plutôt que de principes contraignants. L'élaboration de normes mondiales significatives nécessitera la participation effective de tous les pays, y compris les pays en développement et les pays développés, et les contributions des initiatives régionales, ainsi que l'engagement de toutes les parties prenantes.

Le renforcement des capacités est important dans les efforts visant à aborder les technologies avancées. Des politiques d'alphabétisation en IA, de développement des compétences et de ressources linguistiques pour les langues minoritaires sont nécessaires afin de formuler une approche véritablement mondiale des technologies de pointe.

Confiance, sécurité et confidentialité

Les cadres réglementaires devraient inclure des principes pour aider les médias sociaux et les autres plateformes à remplir leurs obligations de diligence raisonnable pour la gestion des contenus susceptibles de porter atteinte à la démocratie et aux droits de l'homme. Les cadres devraient contribuer à la conversation mondiale sur la modération du contenu en ligne afin de responsabiliser les utilisateurs, y compris les groupes les plus vulnérables et les utilisateurs de langues minoritaires. Les technologies émergentes telles que l'informatique affective, qui examinent comment les ordinateurs peuvent reconnaître, interpréter et simuler les émotions humaines, nécessitent une évaluation éthique approfondie. La transparence dans le fonctionnement et le reporting des systèmes algorithmiques est essentielle pour les droits de l'homme.

L'IA facilite l'observation et l'analyse constantes des données pour personnaliser et cibler le contenu et la publicité. Les expériences en ligne personnalisées qui en résultent risquent de désagréger les espaces d'information en ligne et de limiter l'exposition des individus à la diversité des informations. Le manque de pluralisme de l'information peut favoriser la manipulation et la tromperie - aggravant les inégalités, sapant les débats démocratiques et favorisant potentiellement l'autoritarisme numérique, la haine et la violence.

Les parties prenantes des communautés techniques et non techniques doivent partager leur expertise et collaborer au développement de principes, de lignes directrices et de normes suffisamment flexibles pour être appliqués dans divers contextes et pour favoriser la confiance dans les systèmes d'IA.

Il est important de reconnaître et de respecter les différents contextes institutionnels et culturels des divers pays et communautés, ainsi que de promouvoir l'inclusivité et de permettre la coopération internationale en IA.

Droits et modération du contenu

Il est essentiel que les politiques de gouvernance des contenus par les plateformes en ligne, et leur application, soient conformes aux normes internationales des droits de l'homme. L'intelligence artificielle et les technologies d'apprentissage automatique sont déjà utilisées pour décider si le contenu doit être publié ou supprimé, quel contenu est prioritaire et à qui il est diffusé. Ces outils jouent un rôle important dans le façonnement du discours politique et public d'une manière qui affecte à la fois les droits de l'homme individuels et collectifs, y compris les droits sociaux, économiques et culturels et les droits à la paix et à la sécurité mondiales. Ils sont souvent déployés avec peu ou pas de transparence, de responsabilité ou de contrôle public. Il convient de remédier à cette situation.

Les mêmes technologies qui peuvent être utilisées pour promouvoir les droits de l'homme peuvent également être utilisées pour la surveillance, pour promouvoir des programmes violents et d'autres façons qui enfreignent ces droits. Les conséquences imprévues de la gestion automatisée du contenu peuvent être particulièrement préjudiciables en temps de conflit ou de crise lorsqu'elles peuvent faire taire les voix critiques à un moment où elles sont les plus cruciales.

Les normes techniques jouent un rôle important en permettant le développement et l'amélioration de la valeur des technologies numériques et des infrastructures, services, protocoles, applications et dispositifs connexes.

Ils peuvent aussi avoir de fortes répercussions sur les droits de l'homme. Pourtant, les processus d'élaboration des normes techniques au sein des organisations ne prennent pas pleinement en compte des préoccupations relatives aux droits de l'homme. Ces processus sont souvent opaques, complexes et lourds en ressources pour que la société civile et les autres parties prenantes puissent y accéder et les suivre systématiquement. Cela devrait être résolu.

Примечание: этот перевод доступен благодаря добровольному взносу Центр глобального ИТ-сотрудничества. IGF ему благодарен.

ФОРУМ ПО ВОПРОСАМ УПРАВЛЕНИЯ ИНТЕРНЕТОМ 2022

Аддис-Абебские Послания ФУИ

Настоящий документ[1] представляет собой резюме вопросов, которые были подняты в ходе 17-й ежегодной встречи Форума по вопросам управления Интернетом, проходившей в Аддис-Абебе с 28 ноября по 2 декабря 2022 года.

Взгляды и мнения, представленные в документе, не обязательно совпадают с мнением Секретариата Организации Объединенных Наций. Использованные условные обозначения и термины могут не соответствовать практике Организации Объединенных Наций и не означают выражения какого бы то ни было мнения со стороны Организации.

В рамках обсуждений, проходивших на ФУИ 2022, основное внимание было уделено пяти ключевым темам, которые охватывает Глобальный цифровой договор (ГЦД). Предложение о его разработке было выдвинуто в докладе Генерального секретаря Организации Объединенных Наций «Наша общая повестка дня», опубликованном в 2021 году и приуроченном к 75-летнему юбилею Организации Объединенных Наций, и будет рассматриваться Генеральной Ассамблеей ООН в 2023 году. Это станет одной из составляющих подготовки к Саммиту будущего, который планируется провести в 2024 году.

В ходе ФУИ были рассмотрены следующие темы:

- **подключение всех людей к Интернету и защита прав человека;**
- **недопущение фрагментации Интернета;**
- **управление данными и защита приватности;**
- **обеспечение безопасности, защиты и ответственности;**
- **передовые технологии, включая искусственный интеллект (ИИ).**

Как платформа с участием многих заинтересованных сторон, ФУИ выразил поддержку предложения Генерального секретаря о создании Глобального цифрового договора. Послания, изложенные в настоящем документе, представляют собой вклад со стороны ФУИ в разработку Глобального цифрового договора. Динамичные коалиции ФУИ, которые уже занимаются решением определенных проблем и рассмотрением возможностей, актуальных с учетом предложенных тематических направлений ГЦД, также заявили о своем намерении участвовать как в подготовке, так и в осуществлении процессов ООН, связанных с ГЦД.

[1] Послание, сформулированное в ходе 17-й ежегодной встречи ФУИ. Оно выносилось на публичное обсуждение, в результате которого была собрана обратная связь, впоследствии учтенная в окончательной редакции документа.

Подключение всех людей к Интернету и защита прав человека

Тема

Первым принципом Глобального цифрового договора (ГЦД), создание которого было предложено Генеральным секретарем ООН, является «Подключение всех людей и всех школ к Интернету». Данный принцип основан на том, что подключение и доступ к Интернету стали необходимыми условиями обеспечения средств к существованию, безопасности и образования людей по всему миру, а также на том, что наличие Интернета в школах предусматривает создание ключевых точек доступа, делает информационные ресурсы доступными для всех обучающихся и способствует развитию цифровой грамотности с самого раннего возраста. И все же 2,7 миллиарда человек до сих пор не подключены к Интернету, причем в наиболее неблагоприятном положении находятся жители наименее развитых стран и сельской местности.

Полноценный доступ не ограничивается одним лишь подключением к Интернету и неразрывно связан с защитой прав человека в онлайн-среде. Обеспечение доступа, способствующее росту благополучия обществ, должно опираться на соблюдение прав человека. В числе прочего это предполагает обеспечение возможности свободного выражения мнения пользователями, отсутствие препятствий к политическому и демократическому участию, обеспечение возможности пользования Интернетом всеми людьми без страха подвергнуться преследованию или дискриминации, а также обеспечение реализации прав детей и применения соответствующих мер безопасности, равносильных мерам, существующим в офлайн-пространстве. Интернет является активатором реализации прав и в то же время должен легко инкорпорировать ранее установленные права человека в свою работу, поскольку с течением времени наша цифровая зависимость в части осуществления рутинных функций повышается, а границы между онлайн- и офлайн-средой становятся менее значимыми.

Послания

Цифровое неравенство

- **Цифровой неравенство различных стран и регионов остается мощным фактором, влияющим на национальное и международное развитие**, в том числе на процесс достижения Целей устойчивого развития (ЦУР). Особую обеспокоенность вызывает положение наименее развитых стран и малых островных развивающихся государств (МОРАГ). Цифровое неравенство связано не только с неравномерным подключением к Интернету. Наряду с подключением к Интернету полноценный доступ включает в себя факторы доступности, приемлемости в ценовом отношении, наличия контента, услуг, развитие цифровой грамотности и других навыков. Приемлемость в ценовом отношении представляет собой особую проблему для многих людей, главным образом на Глобальном Юге.

- **Пандемия COVID-19 выявила роль Интернета в обеспечении личной и экономической устойчивости и в то же время продемонстрировала, насколько неблагоприятным является положение тех, кто не подключен к Интернету или не имеет полноценного доступа к нему**, а также потенциально усугубила прочие формы неравенства. Для того, чтобы установить степень влияния и последствия введения мер,

связанных с COVID-19 и касающихся прав человека, доступа к Интернету и его использования, понадобится время.

- **Во всех сообществах существуют группы, которые сталкиваются с более значительными проявлениями цифрового неравенства, чем остальные, или не имеют полноценного доступа к Интернету.** В рамках многих сообществ число женщин, подключенных к Интернету и использующих его, уступает числу мужчин. Особенно неблагоприятным в рассматриваемом контексте является положение уязвимых и маргинализированных сообществ: многие люди испытывают разного рода лишения, обусловленные сочетанием факторов, связанных с возрастом, полом, этнической принадлежностью, языком, социальным положением и так далее. Целевые инициативы в сфере инфраструктуры, устройств и сервисов могут поспособствовать повышению скорости доступа для групп населения, в меньшей степени подключенных к Интернету, но должны сопровождаться мерами, направленными на устранение иных препятствий к обеспечению полноценного доступа, и быть сопряженными с другими мерами по преодолению неравенства и дискриминации.

- **Устойчивость и безопасность цифровой инфраструктуры является ключевым фактором цифровой интеграции. Правительства должны обеспечивать защиту и продвижение требуемой инфраструктуры, в том числе электросетей, автономных энергосистем и сетей связи.** На некоторых территориях Африки и других континентов ввиду значительных расстояний между группами населения, проживающими в сельских и отдаленных районах, в том числе в МОРАГ, обеспечение соединений «последней мили» оказывается коммерчески непривлекательным для частного сектора. Подключение к Интернету, поддержка его скорости и надежности являются важными аспектами создания инфраструктуры. Повышение пропускной способности инфраструктуры и решение проблемы региональных диспропорций, особенно в сельской местности, потребует времени и инвестиций.

- **Для обеспечения и предоставления доступа важно сотрудничество между группами заинтересованных сторон. Правительства и различные заинтересованные стороны, действующие в рамках партнерских отношений, должны поддерживать учреждение и работу эффективных регуляторных органов и нормативно-правовых баз, решать существующие проблемы на коммерчески непривлекательных территориях и поощрять использование инновационных подходов к подключению к Интернету**, в том числе связанных с общественными сетями, надлежащим распределением радиочастотного спектра, доступом, обеспечиваемым низкоорбитальными спутниками, и наличием местного контента, включая контент на местных языках.

Гендерное цифровое неравенство и права женщин

- **Мужчины со значительно большей вероятностью находятся онлайн или имеют доступ к мобильному Интернету, чем женщины**. Гендерный цифровой разрыв особенно велик в наименее развитых странах. Задача 9с ЦУР, направленная на обеспечение всеобщего и приемлемого в ценовом отношении доступа к Интернету, не может быть решена, пока не преодолен данный разрыв.

- **Угроза насилия и преследования сдерживает присутствие женщин в онлайн-пространстве**. Гендерно обусловленное насилие в Интернете является важным фактором, поддерживающим и усиливающим гендерное неравенство в части доступа к Интернету и пользования Интернетом, и приводит к тому, что некоторые женщины покидают онлайн-пространство. Роль технологических сервисов и платформ в распространении гендерно обусловленного насилия должна быть признана и принята во внимание. Необходимо поддерживать женщин, предоставляя руководство к сопротивлению гендерно обусловленному насилию в Интернете и возмещению причиненного ущерба, в том числе с помощью горячих линий, функционирующих на базе сообществ. Ресурсы, правила сообществ и сервисы для сбора жалоб, имеющиеся на платформах, должны быть доступны на местных языках.

- **Понятия «гендерное равенство», «интеграция», «защита женщин и обеспечение их прав» должны быть включены в Глобальный цифровой договор** (ГЦД), в соответствии с предложением структуры «ООН-Женщины».

Права человека и цифровое развитие

- **Всеобщий доступ должен быть обеспечен с учетом прав человека, так чтобы Интернет стал доступным и безопасным для всех**. К данным правам относятся право на свободу выражения мнения, право на свободу объединения с другими, право на неприкосновенность частной жизни и другие гражданские, политические, экономические, социальные и культурные права, изложенные в международных стандартах в области прав человека. Структуры, занимающиеся вопросами управления Интернетом и разработкой цифровых технологий, должны соблюдать данные права. Организации, разрабатывающие стандарты, должны рассмотреть возможность приглашения экспертов в области прав человека в Интернете из всех заинтересованных сообществ к участию в своей работе.

- **Прозрачность, ответственность и должная осмотрительность в части обеспечения прав человека входят в зону ответственности всех заинтересованных групп, включая межправительственные и международные организации, правительства, частный сектор, техническое сообщество и гражданское общество**. Это потребует соответствия практик ведения бизнеса цифровым правам, а также сотрудничества заинтересованных сторон, направленного на решение проблем, связанных с дезинформацией, дискриминацией и разжиганием ненависти, особенно в периоды политической нестабильности, выборов и передачи власти.

- **Доступ в Интернет играет ключевую роль в обеспечении доступа к информации и возможности выражения мнений.** Правительствам следует избегать отключения Интернета, поскольку оно имеет негативные последствия для реализации прав человека и достижения экономического благополучия. Социальные медиа и технологические компании должны поддерживать усилия граждан по защите своих прав и интересов, связанные с отключением Интернета.

- **Важно улучшать мониторинг соблюдения цифровых прав и процесс их осуществления.** Был сделан ряд предложений по созданию международных

механизмов в рамках системы ООН с привлечением многих заинтересованных сторон. Данные механизмы могли бы дополнить и развить существующие механизмы, включая как те из них, которые связаны с цифровым развитием и правами, так и те, которые действуют в иных сферах, например в сфере изменения климата.

- **Интернет обеспечивает возможности для расширения прав на образование** в рамках более общей стратегии улучшения образования. Качество образования на Глобальном Юге, особенно во время пандемии, пострадало вследствие отсутствия подключения к Интернету. Несмотря на то что ИКТ могут обеспечить обучающимся полноценный доступ, различия в глобальных и местных темпах внедрения технологий обострили неравенства, существовавшие до пандемии. Опыт, полученный во время пандемии, может быть использован для повышения эффективности использования цифровых ресурсов в будущем.

- **Необходимо предпринимать усилия по содействию малому и местному бизнесу в получении максимальной выгоды от пользования Интернетом**. Уровень применения цифровых инструментов малыми и средними предприятиями существенно вырос с 2020 года, однако микропредприятия по-прежнему сталкиваются со значительными трудностями при попытках провести цифровую трансформацию бизнес-процессов.

- **Изменения на рынке труда, связанные с функционированием онлайн-платформ, предоставляют возможности для создания рабочих мест и повышения их качества и одновременно служат причиной возникновения соответствующих трудностей**, особенно для женщин, которые составляют бóльшую долю рабочей силы в неформальной экономике, чем мужчины, в большинстве стран. Во многих случаях недостаточная профессиональная подготовка остается барьером, препятствующим тому, чтобы человек в полной мере использовал свой трудовой потенциал.

- **Необходимо развивать цифровые компетенции и адаптировать методики преподавания, обучения и подготовки к новым парадигмам** образования и трудоустройства. Важно выявить и преодолеть разрыв между потребностями промышленности, с одной стороны, и среднего профессионального и высшего образования – с другой.

Недопущение фрагментации Интернета

Тема

Поддержка глобального, открытого и интероперабельного (функционально совместимого) Интернета является ключевой ценностью ФУИ. Это означает, что общие технические стандарты и протоколы продолжают внедряться в целях создания сети взаимосвязанных сетей, преодолевающих границы стран и регионов, а также то, что стандарты качества контента и сервисов находятся в соответствии с правами человека и принципом верховенства закона. Призыв к применению нормативно-правовой базы, приоритизирующей права и свободы пользователей наряду с инфраструктурной, сквозной согласованностью и через нее, нашел отражение в планах по разработке ГЦД.

Риск фрагментации является реальным и только растет. Необходимо решить проблему технической и коммерческой фрагментации, вызванной тем, что функционирование Интернета оказывается под воздействием произвольных и непроизвольных условий и практик ведения бизнеса. Фрагментация, обусловленная государственной политикой, влияющей на открытость и интероперабельность Интернета, также вызывает обеспокоенность.

Послания

Понимание существующих проблем

- **Глобальный цифровой договор предоставляет возможность для утверждения ценности Интернета как открытой инфраструктуры, состоящей из взаимосвязанных сетей, в целях соблюдения положений Устава ООН, достижения Целей устойчивого развития и реализации прав человека**. В рамках Интернет-сообщества существует общепринятое мнение о ценности глобального нефрагментированного Интернета как платформы для различных форм человеческой деятельности.

- **Вопросы, поднятые в ходе обсуждения фрагментации Интернета, отличаются своей многоаспектностью, причем разные заинтересованные стороны разными способами осмысляют и интерпретируют используемый термин**. Некоторые заинтересованные стороны особенно обеспокоены техническими и инфраструктурными аспектами Интернета, в то время как внимание других сосредоточено на вопросах государственной политики, в том числе касающихся доступа к Интернету, прав и форм влияния на пользовательский опыт. Данные вопросы рассматриваются в проекте документа, подготовленном Сетевой рабочей группой по вопросам фрагментации Интернета ФУИ. Уважение и понимание опыта различных людей и их представлений о фрагментации Интернета абсолютно необходимо, если мы стремимся к принятию эффективных и скоординированных мер.

- **Широкий спектр политических, экономических и технических факторов может способствовать фрагментации**. Однако не следует принимать за фрагментацию разнообразие и децентрализацию – глубоко положительные аспекты архитектуры и функционирования Интернета.

Устранение риска фрагментации

- **Эффективные механизмы управления, применяемые с участием многих заинтересованных сторон, играют ключевую роль в управлении глобальным нефрагментированным Интернетом**. Необходимо укреплять доверие к данным механизмам, обеспечивать их надежность и устойчивость, а также содействовать тому, чтобы действия структур управления, развивающихся и реагирующих на новые вызовы, были согласованными.

- **Необходимо проявлять бдительность по отношению к новым или формирующимся рискам фрагментации**. Глобальная кооперация и координация усилий будут крайне важны для обнаружения тревожных признаков на ранних этапах, оценки влияния политик и других разработок, а также подготовки к преодолению последствий подобных изменений. Подход с участием всех заинтересованных сторон наиболее эффективен в части оценки, измерения и отслеживания потенциальных непреднамеренных последствий мер, влияющих на функционирование Интернета, а также в части предложения действенных альтернатив, исключающих или снижающих риски фрагментации. Сетевая рабочая группа по вопросам фрагментации Интернета ФУИ является положительным примером использования описанного подхода.

- **Открытость Интернета играет важную роль в эффективной реализации прав интернет-пользователей, поощряя конкуренцию и равенство возможностей, а также сохраняя генеративный одноранговый характер Интернета**. В данном контексте споры о сетевом нейтралитете и недискриминационном управлении трафиком являются лишь частью более широкой дискуссии. Сетевой нейтралитет необходим, но недостаточен для обеспечения открытости Интернета. Интероперабельность инфраструктур и данных, нейтралитет платформ и устройств также необходимы.

- **Несмотря на то что в разных регионах мира будут использоваться разные правовые, регуляторные и программные подходы, активная координация действий, осуществляемая поверх международных границ, крайне важна для обеспечения того, чтобы фрагментированные подходы не угрожали глобальному охвату и функциональной совместимости Интернета**. Сохранение целостности глобальной сети требует международного регуляторного сотрудничества и консенсуса в отношении основных принципов.

- **На особенности использования Интернета в различных юрисдикциях влияет множество различных факторов, включая отличия социальных, демографических, экономических, культурных и политических условий, а также вопросы технического и инфраструктурного характера**. Стремление к некоторым формам цифрового управления на национальном уровне может повысить риск фрагментации Интернета на техническом уровне. Однако регуляторные базы должны учитывать требования, соответствующие различным условиям, и успевать за стремительными изменениями технологий и сервисов.

- **Необходим более широкий обмен знаниями и информацией между заинтересованными сторонами** для дальнейшего обсуждения вопросов кибердипломатии как развивающегося феномена, а также для рассмотрения возможности допустимых вмешательств. Органы по стандартизации должны

продолжить поддержку заинтересованных сторон и взаимодействие с ними и улучшать взаимопонимание между политическим и техническим сообществами. Технические решения, влекущие за собой политические последствия, должны обсуждаться органами по стандартизации с прямым участием всех затрагиваемых заинтересованных сторон.

Управление данными и защита приватности

Тема

В эпоху цифровизации и глобализации данные являются ключевым ресурсом. Движение данных управляет экономикой, а анализ данных, включая аналитику больших данных, является фундаментом удивительных инноваций в самых разных областях – от финансов до здравоохранения и правоохранительной деятельности.

Однако сложные вопросы, связанные с широким использованием данных, их привычной трансграничной передачей и взаимозаменяемостью, по-прежнему не решены. Как международный коммерческий актив, потоки данных существуют в условиях слабой согласованности национальных правовых режимов и значительных трудностей правоприменения. Конфиденциальность персональных данных слишком часто приносится в жертву при обмене данными, их сборе, применении и хранении, что имеет глубокие последствия для поддержания доверия и обеспечения безопасности.

Чтобы задействовать значительный потенциал данных в экономических и исследовательских целях, необходимо возобновить дискуссии об управлении, целостности, а также о защите приватности.

Послания

Центральная роль данных

- **В эпоху растущей цифровизации данные стали критическим ресурсом**. Потоки данных играют важнейшую роль в международной кооперации во многих областях, включая научные исследования, правоприменение, национальную и глобальную безопасность. Данные, безопасность данных и защита данных являются ключевыми элементами устойчивого развития. Путем эффективного использования данных и обмена ими на глобальном уровне можно решить общие проблемы и устранить угрозы, связанные с целым рядом кризисных явлений, таких как пандемии и изменение климата.

- **Данные одновременно приносят прибыль и имеют серьезную общественную ценность**. Однако выгоды экономики, основанной на данных, до сих пор распределялись неравномерно. Многие люди обеспокоены тем, что становятся главным образом поставщиками данных, а не выгодоприобретателями.

- **Отношения между теми, кто производит данные, и теми, кто использует данные, крайне важны**. Недостаток данных является серьезной проблемой, которая проявляется особенно остро в локальных сообществах и среди уязвимых групп населения. Отсутствие конфиденциальности данных и их недостаточная защита подрывают доверие к механизмам управления данными. Важно развивать грамотность в использовании данных и навыки работы с ними на всех уровнях государственного управления, в рамках образовательных программ и среди широких слоев населения.

- **Управление данными в широком и узком смысле представляет собой сложную проблему национальной и международной политики**. Разработки, связанные с данными, включая аналитику больших данных, инновации в области искусственного интеллекта и машинного обучения, инновации, охватывающие различные аспекты государственной политики и достижения ЦУР, сопряжены с необходимостью уделять должное внимание политическому, экономическому и социальному воздействию описанных разработок, а также осуществлять тонкое политическое вмешательство. Для внедрения эффективных национальных рамочных программ по управлению Интернетом правительству и органам регулирования необходимы соответствующие мощности и инфраструктура. Разработчики приложений обязаны обеспечить их этичное и безопасное устройство.

Конфиденциальность данных и справедливость на основе данных

- **Конфиденциальность данных – это не вопрос удобства или внедрения эффективной практики, а вопрос соблюдения прав человека**. С ней связано не только обеспечение тайны частной жизни, равного отношения и недискриминации, но и других прав человека, в том числе прав на охрану здоровья, образование, получение государственных услуг, а также демократических прав, таких как право на свободу выражения мнения и право объединения с другими. Законы о приватности должны быть содержательными, основанными на фактических данных, осуществимыми, а также доступными для понимания теми, кто подпадает под их действие.

- **Потоки данных и обмен данными должны существовать без ущерба для конфиденциальности данных.** Конфиденциальность персональных данных зачастую приносится в жертву в процессе обмена данными – начиная со сбора информации и заканчивая ее использованием, – с чем связано появление преднамеренных и непреднамеренных угроз доверию и безопасности. Доступ в Интернет и использование Интернета не должны находиться в зависимости от отслеживания данных: пользователи должны иметь право выбирать, каким объемом информации они делятся, в том числе информации, связанной с их действиями в Интернете. Персональные данные не должны экспортироваться в юрисдикции, не предоставляющие надлежащих гарантий.

- **Правовые меры должны быть направлены не только на защиту данных, но и на обеспечение справедливости на основе данных, то есть обеспечение таких условий, при которых человек может выбрать, каким образом будут использованы персональные данные, и получить свою долю доходов и выгод от инноваций**, основанных на наборах данных, которые получены с помощью данных, предоставленных человеком. Таким образом, меры по защите приватности должны способствовать повышению безопасности и процветанию цифровой экономики.

- **Правительства и регуляторы должны обеспечить защиту персональных данных**, определив степень дифференцированной ответственности различных заинтересованных сторон и не возлагая чрезмерную нагрузку или ответственность на отдельных пользователей. Политика управления данными должна разрабатываться

при содействии многих заинтересованных сторон, чтобы сложности, связанные с ее внедрением, были приняты в расчет.

- **Вопросы приватности и защиты данных имеют особое значение для управления искусственным интеллектом и машинного обучения**. Все заинтересованные стороны, участвующие в цепочке поставок ИИ, должны сыграть свою роль в поддержке права на неприкосновенность частной жизни.

- **Необходимо участие независимых надзорных органов, имеющих надлежащие ресурсы**. Службы по защите данных должны иметь полномочия по управлению регистрацией данных, предоставлению указаний, проведению расследований и рассмотрению жалоб субъектов данных.

Управление данными

- **Вопросы, связанные с управлением данными, не должны решаться изолированно или без учета их влияния**. Текущий ландшафт в области управления данными представляет собой раздробленный набор национальных, региональных и международных правил, определяющих ответственность национальных правительств, предприятий частного сектора и отдельных лиц.

- **Для формирования сбалансированного подхода, обеспечивающего использование данных в интересах людей и планеты, необходима бóльшая согласованность действий на глобальном уровне**. Законодательство и нормативно-правовые базы, действующие на национальном, региональном и международном уровнях, зачастую оказываются недостаточными, не поспевают за изменениями в технологиях, приложениях и должны стремиться к тому, чтобы обеспечить соблюдение высоких стандартов безопасности компаниями и другими организациями, ответственными за хранение данных.

- **Различия в условиях и вызовах, истории, культуре, правовой традиции и регуляторных структурах означают, что не может существовать единого, жесткого свода правил, подходящего для всех**. Различные лица и организации видят в широком смысле схожие подходы по-разному. Однако, хотя государства и регионы должны разработать свои собственные подходы к управлению данными, необходимо также обеспечить согласованность и интероперабельность, чтобы упростить передачу данных и предоставить всем равные условия.

- **Прозрачность, участие и ответственность являются важными факторами качественного управления данными**. Управление данными включает в себя следующие значимые аспекты, не ограничиваясь ими: стандарты в области данных и классификацию данных; обмен данными, их совместное использование и интероперабельность; безопасность и конфиденциальность данных; инфраструктуру данных; данные и цифровую идентичность; справедливость и беспристрастность на основе данных; прослеживаемость, прозрачность и объяснимость данных; минимизацию и ограничение данных; точность и качество данных; предвзятость, маргинализацию и дискриминацию данных; жизненный цикл, специфичность и

хранение данных; ответственное использование данных и этику обращения с данными; ущерб от использования данных, безопасность и защиту данных.

- **Многие заинтересованные стороны, в том числе регуляторы, исследователи, организации по стандартизации, потребительские организации и конечные пользователи, играют определенные роли в текущем процессе и должны использовать свою власть и влияние для содействия эффективному управлению данными**. Политика управления данными должна быть разработана при содействии сообщества всех заинтересованных сторон, обладающих как опытом участия в юридической полемике вокруг приватности, так и опытом преодоления «реальных» трудностей, связанных с внедрением эффективных решений в области конфиденциальности данных.

- **Развивающимся экономикам необходимо расширять свои институциональные возможности управления данными, их использования и обработки комплексными, объективными, доказательными методами, в том числе путем региональной и глобальной кооперации**. Для этого требуется сформировать более глубокое представление об институциональном потенциале чиновников и заинтересованных сторон.

Трансграничная передача данных

- **Трансграничная передача данных необходима для осуществления различных процедур, связанных с электронной коммерцией и цифровой торговлей.** Эффективность внутрирегиональной торговли и управления цепочками поставок зависит от бесперебойности движения потоков данных, а также товаров, услуг и капитала. Однако в этой связи требуется разработка комплексных межсекторальных требований, направленных на сближение регуляторных практик, гармонизацию нормативно-правовой базы, управление Интернетом, реформирование политики в области информационно-коммуникационных технологий, а также стратегическое внедрение региональной инфраструктуры.

- **Действующих многосторонних, региональных и двусторонних торговых соглашений недостаточно для обеспечения текущей и будущей трансграничной передачи данных.** Сегодня передача данных осуществляется в почти не регулируемой среде, в условиях слабой согласованности национальных правовых режимов. Используемые подходы различаются и носят контекстуальный характер, что создает торговые барьеры, причем у многих стран сегодня отсутствует соответствующее законодательство или правоприменительный потенциал. Возрастает необходимость разработки и гармонизации мер, направленных на управление трансграничной передачей данных, а также содействующих развитию и извлечению экономической ценности, в зависимости от контекста, и вместе с тем соблюдающих национальный суверенитет и приватность пользователей.

Обеспечение безопасности, защиты и ответственности

Тема

Безопасность Интернета находится под угрозой по нескольким причинам. Кибербезопасность традиционно представляет собой защиту сетей, устройств и данных от неавторизованного доступа или использования в преступных целях. С этим связана текущая проблема кибератак, которые могут осуществляться отдельными лицами или быть санкционированными государством и целью которых являются гражданские, коммерческие или правительственные объекты. Ряд факторов, включая отсутствие широких юридически обязывающих соглашений в области кибербезопасности и недостаточная защищенность сетей, способствует утрате возможностей, связанных с использованием экономических выгод цифровых технологий, особенно в развивающихся странах.

Вопросы безопасности, защиты и ответственности многоаспектны и в числе прочего охватывают темы, связанные с инфраструктурой, сервисами, контентом и другими сторонами функционирования Интернета. Так, наше сегодняшнее представление о безопасности и защите включает в себя подходы к сохраняющимся проблемам дезинформации и появления недостоверной информации в Интернете. В последние годы эти проблемы усугубляли последствия пандемии COVID-19 и создавали значительную угрозу электоральным процессам по всему миру. В данном контексте стала очевидной необходимость введения мер ответственности за действия, связанные с недостоверным контентом, и формирования четких критериев его определения.

Понятие «безопасность» может быть расширено и в таком случае включает в себя экологическую безопасность, в том числе усилия по «озеленению» Интернета и сокращению выбросов углекислого газа, причиной которых является потребление цифрового контента. Необходимость решения проблем, вызванных влиянием цифровизации на окружающую среду, становится все более важной темой для обсуждений, проходящих в рамках ФУИ.

Послания

Роль ответственных лиц и инстанций, реализующих соответствующую политику

- **Кибербезопасность следует рассматривать как центральную проблему интернет-политики.** Соображения, касающиеся доверия и защиты, в том числе уважения к правам человека, открытости и прозрачности принятия политических решений, должны стать неотъемлемой частью процессов обеспечения безопасного, защищенного доступа и разработки подхода с участием всех заинтересованных сторон, отвечающего интересам конечных пользователей.

- **Обеспечение кибербезопасности и предотвращение киберпреступлений являются важными направлениями политики, требующими серьезного внимания и развития соответствующих знаний**. Однако данные направления имеют разные цели и потому требуют разного подхода. Подход, доказывающий свою эффективность при реализации одного направления, не будет эффективным при реализации другого без должной корректировки и пересмотра.

- **Проблемы кибербезопасности и киберпреступности выходят за пределы отдельных организаций или стран. Их решение требует:**

  a) **применения общегосударственного и общесоциального подходов**, предполагающих создание крепких партнерских отношений и осуществление скоординированных усилий со стороны парламентов, регуляторов и других релевантных органов власти и государственных учреждений, а также частного сектора, технического сообщества, научного сообщества и гражданского общества;
  b) **эффективной и результативной региональной и международной кооперации**, которая носила бы межправительственный, многосторонний характер и осуществлялась при участии всех заинтересованных сторон.

- **Правительства, частный сектор и техническое сообщество не должны допускать принятия таких законов и установления таких стандартов в области киберпреступности, которые могли бы негативно отразиться на деятельности сторон, обеспечивающих кибербезопасность.** Следует пригласить к разработке политик все заинтересованные стороны, а также способствовать взаимодействию и обмену опытом и знаниями между различными заинтересованными сообществами.

- **Гражданское общество должно принимать участие в обсуждении как вопросов киберпреступности, так и вопросов кибербезопасности.** Для эффективной работы заинтересованные стороны, представляющие гражданское общество, должны расширять круг своих знаний в области различных релевантных подходов и проблем, а также взаимодействовать с другими заинтересованными сторонами в целях сбора информации и ресурсов, необходимых для полноценного участия в разработке политики.

Кибербезопасность

- **Международное сообщество должно искать практические пути интеграции усилий по укреплению потенциала, связанного с обеспечением кибербезопасности, в более широкий спектр мер, направленных на цифровое развитие**. Некоторые противоречия между стремлением содействовать цифровизации и необходимостью обеспечивать эффективную работу механизмов кибербезопасности препятствуют формированию безопасной, защищенной онлайн-среды и достижению Целей устойчивого развития. Меры по повышению устойчивости цифровой инфраструктуры необходимы, но их недостаточно. Давно созрела необходимость использовать действующие международные соглашения для реализации практически осуществимых мер.

- **Стандарты, направленные на обеспечение кибербезопасности, крайне важны для формирования открытого, защищенного и устойчивого Интернета, способствующего социальному прогрессу и экономическому росту, а также играют особую роль в защите тех, кто еще не подключен к Интернету**. Такие стандарты уже разработаны, но для достижения максимальной эффективности необходимо значительно расширить их использование. Организация Объединенных Наций могла бы ускорить глобальное внедрение ключевых стандартов, включив рекомендации по их применению в Глобальный цифровой договор, поддерживая их защиту и укрепление потенциала, а

также содействуя инициативам по проверке и контролю их реализации. Повышение осведомленности и укрепление потенциала в области стандартов должны входить в круг приоритетных направлений и в тех регионах, где многие люди еще не подключены к Интернету и происходит расширение использования Интернета.

- **Необходимо прилагать дополнительные усилия по повышению осведомленности лиц и органов, принимающих политические решения на национальном уровне и других заинтересованных лиц о проблемах в области кибербезопасности, международных норм и принципов**. Данные усилия должны включать в себя действия по повышению осведомленности и укреплению потенциала в области связи между устойчивым развитием и кибербезопасностью, а также по объединению различных заинтересованных сторон для содействия эффективному, устойчивому и инклюзивному руководству международной кооперацией в целях обеспечения киберустойчивости. Для поддержки данного процесса уже был разработан ряд международных инициатив. Финансирующие учреждения и другие заинтересованные стороны также должны рассмотреть возможности финансирования проектов по достижению киберустойчивости.

- **Нормы кибербезопасности должны качественно изменить прошлый, текущий и будущий опыт интернет-пользователей**. В этой связи, особенно при разработке новых норм, необходимо прислушиваться к опыту отдельных лиц и организаций, ставших жертвами кибератак, а также тех, кто первым реагировал на них и принимал соответствующие меры противодействия.

Киберпреступность

- **Киберпреступность представляет собой растущую угрозу для многих пользователей Интернета**. Положения, связанные с противодействием киберпреступности, должны учитывать размеры, возможности и ресурсы платформ. При введении юридических обязательств необходимо принимать во внимание многообразие субъектов технического сектора и исходить из потребностей и обстоятельств функционирования малого бизнеса при выполнении юридических обязательств, например при противодействии террористическому или насильственному экстремистскому использованию услуг бизнеса.

- **Правительства и политики должны обеспечить, чтобы правовые меры в ответ на преступное или террористическое использование Интернета находились в согласии с принципом верховенства закона и правами человека**, а также в полной мере учитывать право на свободу выражения мнения и обеспечивать прозрачность и подотчетность при реализации мер по борьбе с киберпреступностью.

Контент и дезинформация

- **Проблему дезинформации можно и следует решать с помощью механизмов управления рисками, а именно рисками, с которыми сталкиваются общества и**

отдельные лица, защищая свободу выражения мнения, плюрализм и демократический процесс. Поддержка профессиональной журналистики и медиа, включающая в себя приверженность существующим принципам журналистики, играет важную роль при решении проблемы дезинформации.

- **Навыки в области медиа и цифровой грамотности позволяют гражданам более критически относиться к контенту или обнаруживаемой информации и помогают им выявлять дезинформацию и недостоверную информацию, а также расширять демократическое участие**. Развитие цифровой грамотности может повысить осведомленность в области безопасности в Интернете, особенно среди наиболее уязвимых лиц и сообществ. Соответствующие инициативы должны учитывать потребности и риски, связанные с особенностями различных групп населения. Так, разные подходы в отношении представителей молодежи и более старших поколений должны отвечать различиям в навыках пользования.

- **Дисциплины по развитию цифровых навыков должны быть включены в образовательные программы для обеспечения безопасности детей в онлайн-пространстве.** Соответствующие инициативы должны осуществляться с участием родителей, учителей и опекунов. Законодатели и цифровые платформы должны принять на себя ответственность за обеспечение безопасности детей в рамках нормативной базы по реализации прав детей в цифровом пространстве, соответствующей международным соглашениям в области прав человека, в том числе Конвенции ООН о правах ребенка.

- **В данном контексте система доменных имен имеет ограниченный технический потенциал.** Для определения того, когда и каким образом она должна быть использована для устранения определенных проблем, связанных с контентом, и укрепления процессуальных норм, необходимо продолжать диалог заинтересованных сторон.

- **Шифрование играет важную роль в формировании открытого, безопасного и демократичного Интернета**, способствуя достижению безопасности, приватности пользователей и их свободы выражения мнений. Необходимо решать вопросы, связанные с правоприменением и способностью пользователей управлять доступом для защиты детей и в иных целях.

- **Недостатки перевода создают значительные трудности, которые могут препятствовать полноценному ознакомлению конечных пользователей со стандартами и политиками платформ.** Некачественный перевод ключевых терминов приводит к их неоднозначному толкованию. Взаимодействие различных языковых сообществ в целях повышения точности и уместности перевода, в том числе при передаче понятий, не имеющих прямого эквивалента в языках перевода, имеет особое значение, поскольку позволяет платформам и пользователям понять, что от них требуется.

Передовые технологии, включая искусственный интеллект (ИИ)

Тема

Передовые технологии все больше меняют экономику и общество. В число таких технологий входят системы искусственного интеллекта (ИИ), которые управляют нашим опытом пользования Интернетом, обеспечивают работу умных устройств и влияют как на наши решения, так и на решения, принимаемые другими в отношении нас, а также робототехника и приложения Интернета вещей, используемые в самых разнообразных сферах, например в промышленном производстве, здравоохранении и сельском хозяйстве. Однако помимо потенциала у таких технологий есть и серьезные недостатки. Так, использование алгоритмических систем принятия решений может привести к предвзятости, дискриминации, стереотипизации и усилению социального неравенства, а системы на основе ИИ могут поставить под угрозу безопасность человека и соблюдение его прав. Применение устройств Интернета вещей связано с проблемами в области кибербезопасности и защиты приватности. Использование технологий дополненной и виртуальной реальности сопряжено с вопросами в области общественной безопасности, защиты данных и защиты прав потребителей.

Извлечение выгод из возможностей, предоставляемых передовыми технологиями, и одновременное решение сопутствующих проблем и устранение рисков – это задача, к решению которой ни один актор не может приступить изолированно. Диалог и кооперация всех заинтересованных сторон, в том числе правительств, межправительственных организаций, технологических компаний, гражданского общества и других, необходимы, чтобы обеспечить такое развитие и применение обозначенных технологий, которое ориентировано на интересы человека и соблюдение его прав.

Послания

Управление

- **При разработке передовых технологий, включая искусственный интеллект, должны быть учтены принцип верховенства закона, права человека, демократические ценности и принцип многообразия, а также подготовлены соответствующие меры безопасности.** Передовые технологии должны использоваться на благо людей и планеты, способствуя инклюзивному росту, устойчивому развитию и процветанию. Механизмы надзора и правоприменения должны функционировать в соответствии с определенными принципами и нормами, причем акторы ИИ должны нести ответственность за любой причиненный ущерб.

- **Предположение, что использование технологий всегда способствует достижению равенства, ложно**. Те, кто разрабатывает технологии машинного обучения или подбирает данные, необходимые для обучения программ искусственного интеллекта, зачастую являются нерепрезентативными членами своего сообщества. Технологии могут усилить существующее неравенство и причинить ущерб, в особенности уязвимым и маргинализированным группам населения.

- **Обществам нужно адаптироваться к трансформации, которую повлечет за собой применение ИИ, посредством преобразования рамочных программ по**

сотрудничеству и изменения модели управления. Формирование интеллектуального общества, ориентированного на человека, требует полноценной кооперации правительств, предприятий, общественных организаций и научного сообщества. Постоянный человеческий контроль по-прежнему необходим для недопущения нежелательных или неконтролируемых последствий использования алгоритмов. В этой связи одним из ключевых аспектов является устранение барьеров между инженерами и экспертами в области политики.

- **Глобальное соглашение по вопросам установления норм в области ИИ не может быть достигнуто в результате простой разовой процедуры**. Сегодня уже действуют некоторые нормы, однако они представлены главным образом не обязывающими принципами, а нормами «мягкого» права. Разработка полноценных глобальных стандартов потребует эффективного участия всех стран, включая развитые и развивающиеся, а также региональных инициатив и вовлеченности всех заинтересованных сторон.

- **Укрепление потенциала крайне важно в рамках усилий по решению вопросов, касающихся передовых технологий**. Политика, направленная на повышение грамотности в области ИИ, развитие соответствующих навыков и обеспечение языковых ресурсов для миноритарных языков, необходима для формирования подлинно глобального подхода к применению передовых технологий.

Доверие, безопасность и приватность

- **Нормативно-правовые базы должны включать в себя принципы, дающие социальным медиа и другим платформам возможность соблюдать обязательства, связанные с проявлением должной осмотрительности в отношении управления контентом, который может причинить ущерб демократии и нарушить права человека**. Рамочные программы должны способствовать глобальному диалогу на тему модерации интернет-контента в интересах пользователей, включая представителей наиболее уязвимых групп и носителей миноритарных языков. Аффективные (эмоциональные) вычисления и другие новейшие технологии, связанные с распознаванием, интерпретацией и симулированием человеческих эмоций компьютером, требуют многомерной этической оценки.

- **Обеспечение прозрачного функционирования и отчетности алгоритмических систем абсолютно необходимо для соблюдения прав человека**. ИИ упрощает непрерывный контроль и анализ данных для персонализации и таргетирования контента и рекламы. Вследствие соответствующей персонализации опыта пользования Интернетом возникает риск разделения информационных онлайн-пространств и ограничения доступа отдельных лиц к информации во всем ее многообразии. Отсутствие информационного плюрализма может способствовать манипуляции и обману, тем самым усиливая неравенство, препятствуя демократической дискуссии и потенциально содействуя цифровому авторитаризму, насилию и разжиганию ненависти.

- **Заинтересованные стороны, относящиеся к техническому и другим сообществам, должны делиться знаниями и взаимодействовать в целях разработки принципов, указаний и стандартов**, которые были бы достаточно гибкими для использования в различных условиях и укрепляли доверие по отношению к системам ИИ.

- **Важно учитывать и уважать различный институциональный и культурный опыт стран и сообществ**, а также способствовать инклюзивности и содействовать международной кооперации в области ИИ.

Права и модерация контента

- **Абсолютно необходимо, чтобы политики управления контентом онлайн-платформами и применение данных политик соответствовали международным стандартам в области прав человека**. Технологии искусственного интеллекта и машинного обучения уже используются для принятия решений о том, какой контент стоит публиковать, удалять, приоритизировать, а также о том, среди каких пользователей его следует распространять. Данные инструменты играют важную роль в формировании политического и общественного дискурса и оказывают влияние на реализацию индивидуальных и коллективных прав человека, включая социальные, экономические, культурные права и права, связанные с обеспечением международного мира и безопасности. При этом прозрачность применения таких инструментов, сопряженная с этим ответственность и общественный контроль зачастую оказываются слабыми или полностью отсутствуют. Описанная ситуация должна быть исправлена.

- **Технологии, которые могут применяться для реализации прав человека, также могут быть использованы для слежки, пропаганды насильственных мер и в других целях, нарушающих вышеупомянутые права**. Непреднамеренные последствия автоматизированного управления контентом могут быть особенно пагубными в условиях конфликтов или кризисов, поскольку способны заглушить критические высказывания в ту пору, когда они особенно важны.

- **Технические стандарты являются значимым фактором, способствующим развитию и повышающим ценность цифровых технологий, связанных с ними инфраструктур, сервисов, протоколов, приложений и устройств**. Такие стандарты также оказывают серьезное влияние на реализацию прав человека. В то же время процессы разработки технических стандартов, осуществляемые в рамках организаций по стандартизации, не учитывают соображения, касающиеся прав человека, в полной мере. Зачастую данные процессы характеризуются отсутствием прозрачности, сложностью и значительной ресурсоемкостью. По этой причине гражданскому обществу и другим заинтересованным сторонам сложно получать к ним доступ и осуществлять контроль на регулярной основе. Данная проблема должна быть решена.

FORO DE GOBERNANZA DE INTERNET 2022

Mensajes IGF de Addis Abeba

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.