

# INTERNET GOVERNANCE FORUM 2022

## Addis Ababa IGF Messages

This document is a summary of points raised during the 17<sup>th</sup> 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 75<sup>th</sup> 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.

# 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.