Towards a Global Digital Compact

Guide to key digital policy issues and related processes and organizations

Toolkit for parliamentarians

Internet Governance Forum Secretariat

November 2022

Table of contents

Introduction

1. The IGF and parliaments

2. Access and inclusion

3. Internet fragmentation

4. Data governance

5. Human rights online

6. Safety and security in the digital space

7. AI governance

Annex: Digital policy observatories

Editor: Sorina Teleanu

Introduction

Since 2006, the United Nations Secretary-General has convened the Internet Governance Forum (IGF) as a multistakeholder platform to discuss Internet-related public policy issues. Through annual meetings and various intersessional activities, the IGF facilitates dialogue and cooperation on various topics related to the evolution, use and governance of the Internet and related digital technologies.

In 2020, the Secretary-General issued a *Roadmap for Digital Cooperation,* calling for strengthened global digital cooperation in addressing issues such as connectivity and digital inclusion, capacity development, human rights in the digital space, and trust and security. A year later, in the *Our Common Agenda* report, the Secretary-General proposed the elaboration of a Global Digital Compact (GDC) to 'outline shared principles for an open, free and secure digital future for all'. The GDC is expected to be agreed on during the September 2024 Summit of the Future. In 2022, the IGF decided to focus its annual meeting on the topics envisioned to be tackled by the GDC.

In recent years, the IGF has sought to strengthen the participation of parliamentarians in discussions on some of the most pressing internet governance and digital policy issues. What in 2019 and 2020 took the form of parliamentary roundtables later evolved into extended parliamentary tracks including more activities dedicated specifically to members of parliaments (MPs).

Against this backdrop, this toolkit is intended to:

- Provide MPs with an overview of the IGF ecosystem and its relevance for parliamentary activities.
- Serve as a toolkit to assist MPs navigate several key Internet and digital policy issues (i.e. focus areas) – envisioned to be covered by the GDC and discussed at IGF 2022 – as well as related processes and organizations.

For each of the focus areas outlined in Table 1, the toolkit:

- Provides a brief description of the related policy issues.
- Explores the role of MPs in addressing policy issues relevant to the focus areas, by showcasing points raised during parliamentary events at the IGF.
- Lists examples of relevant instruments and resources, from resolutions and recommendations issued by intergovernmental organizations, to reports are studies that provide insights into the focus areas.
- Lists international and/or regional organizations, processes and initiatives addressing the focus areas.
- Points to relevant IGF work.

Table 1. Toolkit focus areas

Toolkit	GDC	IGF 2022
Access and digital inclusion	Connect all people to the Internet	Connecting all people and safeguarding human rights
Internet fragmentation	Avoid Internet fragmentation	Avoiding Internet fragmentation
Data governance (cover both privacy and data flows)	Protect data	Governing data and protecting privacy
Human rights online	Apply human rights online	(see Connecting all people and safeguarding human rights)
Safety and security in the digital space (cybersecurity & cybercrime, content policy)	Introduce accountability criteria for discrimination and misleading content	Enabling safety, security and accountability
AI governance	Promote regulation of AI	Addressing advanced technologies, including AI

> **Living document**
>
> The lists of instruments, resources, organizations, processes and initiatives provided in this toolkit are illustrative and by no means do they pretend to be exhaustive. The toolkit is intended to be a living, evolving document, so we welcome suggestions that would help us expand these lists. Please send them to parliamentarytrack@intgovforum.org.

1. The IGF and parliaments

1.1. The growing importance of parliaments in Internet governance

Digital technologies underpin every aspect of our societies. In recent decades, they have become enablers and facilitators of a myriad of activities – from innovative online business models and the provision of governmental services, to the way we stay informed and communicate with friends and family. As the Internet grows in pervasiveness and importance, the stakes become higher when it comes to making decisions that affect this technology. Contradictory policy options naturally emerge, reflecting the diversity of interests in society. While digital issues are not purely technical (although it is crucial for parliamentarians to understand their technical aspects), they are intrinsically political.

Parliaments mediate the conflicting views on how society (and the Internet) should be steered. Increasingly, they are being called upon to develop regulations on complex and, often, controversial issues, such as online taxation, digital identity, the gig economy, and the right to be forgotten. They also need to strike a balance between important and sometimes conflicting social needs, such as security and privacy, and evaluate whether regulation is necessary or whether issues should be left to the market to regulate.

In this process, parliamentarians are confronted with the need to reach out to other groups of stakeholders who should be involved in discussions so that balanced decisions can be made and implemented on the ground, such as the technical community, civil society, and the business sector. Parliaments are a focal point where Internet governance takes place on a national level and while they are important building blocks of global Internet governance, they are also confronted with the trans-border nature of the Internet.

One distinguishing feature of the Internet is the way it cuts across jurisdictions and impacts local, regional, and global levels simultaneously. Decisions that are made on the national level are important, but frequently insufficient to tackle policy issues such as cybercrime or the protection of personal data. International and multistakeholder cooperation is necessary. The creation of a space where Internet-related policy discussions can happen is an invaluable contribution of the Internet Governance Forum (IGF) to the synchronisation of policy agendas, the identification of good practices, and the harmonisation of decisions taken at the national level.

1.2. About the IGF

The IGF as an outcome of WSIS

Internet governance was one of the most controversial issues during the first phase of the World Summit on the Information Society (WSIS-I), held in Geneva in December 2003. It was recognised that understanding Internet governance was essential in achieving the development goals of the Geneva Plan of Action, but defining the term and understanding the roles and responsibilities of the different stakeholders involved proved to be difficult.

The UN Secretary-General set up a Working Group on Internet Governance (WGIG) to explore these issues and prepare a report to feed into the second phase of WSIS (WSIS-II), held in Tunis in November 2005. Many elements contained in the WGIG report – developed through an open process and multistakeholder consultations – were endorsed in the Tunis Agenda for the Information Society (one of the main outcomes of WSIS-II). These included, among others, a definition of the term Internet governance, and a recognition that the process of Internet governance involves many stakeholders in a variety of roles.

> Internet governance is the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet. (Tunis Agenda for the Information Society)

WSIS-II requested the UN Secretary-General to convene an Internet Governance Forum, as a multilateral, multistakeholder, democratic and transparent platform for discussions on Internet governance issues.

IGF mandate

Paragraph 72 of the Tunis Agenda sets the mandate of the IGF to:

a) Discuss public policy issues related to key elements of Internet governance in order to foster the sustainability, robustness, security, stability and development of the Internet.
b) Facilitate discourse between bodies dealing with different cross-cutting international public policies regarding the Internet and discuss issues that do not fall within the scope of any existing body.
c) Interface with appropriate intergovernmental organizations and other institutions on matters under their purview.
d) Facilitate the exchange of information and best practices, and in this regard make full use of the expertise of the academic, scientific and technical communities.
e) Advise all stakeholders in proposing ways and means to accelerate the availability and affordability of the Internet in the developing world.

f) Strengthen and enhance the engagement of stakeholders in existing and/or future Internet governance mechanisms, particularly those from developing countries.
g) Identify emerging issues, bring them to the attention of the relevant bodies and the general public, and, where appropriate, make recommendations.
h) Contribute to capacity building for Internet governance in developing countries, drawing fully on local sources of knowledge and expertise.
i) Promote and assess, on an ongoing basis, the embodiment of WSIS principles in Internet governance processes.
j) Discuss, *inter alia*, issues relating to critical Internet resources.
k) Help to find solutions to the issues arising from the use and misuse of the Internet, of particular concern to everyday users.
l) Publish its proceedings.

The initial mandate of the IGF was for five years, between 2006 and 2011. Recognising the importance of the Forum in fostering the sustainability, robustness, security, stability and development of the Internet, as well as its role in building partnerships among different stakeholders, the UN General Assembly renewed the IGF mandate for five years, in 2010 (Resolution A/65/141), and for a further ten years, in 2015 (Resolution A/70/125).

IGF annual meetings

Each year, the IGF annual meeting brings together stakeholders from around the world to discuss some of the most pressing Internet governance issues. Participants represent governments, intergovernmental organizations, the private sector, the technical community, and civil society (including academia). Normally spanning a week, IGF meetings facilitate the exchange of information and the sharing of good policies and practices related to the evolution, use and governance of the Internet.

Starting 2017, IGF Messages are also developed to provide a high-level overview of the discussions and highlight the most important points raised during the discussions (in particular with regard to actions and steps needed to be undertaken to address certain Internet governance issues).

- IGF 2017 Messages
- IGF 2018 Messages
- IGF 2019 Messages
- IGF 2020 Messages
- IGF 2021 Messages

Intersessional activities

Dynamic Coalitions (DCs). They are open, multistakeholder and community-driven initiatives dedicated to exploring a certain Internet governance issue or group of issues. DCs are self-organised, and their work – required to adhere to a series of guidelines and principles – spans multiple years. There are over 20 dynamic coalitions focused on topics such as Internet rights and principles, innovative approaches to connecting the unconnected, accessibility and disability, child online safety, etc. The collective work of the DCs, including their participation at IGF annual meetings, is facilitated by the IGF Secretariat.

Best Practice Forums (BPFs). They provide a platform for stakeholders to exchange experiences in addressing Internet policy issues, and discuss and identify existing and emerging best practices. BPFs are expected to be open, bottom-up and collective processes, and their outputs to be community-driven. Over the years, BPFs have dealt with issues such as spam, Internet Exchange Points, cybersecurity, gender and digital rights, and local content.

Policy Networks (PNs). They are intended to create framework networks that allow for an expert in-depth view on Internet governance issues of broad interest. The purpose of the PNs is to provide in-depth understanding of the focus topic, raise awareness on it, and prompt cooperation across regions and stakeholder groups. Examples of focus areas include meaningful access, digitalisation and environment, and Internet fragmentation.

National, regional and youth IGF initiatives (NRIs)

Over the years, the IGF has triggered the launch of similar initiatives at the national and regional level, focused on facilitating dialogue and cooperation on Internet policy issues of utmost relevance for their respective communities. While being organic and independent, NRIs act in accordance with the IGF main principles (e.g. bottom-up, open, transparent, inclusive, multistakeholder and non-commercial). The NRIs collective work and cooperation is facilitated by the IGF Secretariat.

❖ National initiatives	❖ Regional initiatives	❖ Youth initiatives

1.4. The IGF: A unique space for dialogue and the exchange of experiences among parliamentarians

The IGF provides a platform for discussing both longstanding and emerging issues on the digital agenda, contributing to the identification of possible ways to address them.

It brings together various stakeholders, such as governments, civil society, the technical community, the private sector, and representatives of international organisations, to discuss a broad range of Internet policy issues. While there is no negotiated outcome, the IGF informs and inspires those with policy-making power in both the public and private sectors, offering participants the opportunity to discuss issues, exchange information, and share good practices.

In recent years, the IGF has sought to strengthen the participation of parliamentarians in discussions on some of the most pressing internet governance and digital policy issues. In 2019 and 2020, a parliamentary roundtable was held in the context of the IGF annual meeting. Starting 2021, an extended parliamentary track is included in the IGF programme and features multiple activities aimed to (a) facilitate exchanges of experiences and practices between MPs on various digital issues, and (b) foster dialogue between MPs and other stakeholders.

The main messages that emerge from parliamentary activities at the IGF (with potential guidelines, suggestions and recommendations for parliaments) are captured as formal outputs.

Message from the Meeting of Parliamentarians (Jimmy Schulz Call), IGF 2019	Output document from the Parliamentary Roundtable, IGF 2020	Output document from the Parliamentary Track, IGF 2021

2. Access and inclusion

2.1. Policy issues

Meaningful access

'We recognize the existence of the digital divide and the challenges that this poses for many countries. [...] We recognise the scale of the problem in bridging the digital divide, which will require adequate and sustainable investments in ICT infrastructure and services, and capacity building, and transfer of technology over many years to come. [...] We reaffirm our commitment to turning the digital divide into digital opportunity, and we commit to ensuring harmonious and equitable development for all.'

The above is an excerpt from the 2005 *Tunis Agenda for the Information Society*, one of the key WSIS outcomes. More than 15 years later, the digital divide remains a challenge: In 2021, 63% of the world population had access to the Internet, with significant discrepancies between the world's regions, from 33% in Africa to 87% in Europe.

The COVID-19 pandemic has clearly demonstrated that Internet access is not a luxury, but a necessity. It helped people stay connected, continue to work and go to school, and much more. But the pandemic has also shown that more efforts are needed to advance digital inclusion, connect the unconnected, and ensure that vulnerable and marginalised communities can fully enjoy the benefits of digitalisation and digital transformation. As noted in the UN Secretary-General's *Our Common Agenda*, 'it may be time to reinforce universal access to the Internet as a human right with accelerated steps to connect the remaining 3.8 billion offline to the Internet by 2030, notably those most often left behind, including women, along with indigenous and older people'.

There is a need for creative and accountable approaches to policy, regulation, enabling financing solutions, infrastructures, partnerships and business models that can help achieve meaningful access. Examples include public and private partnerships; local access provision, through, for instance, community networks; use of universal service/access funds in financing access; infrastructure sharing; and decentralised approaches to infrastructure development. Other factors that can contribute to advancing ubiquitous and affordable Internet access range from developing the capacity of regulators and service and content providers, to incentivising the development and use of local language content and locally relevant content.

Digital inclusion

Digital inclusion has multiple facets. It is not merely about deploying infrastructure for people to be able to connect. Issues of affordability, capacities and skills, multilingualism and local content, and even safety and security also come into play. Then, special attention needs to be allocated to advancing the **digital inclusion of women and girls, migrants and refugees, and various marginalised communities**. Digital inclusion also refers to issues of access to the digital labour market and involvement in relevant digital policy processes.

Holistic approaches are needed to address these issues and build truly inclusive digital economies and societies.

Capacity development

Capacity development for Internet-related matters is a global challenge. Despite the significant advances made in recent years, many individuals around the world lack the knowledge, skills, and abilities needed to maximise the opportunities and benefits of the Internet while mitigating its risks.

There is no one-size-fits-all solution to this challenge. Depending on the specific context and needs, different approaches are needed to capacity development. Nevertheless, there are some general principles that can guide capacity development efforts in this area.

First, capacity development should be needs-based. This means that it should be informed by an analysis of the specific skills and capacities that are needed. Second, capacity development should be comprehensive, so as to enable individuals to develop digital skills to use technology in a meaningful and safe way. Third, capacity development should also focus on empowering people to acquire the skills required in a fast-evolving, digitally-driven world of work. Fourth, capacity development should be long-term. It should be viewed as a continuous and iterative process, rather than a one-off event.

Another dimension of Internet-related capacity development relates to the strengthening of individual and institutional capacities when it comes to Internet/digital policy. Nations, organizations, and individuals must actively participate in policy processes in order to ensure Internet governance is effective and legitimate. Adequate capacity in digital policy issues allows for more informed policymaking and better implementation of such policies.

> **Digital technologies and sustainable development**
>
> In an era when digital technologies are reshaping industries, economies, and society generally, the notion of sustainable development becomes ever more relevant.

As enablers, technologies such as the Internet, artificial intelligence, big data and cloud computing can help us bridge divides between and within countries, tackle global challenges such as poverty, hunger, and climate change, and contribute to overall human well-being. But digital transformation also increases inequalities and disrupts social cohesion.

Stakeholders have a joint responsibility in ensuring that digital transformation processes are diverse, inclusive, democratic and sustainable. Commitment and strong leadership from public institutions need to be complemented with accountability and responsibility on the part of private actors.

2.2. What can parliaments do?[1]

Parliamentarians participating in IGF activities over the years have highlighted several 'messages' that are related to advancing digital inclusion:

- Multilateralism and multistakeholder cooperation across sectors and at all levels is essential to tackle common challenges, not least the digital and gender divides, and to promote ICTs and the Internet for the benefit of all. In this regard, the cooperation of national parliaments through the enactment of legislation is critical.
- Parliamentarians have a responsibility to actively contribute to creating legal frameworks for the current and next generations of Internet users which make the Internet accessible, open and safe for everyone. In these people-centred processes, parliaments must be guided by public trust, both in themselves as legislators and in the Internet itself.
- The Internet is all-pervasive; it affects multiple aspects of our lives and has become normative for many people. Yet, despite people's growing dependency on it, many are among marginalized groups. Digital and gender-based divides must be addressed by all, including the parliamentarians, for the sake of everyone benefiting equally from the immense power digital technologies have for sustainable development.
- Parliaments can contribute to improving public trust in the Internet by:
  - promoting good practices of digital technologies supporting sustainable development to showcase the benefits that digital inclusion can bring to people, and to foster people's trust in technologies.
  - advocating for bringing meaningful access to all its people through multistakeholder partnerships and initiatives, and recognise the need for non-state stakeholders to observe principles, rules and norms for responsible behaviour online.

[1] These sections on the role of parliaments are solely based on outputs of parliamentary activities at IGF 2021, 2020 and 2019.

- Given a rapidly growing strong integration of the Internet in people's lives and the fact that online safety also depends on end-users' skilful and informed behaviour, national parliaments can encourage embedding digital literacy in formal educational curricula available to all citizens.

2.3. Instruments and resources

WSIS outcomes

- Geneva Declaration of Principles (WSIS, 2003)
- Geneva Plan of Action (WSIS, 2003)
- Tunis Commitment (WSIS, 2005)
- Tunis Agenda for the Information Society (WSIS, 2005)

UN (General Assembly (GA), Secretary-General)

- GA Resolution 76/189: Information and communications technologies for sustainable development (UN General Assembly, 2021)
- Our Common Agenda (UN Secretary-General, 2021)
- GA Resolution 72/202: Information and communications technologies for sustainable development (UN General Assembly, 2020)
- Roadmap for Digital Cooperation (UN Secretary-General, 2020)
- GA Resolution 74/197: Information and communications technologies for sustainable development (UN General Assembly, 2019)
- Report of the High-Level Panel on Digital Cooperation: The Age of Digital Interdependence (UN Secretary-General's High-Level Panel on Digital Cooperation, 2019)
- Other UN GA resolutions on ICTs for sustainable development
- 2030 Agenda for Sustainable Development (UN General Assembly, 2015)

UN agencies

- International Telecommunication Union (ITU) Plenipotentiary (PP) Resolution 139: Use of telecommunications/information and communication technologies to bridge the digital divide and build an inclusive information society (ITU, 2018)
- ITU PP Resolution 175: Telecommunication/information and communication technology accessibility for persons with disabilities and persons with specific needs (ITU, 2018)
- ITU-D WTDC Resolution 58: Telecommunication/information and communication technology accessibility for persons with disabilities and persons with specific needs (ITU, 2017)
- Regulation for Digital Transformation: Accelerating inclusive connectivity, access and use (ITU, 2021)

- Financing universal access to digital technologies and services (ITU, 2021)
- The Regulatory Wheel of Change: Regulation for Digital Transformation (ITU, 2020)
- The Last-mile Internet Connectivity Solutions Guide (ITU, 2020)
- Inclusive Connectivity: the Future of Regulation (ITU, 2019)
- Best Practice Guidelines on Fast Forward Connectivity for All (ITU, 2019)
- Internet Universality Indicators (UNESCO, 2019)

Regional policies and strategies

- 2030 Digital Compass: the European way for the Digital Decade (European Commission, 2021)
- Digital Transformation Strategy for Africa (African Union, 2020)
- Organization of American States (OAS) Resolution A2953 (L-O/20): The leading role of the Organization of American States in developing telecommunications/ information and communication technologies through the Inter-American Telecommunication Commission (OAS, 2020)
- Association of Southeast Asian Nations (ASEAN) Digital Master Plan 2021–2025 (ASEAN, 2021)
- ASEAN Digital Integration Framework Action Plan 2019–2025 (ASEAN, 2019)

2.4. Organizations, processes and initiatives

Organizations

- International Telecommunication Union, in particular through its Telecommunication Development Sector
- Broadband Commission for Sustainable Development
- Alliance for Affordable Internet

Processes and initiatives

- Partner2Connect Digital Coalition
- EQUALs Global Partnership

2.5. Relevant IGF work

IGF Messages relevant to the issue

- IGF 2022 Messages: Economic and Social Inclusion | Universal access and meaningful connectivity
- IGF 2020 Messages: Inclusion
- IGF 2019 Messages: Digital inclusion

- IGF 2018 Messages: Digital Inclusion & Accessibility

Other relevant IGF work

- Policy Network on Meaningful Access, IGF 2022
- Policy Network on Meaningful Access, IGF 2021
- Policy Options for Connecting and Enabling the Next Billion(s), IGF 2015 – IGF 2018
- Dynamic Coalition on Accessibility and Disability
- Dynamic Coalition on Community Connectivity
- Dynamic Coalition on Gender and Internet Access
- Dynamic Coalition on Internet and Jobs
- Dynamic Coalition on Internet Universality Indicators
- Dynamic Coalition on Public Access in Libraries
- Dynamic Coalition on Schools of Internet Governance
- Dynamic Coalition on Small Island Developing States in the Internet Economy
- Youth Coalition on Internet Governance

3. Internet fragmentation

3.1. Policy issues

The key feature of the Internet's core functions is maintaining the "uniqueness" of identifiers – the numbers (e.g. Internet protocol addresses) and domain names – which ensures global interoperability and connectivity. A large part of the Internet's success is due to it being a "network of networks" with no central command. Its strength and value increase exponentially with the number of participants (network effect). Trust in these identifiers being unique and in the governance system that coordinates these functions is vital for the Internet to function and for it to remain the globally connected unfragmented network it is today.

The Internet does not come without risks. Most of those risks are related to what happens on the Internet (i.e. within the so-called application layer), rather than the underlying technical core functions and processes. For the latter, where risks on the stability or resilience of the Internet were identified, the industry has been putting in place new technologies to reduce these risks, whilst maintaining one global Internet. One could say that the ability of these core technologies to adapt to changes and scale-up is the foundation of the Internet's success.

To recognise, understand and address these risks, both within the application layer and those of the underlying technical infrastructure, while maintaining a global network, we need to think globally. The tendency to seek legislation impacting the core of the Internet's infrastructure on a domestic or regional level threatens the Internet as one unfragmented and globally interoperable space. A national or even regional Internet would never provide the same value as a global one.

In recent years, technical, commercial, legislative and policy developments have furthered the risk that the Internet fragments into siloed parts. At the technical and commercial level, the global and universal nature of the Internet could be impacted by a mix of voluntary and involuntary conditions and business practices. At the policy level, concerns stem from a series of initiatives that involve bans or undue restrictions on international data flows, interference with free expression, privacy, and/or encryption; and Internet shutdowns. These developments may pose a threat to the open, interconnected and interoperable Internet, along with its associated benefits to social and economic development, while also harming human rights. Internet fragmentation can take place at various segments and functions of the Internet, any of which can prevent an open, interconnected and interoperable Internet.

3.2. What can parliaments do?

Parliamentarians participating in IGF activities over the years have highlighted several 'messages' that are related to addressing risks of Internet fragmentation:

- ❖ Parliaments have a responsibility to ensure that the Internet and the broader digital space remain open, and, at the same time, safe and secure.
- ❖ It is recommended that parliaments consider the following elements when developing legislation for the Internet and the digital space: [...]
    - ➢ Consider – and avoid – potential unintended consequences of regulations. For instance:
        - ■ Embed human rights impact assessments in the legislative processes;
        - ■ Assess whether legislation adopted at the national and regional level may impact the global and interoperable nature of the Internet and the digital economy. [...]
    - ➢ Cooperate and exchange information with other parliaments, as a way to (a) learn from each other, and (b) contribute to regulatory coherence and interoperability at regional and global level.

3.3. Instruments and resources

- ITU Resolution 69: Non discriminatory access and use of Internet resources and telecommunications/information and communication technologies (ITU, 2016)

- White Paper: Internet Fragmentation: An overview (World Economic Forum, 2016)
- Emerging Digital Fragmentation: The perils of unilateralism (Global Trade Alert, 2022)

3.4. Organizations, processes and initiatives

At the technical level, organizations working to maintain the Internet global and unfragmented include:

- Internet Corporation for Assigned Names and Numbers (ICANN)
- Regional Internet Registries (RIRs)
- Internet Engineering Task Force (IETF)

3.5. Relevant IGF work

IGF Messages relevant to the issue

- ❖ IGF 2018 Messages: Technical and operational topics

Other relevant IGF work

- Policy Network on Internet Fragmentation (IGF 2022)
- Dynamic Coalition on Core Internet Values
- Dynamic Coalition on DNS Issues

4. Data governance

4.1. Policy issues

Privacy and data protection

As societies become increasingly digitalised worldwide, users leave a digital trail that makes them vulnerable to private tracking and public monitoring. With public and private entities relying on personal data and behavioural information to provide digital services (with varying degrees of transparency), and with surveillance tools increasingly used outside of rule of law frameworks, protecting privacy and personal data in the digital space is an increasingly complex matter. This complexity poses challenges when it comes to defining and implementing relevant legislation. Outlining data subject rights and establishing responsibilities for their protection, clarifying meaningful consent for data processing, and setting conditions for international data transfers are some of the key issues that legislators around the world have to unpack when devising legal frameworks.

A number of governments and international organizations have attempted to update their regulatory framework to protect citizens' rights to data protection and privacy in the digital age. The EU's General Data Protection Regulation (GDPR) is a landmark law, echoed by a number of regulatory initiatives in other continents. Brazil, China, India, Kenya, Japan, South Korea are just some of the countries that have passed new laws, proposed new regulations, or are considering legislative changes aligned to some extent with key principles of the EU's GDPR (consent, data minimisation, confidentiality, and transparency). And while such frameworks are being put in place in many countries around the world, the reality is that there is still a patchwork of different legal approaches to protecting privacy and personal data. Which leads to the question: How do these many legal approaches work together in the framework of a borderless digital space? What is still missing?

At the same time, Internet giants have come increasingly into the spotlight in the wake of a number of data protection scandals. Facebook, Google, Apple, Microsoft, and Twitter, among others, are now under investigation for potential privacy violations in dozens of countries and may face substantial fines in the coming months and years. In 2019, for instance, Google received from the French data protection authority a €50 million fine for violations of the GDPR. In the same year, Facebook agreed to a $5 billion civil penalty imposed by the US Federal Trade Commission for privacy-related violations concerning the Cambridge Analytica scandal.

Data-centred economy and competition

In the digitalised society, data is considered 'the new oil'. Internet companies make intensive use of data to enhance users' experiences with customised services and to enable other companies to market their products more efficiently to selected audiences. For example, roughly 90% of Google's revenue is said to come from advertising. Other businesses, such as telecommunication and hardware companies, car manufacturers, and the emerging artificial intelligence (AI) industry are experiencing a similar rush for data, which will determine their competitiveness.

In this scenario, regulators need to develop frameworks to protect users and preserve competition. New or updated regulation is being enacted in fields such as data protection, consumer protection, platform liability, misinformation, media regulation, and competition. In the latter area, regulators are discussing ways to better detect the barriers of entry created by the ownership of data by large platforms and to update national laws in order to consider the importance of the concentration of data when assessing the competitive effects of mergers and acquisitions. An example of international collaboration in this area is the Common Understanding on Competition and the Digital Economy released by G7 Finance Ministers and Central Bank Governors in 2019.

Data governance and data localisation

The abundance of data is the defining feature of the connected society. The digital universe is expected to reach 180 zettabytes (180 followed by 21 zeros) by 2025. Data governance refers to the norms, principles, and rules governing several different types of data, such as personal, business, and public data. Traditionally, data governance has been carried out on a national basis, reflecting cultural, legal, and historical differences across the globe. Nevertheless, the transborder nature of the Internet means that data is able to easily flow across jurisdictions. This has enabled the boom in services such as cloud computing and data analytics.

In this context, one of the challenges faced by parliaments is the need to reconcile the urge for creating norms on data governance with avoiding a global patchwork of disparate national legislations. Another challenge is related to the current proliferation of norms on mandatory localisation of data within a certain territory. Those in favour of data localisation present it as a way to curb foreign surveillance, to protect citizens and businesses from threats to privacy, to preserve national security, and to ensure that the economic value of data benefits local actors. Concerns over data localisation provisions range from technical to economic and human rights issues. By restricting data flows and competition between firms, localisation could increase costs for Internet users and businesses, could retard technological innovation, and could reduce the ability of firms to use cloud services and data analytics, for example.

Data localisation provisions are in place or being developed in many countries, such as China, India, Nigeria, Russia, and Rwanda.

4.2. What can parliaments do?

Parliamentarians participating in IGF activities over the years have highlighted several 'messages' that are related to data governance issues:

- Acknowledging that protecting privacy and personal data in the digital space is both essential and increasingly complex, it is recommended that parliaments devise or update, as appropriate, relevant legislation with consideration to the following principles:
  - Responsibility, transparency, proportionality, necessity and the rule of law must guide the use of personal data by both private and public entities;
  - Legislation should be mindful not only of protecting data itself, but also of protecting the individuals behind the data;
  - Considering that the right to privacy is not an absolute right, a proper balance – with adequate checks and balances, and accountability mechanisms – needs to be found with other rights and public interests (e.g. public safety and security, access to information);
  - Besides outlining rights and responsibilities, legislation should also contain provisions that enable a strong enforcement of the law, preferably by an independent and adequately resourced regulator;
- Underlining the importance of regulatory coherence and interoperability at the regional and international level, parliamentarians are encouraged to collaborate and exchange information so that the laws they devise
  - (a) acknowledge the cross-border nature of the digital space,
  - (b) provide robust protections for the rights of individuals, including in the context of cross-border data flows, and
  - (c) provide clarity and predictability to companies that operate across jurisdictions, while ensuring they are held accountable for meeting their obligations.

4.3. Instruments and resources

Overarching instruments related to privacy (international and regional)

- Universal Declaration of Human Rights (Article 12)
- International Covenant on Civil and Political Rights (Article 17)
- Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data
- Council of Europe Recommendation No. R(99) 5 for the protection of privacy on the Internet
- European Convention for the Protection of Human Rights and Fundamental Freedoms (Article 8)
- American Convention on Human Rights (Article 11)
- Arab Charter on Human Rights (Articles 16 and 21)

- ❖ African Commission on Human and People's Rights Declaration of Principles on Freedom of Expression in Africa
- ❖ Human Rights Declaration of the Association of Southeast Asian Nations (Article 21)
- ❖ Asia-Pacific Economic Cooperation Privacy Framework

Resolutions of the UN Human Rights Council (HRC) and the UN General Assembly (GA)

- ❖ GA Resolution 75/175: The right to privacy in the digital age (UN GA, 2020)
- ❖ HRC Resolution 42/15: The right to privacy in the digital age (UN HRC, 2019)
- ❖ GA Resolution 73/179: The right to privacy in the digital age (UN GA, 2018)
- ❖ HRC Resolution 37/2: The right to privacy in the digital age (UN HRC, 2018)
- ❖ HRC Resolution 34/7: The right to privacy in the digital age (UN HRC, 2017)
- ❖ GA Resolution 71/199: The right to privacy in the digital age (UN GA, 2016)
- ❖ HRC Resolution 28/16: The right to privacy in the digital age (UN HRC, 2015)
- ❖ GA Resolution 69/166: The right to privacy in the digital age (UN GA, 2014)
- ❖ GA Resolution 68/167: The right to privacy in the digital age (UN GA, 2013)

Reports of the UN High Commissioner for Human Rights

- ❖ The right to privacy in the digital age (Office of the UN High Commissioner for Human Rights)
- ❖ The right to privacy in the digital age (UN High Commissioner for Human Rights, 2021)
- ❖ The impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests (UN High Commissioner for Human Rights, 2020)
- ❖ The right to privacy in the digital age (UN High Commissioner for Human Rights, 2018)
- ❖ Right to privacy in the digital age (focus on surveillance) (UN High Commissioner for Human Rights, 2014)

G7 and G20

- ❖ G7 Roadmap for Cooperation on Data Free Flow with Trust (2021)
- ❖ G7 Digital Trade Principles (2021)
- ❖ G20 Leaders' Declaration, Rome (2021)
- ❖ G20 Leaders' Declaration, Riyadh (2020)
- ❖ G20 Leaders' Declaration, Osaka (2019)
- ❖ G20 Osaka Declaration on Digital Economy (2019)
- ❖ G20 Ministerial Statement on Trade and Digital Economy, Tsukuba (2019)

Regional instruments

- AU Data Policy Framework (African Union, 2022)
- Data Governance Act (European Union, 2022)

- Regulation on a framework for the free flow of non-personal data in the EU (European Union, 2018)
- General Data Protection Regulation (European Union, 2016)

4.4. Organizations, processes and initiatives

Organizations/forums

- World Trade Organization (WTO)
- G7
- G20
- African Union
- European Union

Processes

- G7 work on free data flows with trust
- WTO: Joint Initiative on E-commerce (participation from 86 WTO members)
- WTO: Work Programme on E-Commerce

4.5. Relevant IGF work

IGF Messages relevant to the issue

- IGF 2020 Messages: Data
- IGF 2019 Messages: Data Governance
- IGF 2018 Messages: Cybersecurity, Trust and Privacy

Other relevant IGF work

- Dynamic Coalition on Data and Trust
- Internet Rights and Principles Coalition

5. Human rights online

5.1. Policy issues

Meaningful access to the Internet is strongly linked to 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 boundaries between life "online" and "offline" no longer apply.

Human rights need to be at the centre of inclusive digital societies and economies, and technologies and policies alike need to be designed, used and implemented in a human rights-centred manner. The protection of both civil and political rights, and economic, social and cultural rights in the digital space should remain a priority for all actors.

Adequate regulatory frameworks need to be put in place to provide rules and boundaries for the private sector. Governments need to be accountable for respecting and promoting these rights and for ensuring that others, including companies, also do so. Global companies that operate across borders need to be accountable for their practices and uphold international human rights standards, and users need to be more aware of how to demand respect for their rights. This holistic awareness and integration of human rights can only be achieved through collaboration, learning and capacity development, and open and constructive dialogue among all stakeholder groups.

Examples of digital rights		
Privacy and data protection (covered above)	Freedom of expression	Rights of persons with disabilities
Gender rights online	Children's rights	Right to be forgotten

5.2. What can parliaments do?

Parliamentarians participating in IGF activities over the years have highlighted several 'messages' that are related to digital rights issues:

- In order to stand the test of time, legislation should be principle-based, rather than rule-based. The fundamental human-rights-based principles that should underpin legislation have been set out clearly at the international and regional level (e.g. transparency, accountability, rule of law). Legislation needs to be drafted carefully, to the best tests of human rights standards. Conversely, legislation that is prepared hastily or seeks to set detailed rules for specific technologies risks quickly becoming outdated.
- Parliaments should act as facilitators so that all points of view are heard and taken into account. It is time for concrete multistakeholder discussions about how to achieve the necessary balance between fundamental human rights such as privacy and the right to freedom of expression and access to information, while also taking into account other important values such as consumer protection, innovation and business freedom. Regulators and the judiciary also need to be part of these discussions from the outset, as they will have a key role in applying the rules.
- Parliaments have a responsibility to ensure that the Internet and the broader digital space remain open, and, at the same time, safe and secure. Solutions to digital policy challenges need to be human-centric and have users at their core.
- It is recommended that parliaments embed human rights impact assessments in the legislative processes when developing legislation for the Internet and the digital space.

5.3. Instruments are resources

Overarching instruments related to human rights (international and regional)

- Universal Declaration of Human Rights
- International Covenant on Civil and Political Rights
- European Convention for the Protection of Human Rights and Fundamental Freedoms
- American Convention on Human Rights
- Arab Charter on Human Rights
- African Commission on Human and People's Rights Declaration of Principles on Freedom of Expression in Africa
- Human Rights Declaration of the Association of Southeast Asian Nations

Resolutions of the UN Human Rights Council (HRC)

- Resolution 51/3: Neurotechnology and human rights (UN HRC, 2022)
- Resolution 51/10: Countering cyberbullying (UN HRC, 2022)
- Resolution 51/22: Human rights implications of new and emerging technologies in the military domain (UN HRC, 2022)

- Resolution 50/15: Freedom of opinion and expression (UN HRC, 2022)
- Resolution 49/21: Role of states in countering the negative impact of disinformation on the enjoyment and realisation of human rights (UN HRC, 2022)
- Resolution 47/16: The promotion, protection and enjoyment of human rights on the internet (UN HRC, 2021)
- Resolution 47/23: New and emerging digital technologies and human rights (UN HRC, 2021)
- Resolution 44/12: Freedom of opinion and expression (UN HRC, 2020)

Reports and other resources from the UN High Commissioner for Human Rights

- Internet shutdowns: trends, causes, legal implications and impacts on a range of human rights (Office of the UN High Commissioner for Human Rights, 2022)
- Impact of the digitalization of education on the right to education (Special Rapporteur on the right to education, 2022)
- Report on the impact of new technologies on the promotion and protection of human rights in the context of assemblies (Office of the UN High Commissioner for Human Rights, 2020)
- Explainer: Internet shutdowns and human rights (Office of the UN High Commissioner for Human Rights, 2021)

Other UN-related documents

- General Comment No.25 (2021) on children's rights in relation to the digital environment (Committee on the Rights of the Child, 2021)
- Report on the role of new technologies for the realisation of economic, social and cultural rights (UN Secretary-General, 2020)
- Report on online hate speech (Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 2019)
- Surveillance and human rights (Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 2019)
- Data collection and management as a means to create heightened awareness of violence and discrimination based on sexual orientation and gender identity (Independent Expert on the protection against violence and discrimination based on sexual orientation and gender identity, 2019)
- Privacy and technology from a gender perspective (Special Rapporteur on the right to privacy, 2019)
- Violence against women, its causes and consequences on online violence against women and girls from a human rights perspective (Special Rapporteur on violence against women and girls, its cases and consequences, 2018)

Regional instruments

- Resolution on the protection of women against digital violence in Africa (African Commission on Human and Peoples' Rights, 2022)
- Declaration of principles on freedom of expression and access to information in Africa (African Commission on Human and Peoples' Rights, 2019)
- Resolution on the right to freedom of information and expression on the internet in Africa (African Commission on Human and Peoples' Rights, 2016)

Other resources

- Geneva Declaration on targeted surveillance and human rights (multiple actors, 2022)
- African Declaration on Internet Rights and Freedoms
- Charter of human rights and principles for the Internet (Internet Rights and Principles Coalition, 2011)

5.4. Organizations, processes and initiatives

Organizations/forums

- UN Human Rights Council
- Office of the UN High Commissioner for Human Rights
- African Commission on Human and Peoples' Rights
- Council of Europe

- Access Now
- African Digital Rights Network
- African Internet Rights Alliance
- Article 19
- Association for Progressive Communications
- Electronic Frontier Foundation

Processes

- Freedom Online Coalition

5.5. Relevant IGF work

IGF Messages relevant to the issue

- IGF 2021 Messages: Economic and social inclusion and human rights
- IGF 2018 Messages: Human Rights, Gender and Youth

Other relevant IGF work

- Best Practice Forum on Gender and Digital Rights
- Dynamic Coalition on Accessibility and Disability
- Dynamic Coalition on Children's Rights in the Digital Environment
- Dynamic Coalition on Data and Trust
- Dynamic Coalition on Gender and Internet Governance
- Internet Rights and Principles Coalition

6. Safety and security in the digital space

6.1. Policy issues

Cybersecurity

The borderless nature of the Internet, the digital economy, the increased cyber-physical interdependency through the Internet of things, and the increased use of the Internet in processes such as elections and in the response to global crises such as the pandemic paint a complex policy, legal and operational picture for cybersecurity and stability. Almost all sectors utilise ICTs and rely on the Internet for anything from the simplest to the most strategic tasks. Global supply chains are increasingly interconnected, and the ICT systems supporting them comprise numerous internal and external devices and applications.

Managing these issues, mitigating cybersecurity concerns and addressing risks requires cooperation between the public and the private sectors, the technical community, the academic and research sector, and civil society. Collaboration is needed to build awareness of vulnerabilities and increase resilience. An Internet that is trusted by its users requires combatting online gender-based violence, child safety online, cyberbullying, and misinformation, among other challenges.

Discussions on trust, security and stability of the Internet should cover norms, voluntary standards, guidelines, best practices and capacity building to manage cybersecurity-related risks and foster collaboration between countries, institutions and stakeholder groups.

National security

As all segments of our society become digitalised, they also become vulnerable to cyberattacks. A remotely conducted cyberattack could damage or disrupt government web pages and

e-government services, banks and ATMs, media, hospitals, transport systems, election systems, and even factories and the energy grid. Besides criminals, the perpetrators now include actors with the budgets, motivations, and skills to conduct sophisticated cyber-attacks: political groups, terrorist organisations, and nation states.

Having a robust and resilient digital network, as well as an efficient national cybersecurity framework to respond to incidents, is becoming a top national security priority. To face these challenges, several countries are developing national strategies and national laws on cybersecurity.

- **National cybersecurity strategies** should define priority areas of concern and budgetary focus - such as network resilience, incident response, cyber-crime, protection of critical infrastructure, cyber-defence, education and awareness, and international cooperation. To be fully applicable and accepted by society, it should be developed with strong participation of the private sector and civil society.
- **National laws on cybersecurity** should, at a minimum, define the key national assets and critical infrastructure to be primarily protected from cyber-attacks, set up the lead national authority and point of contact, define roles and responsibilities of various governmental authorities and other stakeholders, and set up national and sectoral incident response teams - first-responders to severe cyber-attacks. Such teams, known as CERTs (computer emergency response teams), CIRTs (computer incident response teams), or CSIRTs (computer security incident response teams) , should be efficient and operational mechanisms with strong capacities and resources, independence, and the ability for cross-sectoral and international co-operation.

Importantly, the strong inter-relation of cybersecurity with economic development and human rights and the complexity of actors involved in securing cyberspace, requires oversight of the security sector and the actions of all involved stakeholders.

Cybercrime

Traditional crimes such as fraud, identity theft, or trade in illegal goods are now conducted through the Internet. The Internet has also enabled some old crimes to evolve, such as credit cards forgery or child sexual abuse. Tools for conducting cyber-crime and cyber-attacks are now affordable, and available on online dark markets. Emerging technologies, such as interconnected devices, augmented and virtual reality, 3D printing of objects, or AI, provide new venues for criminal activity. In spite of such gravity, national and international capacities and legal frameworks for combating cyber-crime are still very limited.

To address cybercrimes – which are by default of a cross-border nature and conducted swiftly – currently inefficient and slow mutual legal assistance treaties (MLATs) need to be supported by a range of bilateral regional and multilateral agreements, as well as the harmonisation of national laws of countries around the world. Various regional blocks have developed legal

frameworks for cybercrime to enable the investigation of cybercrime across their national borders (details below). In addition, digital literacy, education, and awareness as well as the cooperation of the public sector with the Internet industry and civil society, play a critical role in preventing cyber-crimes, in particular protecting children from bullying and abuse.

Violent extremism online

Extremist and terrorist groups are also becoming digitised, in two main ways. They use the Internet as a tool to prepare attacks (i.e., for internal communication or logistics) by using protected online communication channels, or to spread fear and recruit new members (i.e., external communication or propaganda) through social media. They may - and most likely will - also target the Internet and connected systems with the aim of attacking critical components of society (e.g. shutting down financial services).

In addressing violent extremism online, legislators have to work together with the private sector and civil society to find smart ways to remove problematic content and users from main communication and social media platforms. Since content policy always bring risks of endangering human rights and innovation, measures related to content filtering and removal for security reasons should be proportionate: a policy sandbox approach, in which policies can be shaped, implemented, and tested, and then adjusted accordingly based on the impacts on security, economic development, and human rights, may be necessary.

Misinformation and disinformation

The publishing of inaccurate (or false) information is not a new phenomenon to mainstream media. Yet, with the use of social media platforms, such information is easier to create and easier to spread. False information could be particularly damaging ahead of elections, endangering national democratic processes.

In recent years, misinformation and disinformation have been factors in aggravating the effects of the COVID-19 pandemic and have posed significant risks to electoral processes around the world. This has made clear the need for accountability criteria for misleading content, so governments and online platforms have started taking action to tackle the issue through a variety of forms.

Platforms have enacted more stringent community guidelines in the case of content that has been flagged inappropriate and with regard to the removal of fake profiles They have also explored the use of AI to help identify inappropriate content. But AI is a double-edged sword. Recent developments also make it possible for AI to generate deepfakes, i.e., fake content which is difficult to detect by humans and algorithms.

***

Countries have enacted laws and guidelines in the field of content policy. Canada, for instance, has published a Declaration on Electoral Integrity Online. Singapore approved the Protection from online Falsehood and Manipulation bill, which allows government entities to order removal or force correction of online information considered inaccurate. In the UK, the Online Safety Bill outlines rules for internet platforms when it comes to tackling misinformation, disinformation, and other forms of harmful online content.

The EU's Digital Service Act also covers – among other topics – issues related to the roles and responsibilities of online platforms related to Internet safety.

6.2. What can parliaments do?

Parliamentarians participating in IGF activities over the years have highlighted several 'messages' that are related to safety and security online.

- The proliferation of harmful content online, sometimes with dire consequences for democracy, human rights and safety, calls for attention in particular to the need for multistakeholder cooperation in tackling issues such as (a) the abuse directed towards women online, including women parliamentarians[1], which can limit their ability to participate freely in the digital space, and (b) online child sexual exploitation and abuse.
- It is recommended that parliaments ensure that any legislation intended to address harmful online content:
  - Ensures a proper balance between tackling harmful content and protecting freedom of expression and other internationally-recognised human rights;
  - Balances the need to take quick action against harmful content with the need to ensure due process;
  - Embodies principles such as transparency (e.g. on how content moderation works), judicial oversight, and appeal/redress mechanisms;
  - Contains clearly defined legal terms and concepts so that legislation can be implemented and interpreted in a consistent manner.
- Parliaments are called on to encourage (a) awareness raising and capacity development programmes that empower Internet users with critical thinking and media information literacy skills, and (b) initiatives focused on supporting professional journalism, fact-checkers and overall media pluralism.
- Misinformation and disinformation online are a systemic global problem and cannot be dealt with in a single legislative response. This problem requires a systemic approach, where all stakeholders, including legislators, would actively contribute to long-term awareness raising and facilitation of critical thinking among online population, online content creators and online platform owners. Parliaments are advised
  - to take active participation in awareness raising and supporting capacity development on combating misinformation and disinformation online.

- Cyberattacks and criminal online activities are undermining the security and safety of the Internet and need a collective response, which includes the promotion of confidence and capacity building measures as well as the strengthening of the resilience of the billions of Internet users. National parliaments are advised
  - to promote a new culture of cybersecurity and comprehensive cyber-hygiene in the daily use of the Internet;
  - to promote the stability of cyberspace and its infrastructure by protecting, in particular, the public core of the Internet.

- It is recommended thay national parliaments guarantee, that in case new legislation is needed to enhance national security in cyberspace and promote the national digital economy, that individual human rights and fundamental freedoms, as laid down in the Universal Declaration of Human Rights (1948), are fully respected and remain protected

6.3. Instruments and resources

Cybersecurity and cybercrime

International

- Convention on Cybercrime – Budapest Convention (Council of Europe, 2001)
- African Union Convention on Cybersecurity and Data Protection – Malabo Convention (African Union, 2014)
- Reports of the UN Group of Governmental Experts (GGE) on advancing responsible state behaviour in cyberspace and the UN Open-Ended Working Group (OEWG) on security of and in the use of information and communications technologies
  - GGE 2013 report
  - GGE 2015 report
  - GGE 2021 report
  - OEWG 2021 report
- ITU Global Cybersecurity Agenda

Regional

- Samarkand Declaration of the Council of Heads of State of Shanghai Cooperation Organization (Shanghai Cooperation Organisation, 2022)
- ASEAN Cybersecurity Cooperation Strategy - Draft (ASEAN, 2022)
- EU Cybersecurity Strategy (European Commission, 2020)
- CICA Catalogue of Confidence Building Measures (Conference on Interaction and Confidence Building Measures in Asia, 2019)
- Commonwealth Model Law on Computer and Computer Related Crime (The Commonwealth, 2017)
- Directive concerning measures for a high common level of security of network and information systems (EU, 2016)

- Commonwealth of Independent States Agreement (2016)
- EU Directive on Attacks Against Information Systems 2013 (EU, 2013)
- Arab Convention on Combating Information Technology Offences (League of Arab States, 2010)
- Shanghai Cooperation Organisation Agreement on Cooperation in the Field of Ensuring International Information Security (Shanghai Cooperation Organisation, 2009)

Harmful content

- Countering disinformation and promotion and protection of human rights and fundamental freedoms (UN Secretary-General, 2022)
- Code of Practice on Disinformation (European Commission, 2022)
- Charter for a Free, Open and Safe Internet (G7, 2019)
- Council of Europe's Information Disorder Report (2017)

6.4. Organizations, processes and initiatives

Cybersecurity and cybercrime

UN processes

- UN Group of Governmental Experts (GGE) on advancing responsible state behaviour in cyberspace (convened in 2004/2005, 2009/2010, 2012/2013, 2014/2015, 2016/2017, 2019/2021)
- Open-ended Working Group (OEWG) on security of and in the use of information and communications technologies (convened in 2019/2020 and 2021–2025)
- Ad Hoc Committee to elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes (Ad Hoc Committee)

International organizations

- International Telecommunication Union
- Interpol
- FIRST

Multistakeholder processes

- Paris Call for Security and Stability in Cyberspace
- Global Forum on Cyber Expertise

Regional organizations

- African Union

    - AU Cybersecurity Expert Group
    - AfricaCERT
    - African Center for Coordination and Research in Cybersecurity
- ASEAN
- European Union
    - EU Agency for Cybersecurity
    - CERT-EU
- Organization of American States
- Organization for Security and Cooperation in Europe
- Shanghai Cooperation Organisation
- Conference on Interaction and Confidence Building Measures in Asia

Harmful content

- UN Security Council: Counter-Terrorism Committee
- Tech Against Terrorism partnership
- Global Internet Forum to Counter Terrorism (GIFCT)

6.5. Relevant IGF work

IGF Messages relevant to the issue

- IGF 2021 Messages: Trust, Security and Stability
- IGF 2020 Messages: Trust
- IGF 2019 Messages: Security, Safety, Stability and Resilience
- IGF 2018 Messages: Cybersecurity, Trust and Privacy

Other relevant IGF work

- Best Practice Forum on Cybersecurity
- Internet Standards, Security and Safety Coalition

7. AI governance

7.1. Policy issues

Artificial intelligence (AI) is now at the core of multiple digital services and products, from guiding our online experiences and powering smart devices, to shaping the decisions others make about us (e.g. in the context of recruitment processes, financial services, or the judiciary system). In addition, AI is bringing about changes in a myriad of sectors, ranging from financial markets to public health.

The policy implications of AI are far-reaching. For instance, algorithmic decision-making could result in discrimination, harmful stereotypes and wider social inequality. Similarly, while AI can potentially lead to economic growth, there are growing concerns over the significant disruptions it could bring. Issues related to privacy, safety, and security have been brought into focus, as well as the impact of automation on the job market. Calls are being made for the development of norms that can help to ensure that AI applications have minimum unintended consequences and effectively contribute to human-centred economic and social development.

There is no consensus about the magnitude of the impact that AI will have on the job market, since this will depend on unknown factors, such as the speed of adoption of AI and the contribution of AI to job creation. Some countries are discussing mechanisms for social protection, such as the idea of a universal basic income (UBI). The goal is to maintain the incomes of those who lose their jobs and, therefore, keep consumption high in the economy, which will, in turn, help to create jobs. A UBI could also be introduced with some conditionalities, such as the need for the worker to engage in reskilling in order for them to qualify for payment.

Key policy issues related to AI: A few examples

- **Economic and social implications**: AI contribution to sustainable development; the impact of AI on the world of work (automation of some jobs, reskilling and upskilling the workforce, social safety nets; etc.); new forms of digital divides (i.e. some countries and communities reap the benefits of AI, while others are left behind).
- **Safety and security considerations:** autonomous systems (from self-driving cars to autonomous weapons systems) and human safety; cybersecurity risks specific to AI systems; AI implications for national security.
- **Human rights:** privacy and data protection concerns in the context of various AI systems (from online services using user information to personalise/target content, to the challenges of facial recognition technologies); risks of discrimination associated with the use of AI systems in various sectors

(employment, social benefits, etc.); implications for freedom of expression when AI tools are used to detect and remove certain types of illegal or harmful online content.

- **Ethical concerns**: issues of fairness, justice, bias, and discrimination in the use of certain AI systems.

Some jurisdictions around the world have started working on regulatory frameworks to address such pitfalls. Examples include the ongoing work on an EU AI Act and Brazil's legal framework for AI.

But several questions remain open: What is it about AI that needs to be regulated? To what extent do we need new laws and how do existing ones apply to AI? How should regulations for AI be developed, and what principles should they embed? And to what extent can regulations developed in some jurisdictions serve as inspiration for others?

National AI strategies

While legal frameworks covering AI-related issues are slowly emerging around the world, the development of AI strategies and plans at the national level is more advanced. If in January 2019 only 14 countries had official AI strategies in place, this number has been increasing considerably since.

Australia, Brazil, China, Egypt, Germany, Ireland, Mexico, Saudi Arabia, and Russia are just a few examples of countries that have issued AI-related plans and strategies.

7.2. What can parliaments do?

Parliamentarians participating in IGF activities over the years have highlighted several 'messages' that are related to AI:

- Parliaments are called on to encourage:
  - Domestic stakeholders to actively and meaningfully participate in international multilateral and multistakeholder processes and fora focused on promoting ethical and human-rights-based approaches to the development and use of AI;
  - Governmental actors to conclude cooperation agreements with other countries designed to foster exchanges of experiences and technology transfers in the field of AI;

- Domestic stakeholders to develop and deploy AI in a manner that is consistent with principles outlined in documents such as the *OECD Principles for AI* and the *UNESCO Recommendation on the ethics of AI*.

- Noting that some jurisdictions around the world have started working on regulatory frameworks for AI, it is recommended that processes focused on developing legislative approaches to governing the development and use of AI consider the following:
  - Before regulation is developed, there has to be a clear understanding of what needs to be regulated and why. Also needed is an assessment of existing laws and regulations and the extent to which they already apply to AI systems or can be amended to cover such systems;
  - Taking a holistic approach when considering what about AI needs to be regulated: look not only at how AI impacts or may impact individuals and their human rights, but also at broader societal implications (e.g. in terms of public interest and the common good);
  - When requirements are set for the development and use of AI, clarity should be offered in terms of roles and responsibilities for implementing those requirements, as well as for monitoring the implementation;
  - Ensuring that regulation is flexible, agile, future-proof as much as possible, and does not unduly stifle innovation;
  - Paying attention to principles already embedded into guidelines and frameworks for AI developed at international level, such as those developed by the OECD, Council of Europe, and UNESCO (e.g. transparency, human oversight, accountability).
- Parliaments are invited to
  - (a) encourage the responsible use of AI as a tool for advancing sustainable development and improving governmental services, and an instrument for evidence-based policy making, where appropriate, and
  - (b) promote the integration of AI in formal educational curricula and informal training programmes.

7.3. Instruments and resources

International

- OECD Recommendation on Artificial Intelligence (OECD Council, 2019)
- G20 AI Principles (G20, 2019)
- UNESCO Recommendation on the Ethics of Artificial Intelligence (UNESCO, 2021)

- Artificial intelligence and privacy, and children's privacy (Special Rapporteur on the right to privacy, 2021)

Regional

- Blueprint: Artificial Intelligence for Africa (Smart Africa, 2021)
- ACHPR/Res.473 (EXT.OS/XXXI) 2021 – Resolution on the Need to Undertake a Study on Human and Peoples' Rights and Artificial Intelligence, Robotics and other New and Emerging Technologies in Africa (African Commission on Human and Peoples' Rights, 2021)
- Coordinated on Artificial Intelligence (European Commission, 2021)
- Recommendation of the Committee of Ministers on the protection of individuals with regard to automatic processing of personal data in the context of profiling - CM/Rec(2021)8 (Council of Europe Committee of Ministers, 2021)
- Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems (Council of Europe Committee of Ministers, 2020)
- Declaration Decl(13/02/2019)1 on the manipulative capabilities of algorithmic processes (Council of Europe Committee of Ministers, 2019)
- Strategy on Artificial Intelligence (European Commission, 2018)
- Recommendation n°2102(2017) about Technological convergence, artificial intelligence and human rights (Council of Europe Parliamentary Assembly, 2017)

7.4. Organizations, processes and initiatives

- OECD
- UNESCO
- European Union
- African Union (working on developing an AI strategy)
- Council of Europe: Committee on AI
- Partnership on AI

7.5. Relevant IGF work

IGF Messages relevant to the issue

- IGF 2021 Messages (a few references to AI)
- IGF 2020 Messages: Data (a few references to AI)
- IGF 2018 Messages: Emerging technologies

Annex: Digital policy observatories

Resource	Maintained by	Overview
Digital Watch Observatory	Geneva Internet Platform	A digital policy observatory, which provides a neutral one-stop shop for the latest developments, overviews, events, actors, instruments, and other resources covering dozens of digital policy topics.
OECD.AI	OECD	A policy observatory focused on artificial intelligence.