IGF Daily

IGF Daily **No. 2** – Wednesday, 14th November, 2018

REPORTING DAILY FROM THE
13th INTERNET GOVERNANCE FORUM

dig.watch/igf2018

The *IGF Daily* is prepared by the Geneva Internet Platform with support from the IGF Secretariat, ICANN, the Internet Society, and DiploFoundation

HIGHLIGHTS FROM DAY 2

Trust, data, and capacity development were three echoing issues on the second day of the 13th Internet Governance Forum in Paris. Many discussions focused on how to apply this year's IGF theme, the 'Internet of Trust', in practice.

Trust can be increased through more awareness, transparency in dealing with technology, higher accountability of tech companies, and fairness in distributing 'digital dividends'. However, several questions linger in the IGF meeting rooms and corridors. Is trust about technology per se, or about the people and institutions behind technology? Can trust be developed 'by design' via technological solutions, as blockchain proponents argue? How can we ensure that trust is part of our daily digital reality and not an abstract notion? It is clear that trust will remain high on the agenda of the IGF and other upcoming digital policy events.

Data featured highly in yesterday's discussions as a cross-cutting issue affecting legal, economic, and social aspects of digital growth. More specifically, discussions reflected on data protection and the impact of the General Data Protection Regulation (GDPR) on policy developments worldwide. The GDPR has affected not only data protection itself, but also business models and overall approaches to dealing with the impact of technology on modern society. Yesterday's sessions reflected on how countries worldwide can develop data policies and regulations.

Capacity development has been an underlying theme of the IGF process for many years. Yesterday's discussions illustrated that capacity development approaches and strategies need to go beyond simple training. For example, preparing the workforce to deal with AI and the future of work requires much more than training and workshops. It requires a new societal approach to continuous learning beyond school education.

Here, we round up the main highlights, using the *Digital Watch* taxonomy of digital policy issues.

Technology *and Infrastructure*

Emerging technologies are a matter of trust

Trust in the potential of emerging technologies, such as artificial intelligence (AI) and blockchain, is crucial if we want to make the best use of their ability to improve our lives. Blockchain can be used to increase trust in public institutions and government processes, as fully decentralised systems are expected to reduce the need for oversight.

A first step in building trust is raising awareness and understanding of AI and other emerging technologies. Many countries are currently looking for effective ways to use AI for delivering public services, managing content policy, and increasing cybersecurity. Others fear being left behind in AI-driven developments. We may see new divides based on those countries which can effectively employ AI and those which have not yet taken such steps. Those who are

Continued on page 2

Credit: DiploFoundation

Missed the highlights from Day 1? Download yesterday's *IGF Daily*.

HIGHLIGHTS FROM DAY 2

Continued from page 1

falling behind may lose trust in the potential of technology to improve their lives.

Trust may be further built by ensuring transparency, accountability, fairness and due diligence in the use of new technologies. The more human rights are observed in the development of AI, the higher the level of trust likely to be achieved. Some concerns related to the use of AI can be mitigated by human rights impact assessments carried out early in the development process.

Trust is also important in relation to the Internet of Things (IoT), which has evolved from an emerging technology to a daily reality. Day 2 discussions referred to developing security best practices in use of IoT, and embedding a 'security-by-design' approach in the design of IoT, as two ways to mitigate cybersecurity risks.

Infrastructure for access remains a development challenge

It is still difficult to ensure Internet connectivity in small island states and remote areas in countries worldwide. Laying fiber optic cables over long distances is expensive and increases the cost of access. Enabling a regulatory framework is a further challenge in ensuring Internet access.

Yesterday's discussion suggested several ways to stimulate infrastructure development, including public-private partnerships, the use of universal service funds, and incentives to the private sector to invest more. To use new technologies fully, we need new technological standards to ensure that the Internet remains open, interoperable, and globally accessible.

Net neutrality: regulation is not sufficient

While global approaches towards net neutrality vary, there is a growing trend to safeguard this principle, often motivated by the desire to ensure access, speed, and bandwidth. Adopting regulations on net neutrality is not sufficient. Net neutrality principles must be embedded in the commercial practices of Internet carriers to ensure effective implementation, monitoring, and enforcement.

Enforcing net neutrality regulations is not always straightforward: it can be difficult to measure Internet traffic speeds and to identify discriminatory practices. Harmonising methodologies and tools used by regulatory authorities, and using crowdsourcing solutions to allow input from users, can help.

Economic

New technologies bring new economic challenges

Day 2 discussions acknowledged that we have much to learn about how new technologies, such as AI, will affect trade, regional integration, and education. Some challenges are common to many countries. For example, countries across the world are facing questions about the impact of AI on employment. Other challenges are more specific. For example, limited Internet access hinders economic growth for small island developing states. The diversity of digital economic challenges should be reflected in global and regional discussions.

The impact of AI on employment is frequently mentioned in economic discussions. Governments and the private sector share responsibility to make young people employable in the future. However, as the group most strongly affected, youth themselves need to be involved in discussions related to AI and employment.

Yesterday's discussion on economic issues also covered investment and funding of new business models, based on governmental resources, private sector income, or hybrid models. We have seen successful public-private partnerships in developing digital infrastructure that is easily and equally accessible to all.

Day 2's prominent issues

This tag cloud shows the prominent issues of yesterday's discussions. DiploFoundation's Data Team analysed over 50 transcripts, captured from real-time captioning, which were then processed using a custom digital policy dictionary. The exercise was automated with the assistance of text analysis software.

HIGHLIGHTS FROM DAY 2

Cybersecurity

Balancing risks and opportunities

Yesterday's discussions of cybersecurity balanced the risks associated with new technologies against their potential to increase security. For example, while the risks associated with AI are often discussed, AI can also help identify and remove extremist content online, and content which is harmful for children. Best practices, such as the World Economic Forum's Industrial IoT Safety and Security Protocol, offer an example to the private sector of how they can support and increase security.

Internet users should be at the centre of participatory and consultative processes to develop cybersecurity policies and legislation. Developing countries in particular can benefit greatly from building the capacities of users on digital security practices. Civil society organisations have an important role to ensure that technology users are well-represented in the legislative process.

Protecting children from harm

Popular belief suggests that most of the content which could be harmful to children is on the dark web. However, a lot of inappropriate content for children is found on the open web. The fact that the open web is more easily accessed by children makes this content of higher concern when it comes to child online protection.

Methods to help children to protect themselves from online risks include developing their digital and media literacy, and introducing digital literacy elements in sexual education programmes. The tech industry remains a crucial actor in detecting and removing online content which is harmful for children.

While we must protect children from online risks, we also need to remember that children have digital rights. Children's rights should be at the heart of products and services developed for them.

Human rights

Countries assessing data protection frameworks

The EU's GDPR, which came into effect in May 2018, triggered many discussions at the IGF on approaches to data protection worldwide. A number of Commonwealth states, for instance, have limited legislation to address data protection. Such countries need assistance to build capacity and raise awareness; the aim of the newly established Common Threat Network, supported by the UK and Canada, is to help countries develop national data protection frameworks. In Africa, several countries are also updating their laws in line with the GDPR.

Making technology accessible to persons with disabilities

Two sessions on Day 2 addressed the rights of persons with disabilities. Participants discussed the particular challenges persons with disabilities face, and offered recommendations for closing the accessibility gap. Discussions also focussed on the broader perspective of building a more inclusive society and providing training for ICT developers and policy shapers in ensuring accessibility for persons with disabilities.

Persons with disabilities are functionally limited by their environment. To overcome this, technology should be made accessible to persons with disabilities, and standards should be both developed and enforced.

Legal

Digital regulations in focus

'Technology moves much faster than the law' was the underlying message of yesterday's legal discussions, which brought the impact of the GDPR on digital legal developments in focus.

The GDPR's impact beyond EU borders creates mix reactions. It kindles a culture of privacy and data protection, and may inspire other countries to follow this model. However, it also creates challenges of cross-border jurisdiction and highlights the need for digital cooperation to identify internationally accepted solutions and regulations.

Jurisdiction issues in dealing with cybercrime

Jurisdiction issues in dealing with cybercrime featured prominently in yesterday's discussions. The main challenge is how investigating authorities in one country can request data from private actors in another country (e.g. tech platforms).

Two regulatory examples were addressed: the Cloud Act in the USA and the EU e-Evidence regulation (still under development). Discussion suggested a few criteria for cross-border access to data including notice to users, independent judicial authorisation, specific legal processes, provisions in case of conflict, and transparency.

The concern expressed by developing countries about the use of bilateral arrangements to deal with jurisdictional challenges of cybercrime will increase pressure for multilateral regulation. An emerging solution is the new additional protocol to the Budapest Convention which should provide mechanisms for investigating authorities in one country to directly request data from private actors in another country. Ultimately, an effective and balanced approach to jurisdiction for investigation will require interoperable solutions based on harmonised legislation and international cooperation.

HIGHLIGHTS FROM DAY 2

Socio*cultural*

The disruptive effects of fake news

The term 'fake news' is back, despite Day 1 attempts to replace it with 'information disorder'. On Day 2, discussions about content broadened from Monday's debate on hate speech, fake news, and disinformation, to encompass online content during elections and in political processes. Fake news has disrupted recent elections as we have seen in Brazil. Starting from isolated cases, the spread of fake news during elections is emerging as a widespread trend.

How should fake news be regulated? Several camps emerged: on one side were those arguing in favour of a strong approach by governments, and holding Internet platforms more accountable. For instance, Nigeria plans to control and criminalise fake news. A middle approach argues in favour of civil liability rather than holding platforms criminally responsible. More flexible approaches involve collaboration between governments and intermediaries, such as Facebook's partnership with the French government, to use fact-checking tools to combat fake news.

Any solution needs to be supported by developing users' digital literacy. Users (and in particular younger users) need critical thinking skills to help them better assess the authenticity of information.

Development

Digital tools and the SDGs

Yesterday's discussions asked how can we ensure that no one is left behind in digital developments. The sustainable development goals (SDGs) provide a policy and implementation context for ensuring the cross-cutting impact of digital technology on development. A few issue areas were mentioned, including the use of digital technologies for the inclusion of people with disabilities in the realisation of various SDGs. Wikipedia was mentioned as an example of a simple, impactful, and innovative digital tool for contributing to the SDGs by recording and preserving the knowledge of local communities in developing countries.

UNESCO presented the Internet Universality Indicators as a practical tool for assessing Internet development and monitoring the implementation of the SDGs in the digital field.

Developing capacities for the future of work

Capacity development is a cross-cutting issue impacting economic, social, and infrastructure aspects of digital growth. The need for people to acquire new skills to effectively use new technologies remains an over-arching capacity development theme. In order to prepare for the jobs of tomorrow, continuous learning is a task not only for educational systems, but a cultural challenge for all of society.

Yesterday's discussions on capacity development covered awareness and knowledge development for effective data regulations, closing gender gaps, training journalists to deal with misinformation, and strengthening the capacities of individuals and communities to deal with cyberbullying and hate speech.

Digital growth for Small Island Developing States (SIDS)

The Dynamic Coalition on SIDS in the Internet Economy, which had its first meeting at this year's IGF, addressed the following issues: affordability (broadband and Internet price control measures), accessibility (the digital divide, and the role of community Internet resources in education and social development), and emergency accessibility due to the high vulnerability of SIDS, which relates not only to digital access, but also to the diversity of technological options that could be used in the case of emergency.

Prefix *Monitor*

Monitoring the use of prefixes offers us an 'x-ray' of digital discussions. Prefixes signal the direction and nuances of some discussions, and tell us how certain issues are framed.

Based on our analysis of IGF transcripts for Day 1 and Day 2, use of the prefix *cyber* was by far the most prevalent trend. As in previous years, *cyber* was commonly used for cybersecurity-related issues. We saw a tight race between *digital* and *online*, occupying second and third places respectively. A relative newcomer to digital policy lingo, the prefix *tech* came in fifth place, after *net*. The prefix *virtual* was more rarely used during Day 1 and Day 2.