Local interventions, global impacts: How can international, multistakeholder cooperation address Internet disruptions, encryption and data flows

Messages

- While there is increasing awareness of potential unintended impacts of Internet shutdowns, they continue to happen around the world. Shutdowns may affect the exercise of human rights, have economic implications, and may lead to the fragmentation of the Internet (as they often have cross-border effects).
- The motivations behind Internet shutdowns vary, they may be legitimate, but sometimes blocking is used to address problems that could be solved by using the Internet. It is important to have a process in place that ensures: transparency, , adequate oversight, and redress mechanisms.
- Encryption helps promote public security, and allows a better protection of human rights (such as those of activists, journalists, and minorities). It should not be seen as a by-default security threat. Countries that consider bans on encryption should understand the limitations and impacts of such a ban (e.g. cross-border effects, undermining the security of citizens, challenging the human rights of groups or minorities, and determining companies to move to other jurisdictions where such bans are not in place). Tools developed or employed to undermine encryption can come into the hands of those with illegal or criminal purposes. Governments and industry should cooperate and Identified vulnerabilities in encryption/encrypted products should be reported to the vendors.
- Stakeholders should work together on achieving an appropriate balance between the interests of citizens and entities to secure their data and the needs of law enforcement agencies, while not undermining the fundamentals of the technology.
- Data is an important asset in the digital era, due to its multiple uses. As governments and private companies collect and process large amounts of data, there is a need for more transparency and accountability in these processes. Users should be educated on how their data may be used and how to protect it.
- The digital economy depends on the free flow of data, but this should be balanced with data protection. Governments, private companies, and civil society should work together on basic sets of rules that allow data aggregation and data flows, while also protecting the integrity of data and the privacy of individuals.