



# Global Digital Compact

## A Multi-Stakeholder Consultation on Shaping the Global Digital Compact



*Submission From*  
DIGITAL EMPOWERMENT *foundation*

India-Level Multi- Stakeholder  
Consultation to Contribute to the  
Campaign of United Nation's  
**'Global Digital Compact'**





Global  
Digital  
Compact

**Location:** New Delhi

**Date:** March 06, 2023

## Our Common Agenda – Theme 7: Improve Digital Coordination

**Participants:** Multistakeholder; 40 rural information agents from 15 different states of India; around 70 digital innovators from India, Sri Lanka, Bangladesh and other south Asian countries; civil society organisations; bureaucrats, technocrats and academics

**Format and Methodology:** The consultation started with a few keynote addresses from eminent experts on digital access and rights followed by focused groups discussions and the consolidation of inputs by facilitators

The multistakeholder consultation organised by Digital Empowerment Foundation was attended by several stakeholders, including bureaucrats, civil society organisation members, representatives of organisations, government and people from the margins. With the objective of developing comprehensive inputs in each thematic area of the United Nation's Global Digital Compact, the participants split into seven groups and discussed the core principles involved in each and the key commitments that the government, private sector and civil society should adhere to for improving digital coordination while leaving no voice behind.

"The technology is changing fast, and the regulations sometimes stay static; we need short-term policies and regulations on AI," said one of the participants in the discussion on the regulation of Artificial Intelligence. A critical point on how people's right to remain unconnected is as essential as their right to have resources to be connected emerged from the discussion on connecting all people to the internet. The thematic discussion also deliberated how the internet should not be fragmented and the core principles of net neutrality should be upheld. The thematic discussion on applying human rights online pointed out how the lack of basic resources to survive in communities such as Afghan refugees in India limits them and compromises on asserting their human rights online. One suggestion that emerged from the discussion on protecting data was using a message notification whenever the government or third parties use personal data.

## The consultation was led by



**Amandeep Singh Gill**  
UN Secretary-General's  
Envoy on Technology



**Laurent Le Danois**  
Team Leader - Cooperation  
Section, Delegation of the  
European Union to India  
and Bhutan



**Abhishek Singh**  
President & CEO NeGD;  
MD & CEO Digital India  
Corporation



**Osama Manzar**  
Founder and Director,  
Digital Empowerment  
Foundation

## The group discussions were facilitated by



**Mohd Tarique,**  
(Ashoka Fellow  
Director, Koshish, TISS)

**Connect all People to  
the Internet, Including  
all Schools**



**Shalini Kala**  
(Rural Development &  
Agriculture Specialist)

**Accountability for  
Discrimination &  
Misleading Content**



**Natasha Badhwar**  
(Professor at  
Ashoka University)

**Apply Human  
Rights Online**



**Amir Ullah Khan**  
(Professor at  
MCRHRDI)

**Protect Data**



**Amitabh Singhal**  
(Internet & Telecom  
Policy Expert)

**Avoid Internet  
Fragmentation**



**Dr Renata Dwan**  
(Senior Expert, Office  
of the UN Envoy  
to Technology)

**Regulation of  
Artificial Intelligence**



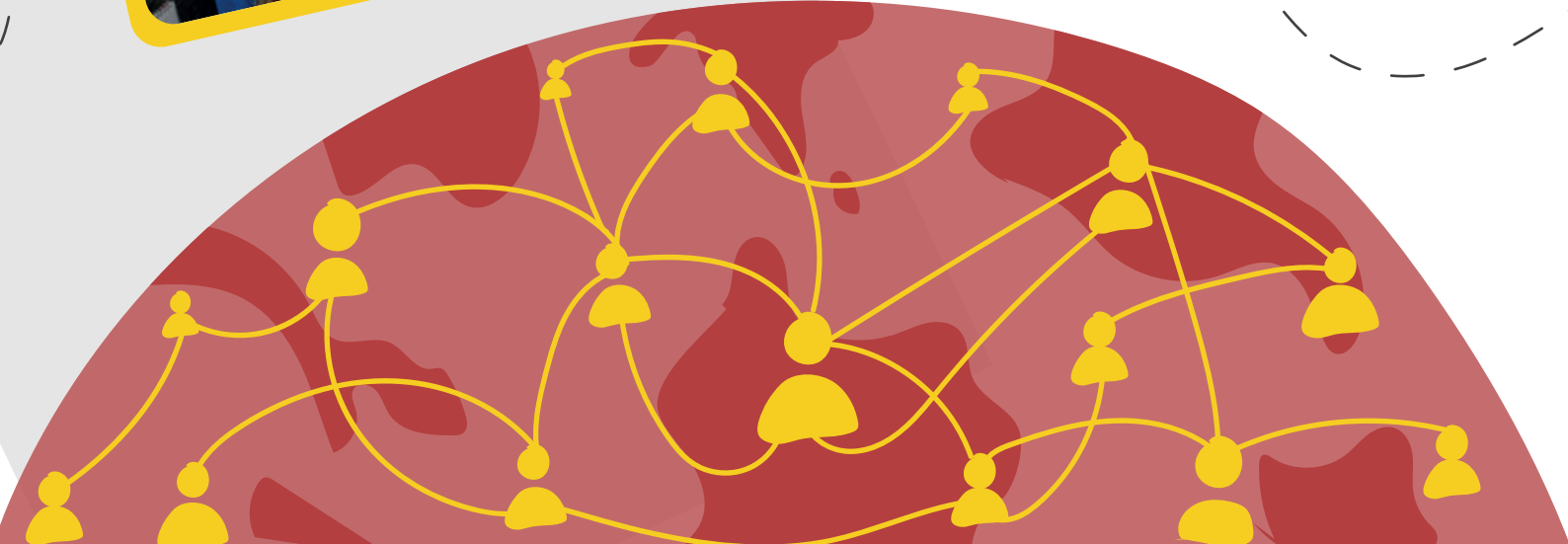
**Syed Kazi**  
(Director at Council for  
Social and Digital  
Development (CSDD))

**Digital Commons as a  
Global Public Good**

# 1



**Connect all people  
to the Internet,  
including all schools**



## Core Principles

- Equal access- everyone, regardless of gender, geography, and economic status, should have access to the Internet.
- Any and all government programs with a digital mode of implementation should be based on real-life contexts - so assuming universal connectivity needs to be noted because it should not be the case that lack of connectivity is going to affect my rights (and therefore, the next point remains important).
- Right to remain unconnected is just as important.

## Key Commitments:

- **Civil Society:** To bring the details, and information about programs to the ground level would be best done by civil society organisations due to their presence. Understanding the resistance of people to some programs is also their responsibility, as well as finding the dark areas/gaps.
- Governments should engage in the scaling up of programs. Cost-effective content development, and flattening the geographical skews in investments is also government responsibility. This includes building infrastructure and investing in people, like teachers.
- The private sector should invest in the research and development of new platforms and applications.

## Action Points:

- An application that works in a hybrid mode, perhaps without internet connectivity.
- Platform and content both have to be available in local/vernacular languages.
- Convergence of different schemes/programs that remove the exclusions  
Two-way partnership between NGOs and Governments to get technology to every individual.
- Increasing the number of Community Resource centres like the existing ones, (similar to the ones maintained by DEF) because they provide an effective model.

# 2

## **Avoid Internet fragmentation**



## Core Principles

- Counter a potential threat to the One World One Internet, a key pillar towards building a Free to Access, Open and an interoperable Internet
- Fragmentation, or Splintering the Internet or Balkanization of the Internet is real and happens in many ways all around us and remains a threat to Free and Open Internet. It threatens the very core – Network neutrality.
- Caused by government actions blocking access to the internet, commercial interests charging differential fees and for preferential access
- Leads to security vulnerabilities, and lesser democratisation

## Key Commitments:

**Governments:** Government/Regulatory policies, rules and actions should by default keep the Internet open & freely accessible and limit interference to the minimum and strengthen Network Neutrality principles.

**Private sector** players must promote open and interoperable Internet, using and adopting open standards and avoiding proprietary protocols, not insist on commercial prioritization of paid-for traffic.

Both **government and private sector** must contribute to Strengthening Global Internet Governance to keep developing and establishing norms and practices, standards and protocols to more robustly prevent instances of fragmentations

**Civil Society:** Internet Governance Organisations must deepen engagements with governments to keep facilitating and sensitizing governments, business and civil society to keep coordinating and working together to prevent Fragmentation. Elaborate capacity building & resource allocations especially in developing and LDCs areas for training and skill development and building Infrastructure, where little or none exists.

All three must work together towards:

- Encouraging encryption and privacy applications and practices
- Wider adoption of various Security protocols and standards (DNSSEC, TLS, PKI, MANRS, KINDNS, DANE, SPF, DKIM, DMARK, etc.) – Building resilience.
- Standardized and improved protocols viz BGP and OSPF – better interoperability, and Universal adoption of IPv6 protocols. Promote building more ubiquitous infrastructure/networks and lowering costs of devices and access.



# 3

## Protect data



## Core Discussion:

People discussed what data is and what public and personal data is, whether this data needs to be protected, whether people 'have anything to hide' should be a criterion for the right to privacy, why we worry about privacy and vulnerability, on how AI/algorithms work on data, on surveillance, and more.

## Core Principles

- Personal data is important and needs to be protected. Data is not one homogeneous unit- it needs to be classified because along with public data, there is also data that is sensitive and confidential. Bank and Aadhaar ID details, or health data would fall into this category.
- Consent on what data is being used and where is required, and needs to be made understood.
- AI and its impacts are not properly understood, but it is a threat when AI finds and sorts personal data without a proper system in place.
- An international standard for data protection.

## Key Commitments:

Do *Governments and the Private Sector* that collect sensitive data actually have strong mechanisms to keep data safe? In light of several incidents of breaches, these have to be ensured after being promised to the public.

*Civil Society, and the International Community in particular*, like the EU or the UN has to take the lead in internationalising a law for data protection, something that sets a global standard and is adopted by nation-states. The Government has to ensure this strong data protection law is enforced immediately.

# 4

**Apply human  
rights online**



## Core Discussions:

A rich discussion took place on a variety of issues, and among a diverse crowd there were people who worked on the ground with several communities, both for bringing them connectivity and digital literacy, as well as looking into other challenges like the many aspects of human rights that were violated. They included two people from Assam, who worked with tea plantation labourers; others from Mewat, an area that witnesses violence against the minority community; some working with artisans in Punjab; and some working with migrant workers and other thrust communities who were stuck without food and rations during the pandemic; some representing Afghan refugees. The discussion highlighted the challenges of poverty and literacy in rural areas, leading to both limited human rights and digital fraud. How do people who do not have basic access to food/resources raise the issues of human rights? There is an increase in people falling prey to digital frauds linked to OTPs across social classes and geographies. Blame cannot be allocated saying people were illiterate or did not attend training programs. Many children during the pandemic were better able to identify fake news and misinformation about the coronavirus spread and vaccines than several older, mature members of the press and even the government who took to blaming marginalised castes and communities.

## Key Commitments:

**Governments** should implement cyber-security laws, and laws to discourage misinformation. They should work on stopping internet shutdowns. People who raise their voices offline are charged cases, and those who raise their voices online are met with internet shutdowns. The shutdowns also prevent the adoption of digital services. To this end, perhaps **the International Community and Organisations** should enact and pressure the governments for a law to prevent governments from engaging in internet shutdowns.

**Private Sector:** While soft skill training is necessary, hardware is just as important. Funding, support and strategy for hardware can be sourced from the private sector. This is also something NGOs and Civil Society organisations can work on. Additionally, they also should work with the Government and Private sectors to ensure their commitments are properly met.

# 5

**Introduce accountability  
criteria for discrimination  
and misleading content**



## Core Principles

- Who is to be held accountable? How much are the governments, the companies or the people themselves accountable? There needs to be an understanding as well as a template of accountability.
- Technology has to be responsible, it should not be promoting misleading content.
- Ensure all marginalised groups or the groups that tend to get ignored - have to be focused on.
- Laws in place that are not being enforced need to be enforced.  
A balance between accountability for content while not stifling freedom of speech and creativity.

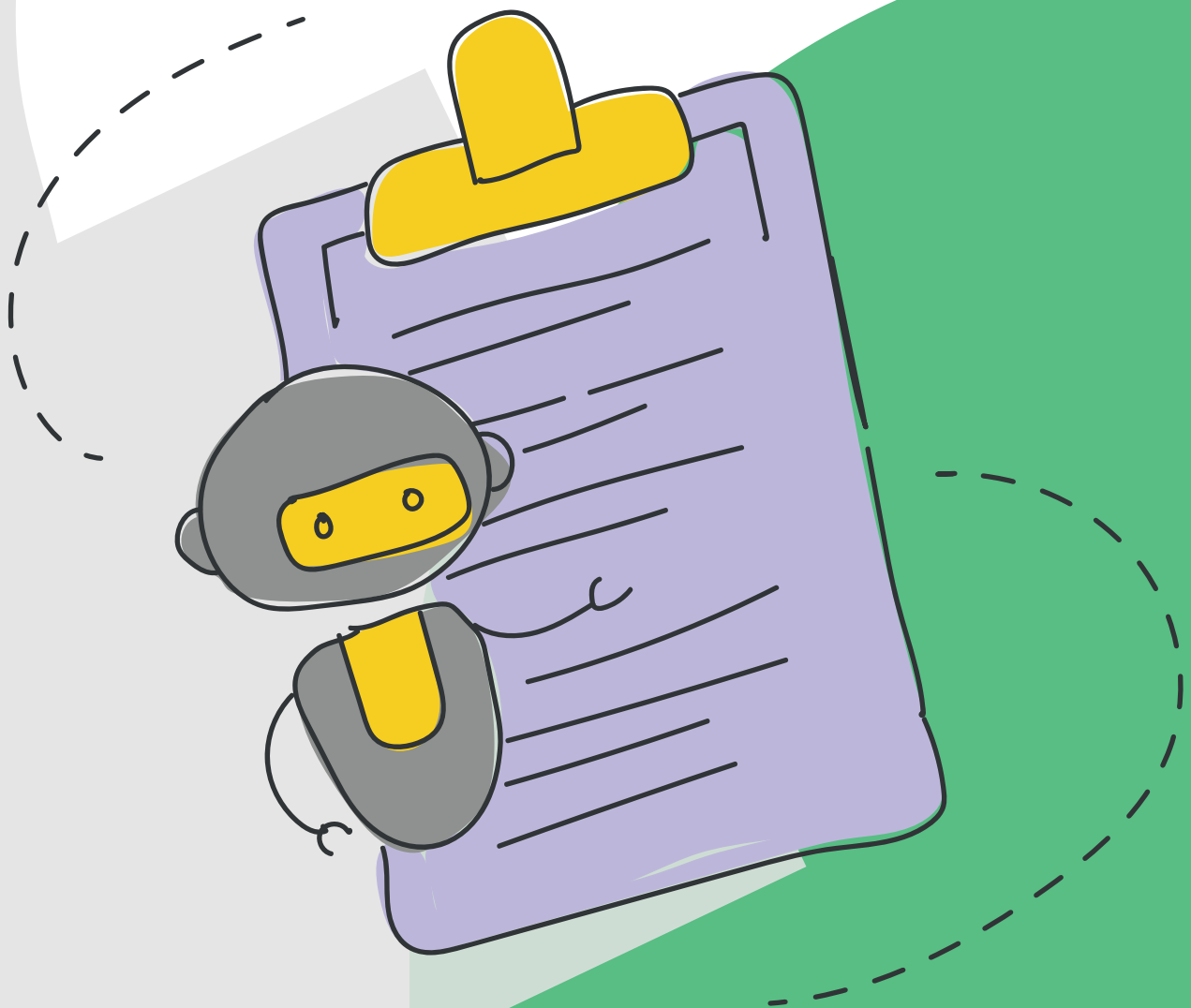
## Key Commitments:

All sectors should work together on building a template of accountability. The UN should also coordinate this process. In addition,

- **Governments:** define, and design-compliant redressal mechanisms and prevent repeat offences for misleading content - while also not discouraging creativity and freedom of expression.
- **Private Sector:** To design and build responsible platforms that discourage fake news and misinformation. Redressal mechanisms also need to be built into the platforms.
- **Civil Society:** Bring issues they see on the ground to the notice of the government. Aid in the timely verification of content by working with institutions on the ground.

# 6

## Promote regulation of Artificial Intelligence



## Core Discussions:

Why does there need to be regulation? Because it is about machines simulating human actions and behaviours. It can also reinforce the digital divide between those who have access to data (in both designing systems and being represented in data) and those who do not get to participate. AI is also going to regulate future human thinking, and therefore some intervention is necessary to decide how we want the future of critical thinking to be.

Three 'E's – **E**thical: human-centred, the biases fed into AI systems through faulty or incomplete data; **E**quity: access needs to be equitable to prevent gaps of people who are outside data; **E**xpertise: AI will not achieve its goals and won't be useful if the data which it draws is not good. How do we look at the verifiability and authenticity of the data?

## Key Commitments:

Apply a shorter time frame to regulations, given the nature and speed of development of AI technology.

- Think about a conversation-type model for regulation rather than laws; This can be between communities, sectors, and countries to collectively try and resolve challenges.
- We need a careful definition of AI.
- A critical part of the regulation of AI is data literacy. This is where Civil Society Organisations come in. This education will bring the empowerment to participate in the conversation about AI. This connects to the question of how much under the hood of an AI tech we need to know and understand to resolve the challenges.



# 7

## Digital Commons as a global public good



A comparatively lesser participation in this table than in the others, given the confusion and lack of clarity on what the Digital Commons is. Is it a public hood, how can it be one, and what are the narratives around this?

### **Key Commitments:**

- Digital resources and access are critical for everyone
- An understanding and awareness of the Digital Commons are important.
- The Digital Commons must be based on right-based principles - based on universality, diversity, and accessibility; it must be access-restrictions-agnostic.

### **Key Commitments:**

- **Governments:** Policy and programs must be facilitative of promoting the Digital Commons at the levels of central and local governances, i.e, decentralised. An international charter which the governments could follow would be helpful towards UN SDGs.
- **Private Sector:** In making the digital commons more accessible and participative since the private sector owns most licences and content.
- **Civil Society:** In building awareness in the community on the digital commons, its needs and making it participative for everyone.



*Submission to the*  
**'Global Digital Compact' by**  
**DIGITAL EMPOWERMENT *foundation***

---

India



Soochna  **preneur**  
Information, Entitlements & Empowerment



## About Digital Empowerment Foundation

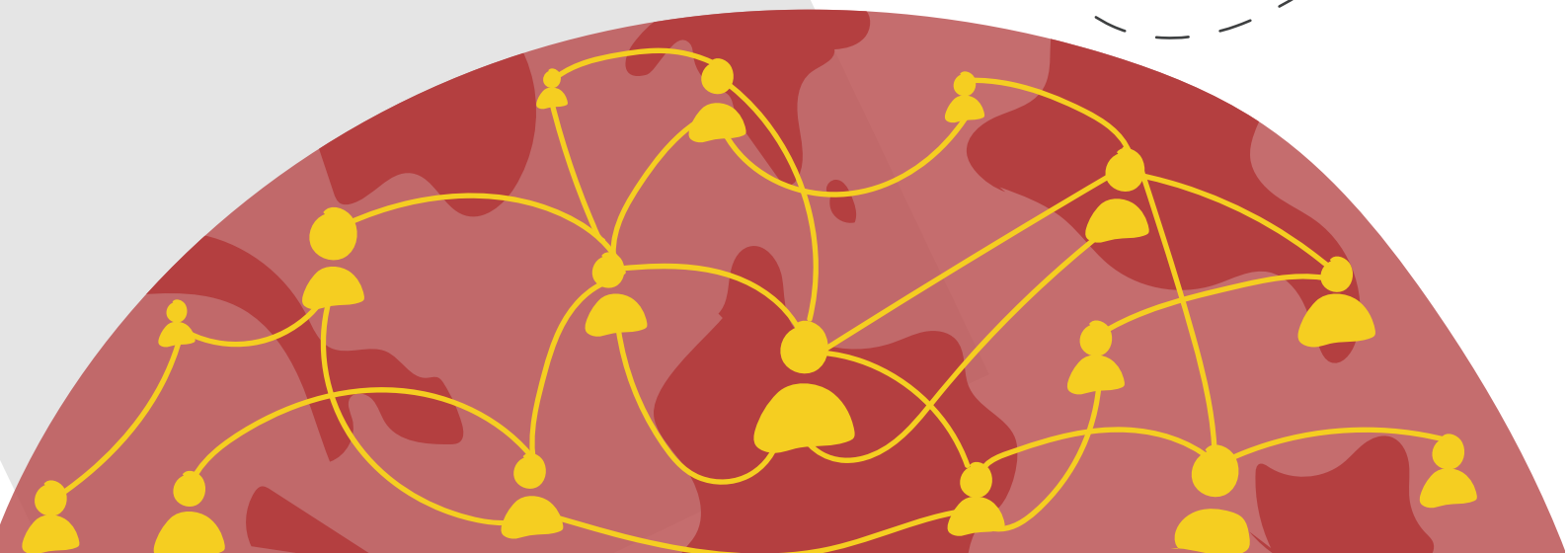
Founded in 2002, Digital Empowerment Foundation has been working to empower marginalised and unconnected communities living at the edge of information by enabling them with digital capacity, access and rights across the pillars of education and entertainment, livelihood and finance, health and agriculture, culture and heritage, with a special focus on digital rights for women and adolescents. With a 10,000 strong cadre of digital foot soldiers across India, DEF has interventions in 2,000 locations in 135 districts across 24 states in India. Additionally, DEF has a strong network in South Asia and is also an influential member of several global digital initiatives and organisations like Internet Governance Forum (IGF), Internet Society (ISOC), Association of Progressive Communications (APC), World Wide Web Foundation (WWW) and Global Network Initiatives (GNI). Going forward from 2021 to 2030, DEF is focused on working to connect the unconnected, as well as develop a healthy ecosystem wherein those who are connected can live a life free from fake news, misinformation and Internet shutdowns



# 1



**Connect all people  
to the Internet,  
including all schools**



## Core Principles

**a. Universal Connectivity:** Universal Affordable and Accessible Connectivity for all social groups and communities based on equality and equity principles and fairness. According to the International Tele Communication Union, 2.9 billion people, more than one-third of the world population, still remain offline. This percentage is higher for developing and least developed countries.

**b. Meaningful Connectivity:** A level of connectivity that allows users to have a safe, satisfying, enriching and productive online experience at an affordable cost (ITU, 2022) without allowing unjust and covert practices by telecom service providers.

**c. Freedom to remain unconnected:** As internet is not a natural good, if people so choose, they should have the freedom to remain unconnected as well as have equal access to rights and entitlements offline.

**d. Sustainability:** To ensure sustainability in the context of exceeding planetary boundaries, uncontrolled growth in digital itself must be curtailed. Instead of looking at digitalization as the answer to everything, we should also explore low-technology or no-technology solutions and innovations. Looking this issue from the point of adverse climate change effects, internet outages and its unimaginable consequences.

## Key Commitments

**a. Governments:** Ensuring equity in connectivity with respect to geography, caste, gender, (dis)ability (both hidden and visible), age, language (with special focus on local languages and indigenous languages) and religion. Legislate internet access as a basic right. Connect all government run / public funded schools at all levels (primary, lower secondary, upper secondary and secondary), all households, and community centers. Target: ITU 2030 targets.

**b. Private Sector:** Provide technical support to community networks in unconnected areas. Provide support to connecting all government run / public funded schools. To ensure sustainability, private sector must also commit to discarding practices of planned obsolescence and must incorporate repairability. Transfer surplus and unused data for public purpose and usage in schools and community centers.

**c. Civil Society:** Highlight the plight of internet dark areas and ensure that they are not excluded from availing benefits and services. Civil society must take initiatives to monitor digital supply chains for environmental and labor violations.

**d. International community:** digital economy has environmental impacts in the form of energy use due to increased use of devices and increased bit rate that is not offset due to gains in energy efficiency, e-waste and mining/ extraction, uncontrolled growth in digital would not be feasible. As such, users, especially in the global north must be encouraged to limit their uses.

# 2

## **Avoid Internet fragmentation**



## Core Principles

- a. Free and open Internet
- b. Decentralized but interconnected internet

## Key Commitments

**a. Governments:** Internet content takedowns must only be done in a transparent manner in accordance with the procedure set by the law. The emergency powers can't be extended perpetually.

**b. Private sector:** Private sector must respect inter-operability and backward compatibility in technical standards. To make the internet more inclusive, they must also support Internationalized Domain Names (IDN) using local language scripts. Encourage open hardware and open software.

**c. International community:** International community and UN must urge the governments against misusing emergency powers and national safety concerns to limit access to content critical of the government..



# 3

## Protect data



## Core Principles

- a. Democratic formulation of data protection legislations
- b. Accountability
- c. Purpose limitation

## Key Commitments

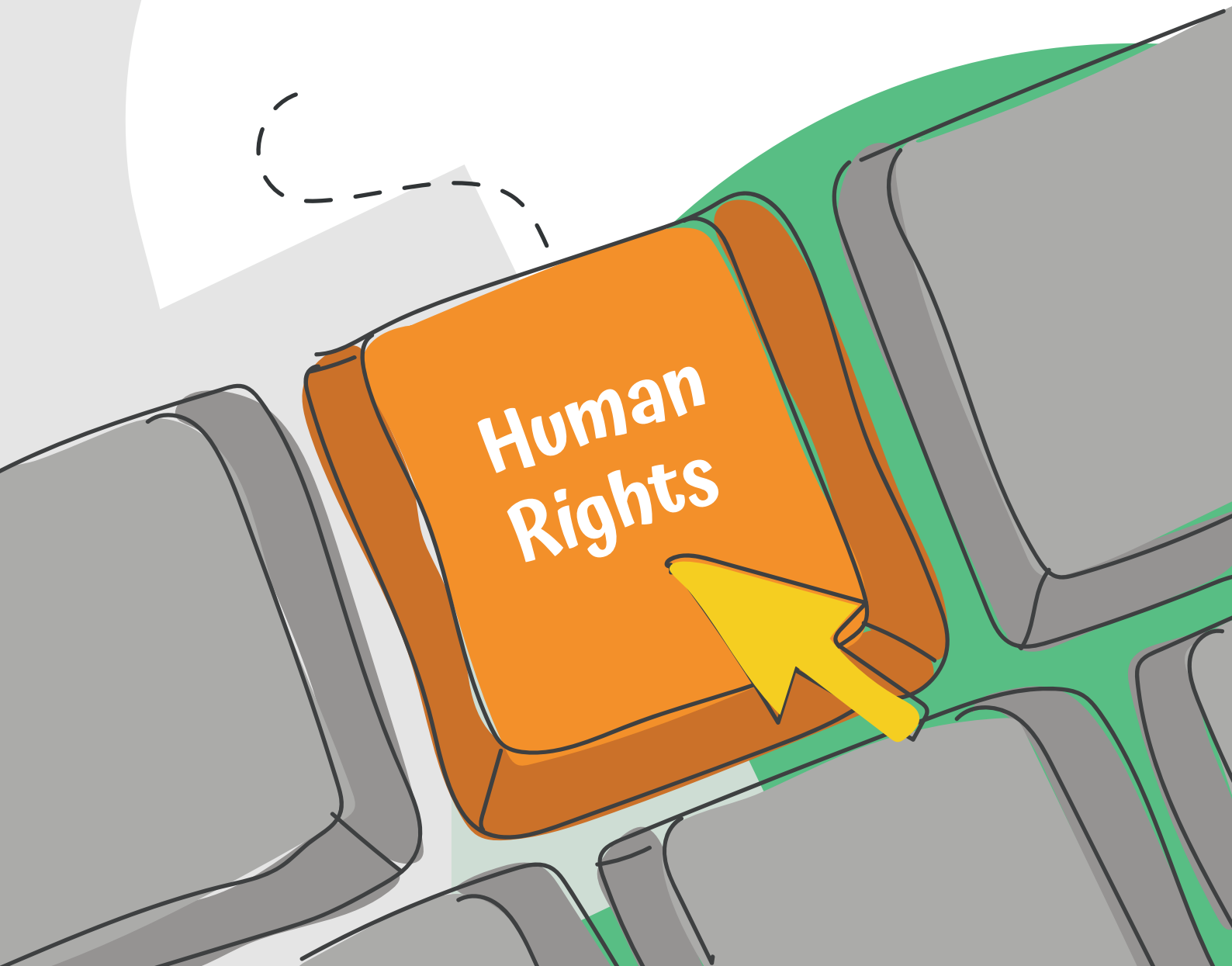
**a. Governments:** Legislations on data must be formulated on the basis of extensive and democratic consultation. They must be thoroughly debated in the legislature. Definitions of important concepts and deriving principles must not be left for executive discretion but formed through extensive democratic deliberation. The local governments in each country and its agencies must have greater say, role and accountability to manage data governance of the local communities. Formulation of digital / data charters must be transparent and accountable.

**b. Private sector:** Terms and conditions for obtaining consent for data collection must be stated in simple language. They must also be available in local languages as well as easy-to-understand formats (e.g., Video). User data cooperatives must be set up to oversee the use of customer/ consumer data.

**c. Civil Society:** Civil society must proactively take steps to educate customers/ users on data literacy and data rights.

# 4

**Apply human  
rights online**



## Core Principles

- a. Freedom of expression
- b. Freedom of democratic participation
- c. Freedom to engage in business/ livelihood activities online

## Key Commitments

**a. Governments:** Protect freedom of expression online by employing strict action against cyberbullying, trolling and online hate speech, especially against women, gender and sexual minorities and persons from other marginalized social locations.

**b. Private Sector:** Strong and immediate actions to restrict access to social media platforms for individuals / that engage in hate speech, hate content and violent content.

**c. International community:** As held by the Supreme Court of India in *Anuradha Bhasin vs Union of India*, (2020) 3 SCC 637, internet shutdowns are drastic measures and must be imposed only when lawful, necessary, proportionate and only after publishing orders. The international community and the UN must urge countries to respect the right to connectivity and minimize internet shutdowns.

# 5

**Introduce accountability  
criteria for discrimination  
and misleading content**



## Core Principles

- a. Prevention of online polarization
- b. Nurturing critical digital literacy
- c. 'Right to Right Content' as against rising false and wrong content

## Key Commitments

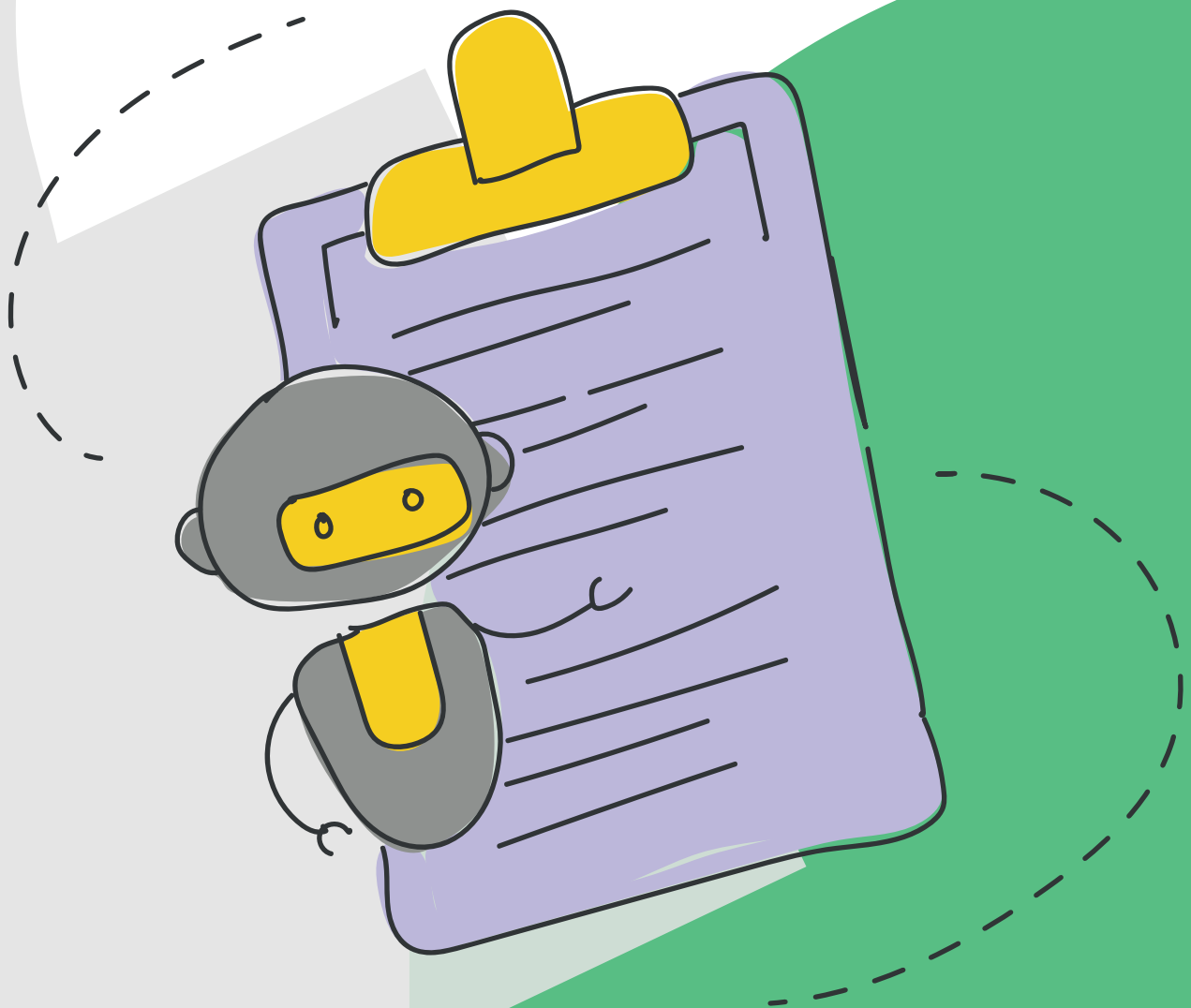
**a. Governments:** Accurate official information must be released in a timely and accessible manner to the public so that misinformation / disinformation can be countered. Public's right to information must be respected. There must be regulations on advertisement-based revenue models that foster filter bubbles and online polarization.

**b. Private Sector:** Nonpartisan and fair fact-checking and labelling must be employed. Considering the mental health cost of fact checking and hate speech moderation, these 'digital janitors' must be well compensated and supported.

**c. Civil Society & Academia:** Civil Society and academia must encourage initiatives to cultivate critical digital literacy – the ability to consume, produce and disseminate digital content critically.

# 6

## Promote regulation of Artificial Intelligence



## Core Principles

- a. Democratic overview over algorithmic decision making
- b. AI for social good
- c. Fair and consensual collection of training data

## Key Commitments

- a. Private sector:** AI models can't be trained on publicly available data without the consent of the data generators. An ethics committee should be in place within IT companies to ensure inclusion, prevent biased data collection, ensure representation.
- b. Governments:** In governance related decisions, AI decision logic must be made transparent and under democratic review
- c. Academia:** Syllabuses of AI courses must include data and algorithmic justice.



# 7

## Digital Commons as a global public good



## Core Principles

- a. Public/ user participation in governance:
- b. Conceptual clarity:
- c. Non exclusionary

## Key Commitments

**a. Private sector:** Private sector must commit to respecting the labor rights of the workers. Platform users (e.g., Unions of Delivery executives, drivers and customers) must be part of the governance decisions in platforms to regulate centralization of power, misuse of data and labor exploitation

**b. Governments:** Governments should regulate on platforms so that labor exploitation and monopolistic behavior is addressed. Non digital options for public digital infrastructure should be made available so that those who lack access to devices, connectivity or digital literacy are not excluded from accessing citizen benefits and services. Decision making regarding digital public infrastructure must be participatory and democratic.

**c. Civil Society:** since common and public indicate different property regimes, civil society must take the initiative to bring clarity to the concept of 'digital commons as public good'. Civil society must also lead the discussions on digital commons so that it is not captured by private sector to the detriment of the public.