Core principles for digital rights policies

- **Access to the internet:**
  - Internet shutdowns, throttling, service specific blocking, whitelisting of permitted services or connections and any means of intentional disruption of access to the internet and digital communications platforms even in times of crisis must be prohibited. Internet shutdowns are inherently disproportionate and cause severe harms to human rights, particularly for marginalised and at-risk communities and individuals.
  - There must be no discrimination between types of services or content to be accessed through the internet, through a policy of net neutrality.

- **Content governance:**
  - Content governance policies must have a clear legal basis, a precisely outlined scope, and specific application. This is necessary for certainty, foreseeability, and to avoid creating a "chilling effect" on free speech.
  - Content governance policies must not give the government unilateral or overbroad powers to block and remove content and their implementation must be subject to independent oversight. People must have an enforceable right to redressal, including judicial review, against restrictions on speech and expression.
  - Content governance policies must incorporate the need for social media services and other private companies with an effect on online speech to protect people's human rights. This can include holding platforms accountable by requiring meaningful transparency reports, consultations with stakeholders in policy and product development.
  - Platform accountability must not become a tool for censorship — content governance policies must allow for exemptions from liability with clear and reasonable conditions for liability which do not incentivize private companies to take down more speech than is necessary.
  - Content governance policies must not impose any general monitoring obligations on digital platforms, nor create arbitrary or disproportionate take-down procedures. . They should clearly identify the specific types of illegal content which are to be targeted and adopt different response mechanisms to address them. Rights-respecting notice-and-action procedures must be adopted to ensure that the concerned person is given a hearing, and has access to independent review and redressal mechanisms.
  - Cybersecurity and cybercrime laws must not be used to criminalise expression. offences relating to expressions such as "rumours," "disinformation," defamation, criticism or other forms of lawful expression should not be introduced through cybercrime legislation.

- **Privacy and security:**
  - The state must not compel digitalisation of public services linked to a centralised digital ID without a prior, public assessment of their necessity and proportionality

at both the policy and system level. Such systems must be subject to impact and need assessments, offer equally-accessible non-digital alternatives, ensure strong security for people's personal data, and operate with full transparency.
    - The state must establish strong cyber security standards and practices, and ensure good cyber hygiene incorporating independent audits, research, and feedback.
    - Strong encryption, including end-to-end encryption, must be protected. The state must not require backdoors, exceptional access mechanisms, traceability requirements or other measures that systematically weaken encrypted communications.
    - The state must implement frameworks for accountability and transparency into the use of spyware and surveillance technology, including by law enforcement. People must be able to question the government and know how their privacy is affected.
    - Surveillance and interception powers must be clearly provided by law and comply with the principles of legality, necessity and proportionality. Their use must be subject to independent authorisation and oversight, and effective remedies must be available where surveillance powers are misused.

- **Data protection:**
    - Data protection laws must prioritise privacy and be based on core principles, including fair and lawful use; purpose and retention limitations; data minimisation; necessity and proportionality; accuracy, integrity and confidentiality; users' rights; and adequacy for cross-border data flows. These principles must be asserted and incorporated in the law.
    - People must have explicitly stated actionable rights, including the right to information about how their data is being used and to object to any such use; to erasure, rectification, and explanation; and to portability, which ensures that digital service providers are unable to exploit users by locking them into their service. This also places an obligation on data controllers, including the state, to implement human rights respecting data practices.
    - The state and its agencies must not be exempted as such from data protection obligations. The state tends to be the biggest collector and user of people's data, which can lead to the building of surveillance systems. Inter-agency data sharing must be subject to strict conditions and aligned with data protection principals.
    - Data protection laws must not give the state a wide discretionary power to exempt entities from data protection obligations. Exemptions must be reasonable and proportionate. For example, it is reasonable to exempt journalists from the obligation to not publish personal data when there is a legitimate public interest in such information.
    - Formulation, implementation and enforcement of data protection policies requires an independent, well-resourced data protection authority with binding powers, technical and adjudicatory functions, and the ability to engage with all stakeholders. It must be institutionally independent from the bodies responsible for operating or coordinating government data systems, and people must have access to effective complaint and redress mechanisms.

- **Artificial intelligence:**
    - Human rights must be a core principle governing the development and use of artificial intelligence and automated decision-making systems. High-impact areas require stricter safeguards.
    - Applications of artificial intelligence and automated decision-making that are incompatible with fundamental human rights must be prohibited.
    - The use of AI in high-impact areas, including public services, healthcare, education, law enforcement and other areas affecting people's rights and access to essential services, must be subject to stronger safeguards, meaningful consultation and human rights impact assessments.
    - All public-sector uses of artificial intelligence and automated decision-making systems must be transparent, including through publicly accessible information on where and for what purposes such systems are being used.
    - People must not be subject to decisions with legal or similarly significant effects solely through automated processes. They must be able to seek meaningful human review, request an explanation, challenge the decision and access effective redress.
    - The state must prohibit the use of artificial intelligence-based facial recognition systems for widespread use in public spaces, where meaningful consent or choice are not possible.
    - AI systems must protect people's privacy and personal data by default, and AI tools should not weaken existing security protections, including encryption.