REGULATORY PATHWAYS TO ONLINE SAFETY: *WHAT CAN BE ACHIEVED BY GOVERNMENT AGENCIES?*

Digital and online systems now mediate nearly every aspect of life. Communication, education, work, healthcare, finance, civic participation, and public debate increasingly take place through digital infrastructures that are no longer peripheral tools, but cross-border, foundational systems shaping how societies function.

Questions of safety, accountability, and human agency have shifted from the margins of technology policy to the core of governance. Governments must govern systems that are more interconnected, opaque, and dynamic than most of the legal and institutional frameworks designed to address them.

National governments do not control the internet, nor can they unilaterally regulate global platforms in their entirety. The scope of regulation is constrained by jurisdictional reach, trade dynamics, and enforcement capacity. At the same time, the scope of protection and support for people experiencing harm is firmly within national responsibility. Policymakers must navigate how to enable progress while protecting people, often with limited data, fragmented institutional mandates, and constrained resources.

Rather than attempting to control all online activity, effective national regulation focuses on setting minimum standards, aligning existing laws, and strengthening systems that reduce harm and improve accountability.

IREX
DEVELOPMENT GATEWAY
An IREX Venture

WHAT GOVERNMENTS CAN DO

1. Set and enforce minimum safety standards at the national level

Governments can require digital platforms and online service providers operating within their jurisdiction to meet baseline safety obligations, even when those companies are based abroad. These standards increasingly focus on prevention and include:

- Content-based regulation, where specific categories of harmful or illegal content are clearly defined and regulated, such as child sexual exploitation material or non-consensual intimate images.
- Procedural safeguards, such as mandatory risk assessments and impact assessments that identify harm and document mitigation efforts.
- Transparency mandates, requiring platforms to disclose information about content moderation practices, complaint handling, algorithmic systems, and risk management.
- Design-based regulation, which targets technical and interface choices that shape user behavior and exposure to harm. This includes data protection, safer default settings, and limits on harmful amplification and exploitative design.

These approaches do not require governments to dictate technical solutions. They set expectations for outcomes and accountability.

2. Align and strengthen enforcement of existing national laws

Many countries already have robust legal frameworks related to cybercrime, data protection, gender-based violence, and child protection. The challenge is rarely the absence of law, but fragmented enforcement. Governments can strengthen their response by:

- Improving coordination between law enforcement, regulators, and judicial actors.
- Investing in digital forensics, evidence collection, and investigative capacity.
- Streamlining reporting pathways and survivor support mechanisms.
- Prosecuting offenses that fall within national jurisdiction, even when platforms operate transnationally.

While cross-border harms complicate enforcement, national capacity building remains essential for credibility and deterrence.

3. Strengthen institutional coordination and governance mechanisms

Online safety cuts across multiple mandates. Governments can create or reinforce coordination mechanisms that link:

- Digital and communications regulators
- Justice and law enforcement agencies
- Gender equality and social services institutions
- Child protection authorities
- Data protection and cybersecurity bodies

Such coordination reduces duplication, clarifies responsibility, and improves survivor experience. Participation in regional and global regulator networks supports alignment across borders.

4. Use co-regulatory frameworks and codes of practice

Where direct regulation is limited, governments can promote co-regulatory approaches, including voluntary or mandatory codes of practice developed with industry, civil society, and regulators. These mechanisms are particularly valuable for addressing cross-border platform risks and emerging technologies where formal legislation may lag.

Regional alignment, whether through regional mechanisms, such as African Union, or global regulator networks, can amplify national influence and reduce regulatory fragmentation.

5. Engage domestic technology ecosystems to support prevention

Governments can work with local technology companies, internet service providers, and telecommunications actors to promote safety-by-design adoption through incentives rather than sanctions. Regulatory sandboxes, public-private partnerships, and procurement standards can encourage safer product development and responsible innovation.

National regulatory action remains essential despite global constraints. Digital harms cross borders, but their impacts are felt locally by individuals and communities. Setting clear expectations, strengthening institutional capacity, and supporting prevention contribute to safer digital environments and greater accountability.