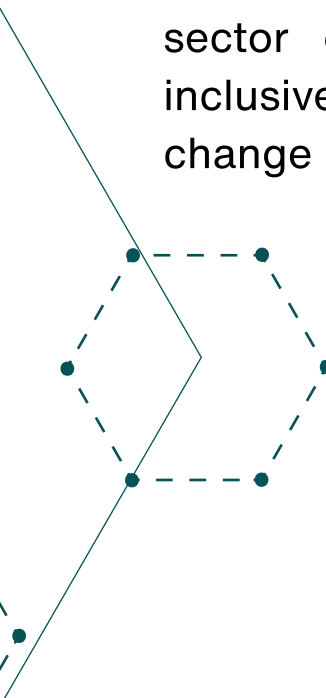


REGULATORY PATHWAYS TO ONLINE SAFETY: *GLOBAL LESSONS*



We live at a moment when digital platforms, data infrastructures, and increasingly artificial intelligence (AI) systems shape nearly every dimension of social, economic, and civic life. While digital development brings opportunities, online spaces and digital engagement contain risks. Online harms, such as cybercrime, harassment, trolling, and image-based abuse of children and adults, are shaped by platform design, data practices, and cross-border service delivery.

The question is no longer whether regulation has a role to play in online safety, but how governments, civil society, and the private sector can pursue regulatory pathways that are effective, inclusive, and resilient in the face of constant technological change and longstanding barriers such as:

- 
- Fragmented regulatory mandates designed for the analogue era.
 - Public authorities frequently operating with far less resources, technical capacity, data access, and operational visibility than the private platforms they must oversee.
 - Incomplete, dispersed, or inaccessible data on technology facilitated harms.

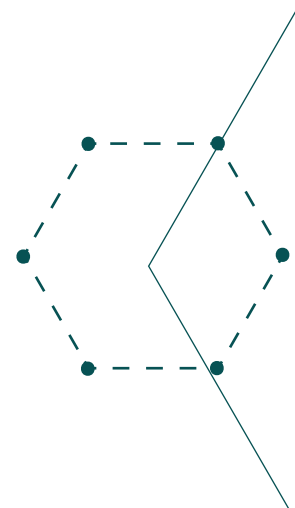


As a result, global digital policy landscape and frameworks remain uneven:

- ◆ Child online safety frameworks have advanced more quickly than adult safety, supported by clearer legal definitions and stronger international consensus.
- ◆ Cybercrime approaches often prioritize prosecution over prevention.
- ◆ Data protection, media regulation, telecommunications governance, and gender equality mandates too often operate in parallel rather than in concert.

In addition, despite growing recognition of online harms, many governments face persistent structural, legal, operational, political, and technical capacity gaps that slow progress. At the same time, many governments face pressure to move quickly, especially in AI adoption, sometimes by using regulatory models developed elsewhere without sufficient adaptation to legal realities, institutional capacity, or human rights safeguards.

However, national regulation remains a critical lever for setting expectations, protecting people, and shaping incentives that influence platform behavior well beyond national borders. Effective pathways to coherent and future-proof regulation are possible.



What National Governments Can Realistically Accomplish:

- Set and enforce minimum safety standards at the national level
- Align and strengthen enforcement of existing national laws
- Strengthen institutional coordination and governance mechanisms
- Use co-regulatory frameworks and codes of practice
- Engage domestic technology ecosystems to support prevention

Regulators do not have to do it alone. Actors within and outside the public sector can collaborate to ensure that digital development advances universal human potential.

When these public sector actors work together they are able to clarify responsibilities, strengthen trust, allocate resources, and sustain action in the face of rapidly evolving digital risks

Non-government actors are able to help governments overcome capacity constraints, improve data and evidence, depoliticize sensitive debates, and sustain progress

- Policymakers and Legislative Bodies
- Regulatory Authorities
- Law Enforcement and Prosecutorial Authorities
- Judiciary and Courts
- Human Rights and Equality Institutions
- Social Welfare, Health, and Survivor Support Services
- Education and Preventive Institutions
- Local and Sub-National Governments

- Technology Platforms, Service Providers, and Infrastructure Actors
- Funders and Development Partners
- Multilateral Development Banks and International Financial Institutions
- Civil Society Organizations
- Education Systems and Cultural Institutions
- Academic and Research Institutions
- Media, Journalism, and Entertainment
- Grassroots and Community Networks

When public actors are supported in their mandate and collaborate with non-governmental groups, together they can create political space for technical engagement, openness to cross-governmental collaboration to create clarity, recognition that harms exist, with identifiable entry points as an advantage, openness to coalition-based approaches, acceptance of iteration and uncertainty, and willingness to build a shared understanding of purpose and outcomes. They can:

1. Re-envision public sector readiness as a continuous, collective practice
2. Layer protections to reflect different risk profiles across populations
3. Combine general safeguards with targeted measures to protect the most at risk
4. Engage commercial technology actors as partners in implementation
5. Use safety-by-design to align incentives and expand adoption
6. Engage the public through co-designed education and awareness
7. Build public demand as a driver of safer digital systems

Regulatory pathways to online safety are not linear. They are a forward strategy for navigating uncertainty. They allow governments and partners to move from abstract commitments to practical building blocks, while remaining flexible to respond to evolving technologies, harms, and social expectations. They also keep survivor experiences and public trust at the center, reminding institutions that the effectiveness of governance is ultimately measured by whether people can participate safely and with dignity in digital life.