REGULATORY PATHWAYS TO ONLINE SAFETY: *GAPS WITHIN GOVERNMENTS THAT IMPEDE REGULATORY PROGRESS*

Despite growing recognition of online harms, many governments face persistent structural, legal, operational, and political gaps that slow progress. These gaps stem from institutional fragmentation, legacy legal frameworks, constrained resources, and the politicization of digital governance agendas. Understanding these constraints is essential to designing regulatory pathways that are realistic, credible, and capable of delivering impact.

Structural and Institutional Gaps

Fragmentation of mandates across government institutions: Responsibilities related to online safety, digital governance, gender-based violence, cybersecurity, data protection, and law enforcement are typically distributed across multiple agencies, resulting in unclear ownership, duplication of effort, and gaps.

- *Coordination mechanisms:* Where they exist, coordination mechanisms between relevant government agencies are often informal or activated only on a case-by-case basis, limiting sustained collaboration and placing the burden of navigating systems on survivors.
- *Enforcement capacity:* Governments' enforcement capacity tends to be uneven, with specialized cybercrime or digital forensics units concentrated in major urban centers, creating geographic disparities in access to justice.
- *Absence of survivor-centered reporting and evidence systems:* Most reporting mechanisms were designed for offline crimes or single-agency workflows and are poorly suited to online harms that unfold across platforms and jurisdictions, resulting in unclear or burdensome guidance for survivor reports.
- *Low trust:* Low levels of trust between citizens and enforcement institutions further discourages reporting.

Legal and Regulatory Gaps

- *Fragmented or outdated legal frameworks addressing elements of online harm:* Many existing government statutes predate social media platforms, algorithms, and AI. In some cases, newer laws exist but require amendment to address emerging risks. In others, overlapping laws regulate similar conduct but impose different penalties or procedures, creating confusion.

Operational and Capacity Gaps

- *Limited resources, skills, and institutional readiness:* Agencies often lack sufficient personnel, specialized training, and technical tools to investigate digital harms effectively.
- *Public engagement is limited:* Public awareness of reporting pathways is low, and consultative processes for policy development are often slow and outdated. These processes frequently lack sustained engagement with the technology sector, civil society, and survivors, reducing relevance and responsiveness to evolving harms.

Political and Financial Constraints

- *Politicization of online safety:* Online safety, particularly where it intersects with freedom of expression, platform accountability, gender equality, and electoral dynamics, is often highly politicized. Regulatory debates can become polarized, framed as trade-offs between safety and rights, or leveraged for short-term political gains. This politicization can slow consensus-building, discourage proactive leadership, and make governments risk-averse in pursuing reforms.
- *Financial constraints:* Budget allocations rarely match the scale or complexity of digital harms. Online safety units, survivor support services, and enforcement bodies are often underfunded. In this context, preventive and enabling measures, such as digital literacy education and school-based interventions, are likely to fall off the agenda in LMIC settings.

Additional Contextual Gaps: High-Income and Low- and Middle-Income Settings

The challenges associated with online safety governance manifest differently depending on institutional maturity, resources, and political economy.

- *HICs:* Regulatory institutions are better resourced and supported by more comprehensive legal frameworks. Data protection regimes, platform obligations, and online safety laws are often well developed. At the same time, politicization, coordination failures, and persistent power and data asymmetries between governments and global platforms limit effectiveness. Even where sophisticated laws exist, enforcement often remains reactive, and survivor experiences can still be fragmented across institutions. Preventive measures, including digital literacy education, are more consistently employed, but do not fully compensate for gaps in coordination, accountability, or platform transparency.
- *LMICs:* Capacity and financial constraints are more acute. Limited funding, fewer specialized personnel, uneven digital infrastructure, and competing development priorities constrain enforcement and oversight. Regulators face greater asymmetries of power and information in their engagement with global platforms, alongside fewer opportunities to influence platform design choices or cross border accountability mechanisms. Preventive and enabling measures such as digital literacy education, school-based programs, and public awareness campaigns, are particularly vulnerable to being deprioritized or treated as discretionary.

Taken together, these dynamics explain why progress on online safety is often slow despite the existence of laws, institutions, and growing international attention.

This is why IREX's regulatory engagement work is essential. IREX does not assume that new legislation alone will resolve these challenges. Instead, we focus on strengthening coordination, clarifying roles, improving survivor-centered reporting and data flows, increasing institutional trust, and embedding preventive Safety-by-Design approaches within existing systems. By working pragmatically within political, financial, and institutional constraints, IREX supports governments to move from intent to action and to build more effective, inclusive, and accountable online safety governance.

The most common capacity needs for trainings for civil servant/government officials focused on adult online safety:

1. The Evolving Digital Ecosystem

- Common digital platforms, services, and use cases in target countries
- Core technical concepts (algorithms and recommender systems, deceptive or manipulative design patterns, generative AI)
- How platform design, data flows, and business models shape risk, harm, and response options

2. Digital Harms and Online Risk

- Key definitions and typologies of digital harms
- Prevalence, severity, and patterns of exposure to risk
- Individual- and community-level impacts on vulnerable and marginalized populations
- Social and economic impacts, including participation, productivity, and trust
- Differentiating risk and impact across user groups

3. Digital Regulation and Governance: Global Approaches and Trends

- Digital regulation models and governance approaches
- Risk-based and outcomes-oriented regulatory frameworks
- AI governance and oversight of emerging technologies
- Relevant international norms, treaties, and cooperation mechanisms
- Lessons from different countries' experience
- Survivor-centered and rights-respecting regulatory approaches
- Tradeoffs, limits, and political-economy considerations in digital regulation

4. Institutional Roles, Mandates, and Coordination

- Allocation of institutional responsibility and regulatory authority across government
- Clarifying boundaries between policy, regulation, enforcement, and service provision
- Simulation exercise: whole-of-government response to digital harms
- Collaborative and cross-sectoral coordination models, informed by global practice

5. Public Awareness, Trust, and Digital Citizenship

- Gaps in public understanding of rights, responsibilities, and available remedies
- Perpetration, bystandership, and social norms in digital environments
- Best practices for public communication and outreach
- Distinguishing prevention messaging, user guidance, and survivor-facing information

6. Private Sector Engagement and Platform Accountability

- Safety-by-design
- Regulatory and supervisory approaches to digital service providers, such as voluntary regulatory compliance standards
- Monitoring compliance and addressing systemic risk
- Global experience engaging large platforms and local digital ecosystems
- Balancing accountability, innovation, investment, and rights protection

7. Managing Reporting, Data, and Access to Remedies

- Survivor-centered data flows and information-sharing protocols
- Platform reporting and redress mechanisms
- Law enforcement and administrative reporting channels
- Social protection and social service entry points
- Coordination across systems and sectors
- Safeguarding and implications for service provision
- Risks created by reporting systems (privacy, retaliation, exclusion)

8. Survivor-Centered Services

- Survivor experiences and pathways to support
- Survivor-centered, trauma-informed, and rights-based approaches
- Government, civil society, and community-based roles
- Mapping existing services and referral mechanisms
- Managing consent, confidentiality, choice, and safety risks

9. Law Enforcement and Investigative Functions

- Role of law enforcement within a broader regulatory and service ecosystem
- Intake and handling of digital evidence
- Survivor-centered investigative protocols
- Criminal law provisions relevant to digital harms
- Appropriate scope and limits of law-enforcement responses

10. Justice Sector Response and Prosecution

- Legal frameworks applicable to digital harms
- Roles of prosecutors, judiciary, law enforcement, and coordinating bodies
- Survivor-centered and trauma-informed justice processes
- Preservation of digital evidence, chain of custody, and digital forensics
- Avoiding secondary harm and unnecessary criminalization

11. Monitoring, Evaluation, and System Learning

- Ethical and responsible data collection and analysis
- Institutional feedback mechanisms and stakeholder engagement
- Survivor-defined indicators of effectiveness and trust
- Using evidence to adapt policy, regulation, coordination, and services