**INSTITUTUM LEX FEMINAE | POLICY BRIEF | REPUBLIC OF KOREA**
**ILF-ROK-PB-2026-04-EN | SEPTEMBER 2026**

# FROM REMOVAL TO DURABLE SUPPRESSION: A policy-design submission for the 2026 국민생각함 digital-sex-crime consultation

## Executive Summary

South Korea has already moved beyond a deletion-only model. The August 2026 joint-government plan targets the illegal-site ecosystem itself through criminalization of site establishment, advertising-revenue disruption, emergency blocking, specialist investigations and possible "active defense" powers. The open 국민생각함 consultation therefore presents a narrower and more valuable design question: how should Korea make those tools work as one enforceable chain rather than as separate outputs?

Institutum Lex Feminae recommends four mechanisms that can be built on existing Korean institutions: a victim-linked persistent reappearance watch, an infrastructure escalation ladder, evidence-preservation before destructive takedown, and a durable-suppression metric measured at 30, 90 and 180 days. The objective is to shift the burden of rediscovery away from victims and to make recurrence, provider non-compliance and enforcement conversion visible.

## Why Intervention Is Timely

The consultation is open from 16 September through 31 December 2026 and expressly seeks proposals on prevention, victim protection/support, and stronger punishment or sanctions. It follows the 20 August Integrated Response Plan, while several legislative changes are still being developed or have only recently been filed. This is a pre-policy and implementation-design window, not a retrospective consultation.

The baseline shows why design matters. Government analysis found 6,683 of 34,628 previously collected illegal sites still accessible in August 2026. An estimated 2.15 million Korea-related videos were hosted on 1,316 Korean-language or Korea-category sites. The 2025 Victim Support Report recorded 10,637 supported victims and 352,103 support actions; 45.1% were continuing-support victims. Deletion support represented 90.3% of all support actions, while the non-compliance rate for illegal/harmful sites increased from 24.7% to 28.5%.

## The Policy Gap

Korea can count deletion requests, blocks, investigations and arrests. Those figures do not by themselves establish that a victim's material has stopped circulating. A blocked domain can remain live abroad; a removed URL can reappear under another path; an arrested operator may leave the original server intact; and a victim can be forced to report the same material repeatedly. The unit of success should therefore move from the individual URL to the persistence of the exploitation asset and the recurrence burden imposed on the victim.

## Recommendations

### 1. Create a "report once, remain protected" persistent reappearance watch

When a victim consents, the Central Digital Sex Crime Victim Support Center should generate a privacy-preserving fingerprint or case-linked signature for verified illegal material and associated identifying information. The system should continuously search participating platforms, known illegal sites and newly detected mirror domains for materially identical or derivative reuploads. A new match should trigger review and removal action without requiring the victim to rediscover and resubmit the same material.

This can be anchored in the Central Center's existing statutory functions under Article 7-4 of the Sexual Violence Prevention and Victims Protection Act, including deletion support, prevention research, domestic/international cooperation and operation of a comprehensive victim protection/support management system. Safeguards should include victim consent, strict access controls, purpose limitation, audit logs and deletion/retention rules.

### 2. Replace one-step takedown with a statutory infrastructure escalation ladder

For sites that repeatedly ignore verified deletion requests, agencies should follow a documented escalation sequence: content notice → platform/account action → domain or access restriction → CDN action → hosting termination request → advertising/payment disruption → investigation/referral → server seizure or legally authorized active-defense action where available. Each escalation should have a time stamp, responsible agency and outcome code.

The ladder would not require every case to reach the final stage. It would require government to show why escalation stopped. This matters because the September results show 68 sites were the subject of formal hosting-termination requests to five providers, yet only one hosting termination had resulted at the reporting point.

### 3. Preserve prosecution-grade evidence before destructive removal

Rapid deletion and successful prosecution should not compete. Before an original server, account or file is disabled or remotely deleted, investigators should preserve a standardized evidentiary packet: verified URL/domain history, timestamps, content

hash, administrator identifiers where lawfully obtained, hosting/CDN information, advertising/payment links, victim-linked case reference and chain-of-custody record. The packet should be transferable to police and prosecutors without requiring the victim to reconstruct the circulation history.

For emergency cases, preservation should be automated or near simultaneous with removal. This would make the proposed active-defense model more legally resilient and reduce the risk that successful disruption destroys the evidence needed to prosecute the operator or recover criminal proceeds.

### 4. Make "durable suppression" the principal outcome metric

For each verified exploitation asset or site network, measure whether it remains unavailable or materially suppressed at 30, 90 and 180 days. Publish separate rates for URL deletion, domestic blocking, server/hosting termination, operator disruption and recurrence under mirror domains. A site should not be counted as durably suppressed merely because one domain is blocked.

Add a victim-centered recurrence indicator: number of verified reappearances per protected case and median time from reappearance detection to action. This measures whether the system reduces the continuing burden documented in the 2025 report, where continuing-support victims rose to 45.1% of all supported victims.

## Legal And Institutional Fit

These recommendations build on existing authority rather than requiring a new agency. Article 7-4 already assigns the Central Digital Sex Crime Victim Support Center deletion support, prevention, research, cooperation and comprehensive management functions. The 2026 government plan already contemplates emergency blocking, advertising disruption, specialist investigations, stronger platform duties and active-defense powers. The proposed architecture connects those tools and creates auditable handoffs between the Ministry, support center, police, communications regulators, prosecutors and overseas infrastructure providers.

## Intended Recipients

Primary: Ministry of Gender Equality and Family and Anti-Corruption and Civil Rights Commission through 국민생각함. Operational recipients: Korean National Police Agency; Broadcast Media and Communications Commission; Broadcast Media and Communications Standards Commission; Supreme Prosecutors' Office; Ministry of Justice; Korea Women's Human Rights Promotion Agency/Central Digital Sex Crime Victim Support Center.

## Intervention Stage

PRE-POLICY / IMPLEMENTATION DESIGN. Consultation closes 31 December 2026. The recommendations are intended to influence implementation of architecture while the government's post-August legal and operational reforms remain alterable.

In fine, Korea's next step should not be another larger deletion count. It should be a system in which a victim reports once, government follows the material and infrastructure across reuploads, evidence survives takedown, and success is measured by whether the exploitation asset stays down. That is a feasible shift from reactive removal to durable suppression.

### Official sources


- Ministry of Gender Equality and Family, "Digital Sex Crime OUT! 국민 레이더 ON," consultation open 16 September–31 December 2026. https://www.mogef.go.kr/nw/enw/nw_enw_s001.do?mid=mda700
- Government of the Republic of Korea, Joint Government Integrated Response Plan for Illegal Digital-Sex-Crime Sites, 20 August 2026. https://www.korea.kr/briefing/policyBriefingView.do?newsId=156775030
- Ministry of Gender Equality and Family, third inter-agency Digital Sex Crime Response Council results, 22 September 2026. https://www.mogef.go.kr/nw/enw/nw_enw_s001.do?mid=mda700
- National Law Information Center, Sexual Violence Prevention and Victims Protection Act, Arts. 7-3 and 7-4. https://www.law.go.kr/lsLinkCommonInfo.do?chrClsCd=010202&lsJoLnkSeq=1029705875
- Ministry of Gender Equality and Family / Korea Women's Human Rights Promotion Agency, 2025 Digital Sex Crime Victim Support Report. https://www.mogef.go.kr/nw/enw/nw_enw_s001d.do?bbtSn=713466&mid=mda703