INSTITUTUM LEX FEMINAE | POLICY BRIEF | REPUBLIC OF KOREA
ILF-ROK-PB-2026-05-EN | SEPTEMBER 2026

BLOCKED IS NOT REMOVED: An enforcement-effectiveness framework for South Korea's digital-sex-crime crackdown

Executive Summary

South Korea's September 2026 enforcement results show substantial activity: active illegal sites fell from 6,683 to 4,736; 66 sites were taken out of operation; 32 operators were arrested, including nine detained; KRW 2.7 billion in criminal proceeds was provisionally confiscated or recovered; 5,077 sites received blocking corrective requests; and 380 sites were subjected to CDN access restrictions. These are important outputs. They are not yet a complete measure of effectiveness.

The most revealing figure is the conversion gap: formal service-termination requests were sent to five hosting providers concerning 68 sites, but only one hosting termination had resulted at the reporting point. Institutum Lex Feminae therefore proposes an Effectum-style evaluation architecture that distinguishes domestic blocking from infrastructure removal, measures recurrence after intervention, links disruption to prosecution and sentencing, and measures the continuing burden on victims.

What Changed

On 22 September 2026 the third inter-agency Digital Sex Crime Response Council published implementation results following the 20 August Integrated Response Plan. Four dedicated illegal-site investigation teams, totaling 20 officers, were established in Seoul, Busan, southern Gyeonggi and Jeonnam; 76 sites were under investigation. The government also reported remote seizure/deletion on 16 sites after developers were apprehended, and continued work on legislative changes including independent criminalization of illegal-site establishment, advertising-revenue restrictions, emergency blocking powers and platform reporting duties.

Why Output Statistics Are Insufficient

A domestic access block can reduce immediate exposure without removing the source. A hosting termination can disable infrastructure but may be reversed by migration. An arrest may disrupt management without removing stored content. A deletion request may be complied with once while mirror domains continue distributing the same material. Each action has a different enforcement value and should not be aggregated into a single success narrative.

The 2025 support data reinforce this point. Continuing-support victims increased by 26.3% and represented 45.1% of all supported victims. Illegal/harmful-site deletion support increased 26.9%, while the non-compliance rate rose to 28.5%. Effectiveness therefore has to be measured against recurrence and victim burden, not only administrative volume.

Recommendations

1. Publish a five-level Digital Exploitation Disruption Index

Every targeted site/network should be assigned a status that distinguishes: Level 1 - domestic access blocked; Level 2 - specific content/account removed; Level 3 - CDN/domain/hosting infrastructure disabled; Level 4 - operator or administrator disrupted and criminal proceeds targeted; Level 5 - durable suppression, defined as no material reappearance of the same network at 30, 90 and 180 days. Government reporting should publish movement between levels rather than combining unlike interventions.

This prevents a blocked but fully operational overseas site from being reported as equivalent to a server that has been seized and permanently disabled.

2. Create a provider compliance and escalation scorecard

For hosting, CDN, platform and other infrastructure providers receiving verified Korean notices, record: number of notices, median response time, removal/termination rate, repeat non-compliance, migration of the same network, and escalation taken by Korean authorities. Publish aggregated provider-level results where legally permissible.

The 68-to-1 hosting termination result should become a measurable conversion rate, not a footnote. Persistent non-compliance should automatically trigger the next lawful escalation step, including regulatory, investigative, advertising/payment or international-cooperation routes.

3. Link enforcement outputs to criminal-justice outcomes through a persistent site/network ID

Assign each priority illegal-site network a non-public persistent identifier used across the support center, police and prosecution systems. This allows government to follow the same network from victim-support detection → deletion/blocking → investigation → arrest → referral → indictment → conviction/acquittal → sentence → confiscation/recovery → 30/90/180-day recurrence.

Publish aggregated conversion rates. For example, the reported 32 operator arrests should eventually be traceable to prosecution dispositions and sentencing outcomes. Without this linkage, Korea can measure police activity but not whether enforcement converts into criminal accountability.

4. Add a Victim Recurrence Burden metric

For consenting supported victims, measure how often verified material reappears after an intervention, how many separate removal actions are required, and the median number of days until durable suppression. Do not publish victim-identifying data. Report aggregate recurrence burden by distribution environment and intervention type.

A successful system should reduce the number of times a victim must return to the support system for the same underlying exploitation asset. This directly tests whether enforcement is reducing continuing harm rather than simply processing more deletion requests.

Implementation Dashboard

- Durable suppression rate at 30 / 90 / 180 days.
- Hosting/CDN/platform notice-to-action conversion rate and median response time.
- Mirror-domain recurrence rate after blocking or hosting termination.
- Site/network investigation → referral → indictment → conviction → sentence conversion.
- Criminal-proceeds preservation and final confiscation/recovery rate.
- Victim recurrence burden: reappearances and repeat removal actions per protected case.

Institutional Recipients

Ministry of Gender Equality and Family; 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. The inter-agency Digital Sex Crime Response Council is the natural governance body for a shared dashboard.

Intervention Stage

IMPLEMENTATION EVALUATION. The government has begun deploying the August plan and has already published the first substantial implementation dataset. The proposed framework should be adopted before different agencies entrench incompatible definitions of 'blocked,' removed,' closed' and 'disrupted.'

In fine, South Korea's enforcement surge is significant. The next accountability question is whether the system is destroying exploitation capacity or temporarily changing how Korean users reach it. A credible evaluation model should follow the same site, infrastructure, operator and victim harm over time. "Blocked" is an intervention. "Removed" is an outcome. "Durably suppressed" is the effectiveness test.

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