

정책 브리프 | 대한민국 | 2026 년 9 월

ILF-ROK-PB-2026-02-KR

신고에서 피해자 보호까지: 디지털 성범죄 대응체계의 안전한 집행 구조 구축

요약

정부가 디지털 성범죄 정책 제안과 불법사이트·유포 채널에 대한 국민 제보를 확대하고 있다. 그러나 신고 확대가 실질적인 피해자 보호로 이어지려면 신고부터 삭제·차단, 수사의뢰까지 이어지는 과정에서 개인정보 보호, 처리 책임, 결과 추적이 함께 보장되어야 한다.

즉시 필요한 조치

- 최소정보 원칙을 적용한다. 신고·삭제 요청 과정에서 피해자 신원정보 수집을 최소화하고 불필요한 개인정보는 자동 삭제·가림 처리한다.
- 정보 전달 경로를 통제한다. 정부기관, 지원기관, 플랫폼 및 제 3 자 간 정보 제공·보관·재전달 기준을 명확히 규정한다.
- 집행 과정을 추적한다. 신고 접수부터 확인, 삭제·차단, 수사의뢰 및 후속조치까지 처리 단계와 책임기관을 기록한다.
- 피해자 보호 성과를 공개한다. 신고 건수뿐 아니라 삭제·차단, 재유포, 처리기간 및 수사의뢰 결과를 구분하여 공개한다.
- 정보 노출 대응 절차를 마련한다. 피해정보 유출 시 신속한 통지, 재노출 확인, 법률지원 및 피해구제 절차를 보장한다.

무엇이 문제인가?

성평등가족부와 국민권익위원회는 2026 년 9 월 16 일부터 12 월 31 일까지 국민신문고 ‘국민생각함’을 통해 디지털 성범죄 근절을 위한 정책 제안과 불법사이트·유포 채널 제보를 접수하고 있다. 대상에는 불법촬영물, 딥페이크 성착취물인 허위영상물, 아동·청소년 성착취물이 포함된다. 접수된 정보는 확인 후 삭제·차단과 수사의뢰 등에 활용될 수 있다.

이는 한국의 디지털 성범죄 대응이 단순 삭제지원에서 사이트 분석, 차단, 수사 및 국제공조를 연계하는 통합 집행체계로 확대되는 과정의 일부다. 정부는 이미 AI 기반 24 시간 탐지·신고와 삭제요청 자동화 체계를 도입했다.

그러나 집행 범위가 확대될수록 피해자와 신고자의 정보가 이동하는 경로도 길어진다. 최근 개인정보보호위원회는 구글에 전달된 디지털 성범죄물 삭제 요청 정보가 외부 웹사이트에 공개된 사건을

조사하고 있다. 조사 대상에는 제공된 개인정보의 규모와 항목, 제공 기간, 제 3자 제공의 적법한 처리근거 및 민감정보 처리 과정이 포함된다. 개인정보위는 이 사건에서 2차 피해 가능성도 지적했다.

따라서 새로운 신고체계의 성과는 얼마나 많은 정보를 수집하는지가 아니라, 얼마나 적은 개인정보로 얼마나 신속하고 안전하게 불법 콘텐츠를 제거하고 피해자를 보호하는지를 기준으로 평가해야 한다.

무엇을 할 수 있는가?

1. 신고 단계부터 개인정보를 최소화한다

정부는 디지털 성범죄 신고에 필요한 정보와 피해자 식별에 필요한 정보를 구분해야 한다. 불법사이트 또는 유포 채널의 존재를 확인하기 위한 신고라면 URL, 콘텐츠 유형, 사이트 운영 방식 등 집행에 필요한 최소정보를 우선 수집해야 한다.

피해자의 이름, 연락처 또는 기타 식별정보가 반드시 필요하지 않은 경우 이를 요구해서는 안 된다. 필요한 경우에도 사건정보와 분리하여 저장해야 한다. 특히 신고자가 불법 콘텐츠를 입증하기 위해 이를 직접 다운로드하거나 재전송하도록 만드는 구조를 피해야 한다.

신고 화면에서 불법 콘텐츠 자체가 아니라 URL 과 최소한의 확인정보를 제출할 수 있다는 점을 명확히 안내해야 한다. 이를 통해 신고 참여를 확대하면서도 새로운 개인정보 노출이나 불법 콘텐츠의 추가 복제를 방지할 수 있다.

2. 정보의 전체 이동 경로를 통제한다

피해자 보호는 정부기관이 정보를 수집하는 순간 끝나지 않는다. 신고정보가 지원기관, 수사기관, 플랫폼 또는 외부기관으로 전달된다면 각 단계에서 누가 어떤 정보를 어떤 목적으로 받는지 확인할 수 있어야 한다.

정부는 제 3자 제공, 접근권한, 보관기간, 재전달, 삭제 및 사고 통지에 관한 최소기준을 마련해야 한다. 플랫폼에 삭제나 차단을 요청할 때에도 피해자 식별정보가 실제 집행에 필요한지를 먼저 검토해야 한다.

구글 관련 개인정보위 조사는 이 문제가 이론적 위험에 그치지 않음을 보여준다. 디지털 성범죄 대응체계는 콘텐츠를 제거하는 동시에 피해자의 개인정보가 새로운 노출 경로를 만들지 않도록 설계되어야 한다.

3. 신고에서 집행까지 추적 가능한 체계를 만든다

신고 건수만으로 제도의 효과를 평가해서는 안 된다. 각 신고에는 접수, 확인, 삭제요청, 차단, 수사의뢰 및 종결 등 주요 처리단계를 확인할 수 있는 추적체계가 필요하다.

정부는 기관별 책임과 기본 처리기한을 명확히 하고, 가능한 범위에서 신고자 또는 피해자가 사건의 진행상태를 확인할 수 있도록 해야 한다. 동일 콘텐츠가 다른 URL 이나 도메인에서 다시 유통되는 경우에는 최초 삭제를 사건 종결로 간주하지 않고 재유포 여부를 지속적으로 확인할 수 있는 절차가 필요하다.

이는 정부가 구축하고 있는 AI 탐지, 삭제요청 자동화, 사이트 분석 및 수사연계 체계를 측정 가능한 집행 과정으로 전환하는 데 필요하다.

4. 삭제 건수가 아니라 피해자 보호 결과를 측정한다

정부가 공개하는 통계는 신고, URL, 콘텐츠, 사이트, 피해자, 삭제·차단 및 수사의뢰를 서로 다른 지표로 구분해야 한다. 하나의 피해사건에서 수백 개의 URL 이 생성될 수 있기 때문에 삭제 건수의 증가를 피해자 수 증가 또는 보호성과 향상으로 해석해서는 안 된다.

정부는 평균 처리기간, 삭제·차단 성공률, 재유포 확인, 반복 도메인, 수사의뢰 및 후속조치 등을 함께 공개할 필요가 있다. 특히 피해정보가 외부에 노출된 경우에는 피해자 통지, 추가 삭제, 모니터링, 법률지원 및 피해구제 조치도 별도로 측정해야 한다.

한국의 디지털 성범죄 대응체계가 확대되는 단계에서는 얼마나 많이 처리했는가보다 실제로 무엇이 보호되었는가를 평가하는 것이 중요하다.

결론

국민 참여 확대는 디지털 성범죄 대응의 중요한 수단이 될 수 있다. 그러나 신고 확대 자체가 피해자 보호를 보장하지는 않는다. 정부는 신고부터 삭제·차단과 수사의뢰까지 이어지는 전체 정보 흐름에 개인정보 최소화, 전달 통제, 처리 추적 및 피해구제 원칙을 적용해야 한다. 최근 구글 삭제요청 정보 노출 사건은 콘텐츠 삭제를 위한 절차 자체가 새로운 개인정보 위협을 만들 수 있음을 보여준다.

이번 국민 의견수렴은 이러한 보호장치를 사후 보완하는 것이 아니라 처음부터 대응체계에 포함시킬 수 있는 정책적 기회다.

정책 개입 단계

제도 개선 전 사전 개입

의견 제출 기한: 2026 년 12 월 31 일

주요 출처

성평등가족부·국민권익위원회, 「디지털 성범죄 근절을 위한 정책 제안」 국민 의견수렴, 2026 년 9 월.

개인정보보호위원회, 구글 디지털 성범죄 피해자 정보 노출 관련 조사 발표, 2026 년 9 월 11 일.

성평등가족부, 디지털 성범죄 피해지원 및 AI 기반 24 시간 탐지·삭제지원 관련 정부 자료.