

ESPAÑA EFICIENTE

POLICY BRIEF | PROTECCION AL MENOR

Protección Digital del Menor: Detección Proactiva, Intervención Inmediata, Tolerancia Cero

1. Resumen Ejecutivo

La explotación sexual de menores en el entorno digital es uno de los delitos mas graves que existen y uno de los que mas crecen. El sistema actual es reactivo: actúa cuando hay denuncia, cuando el daño ya esta hecho. Los depredadores digitales lo saben y actúan en el espacio que existe entre la conducta delictiva y la denuncia formal. España Eficiente propone un modelo proactivo de protección digital del menor basado en tres pilares: detección temprana mediante análisis de patrones en contenidos públicos y plataformas digitales, intervención inmediata coordinada entre las 17 oficinas autonómicas, la Fiscalía y las fuerzas de seguridad, y educación preventiva sistemática en colegios y familias. Todo ello dentro de un marco constitucional y legal riguroso que garantiza que ninguna actuación vulnera derechos fundamentales.

La explotación sexual infantil no tiene justificación, no tiene matices y no admite impunidad.

El sistema actual espera a que el daño ocurra. España Eficiente actúa antes.

2. El Problema: Un Sistema Reactivo ante un Delito Proactivo

- Los depredadores digitales operan en espacios públicos y semipúblicos de internet antes de contactar con menores de forma privada. Ese espacio previo es donde la detección es posible y legal.
- El sistema actual actúa tras la denuncia. En muchos casos la denuncia llega tarde: el daño psicológico, físico o la producción de material de abuso ya ha ocurrido.
- La fragmentación institucional entre comunidades autónomas, fuerzas de seguridad, fiscalía y servicios sociales genera retrasos y gaps de información que los agresores explotan.
- Las plataformas digitales tienen obligaciones legales de reporte pero su cumplimiento es desigual y los protocolos de respuesta son lentos.
- La educación preventiva en colegios y familias es puntual y no sistemática, dejando a los menores sin las herramientas para identificar y denunciar situaciones de riesgo.

3. Tres Pilares del Modelo

3.1 Detección Proactiva: Anticiparse antes de la Denuncia

El modelo propone una unidad de análisis digital centralizada que opera dentro de los límites legales precisos:

Tipo de análisis	Como funciona	Límite legal
Análisis de contenido público	Monitoreo de foros, grupos y espacios públicos digitales. Algoritmos detectan palabras clave, imágenes conocidas (hashes de pornografía infantil) y comportamientos típicos de grooming.	Legal: contenido público. No requiere autorización judicial.
Detección de hashes de abuso	Comparación automática de imágenes contra bases de datos de material de abuso conocido (NCMEC, Interpol).	Legal: tecnología PhotoDNA y equivalentes. Ya usada por Meta, Google y Microsoft.
Análisis de patrones de comportamiento	IA detecta patrones de conducta típicos de depredadores en plataformas: contacto sistemático con menores, petición de datos personales, escalada de intimidad.	Legal en espacios públicos. Comunicaciones privadas requieren autorización judicial previa.
Alertas tempranas a fuerzas de seguridad	Cuando se detecta patrón de riesgo, alerta inmediata a la unidad especializada. No se actúa contra el usuario hasta validación judicial.	Legal: la alerta es interna. La acción sobre el usuario requiere base jurídica suficiente.

Límite constitucional clave: Art. 18 CE.

La interceptación de comunicaciones privadas solo puede realizarla la Policía o Guardia Civil con autorización judicial.

El sistema detecta en espacios públicos y prepara la intervención. La acción sobre el usuario siempre requiere base legal suficiente y control judicial.

3.2 Intervención Inmediata y Coordinada

Cuando se detecta riesgo real para un menor, el protocolo de intervención se activa de forma inmediata y coordinada entre todos los actores:

- La oficina autonómica correspondiente recibe la alerta y evalúa el nivel de riesgo en menos de 2 horas.
- Si hay riesgo acreditado para un menor identificable: activación inmediata del plan de protección con coordinación entre servicios sociales, policía local y fiscalía de menores.
- Derivación a Policía Nacional o Guardia Civil (unidades especializadas UCRIF o equivalente) para los casos que requieren investigación penal con autorización judicial.
- Coordinación con plataformas digitales a través de los canales legales establecidos (INHOPE, reportes directos) para retirada inmediata de contenido ilegal.
- Seguimiento continuo del menor afectado: apoyo psicológico, legal y familiar desde el primer momento.

3.3 Educación Preventiva Sistemática

La prevención es la primera línea de defensa. Un menor que sabe identificar y denunciar una situación de riesgo es un menor mas protegido:

- Programa educativo obligatorio en todos los centros educativos sostenidos con fondos públicos desde los 10 años: identificación de grooming, derechos digitales, como denunciar y a quien acudir.
- Formación específica para docentes y equipos de orientación sobre señales de alerta y protocolos de actuación.
- Campanas dirigidas a familias sobre supervisión del entorno digital de los hijos, configuración de privacidad y comunicación abierta sobre riesgos.
- Alertas preventivas a colegios y familias cuando se detecta actividad sospechosa en plataformas populares entre menores en una zona geográfica.

4. Las 17 Oficinas Combinadas: Protección Ciudadana y Protección Infantil

Las oficinas de protección al menor se integran en las mismas oficinas híbridas que cubren la protección ciudadana general, con un departamento especializado independiente:

Departamento	Personal por oficina	Funciones principales
Protección Ciudadana General	3 personas (coordinador, gestor, atención)	Fraudes, abusos económicos, mediaciones, estafas.
Protección Infantil	3 personas (coordinador especializado, gestor, atención)	Explotación online, grooming, pornografía infantil, derivación a Fiscalía y Policía.
TOTAL POR OFICINA	6 personas	Cobertura integral ciudadana e infantil en una sola sede.

Concepto	Coste estimado
Salarios y cargas sociales (102 personas totales)	~4.352.000 euros/año
Servicios y mantenimiento (17 oficinas combinadas)	~85.000 euros/ año
Equipamiento inicial	~204.000 euros (inversión única)
TOTAL PRIMER AÑO (ambos departamentos)	~4.641.000 euros
COSTE A PARTIR DEL SEGUNDO AÑO	~4.437.000 euros/año
Coste por ciudadano	Menos de 0,10 euros al año

Menos de 10 céntimos por ciudadano al año.

Para un sistema que detecta depredadores digitales antes de que actúen, interviene en horas y protege a los menores con seguimiento continuo.

5. Cooperación con Plataformas Digitales

Las grandes plataformas tienen obligaciones legales de reporte y deben cooperar activamente con el sistema:

- Google, Meta, Telegrama, WhatsApp y equivalentes deben reportar contenido ilegal de abuso infantil a través de los canales establecidos (NCMEC, INHOPE, Policía Nacional).
- La Ley 34/2002 de Servicios de la Sociedad de la Información obliga a las plataformas a retirar contenido ilegal de forma inmediata cuando sean notificadas.
- El sistema español puede exigir a plataformas operantes en España el cumplimiento de los protocolos de reporte bajo pena de sanción significativa.
- Coordinación con Europol e Interpol para casos con dimensión internacional, que son la mayoría en explotación digital de menores.

6. Base Legal Completa

Función	Marco legal
Tipificación de delitos de explotación infantil	Arts. 189-195 CP. Explotación sexual, grooming y pornografía infantil.
Protección integral del menor	LO 1/1996 de Protección Jurídica del Menor. Arts. 4-5.
Limite de la intervención digital	Art. 18 CE. Solo análisis de contenido publico sin autorización judicial. Comunicaciones privadas requieren orden judicial.
Cooperación con plataformas digitales	Ley 34/2002 de Servicios de la Sociedad de la Información + INHOPE.
Procedimiento garantista en actuaciones	Ley 39/2015 + Art. 24 CE. Derechos de defensa respetados incluso en medidas preventivas.
Protección de datos de menores	RGPD + LOPDGDD. Máxima seguridad y anonimización en alertas.
Coordinación institucional	Ley 17/2015 de Protección Civil. Arts. 3-8. Cooperación entre oficinas, Fiscalía, Policía y Guardia Civil.
Violencia contra la infancia	LO 8/2021 de Protección Integral frente a la Violencia contra la Infancia.

7. Conclusión

Un menor no puede protegerse solo de un depredador digital adulto.

El Estado tiene la obligación de actuar antes de que el daño ocurra.

Detección proactiva en espacios digitales públicos.

Intervención inmediata coordinada entre todos los actores.

Educación preventiva sistemática desde la infancia.

Todo ello por menos de 10 céntimos por ciudadano al año.

Porque la protección de los menores no tiene precio.

Pero si tiene coste. Y es perfectamente asumible.

Este Policy Brief forma parte de España Eficiente: El Modelo Completo.

**Relacionado con: Protección al Menor (Bullying) | DVO y AUXILIA | Integridad Pública
| Administración Digital.**