

IA, seguridad infantil en línea y el desafío de la gobernanza digital
www.360geopolitica.org

La inteligencia artificial está transformando la protección infantil en línea. Si bien la IA ofrece nuevas herramientas para la detección y la investigación, también está haciendo que la explotación sexual infantil sea más sofisticada, escalable y difícil de combatir policialmente. Los gobiernos, las empresas tecnológicas y las agencias de aplicación de la ley enfrentan ahora un doble desafío: contrarrestar los abusos facilitados por la IA al tiempo que garantizan que las respuestas regulatorias no socaven la privacidad, la ciberseguridad y los derechos fundamentales.

Las autoridades alemanas ilustran la magnitud de este cambio. La Oficina Federal de Policía Criminal (BKA) registró a más de 20.000 víctimas de abuso sexual infantil en 2025, y los delitos en línea siguen en aumento. Los investigadores informan de un crecimiento significativo en el acoso cibernético (grooming), el abuso sexual sin contacto físico y la transmisión en vivo de abusos llevados a cabo a través de las fronteras. Las tecnologías digitales permiten cada vez más que los agresores tomen como blanco a los niños de forma remota, lo que complica las investigaciones y refuerza la naturaleza transnacional de estos delitos.

La IA está acelerando estas tendencias al reducir las barreras técnicas para los agresores. La IA generativa puede crear identidades falsas convincentes que los depredadores utilizan para establecer confianza mediante conversaciones personalizadas, mientras que las herramientas de generación de imágenes pueden manipular fotografías inocuas para convertirlas en material de abuso sexual infantil o regenerar contenido ilegal existente, lo que dificulta la detección y la atribución. En consecuencia, las fuerzas del orden deben abordar tanto el volumen creciente de material ilegal como el desafío de distinguir la evidencia auténtica del contenido generado por IA.

Los gobiernos están respondiendo con una regulación digital más firme. Australia ha restringido el acceso a las redes sociales para los menores de 16 años, mientras que la Unión Europea está desarrollando un marco común de verificación de edad para los servicios en línea. Estas iniciativas buscan reducir la exposición de los niños a contenidos nocivos y fortalecer el cumplimiento de las restricciones de edad en las plataformas digitales.

Sin embargo, la verificación de la edad sigue siendo un tema muy disputado. Los defensores de la privacidad y los expertos en ciberseguridad advierten que los sistemas centralizados que exigen documentos de identidad, información biométrica o reconocimiento facial podrían crear objetivos atractivos para los

ciberdelincuentes y ampliar las capacidades de vigilancia. Otros argumentan que asignar la verificación de identidad a las grandes empresas tecnológicas concentraría aún más el poder digital al tiempo que permitiría una mayor recopilación de datos. También existen preocupaciones de que la infraestructura de identidad introducida para la protección infantil pueda reutilizarse más tarde para formas más amplias de control digital.

Más allá de la privacidad, muchos especialistas en protección infantil sostienen que la verificación de la edad aborda los síntomas en lugar de las causas subyacentes. Organizaciones como UNICEF enfatizan que muchos riesgos en línea provienen del diseño mismo de las plataformas. Los algoritmos de recomendación que amplifican el contenido sensacionalista, las funciones impulsadas por la participación como el desplazamiento infinito y los modelos publicitarios que priorizan la atención del usuario pueden exponer a los niños a material nocivo independientemente de las restricciones de edad. Sin abordar estos incentivos estructurales, es poco probable que los controles de acceso por sí solos proporcionen una solución integral e incluso pueden empujar a los menores hacia entornos en línea menos regulados.

Estos debates reflejan un desafío más amplio de gobernanza digital. Los encargados de formular políticas deben proteger simultáneamente a los niños, fortalecer la aplicación de la ley, preservar la privacidad y el anonimato, y evitar la concentración excesiva de poder dentro de un pequeño número de empresas tecnológicas. Por lo tanto, una gobernanza eficaz requiere más que controles de identidad. También exige la rendición de cuentas de las plataformas, tecnologías que preserven la privacidad, cooperación internacional y marcos regulatorios capaces de abordar tanto la actividad delictiva facilitada por la IA como los incentivos comerciales que configuran los ecosistemas digitales.

La brecha de gobernanza digital en Colombia y el reclutamiento en línea de niños ilustra cómo la gobernanza digital se ha convertido en un asunto de seguridad nacional. Si bien los grupos armados ilegales dependían históricamente del control territorial para reclutar niños, niñas y adolescentes, el reclutamiento comienza cada vez más en línea. Las plataformas de redes sociales brindan oportunidades para identificar a menores vulnerables, establecer contacto, manipularlos mediante técnicas de acoso, difundir propaganda y facilitar el reclutamiento mucho antes de que ocurra cualquier encuentro físico.

El marco regulatorio de Colombia no ha seguido el ritmo de esta evolución. La legislación existente aborda el acceso a internet, la ciberseguridad y la protección de datos, pero impone pocas obligaciones a las plataformas digitales para prevenir la explotación

criminal de menores y carece de mecanismos eficaces que regulen el acceso de los niños a las redes sociales. El resultado es una brecha de protección significativa que permite a las organizaciones criminales explotar los algoritmos de las plataformas, los servicios de mensajería privada y las comunidades en línea con una supervisión limitada.

Estas vulnerabilidades se ven reforzadas por la débil presencia del Estado en las regiones afectadas por el conflicto, la pobreza persistente y la expansión territorial de los grupos armados ilegales y las redes de delincuencia organizada. Desde 2022, estos actores han consolidado formas de gobernanza local en varias regiones, a la vez que explotan cada vez más las plataformas digitales para expandir el reclutamiento. La reticencia del gobierno colombiano a adoptar medidas de gobernanza digital más firmes también está moldeada por consideraciones políticas.

Durante la Paz Total, la administración de Petro ha buscado acuerdos negociados con grupos armados ilegales y organizaciones criminales, lo que reduce los incentivos para perseguir medidas regulatorias o de cumplimiento más sólidas que puedan perturbar dichos compromisos. Los analistas argumentan que estos grupos también conservan una influencia significativa sobre las dinámicas políticas nacionales y locales, como se demostró durante las elecciones legislativas y presidenciales de 2026, donde implementaron la "los votos-pistola" para favorecer al movimiento político de Petro y del senador Iván Cepeda.

La experiencia internacional demuestra que los gobiernos tratan cada vez más la seguridad en línea de los niños como un asunto de política pública y no únicamente como una responsabilidad parental o un

acuerdo político. Australia ha adoptado restricciones de edad obligatorias para las redes sociales, mientras que España ha combinado una regulación más estricta con iniciativas de alfabetización digital. Aunque estos enfoques difieren, ambos reconocen que las plataformas digitales se han convertido en componentes críticos de la política de protección infantil.

Para Colombia, sin embargo, el desafío va más allá de la seguridad en línea. Las plataformas de redes sociales se han convertido en parte del entorno de seguridad más amplio del país. Las organizaciones internacionales han documentado su uso por parte de grupos armados para reclutar niños, difundir propaganda, normalizar la violencia y facilitar la actividad delictiva. A medida que el reclutamiento se traslada cada vez más a los espacios digitales, la ausencia de una regulación eficaz de las plataformas afecta directamente tanto a la protección infantil como a la seguridad nacional.

La pregunta central de política pública es, por lo tanto, si Colombia continuará dependiendo de una regulación fragmentada o adoptará una estrategia integral de protección infantil digital que combine la rendición de cuentas de las plataformas, el monitoreo de riesgos, salvaguardas de edad específicas e intervenciones preventivas.

En una era donde el reclutamiento comienza cada vez más en línea, la gobernanza digital ya no es simplemente un problema tecnológico; es un asunto de protección infantil, seguridad pública, y de capacidad y responsabilidad estatal.

360° geopolítica.