

302 ألف بلاغ استغلال .. ثغرات التشريع تترك أطفال مصر فريسة للاستدراج والابتزاز عبر «الدارك ويب»



الخميس 3 سبتمبر 2026 06:00 م

تكشف 302 ألفًا و829 بلاغًا مرتبطًا بمواد الاستغلال الجنسي للأطفال خلال 2024 أن الخطر الرقمي لم يعد احتمالاً بعيدًا، بل تهديدًا يقتحم حياة القصر يوميًا.

وتطرح الأرقام سؤالًا ملجأ: هل تكفي التشريعات المصرية الحالية للردع، أم أن تشتتها وبطء إنفاذها يمدحان شبكات الاستغلال مساحة للتخفي وتكرار جرائمها؟

قوانين متعددة وردع منقوص

لا يخلو القانون المصري من أدوات لمواجهة الاعتداءات الرقمية على الأطفال، لكنه يوزع الحماية بين تشريعات متعددة، لكل منها نطاق مختلف وآليات تطبيق منفصلة.

يأتي قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018 في مقدمة الأدوات، إذ يجرم اختراق الحسابات والاعتداء على الخصوصية والاستخدام الإجرامي للبيانات.

ويمنح قانون الطفل رقم 12 لسنة 1996، وتعديلاته، حماية للقصر من الاستغلال الجنسي، وإنتاج المواد الإباحية التي تتضمنهم أو حيازتها أو عرضها أو تداولها.

كذلك يواجه قانون العقوبات التهديد والابتزاز والاعتداءات الجنسية، بينما يتدخل قانون مكافحة الاتجار بالبشر عندما يتحول الاستغلال إلى تجنيد منظم أو منفعة مادية.

هذه المنظومة تبدو واسعة على الورق، غير أن اتساعها لا يعني اكتمالها؛ لأن الجريمة تبدأ غالبًا قبل الصورة الفاضحة أو طلب المال.

فالاستدراج الرقمي يبدأ برسالة ودية داخل لعبة أو منصة مفتوحة، ثم ينتقل إلى كسب الثقة وجمع المعلومات ودفع الطفل تدريجيًا لإرسال محتوى خاص.

ولا يحمل هذا المسار المتدرج دائمًا توصيفًا جنائيًا مستقلاً وواضحًا منذ بدايته، ما قد يؤخر التدخل حتى يظهر تهديد صريح أو ضرر قابل للإثبات.

وهنا تكمن فجوة الردع؛ فالقانون يستطيع معاقبة نتائج الاعتداء، لكنه يواجه صعوبة أكبر في اعتراض مرحلة الإعداد النفسي السابقة على الجريمة المكتملة.

ويصبح معيار الكفاية الحقيقي هو قدرة التشريع على منع الضرر مبكرًا، لا زيادة العقوبات بعد انتشار الصور أو تحطيم الضحية نفسيًا واجتماعيًا.

لذلك تمثل النصوص الحالية أساسًا للمحاسبة، لكنها ليست حائط صد كاملًا أمام جريمة سريعة ومشفرة وعابرة للحدود، تستهدف طفلًا يسهل خداعه وإسكاته.

الأرقام تكشف فجوة التنفيذ

بلغت البلاغات المرتبطة بمصر عبر نظام «سايبر تيب لاین» 431 ألفًا و44 بلاغًا في 2022، ثم قفزت إلى 627 ألفًا و802 خلال 2023. وتراجعت إلى 302 ألف و829 بلاغًا في 2024، لكن الانخفاض لا يثبت وحده انحسار الجرائم، ولا يعبر بالضرورة عن عدد الضحايا داخل مصر مع ذلك، يفرض حجمها أسئلة حول سرعة فحص الإحالات، وتحديد الأطفال المعرضين للخطر، والوصول إلى الجناة قبل محو الأدلة أو نقلها بين الخوادم.

وتعزز المخاوف واقعة أعلنتها هيئة الرقابة الإدارية في فبراير 2025، بعد ضبط متهم باختراق حسابات أكثر من مئة فتاة قاصر من جنسيات مختلفة.

واستخدم المتهم، وفق الواقعة المعلنة، الصور الخاصة في التهديد والابتزاز، ما يثبت أن منصة عادية قد تصبح بوابة للجريمة دون دخول الضحية للشبكات المظلمة.

كما سجل خط نجدة الطفل 16000 خلال 2025 نحو 584 ألفًا و809 مكالمات، بينها 27 ألفًا و700 بلاغ، بزيادة 29.3% عن العام السابق. وتضمنت البلاغات حالات مرتبطة باستغلال الأطفال عبر الإنترنت، بما يؤكد أن المشكلة تتجاوز الوقائع الفردية، وتحتاج قدرة مؤسسية على الفرز والتحليل والتدخل المتخصص.

وفي يناير 2026، سجل مؤشر حماية الطفولة من مخاطر الإنترنت 64.3 نقطة، بينما بلغ مؤشر الاستخدام الرقمي الآمن للأطفال 75.6 نقطة.

لا يتحقق الردع بحبس الجاني فقط، بل بارتفاع احتمال اكتشافه سريعًا، وحفظ الدليل الرقمي، وربط الحسابات المستعارة، ومنع إعادة تداول المواد المسيئة.

غير أن التشفير والحسابات المؤقتة والخوادم الأجنبية وأدوات إخفاء الهوية تجعل التحقيق التقليدي أبطأ من حركة المجرمين بين التطبيقات والمنصات والبلدان.

كما يظل خوف الطفل من اللوم أو الفضيحة عائقًا أمام الإبلاغ، فتبدأ العدالة متأخرة بعدما يحصل المبتز على مزيد من السيطرة والمواد الخاصة.

وبذلك تبدو أزمة التنفيذ مساوية لأزمة النصوص، وربما أشد؛ لأن العقوبات تفقد أثرها حين تغيب وحدات متخصصة واستجابة موحدة ونتائج معلنة للرأي العام.

إصلاح يسبق الجريمة

يتطلب سد الفجوات تعريفيًا قانونيًا واضحًا للاستدراج الإلكتروني للأطفال، يشمل بناء الثقة بقصد الاستغلال، حتى قبل الحصول على صورة أو ترتيب لقاء مباشر.

كما تحتاج مسؤولية المنصات إلى قواعد محددة لاستقبال البلاغات، والحفاظ العاجل على الأدلة، وتعطيل الحسابات الخطرة، وإحالة الوقائع إلى جهات التحقيق.

ولا يعني ذلك فرض مراقبة شاملة؛ فالحماية الفعالة يجب أن تخضع للضرورة والتناسب والرقابة القضائية، كي لا تتحول مكافحة الجريمة إلى انتهاك جماعي للخصوصية.

المطلوب أيضًا بروتوكول وطني موحد يجمع الداخلية والاتصالات والنيابة العامة وتنظيم الاتصالات والطفولة والأمومة، مع نقاط اتصال تعمل طوال اليوم دون تضارب اختصاصات.

ويجب أن يحدد البروتوكول زمنيًا للاستجابة، ومسارًا عاجلًا لإنقاذ الطفل، وآلية لحذف المحتوى من مصادره، وإجراءات تمنع إعادة نشره أو مواصلة الابتزاز بواسطته.

ويستوجب البعد العابر للحدود توسيع المساعدة القانونية وتبادل المعلومات، لأن حسابًا يستهدف طفلًا في القاهرة قد يديره مجرم من دولة أخرى.

في المقابل، يجب ألا يتحول الطفل إلى متهم بسبب صورة أُجبر على إرسالها، بل يعامل باعتباره ضحية تحتاج الحماية النفسية والقانونية وإزالة المحتوى.

وتقتضي الحماية توفير محامين ومتخصصين نفسيين، وضمان سرية البلاغ، ومنع كشف الهوية، وتجنب تكرار استجواب الطفل بصورة تزيد صدمته أو تدفعه للتراجع

وتظل الأسرة خط الدفاع الأول، لكن تحميلها المسؤولية وحدها يبرئ المنصات والمؤسسات؛ فالرقابة الأبوية لا تستطيع وحدها مواجهة شبكات محترفة وأدوات تقنية معقدة

وتحتاج المدارس إلى تعليم السلامة الرقمية عملياً، بما يشمل رفض المحادثات المريبة، وعدم إرسال الصور، وحفظ الدليل، والحظر، والإبلاغ دون خوف من العقاب

كما ينبغي إعلان بيانات دورية توضح البلاغات المحالة والتحقيقات والأحكام ومدة الاستجابة، بدل الاكتفاء بأرقام ضخمة لا تكشف مصير الحالات أو فعالية التدخل

الإجابة ليست نعم أو لا مطلقة؛ فالتشريعات توفر أساساً للمحاسبة، لكنها لا تواكب كل مراحل الاستدراج ولا سرعة التحولات التقنية التي يستغلها المجرمون

ومن دون تجريم مبكر وتحقيق متخصص وتعاون دولي ومسؤولية واضحة للمنصات، ستظل العقوبة تصل بعد الضرر، بينما يواصل المعتدي البحث عن ضحية جديدة

إن حماية الأطفال لا تبدأ عند أبواب «الدارك ويب»، بل من أول رسالة مريبة على لعبة أو تطبيق، ومن دولة تتحرك قبل تحول الصمت إلى كارثة