

ورقة عمل بعنوان:

"دور مؤسسات المجتمع المدني في تعزيز الحماية الرقمية للأطفال"

ورقة عمل نتقدم بها لمؤتمر الشبكة العربية للمؤسسات الوطنية
لحقوق الإنسان بخصوص "حماية الأطفال في الفضاء الرقمي:
التحديات والتشريعات والإجراءات الوقائية"

جمعية مبادئ لحقوق الإنسان

"حاصلة على الصفة الاستشارية من المجلس الاقتصادي
والاجتماعي للأمم المتحدة"

12 يناير 2026م

"المنامة – مملكة البحرين"

المقدمة:

يشهد العالم اليوم اندماجًا متسارعًا للأطفال في الفضاء الرقمي، حيث يستخدمون الإنترنت والتقنيات الحديثة في سن مبكرة. ورغم ما يوفره هذا الاندماج من فرص تعليمية وترفيهية، إلا أنه يطرح تحديات جسيمة تتعلق بسلامة الأطفال وحقوقهم. تهدف هذه الورقة إلى استعراض أبرز التحديات التي تواجه الأطفال في الفضاء الرقمي، وتحليل الإطار التشريعي البحريني لحماية الأطفال على الإنترنت، مع إيراد مقارنات مختصرة من التشريعات الأوروبية والأمريكية وبعض التشريعات العربية، ثم تقديم إجراءات وقائية وممارسات جيدة وتوصيات عملية موجّهة للقانونيين ومؤسسات المجتمع المدني.

أولاً: التحديات الرئيسية في الفضاء الرقمي

يواجه الأطفال على الإنترنت عددًا من المخاطر والتحديات المتنوعة التي قد تؤثر على سلامتهم البدنية والنفسية وحقوقهم، ومن أهمها:

1) التحرش والاستغلال الجنسي عبر الإنترنت

تُعد جرائم الاستدراج الجنسي للأطفال عبر المنصات الرقمية من أخطر التهديدات. يستغل بعض الجناة سهولة التواصل لإيقاع الأطفال في فخاخ التحرش أو الابتزاز أو دفعهم لمشاركة صور ومقاطع مسيئة، وقد تتطور الجريمة إلى استغلال مباشر أو اتجار أو إنتاج/تداول محتوى إباحي يتعلق بالأطفال. يترتب على هذه الجرائم آثار نفسية واجتماعية عميقة، وتستدعي استجابة قانونية صارمة وآليات إبلاغ سريعة وحماية متخصصة للضحايا.

2) التنمر الإلكتروني

انتقل التنمر إلى فضاءات التواصل الرقمي، ويشمل الإهانات، التشهير، نشر الشائعات، مشاركة صور أو مقاطع بهدف الإذلال، أو إقصاء الطفل من المجموعات الرقمية. ويزداد أثره بسبب استمراره خارج المدرسة، وسرعة الانتشار، وصعوبة محو الأثر الرقمي، ما قد يؤدي إلى القلق والاكتئاب والعزلة وترك الدراسة.

(3) انتهاك الخصوصية وجمع البيانات

يشكل جمع البيانات عن الأطفال دون وعي أو دون موافقة ولي الأمر خطرًا مركبًا: تجاريًا (الإعلانات المستهدفة)، وأمنيًا (انتحال الهوية)، واجتماعيًا (الابتزاز أو التنمر). كما أن الأطفال قد يشاركون معلومات حساسة دون إدراك للعواقب، ما يتطلب قواعد خصوصية صارمة وإعدادات افتراضية حامية وتوعية قانونية وتقنية.

(4) الإدمان الرقمي والتأثيرات النفسية

الاستخدام المفرط للأجهزة والألعاب والمنصات قد يتحول إلى إدمان يؤثر على النوم، والتحصيل الدراسي، والقدرة على التركيز، والتوازن النفسي والاجتماعي. وتزداد المشكلة مع تصميم بعض التطبيقات على تعزيز (الارتباط القهري) عبر الإشعارات والخوارزميات والمكافآت الرقمية.

(5) الوصول إلى محتوى غير لائق أو ضار

قد يصل الأطفال إلى محتوى إباحي أو عنيف أو خطاب كراهية أو تحديات خطيرة أو مواد تحرض على إيذاء النفس أو الآخرين. ويمثل ذلك تحديًا تشريعيًا (تنظيم المحتوى)، وتقنيًا (التصفية والتحقق العمري)، وتربويًا (التوجيه وبناء المناعة المعرفية).

ثانيًا: الإطار التشريعي لحماية الأطفال على الإنترنت في البحرين

تقوم الحماية القانونية للطفل في البحرين على منظومة تشريعية متداخلة تشمل حماية الطفل من الاستغلال والاعتداء، وتجريم الأفعال الرقمية الضارة، وحماية البيانات الشخصية. من أبرز ملامح هذا الإطار:

(1) قانون الطفل الصادر بالقانون رقم (37) لسنة 2012م

يضع قانون الطفل قواعد لحماية الطفل من الاستغلال والإيذاء، ويتضمن تجريمًا لأشكال من الاستدراج أو التحرش أو التعريض لمحتوى غير مناسب عبر الوسائل الإلكترونية، مع تشديد على حماية الطفل من الاستغلال الجنسي وأي صور من الاعتداء أو التغيرير.

(2) قانون مكافحة جرائم تقنية المعلومات (الجرائم الإلكترونية) رقم (60) لسنة 2014م

يركّز على تجريم الأفعال المرتبطة باستخدام أنظمة وتقنيات المعلومات، بما يشمل جرائم نشر أو تداول أو حيازة محتوى إباحي، وتشديد العقوبة عندما يتعلق الأمر بالأطفال، فضلاً عن الجرائم التي قد يكون الطفل ضحية لها مثل الابتزاز، والتهديد، والاختراق، وانتهاك الخصوصية الرقمية.

(3) قانون حماية البيانات الشخصية

يؤسس لمبادئ ومعايير لمعالجة البيانات الشخصية (الجمع، الاستخدام، الإفصاح، التخزين)، ويدعم حماية خصوصية الأفراد بمن فيهم الأطفال، ويعزز فكرة الموافقة والشفافية والغرض المحدد وتقليل البيانات والأمن السيبراني، بما ينعكس على حماية بيانات الأطفال بشكل مباشر أو عبر ممثليهم القانونيين.

(4) تكامل التشريعات مع آليات الحماية

إلى جانب التجريم، تظهر أهمية وجود آليات حماية عملية مثل قنوات البلاغات، وجهات التحقيق المتخصصة، والخدمات الاجتماعية والنفسية، وتنسيق الاستجابة بين الجهات الأمنية والاجتماعية والتعليمية والصحية، بما يضمن عدم إعادة إيذاء الطفل أثناء الإجراءات.

ثالثاً: المقارنة الدولية

تهدف المقارنة هنا إلى الاستفادة من بعض النماذج التشريعية دون نسخها حرفياً، مع مراعاة الخصوصية التشريعية في تشريعات مملكة البحرين:

(1) الاتحاد الأوروبي حماية البيانات GDPR

يركز على حماية البيانات والخصوصية ويمنح الأطفال حماية إضافية عند معالجة بياناتهم، لا سيما في الخدمات الرقمية القائمة على الموافقة، مع توجهات داعمة لتصميم منصات أكثر أماناً للأطفال وإعدادات خصوصية افتراضية أعلى.

(2) الولايات المتحدة (COPPA)

يعالج خصوصاً جمع البيانات من الأطفال في الخدمات والمواقع الموجهة لهم، ويشترط الموافقة الأبوية قبل جمع معلومات الطفل، ويشدد على شفافية سياسات الخصوصية وعلى التزامات مقدمي الخدمة.

رابعاً: الإجراءات والممارسات الوقائية

الحماية الفعّالة لا تقتصر على النصوص؛ بل تتطلب إجراءات وقائية متعددة المستويات:

1) على مستوى مؤسسات المجتمع المدني

- تنفيذ برامج توعية قانونية/رقمية للأطفال والأهالي.
- إنشاء شراكات مع المدارس والجهات الرسمية لتنفيذ حملات مستدامة.
- تقديم خدمات دعم وإرشاد للضحايا (نفسية/اجتماعية/قانونية).
- تعزيز ثقافة الإبلاغ وعدم لوم الضحية، وتدريب العاملين على حماية الطفل.

2) على مستوى الأسرة

- وضع قواعد واضحة لاستخدام الأجهزة والإنترنت بحسب العمر.
- تفعيل أدوات الرقابة الأبوية وتصفية المحتوى وضبط الخصوصية.
- تعزيز الحوار مع الطفل وبناء الثقة وتشجيعه على الإبلاغ المبكر.
- تعليم الطفل مبادئ السلامة: عدم مشاركة معلومات شخصية، عدم التواصل مع غرباء، عدم إرسال صور خاصة.

3) على مستوى البيئة التعليمية

- إدماج التنقيف الرقمي والحقوق الرقمية في المناهج والأنشطة.
- سياسات مدرسية واضحة للتعامل مع التنمر الإلكتروني وحالات الابتزاز.
- توفير مرشدين مدربين وتسهيل الإبلاغ داخل المدرسة.
- برامج توعية مشتركة مع أولياء الأمور.

4) على مستوى المنصات ومقدمي الخدمة

- إعدادات افتراضية عالية الخصوصية لحسابات القُصّر.

- آليات تحقق عمري مناسبة ومتوازنة مع الخصوصية.
- أدوات تحكم أبوية سهلة الاستخدام.
- تسهيل الإبلاغ عن المحتوى الضار والاستجابة السريعة للبلاغات.

خامساً: توصيات لتعزيز الإطار التشريعي والوقائي في البحرين

1. مراجعة دورية للتشريعات: لمواكبة الجرائم المستحدثة (مثل الابتزاز الجنسي الرقمي وأساليب الاستغلال الجديدة).
2. تطوير لوائح/إرشادات تنفيذية: متخصصة لحماية بيانات الأطفال ضمن منظومة حماية البيانات الشخصية، خاصة فيما يتعلق بالإعلانات المستهدفة وجمع البيانات في التطبيقات الموجهة للأطفال.
3. تعزيز التخصص القضائي والتحقيقي: عبر تدريب القضاة وأعضاء النيابة وضباط التحقيق على أدلة الجرائم الرقمية وآليات مقابلة الأطفال الضحايا.
4. توسيع أدوات الإبلاغ والحماية: خطوط مساعدة متعددة القنوات، دعم نفسي واجتماعي وقانوني، إجراءات سريعة لحجب المحتوى الضار عند الضرورة.
5. إدماج التثقيف الرقمي إلزامياً: في المدارس (حقوق الطفل الرقمية، خصوصية البيانات، التمر الإلكتروني، مهارات التفكير النقدي).

المستشار المحامي الحقوقي

حمد راشد

عضو جمعية مبادئ لحقوق الانسان