
EGYPTIAN INITIATIVE FOR PERSONAL RIGHTS
مبادرة المصرية لحقوق الشخصية
مسار
masaar
Technology & Law Community
بلا مقايضة
نحو حماية الأطفال على الإنترنت مع احترام حقوقهم

بلا مقايضة:

نحو حماية الأطفال على الإنترنت مع احترام حقوقهم

دراسة

أبريل 2026

"مسار" مجموعة من القانونيين والتقنيين المهتمين بالعمل على تعزيز الحقوق الرقمية والحريات المرتبطة بها في مصر، وتركز في عملها على الدمج بين التقنية والقانون وفهم تأثيرهما على الأفراد والمجتمع والحريات الأساسية. تستهدف "مسار" تركيز أنشطتها على الحريات الرقمية في النطاق المصري إلا أن ذلك لا يعزلها عن قضايا حقوق الإنسان في باقي مجتمعات المنطقة العربية والعالم.
للاتصال بمسار: masaarnet@gmail.com

المبادرة المصرية للحقوق الشخصية منظمة حقوقية مستقلة تعمل في مصر منذ عام 2002 على تعزيز وحماية الحقوق والحريات الأساسية في مصر، وذلك من خلال أنشطة البحث والدعوة والتقاضي في مجالات الحريات المدنية، والعدالة الاقتصادية والاجتماعية، والديمقراطية والحقوق السياسية، والعدالة الجنائية. للاتصال بالمبادرة: eipr@eipr.org

خلفية

شهد المجال العام المصري منذ أواخر يناير وبداية فبراير 2026 انتقالًا سريعًا من خطاب عام يدور حول مخاطر السوشيال ميديا والألعاب على الأطفال إلى مسار سياسي وتنظيمي مباشر تشارك فيه مؤسسات الدولة على مستويات متعددة، بما يجعل الملف أقرب إلى ورشة صياغة سياسة عامة تستعد الدولة من خلالها لإصدار تشريع جديد.

بدأت ملامح هذا التحول عندما أعلن الرئيس المصري عن توجيهاته في النظر إلى تنظيم استخدام الأطفال للإنترنت والشبكات الاجتماعية وتبع ذلك إشارات برلمانية واضحة تتحدث عن اتجاه تشريعي لوضع ضوابط لاستخدام الأطفال لتطبيقات ومواقع التواصل، مقرونًا بدعوة إلى حوار مجتمعي حول الصياغة وآليات التنفيذ.

وخلال أيام قليلة، اتسع نطاق النقاش داخل مجلس الشيوخ ليضم الهاتف المحمول والإنترنت ووسائل التواصل والألعاب الإلكترونية في جلسة عامة، ثم اتخذ مسارًا مؤسسيًا أكثر رسوخًا عبر إحالة طلبات المناقشة إلى لجنة مشتركة تضم أكثر من لجنة نوعية. هذه الإحالة تحمل دلالة سياسية وتنظيمية مهمة، لأنها تقدم الملف باعتباره قضية متعددة الأبعاد تمس التعليم والصحة والاتصالات والشباب والحماية الاجتماعية في وقت واحد، بما يفتح الباب أمام تدخلات تتجاوز فكرة محتوى ضار إلى تصور أشمل عن إدارة العلاقة بين الطفل والفضاء الرقمي.

وبالتوازي مع المسار البرلماني، صعد الملف إلى مستوى تنفيذي أعلى عبر اجتماع رسمي برئاسة رئيس مجلس الوزراء لمناقشة إجراءات حماية الأطفال والنشء من المحتوى الضار على وسائل التواصل، مع ربط مباشر بالتوجيهات الرئاسية وإعلان نية إعداد إطار تنظيمي يُلزم المنصات بتدابير وقائية. اللافت في هذا المسار أن التصور المعروض لم يقف عند حدود التوعية، بل تضمن ملامح عملية تشير إلى نموذج ضبط أكثر صرامة، من قبيل تصنيف عمري موحد وآليات تحقق وأدوات رقابة أبوية وعقوبات.

وفي المناخ السياسي المصري عادة ما تميل الإجراءات التنفيذية السريعة إلى التقدم على النقاش المجتمعي المتأني، وتظهر ملامح ذلك في خيارات تتجه إلى المنع والحجب بوصفها استجابة فورية للمخاطر المتصورة. قرار حجب منصة ألعاب روبلوكس مع التنسيق الفني للتنفيذ عبر شركات الإنترنت يقدم مثالًا على حضور أدوات التقييد الشامل كخيار عملي مطروح، لا كافتراض نظري، حيث يُقدَّم الملف باعتباره تهديدًا عاجلًا يستدعي تدخلًا سريعًا.

مقدمة

تأتي هذه الدراسة استجابةً لحاجة إلى مقاربة حقوقية واضحة في التعامل مع ملف حماية الأطفال والمراهقين في الفضاء الرقمي، في لحظة يزداد فيها خلط شائع بين هدفي حماية الطفل من أضرار محددة يمكن رصدها ومعالجتها، و توسيع أدوات الضبط العام للاتصال والمحتوى تحت زريعة الحماية.

تنطلق الدراسة من أن سلامة الأطفال على الإنترنت ليست عنوانًا فضفاضًا يصلح لتبرير أي إجراء، بل مجال سياسات دقيقة ينبغي أن يُبنى على فهم طبيعة المخاطر، وعلى التزامات الدولة بحماية الحقوق الأساسية، وعلى تحميل المنصات مسؤولية تصميم بيئات أقل ضررًا.

وتُميز الدراسة بين سلامة الأطفال باعتبارها سياسة وقائية تستهدف تقليل احتمالات التعرض للاستغلال أو التنمر أو المحتوى شديد الضرر، وبين الرقابة على الإنترنت باعتبارها نهجًا يعتمد على المراقبة الواسعة أو الحجب أو تقييد الوصول.

لذلك تلتزم الدراسة بمبدأ حماية الأطفال كهدف مشروع وضروري، لكنه لا يجوز أن يتحقق على حساب الخصوصية للجميع، ولا عبر بناء مسارات دخول قائمة على جمع بيانات موسع، ولا عبر إجراءات تُقيد حق الوصول إلى المعرفة والتواصل بصورة غير متناسبة.

وتركز الدراسة على نطاق واضح يضم الأطفال والمراهقين بوصفهم الفئة الأساسية المعنية بالحماية، ويشمل منصات التواصل الاجتماعي بما تتضمنه من توصية خوارزمية وإعلانات واستهداف سلوكي ورسائل خاصة، ويشمل كذلك الألعاب الإلكترونية المتصلة بالإنترنت، خصوصًا تلك التي تعتمد على التواصل بين المستخدمين أو المحتوى الذي يصنعه المستخدمون داخل اللعبة، إضافة إلى الهاتف الذكي بوصفه بوابة الوصول الأكثر انتشارًا للخدمات والمنصات.

كما تتناول الدراسة البنية التنظيمية التي يُتوقع أن تُستخدم في هذا الملف، مثل التصنيف العمري، وآليات التحقق من السن، وأدوات الرقابة الأبوية، والالتزامات المفروضة على المنصات، وأي تدابير تقييدية مثل الحجب أو المنع، مع التركيز على آثار كل خيار على الحقوق والحريات الرقمية.

وتأتي هذه الدراسة في سياق حساسية الوضع الحقوقي والسياسي المصري. إذ أن الاعتماد الواسع على أدوات الحجب كإجراء حاضر في إدارة المجال الرقمي، يجعل أي نقاش عن حماية الأطفال معرضًا لأن ينزلق سريعًا إلى إجراءات تقييد شاملة بدل حلول دقيقة. كما أن محدودية الشفافية المؤسسية وآليات المساءلة المستقلة، تضعف القدرة على تقييم ما إذا كانت التدابير المقترحة ضرورية ومتناسبة، ويجعل من الصعب تتبع كيفية اتخاذ القرارات ومن يملك سلطة إنفاذها ومعاييرها. بالإضافة إلى مخاطر التوسع الوظيفي، أي انتقال الأداة من غرضها المعلن إلى أغراض أوسع مع مرور الوقت، بحيث تتحول تدابير وُضعت لحماية الأطفال إلى بنية دائمة لإدارة الهوية أو مراقبة الاستخدام أو ضبط المحتوى على نطاق عام، بما يمس المجتمع ككل.

بناءً على ذلك، تركز الدراسة على أن السياسات الفعالة لا تتعامل مع وجود الأطفال على الإنترنت باعتباره المشكلة، بل تتعامل مع نقاط ضرر محددة داخل تصميم المنصات والألعاب وطريقة تشغيلها. والمقاربة التي تتبناها تعطي الأولوية لتغييرات ملموسة تقلل فرص الاستدراج والتواصل غير الآمن، وتحد من الاستهداف الإعلاني والتتبع السلوكي، وتضبط خصائص التوصية التي تدفع المحتوى نحو التطرف أو العنف أو الإيذاء النفسي، وتقوي آليات الإبلاغ والاستجابة والدعم.

هذه المقاربة تضع المسؤولية في مكانها الصحيح، عند الجهات التي تبني بيئات رقمية مربحة من تعظيم الانتباه والتفاعل، بدل أن تنقل العبء إلى الأطفال والأسر عبر حلول عامة تُجبر الجميع على المرور من بوابات تحقق واسعة أو تواجه المجتمع بعقوبات وحجب.

أولًا: منهجية الدراسة

تتبنى الدراسة إطارًا يركز على الانتقال من توصيف عام وفضفاض لمخاطر الإنترنت على ال إلى خريطة ضرر دقيقة تُميّز بين مسارات مختلفة، لكل منها طبيعة خاصة وأدوات تدخل مختلفة. في هذا السياق، تعتمد على الدراسة على نموذج الأربعة سيهات (4Cs Model) بوصفه إطارًا تصنيفيًا مبسطًا لمخاطر البيئة الرقمية على الأطفال والمراهقين، يقوم على تقسيم مصادر الضرر إلى أربعة مسارات رئيسية متمايزة، هي المحتوى (Content)، والتواصل (Contact)، والسلوك (Conduct)، والتجارة/الاستغلال الاقتصادي (Commerce). يتيح هذا التقسيم تحويل الحديث العام عن مخاطر الإنترنت إلى خريطة ضرر قابلة للرصد والتنظيم، لأن كل مسار يرتبط بأنواع مختلفة من الأذى وبأدوات تدخل مختلفة.

المحتوى (Content)

يرتبط هذا المسار بما يتعرض له الطفل أو المراهق من مواد رقمية قد تحمل ضررًا مباشرًا أو تراكميًا. لا يقتصر الأمر على مشاهد العنف أو المحتوى الجنسي الصريح، بل يشمل كذلك محتوى يحرض على إيذاء النفس، أو يروّج لسلوكيات خطرة، أو يقدّم معلومات مضللة تُستغل فيها قلة الخبرة وصغر السن.

يتضمن هذا المسار أيضًا المحتوى الذي يطبّع الكراهية أو الإهانة أو الوصم، بما ينعكس على الصحة النفسية وإحساس الطفل بالأمان والانتماء. ويكتسب هذا المسار أهمية إضافية بسبب انتشار إعادة النشر على نطاق واسع داخل مجموعات وتطبيقات لا تخضع عادةً لرقابة عمرية فعالة، وبسبب سرعة انتقال المقاطع بين المنصات، بما يجعل الحد الفاصل بين مشاهدة عابرة وتعرض متكرر شديد الهشاشة.

التواصل (Contact)

يتعلق هذا المسار بطبيعة العلاقات التي تنشأ عبر الفضاء الرقمي، وبالاحتكاك المباشر بين الطفل أو المراهق وأشخاص آخرين، سواء كانوا معروفين أو غرباء. تظهر المخاطر هنا في أشكال متعددة، منها الاستدراج والتلاعب العاطفي، ومحاولات الحصول على صور أو معلومات شخصية، والابتزاز، ودوائر ضغط تتشكل داخل المحادثات الخاصة أو مجموعات اللعب.

هذا المسار لا يفترض أن الخطر يأتي دائمًا من الغريب، لأن جزءًا منه يتصل بعلاقات بين أقران داخل المدرسة أو الحي أو دوائر الاهتمام المشتركة، ثم تتحول إلى إساءة عبر القنوات الرقمية. وخطورة هذا المسار تنبع من أنه يعمل عبر التراكم البطيء وبناء الثقة، ثم يتحول في لحظة إلى ضرر يصعب احتواؤه، خصوصًا عندما يرتبط بتهديدات أو نشر معلومات أو صور.

السلوك (Conduct)

يرتبط هذا المسار بما يصدر عن الأطفال والمراهقين أنفسهم في تفاعلهم الرقمي، وبما يقع داخل الجماعات الرقمية من أنماط سلوك قد تتحول إلى أذى. يتضمن ذلك التنمر، والتحرش اللفظي، والتشهير، والملاحقة، ونشر الأسرار، والمشاركة في تحديات خطرة، وتبادل المحتوى المهين، أو إعادة توجيه إساءات حدثت أصلًا في المدرسة إلى فضاء أوسع وأكثر إيذاءً.

يتميز هذا المسار بأن الأذى لا ينتج فقط من وجود مادة ضارة أو شخص سيئ النية، بل من ديناميكيات جماعية تشجع التصعيد،

وتكافؤ الإهانة بالضحك أو التفاعل أو الانضمام للتيار السائد. في حالات كثيرة يصبح الانسحاب من المجموعة أو اللعبة مكلفًا اجتماعيًا للمراهق، لأن الانتماء الرقمي يتداخل مع الانتماء الواقعي، فيستمر الضرر ويتكرر، وتصبح آثاره ممتدة.

التجارة والاستغلال الاقتصادي (Commerce)

يصف هذا المسار ما يتعرض له الأطفال والمراهقون بوصفهم مستهلكين داخل بيئات رقمية صُممت لتحقيق عائد اقتصادي. يظهر ذلك في الإعلانات الموجهة، والشراء داخل التطبيقات والألعاب، والعروض التي تدفع المستخدم إلى الدفع المتكرر، أو إلى تبادل بياناته ووقته مقابل امتيازات رقمية. كما يشمل هذا المسار استغلال الانتباه بوصفه موردًا اقتصاديًا، بحيث تصبح التجربة الرقمية مبنية على دفع المستخدم إلى البقاء أطول، والنقر أكثر، والعودة سريعًا، حتى وإن أدى ذلك إلى ضغط نفسي أو اضطراب يومي.

في هذا المسار لا يكون الطفل هدفًا لضرر عرضي، بل جزءًا من سوق، بما يستدعي أن تكون الحماية هنا تنظيمًا للممارسات التجارية داخل هذه الخدمات، وليس فقط توصية أخلاقية عامة.

1. مسارات الضرر

تُنتج مسارات الضرر السابقة أثرها داخل بنية تشغيل تجعل الضرر قابلًا للتكرار وإعادة الإنتاج، إذ يقوم المحرك الأساسي لهذا الضرر على مزيج من نماذج ربح تعتمد على كثافة الاستخدام، وتصميمات تستهدف جذب الانتباه وإعادة تدويره، وآليات تمنح الأفضلية للمحتوى الأكثر إثارة أو صدمة أو استفزازًا لأنه يحقق معدلات تفاعل أعلى.

ضمن هذه البيئة ترتفع احتمالات التعرض للمحتوى الحاد، وتتزايد كثافة التواصل مع غرباء أو دوائر ضاغطة، ويصبح السلوك الجماعي أكثر قابلية للتصعيد، كما يزداد حضور البعد التجاري لأن الاستغلال الاقتصادي مدمج في تجربة التصفح أو اللعب نفسها.

ويقود التعامل مع مخاطر الأطفال والمراهقين بوصفها مشكلة واحدة إلى حلول عامة لا تمس هذا المحرك البنيوي، بينما يتيح نموذج 4Cs فهمًا أدق للأذى بوصفه متعدد المسارات ومتداخلًا، ويؤسس لسياسة عامة تستهدف مصادر الضرر المحددة، وتُميّز بين ما يتطلب ضبطًا تقنيًا، وما يحتاج حماية قانونية، وما يستدعي سياسات تعليمية ودعمًا اجتماعيًا، دون إذابة المسارات المختلفة في عنوان واحد.

ويستدعي هذا المنظور النظر إلى محركات الضرر داخل التطبيقات والمنصات والألعاب، ولا سيما ما يتصل بخوارزميات التوصية ومنطق الربح وآليات الشراء داخل التطبيقات والألعاب وغيرها من العوامل المشغِّلة. إذ تعمل خوارزميات التوصية في منصات التواصل وفق منطق انتقاء ما يُبقي المستخدم مدة أطول وما يرفع احتمالات التفاعل، فتدفع المحتوى نحو أنماط أكثر إثارة أو صدمة أو استفزازًا لأنها غالبًا ما تولّد نقرات وتعليقات ومشاهدات أعلى.

وتأتي الإشعارات كأداة لضبط إيقاع الانتباه على مدار اليوم؛ فهي لا تكتفي بإبلاغ المستخدم بالمستجدات، بل تُصمَّم لتقاطع الحياة اليومية وتعيد جذبه إلى الدورة ذاتها. ويتضاعف هذا الأثر مع خصائص التمرير اللانهائي وتشغيل الفيديو تلقائيًا وسلاسل المقاطع المتتابعة، إذ تُلغى لحظة التوقف الطبيعية التي تسمح بالاختيار الواعي، وتتحول التجربة إلى تدفق مستمر يستهلك الوقت ويزيد التعرض المتكرر لمحتوى غير مناسب، أو لعلاقات تواصل غير آمنة، أو لصراعات تفاعلية بين الأقران.

وفي الألعاب المتصلة بالإنترنت يتخذ محرك الضرر صورة أكثر صراحة، لأن الربح غالبًا ما يعتمد على المشتريات داخل اللعبة وليس

على الإعلانات وحدها. إذ تُصمَّم مسارات التقدم بما يُغري بالدفع لتسريع الإنجاز، أو لتجاوز عوائق مصطنعة، أو للحصول على عناصر تجميلية تُستخدم للتمايز الاجتماعي بين اللاعبين.

كما تفرض بيئات المحتوى الذي يصنعه المستخدمون داخل اللعبة واقعًا إضافيًا، لأن الطفل لا يتلقى تجربة جاهزة فحسب، بل ينخرط في مجتمعات تُنتج محتوى وتبادلًا وتنافسًا، ومعها تتسع مساحة الدردشة النصية أو الصوتية وما يرتبط بها من ضغط جماعي أو تحرش أو استدراج، إلى جانب صعوبة الإشراف الفعال على هذا الفضاء المتجدد.

وبناءً على ذلك، تبدو الحلول العمرية وحدها مقاربة سطحية عندما تُعرّف المشكلة باعتبارها مسألة من يدخل ومن لا يدخل، فيما تظل المحركات التي تُنتج الضرر قائمة على حالها.

وفعليًا، قد تمنع بوابة العمر بعض أشكال الوصول أو تدفع المستخدمين إلى التحايل، لكنها لا تغيّر منطق التوصية الذي يضخ المحتوى الحاد، ولا توقف آليات الإشعار التي تعيد تدوير الانتباه، ولا تُصلح تصميمات الألعاب التي تحوّل الضغط الاجتماعي والمنافسة إلى حوافز للإنفاق أو للبقاء لفترات أطول. وبالتالي فإن السياسة الفعالة في هذا الملف ينبغي أن تنطلق من إعادة توجيه الحوافز داخل المنصة واللعبة عبر قواعد سلامة حسب التصميم تحد من الخصائص التي تُنتج الأذى وتُعيد إنتاجه، بدل الاكتفاء بعتبة عمرية تُضاف فوق نظام قائم على تعظيم التفاعل والربح.

ثانيًا: الإطار الحقوقي (حقوق الطفل في البيئة الرقمية)

تتبنى هذه الدراسة إطارًا حقوقيًا باعتباره المرجعية الأكثر اتساقًا عند تناول وجود الأطفال والمراهقين في البيئة الرقمية، لأن الحقوق تُقدّم معايير محددة يمكن القياس عليها، وتُحوّل النقاش من أحكام عامة إلى التزامات واضحة وحدود دقيقة لأي تدخل تنظيمي أو تقني.

في هذا الإطار لا يُنظر إلى الطفل باعتباره متلقيًا للحماية فقط، بل باعتباره صاحب حقوق تُمارَس في الفضاء الرقمي كما تُمارَس خارجه، مع الاحتياج إلى ضمانات إضافية تتناسب مع السن، وتمنع الاستغلال، وتحد من الأثر السلبي للتصميمات الرقمية على السلامة والنمو.

ويعني اعتماد المرجعية الحقوقية أيضًا أن تقييم السياسات يمتد إلى آثارها الفعلية على الحقوق الأساسية وعلى الفئات الأكثر هشاشة. كما يفترض هذا الإطار أن مسؤولية الحماية ليست عبئًا يُلقى على الطفل وحده، بل هي واجب موزع بين الدولة بصفتها جهة تنظيم وحماية، وبين الشركات والمنصات بصفتها جهات تُنشئ بيئات رقمية وتحدد قواعدها وتتحكم في خصائصها، وبين المؤسسات التعليمية والاجتماعية بصفتها جهات دعم وتمكين.

1. الخصوصية وحماية البيانات

تتخذ الخصوصية في البيئة الرقمية شكلًا عمليًا يتجاوز السرية إلى التحكم في كيفية جمع البيانات ومعالجتها ومشاركتها، لأن تجربة الطفل اليومية عبر التطبيقات والمنصات تنتج بيانات دقيقة عن العادات والدوائر الاجتماعية والميول وأنماط الحركة والاستهلاك. وتزداد أهمية هذا الحق حين تكون الخدمات موجهة إلى القُصّر أو شائعة بينهم، لأن البيانات قد تُستخدم للتنبؤ بالسلوك أو توجيه التجربة أو التأثير على الاختيار بطريقة لا تتناسب مع سن المستخدم.

لذلك تبرز ضرورة ضمانات مثل تقليل البيانات إلى الحد الأدنى، وتقديم إعدادات افتراضية أكثر حماية، وإتاحة معلومات مبسطة ومناسبة للعمر حول ما يُجمع ولماذا، والتعامل مع أمن البيانات كجزء من الحماية وليس مسألة تقنية منفصلة.

2. حرية التعبير وتلقي المعلومات

يشمل هذا الحق قدرة الطفل والمراهق على الوصول إلى المعرفة والمحتوى الملائم للعمر، والتعبير عن الرأي وبناء العلاقات الاجتماعية والانخراط في اهتمامات ثقافية وتعليمية. في البيئة الرقمية تتأثر حرية التعبير بتصميم المنصات وبقرارات الإشراف على المحتوى وبطرق الإبلاغ والحجب داخل الخدمة، وهي قرارات قد تنتج عنها آثار واسعة غير مقصودة على الوصول إلى محتوى تعليمي أو صحي أو توعوي.

لذلك يفترض الإطار الحقوقي أن أي قيود أو سياسات إشراف يجب أن تكون محددة الهدف، واضحة المعايير، قابلة للتفسير والمراجعة، وأن تتضمن مسارات إنصاف تسمح بتصحيح الأخطاء، لأن الخطأ في إدارة المحتوى بالنسبة للأطفال لا يعني فقط حذف منشور، بل قد يعني حرمانًا من مورد معرفي أو مساحة تواصل.

3. الحماية من العنف والاستغلال

تتعلق الحماية هنا بمنع أشكال متعددة من الأذى التي تقع على الأطفال والمراهقين في السياقات الرقمية، بما في ذلك الاستدراج، والابتزاز، والتحرش، والاستغلال، والتنمر، وغيرها من أشكال العنف النفسي أو الاجتماعي التي قد تبدأ بتفاعل بسيط ثم تتسع آثارها بسرعة.

يترجم هذا الحق إلى واجبات عملية مثل توفير أدوات إبلاغ مفهومة وسهلة الاستخدام، واستجابة سريعة تراعي حساسية العمر، وحماية الضحايا من إعادة الإيذاء أثناء التعامل مع البلاغ، وإدارة فعالة للأدلة الرقمية توازن بين الحاجة إلى التحقيق حماية الطفل من التعرض لمزيد من الضرر.

كما يقتضي أن تتحمل المنصات جزءًا واضحًا من المسؤولية عبر تصميم يقلل فرص الاستهداف ويعزز السلامة افتراضيًا بدل أن يترك الطفل يتعامل مع المخاطر وحده.

4. عدم التمييز

يضمن هذا الحق أن السياسات الرقمية لا تُنتج، بحكم تصميمها أو تطبيقها، تمييزًا ضد فئات بعينها من الأطفال. في الواقع العملي قد يظهر التمييز عندما تُبنى التدابير على افتراضات لا تتوفر للجميع، أو عندما تُصمم الأدوات والواجهات دون مراعاة الفروق في الإتاحة أو مستوى المهارات الرقمية أو ظروف الاتصال.

كما يظهر التمييز عندما تتجاهل السياسات احتياجات الأطفال ذوي الإعاقة أو الفئات الأكثر هشاشة اجتماعيًا، أو عندما تؤدي الإجراءات إلى تفاوتات في الوصول إلى خدمات مفيدة. لذلك يقتضي هذا الحق إدماج اعتبارات العدالة الرقمية والإتاحة منذ البداية، وتقييم الأثر على الفئات المختلفة قبل اعتماد أي تدبير واسع.

5. الحق في التعلم والمشاركة

لا يقتصر هذا الحق على التعليم المدرسي، بل يمتد إلى فرص التعلم غير الرسمي، والوصول إلى مصادر المعرفة، والمشاركة في مساحات ثقافية واجتماعية ملائمة للعمر.

وفي البيئة الرقمية قد تتداخل المنصات والألعاب مع التعلم والمهارات وبناء الاهتمامات، وقد تتحول إلى مصادر دعم أو تبادل

خبرات أو مشاركة في مبادرات مجتمعية. لذلك يفترض الإطار الحقوقي أن السياسات يجب أن تحمي إمكانات التعلم والمشاركة بدل أن تُقيدها بصورة عامة، وأن تُعزز أدوات التمكين والمعرفة بالسلامة الرقمية، وأن تراعي أن المشاركة ليست ترفًا بل جزء من النمو الاجتماعي والثقافي للمراهقين.

6. القدرات المتطورة للمراهقين وحقهم في الاستقلال التدريجي

يشير هذا المبدأ إلى أن المراهقين ليسوا في موقع ثابت، بل تتطور قدراتهم على الفهم واتخاذ القرار والمسؤولية تدريجيًا. ويترتب على ذلك أن التدابير المتصلة بحمايتهم ينبغي أن تُصمم بصورة تراعي هذا التدرج، وأن تمنح مساحة متزايدة للاختيار مع تقدم العمر، مع توفير حماية مناسبة من الاستغلال والضغط.

كما يستدعي الاعتراف بحاجات المراهق إلى مساحة شخصية وخصوصية، وإلى الوصول إلى قنوات دعم آمنة عند الضرورة، دون أن تتحول الحماية إلى وصاية دائمة تُضعف الاستقلال أو تدفع إلى ممارسات التفاف غير آمنة. هذا التوازن هو جوهر المقاربة الحقوقية، لأنه يربط بين الأمان والنمو، ويمنع اختزال المراهقة في مجرد فئة تحتاج المنع.

ثالثًا: المبادئ الحاكمة للتنظيم

تعتمد هذه الدراسة على مجموعة مبادئ حاكمة تضبط تصميم أي سياسة عامة تستهدف حماية الأطفال والمراهقين في البيئة الرقمية، وتحدد حدود التدخل المقبول، وتمنع انزلاق التنظيم إلى إجراءات واسعة الأثر لا تخدم الهدف المعلن.

1. المصلحة الفضلى لا تعني المنع الشامل

يُفهم مبدأ المصلحة الفضلى باعتباره معيارًا لقياس أثر التدخل على رفاه الطفل وسلامته ونموه، لا باعتباره تفويضًا مفتوحًا لتقييد الاستخدام أو إغلاق مساحات رقمية كاملة. التنظيم الذي يستند إلى هذا المبدأ بصورة سليمة يركز على تقليل الأذى المحدد وإزالة مسبباته، مع الحفاظ على إمكانات التعلم والتواصل والمشاركة التي أصبحت جزءًا من التجربة اليومية للأطفال والمراهقين.

ويستلزم هذا المبدأ أن تكون التدابير متدرجة ومصممة بحسب طبيعة الخطر والسياق، وأن تُراجع على ضوء أثرها الواقعي بدل الاكتفاء بإعلان حسن النية.

2. اللجوء المبَّرر وحدود التدخل

يضع هذا المبدأ حدًا واضحًا للتدخل التنظيمي، بحيث يُقاس كل إجراء بقدرته على تحقيق هدف الحماية وبحجم أثره الجانبي على الحقوق. الضرورة تعني أن التدخل لا يُعتمد بوصفه خيارًا أول، بل بعد استنفاد البدائل الأقل تقييدًا والأكثر استهدافًا لمصدر الأذى. والتناسب يعني أن نطاق الإجراء وزمنه وشدته لا يتجاوزان ما يلزم لتحقيق الهدف، وأن آثاره على الخصوصية وحرية التعبير والوصول لا تتحول إلى تكلفة جماعية تفوق المنفعة المتوقعة. ويستلزم هذا المبدأ أيضًا وضوح المعايير، وإتاحة مسارات مراجعة وتظلم فعالة، بما يمنع تحول القيود إلى وضع دائم غير قابل للتصحيح.

3. تقليل البيانات

يشكل تقليل البيانات قاعدة تنظيمية أساسية لأن كثيرًا من التدابير المقترحة لحماية القُصّر قد تُبنى عمليًا على زيادة جمع البيانات أو توسيع تتبع المستخدمين. يقتضي هذا المبدأ حصر البيانات في الحد الأدنى الضروري لتحقيق غرض محدد ومعلن، ومنع التوسع في الغرض أو الاحتفاظ الممتد، واشتراط ضمانات أمنية قوية، وتفضيل الحلول التي تقلل التعرف على الهوية وتحد من قابلية الربط بين النشاط الرقمي والبيانات التعريفية. كما يرسخ هذا المبدأ فكرة أن السلامة لا تُبنى على زيادة المعرفة بالمستخدم بقدر ما تُبنى على تعديل خصائص الخدمة لتكون أقل ضررًا بصورة افتراضية.

4. واجب الدولة في التنظيم وواجب الشركات في احترام الحقوق

يفترض هذا المبدأ توزيعًا واضحًا للمسؤوليات. واجب الدولة يتمثل في وضع إطار تنظيمي يحمي الأطفال من الاستغلال والعنف، ويضمن قواعد شفافة ومعلنة، ويمنع التمييز، ويتيح الإنصاف، ويضمن أن تكون التدابير قابلة للمساءلة. وفي المقابل تلتزم الشركات والمنصات باحترام الحقوق بوصفه التزامًا أصيلًا لا يتوقف على وجود شكوى أو حادثة، ويشمل اتخاذ العناية الواجبة لتقييم المخاطر وتخفيفها، وتحسين التصميمات الافتراضية للسلامة، وتوفير آليات إبلاغ واستجابة ودعم، وإتاحة قدر من الشفافية يسمح بتقييم الأداء عوضاً عن ترك السلامة لتقديرات داخلية غير قابلة للفحص.

رابعًا: الواقع الرقمي للأطفال والمراهقين

1. أنماط الاستخدام في مصر

يتشكل واقع الأطفال والمراهقين رقميًا داخل مجتمع شديد القوة ديموجرافيًا، إذ تُشير تقديرات الأمم المتحدة عبر بيانات الجهاز المركزي للتعبئة العامة والإحصاء إلى أن نحو نصف السكان يقع ضمن الفئة العمرية 0–24 عامًا، وهو ما يعني أن أي سياسة تُصاغ للفضاء الرقمي تمس قطاعًا واسعًا من المجتمع لا فئة هامشية يمكن عزلها تنظيميًا.

وفي الوقت نفسه، توسّع الاتصال بالإنترنت والهواتف المحمولة خلال السنوات الأخيرة بصورة تجعل الهاتف الذكي هو بوابة الاستخدام الأكثر شيوعًا عمليًا، سواء للتواصل أو الترفيه أو التعلم غير الرسمي. فبيانات الحالة الرقمية في مصر تشير إلى 121 مليون خط هاتف محمول نشط بنهاية 2025، وإلى أن عدد مستخدمي الإنترنت بلغ 98.2 مليونًا في أكتوبر 2025 بنسبة نفاذ تقارب 82.7% من السكان.

في هذا السياق، يتداخل استخدام الأطفال والمراهقين بين منصات اجتماعية كبرى وخدمات فيديو قصيرة وطويلة، مع قنوات مراسلة تستخدم على نطاق واسع للتنسيق المدرسي والعائلي والاجتماعي. وتُظهر بيانات منصات الإعلان، رغم أنها لا تمثل كل المستخدمين بدقة ولا تفصل الأطفال عن البالغين فصلًا كافيًا، صورة تقريبية لحجم الحضور. فيسبوك يقدّر وصوله إلى 51.6 مليون مستخدم في مصر أواخر 2025، ويوتيوب إلى 49.3 مليونًا، وتيك توك إلى 48.8 مليونًا من المستخدمين البالغين (+18) مع تنبيه منهجي مهم يتعلق بأن بيانات الإعلانات لا تعرض تقديرات أقل من 18 عامًا، وإن كانت الإعلانات يمكن توجيهها لمن هم +13 في أدوات المنصة. وعلى نحو مشابه، يظهر إنستجرام عند 21.7 مليون مستخدم، وسناب شات عند 20.6 مليونًا أواخر 2025.

على مستوى الألعاب، يظل الهاتف المحمول هو المنصة الأكثر حضورًا في الاستخدام اليومي، مع انتشار ألعاب تنافسية متعددة اللاعبين وألعاب رياضية وألعاب تعتمد على الدردشة أو التفاعل الاجتماعي. وتوفر مؤشرات ترتيب التطبيقات في مصر صورة قريبة من المشهد: تظهر ألعاب مثل PUBG MOBILE في صدارة فئة "الأكشن" على أندرويد داخل مصر، وتظهر Free Fire ضمن الألعاب الأعلى انتشارًا/عائدًا في التصنيفات، كما تظهر ألعاب كرة القدم (مثل eFootball) في صدارة الألعاب الأعلى تحقيقًا للعائد على أندرويد في مصر خلال مطلع 2026.

دلالة هذه المؤشرات لا تتعلق بذائقة اللعب فقط، بل بطبيعة التجربة؛ إذ ترتبط كثير من الألعاب الأعلى ربحًا بنماذج مشتريات داخل اللعبة، وما يرافقها من إغراءات إنفاق أو منافسة اجتماعية أو ضغط جماعي داخل مجموعات اللعب.

2. مسارات الضرر الأكثر حضورًا محليًا

يظهر مسار الاستدراج والابتزاز في الوعي الاجتماعي المصري بوصفه أحد أكثر المخاطر إثارة للقلق، خصوصًا مع انتقال جزء كبير من تفاعلات المراهقين إلى الرسائل الخاصة ومجموعات اللعب والتطبيقات التي تسهّل بناء الثقة ثم قلبها إلى تهديد.

وعلى الرغم من محدودية البيانات العامة المنشورة التي تُمكّن من تقدير الحجم بدقة، فإن التصاعد العالمي لابتزاز الأطفال جنسيًا وماليًا عبر الإنترنت يقدّم سياقًا ضاغطًا لفهم الخطر، ويكشف عن نمط متكرر يقوم على الاستدراج ثم التهديد بالنشر أو الفضيحة، مع ازدياد حاد في بلاغات الابتزاز الجنسي المالي على مستوى شبكات الإبلاغ الدولية خلال 2022–2023. وفي السياق المصري، تتضاعف هشاشة الضحايا بسبب كلفة العار الاجتماعي، وضعف قنوات الدعم الموثوقة، وخوف كثير من الأسر من الإبلاغ، وهي عناصر تجعل الضرر ممتدًا حتى عندما لا يتحول إلى بلاغ رسمي.

أما التنمر الرقمي، فهو مسار تتقاطع فيه المدرسة والحي والمنصة في وقت واحد، بحيث لا يبقى الأذى محصورًا داخل الفصل، بل ينتقل إلى مجموعات المحادثة والصفحات والحسابات، ويتغذى على إعادة النشر والسخرية الجماعية. وتوجد دراسات حديثة ترصد انتشار الظاهرة بين طلاب المدارس الثانوية، وتربطها بزمن الاستخدام وبفجوات الوقاية داخل المدرسة، وتُظهر تأثير النوع الاجتماعي كعامل مؤثر في الخبرة. أهمية هذا المسار محليًا أنه غالبًا ما يظهر في صورة نزاعات صغيرة تتحول تدريجيًا إلى تشهير واسع، ثم تترسخ كوصم اجتماعي يصعب محوه، خصوصًا مع بقاء المحتوى متداولًا أو قابلًا للاستخراج بعد الحذف.

أما تسريب الصور والخصوصية، فهو نقطة التقاء بين العنف القائم على النوع الاجتماعي وبين أدوات المنصات التي تُسهّل النسخ والمشاركة والتخزين. في حالات كثيرة يتحول الهاتف نفسه إلى مساحة تهديد، ليس فقط بسبب اختراق تقني، بل بسبب علاقات قوة داخل الأسرة أو بين الأقران، أو بسبب استدراج ينتهي بطلب صور ثم استخدام الصور كسلاح اجتماعي. ويتقاطع هذا المسار مع التنمر والابتزاز في آن واحد، ويصبح شديد الخطورة على الفتيات بصورة خاصة تحت ضغط المعايير الاجتماعية الصارمة، وعلى الفتيان كذلك حين يرتبط الأمر بالابتزاز المالي.

وفي مسار الإعلانات والاستهداف التجاري، تتخذ المخاطر المحلية شكلين متداخلين. الشكل الأول هو التعرض المكثف لإعلانات وخدمات تُسعّر الانتباه وتستثمر في التتبع، في بيئة رقمية تتسع فيها الممارسات التسويقية غير المنضبطة وتضعف فيها قابلية المستخدم الصغير على تمييز الإعلان من المحتوى.

والشكل الثاني هو قابلية الاستغلال الاقتصادي داخل الألعاب عبر مشتريات داخل اللعبة، وهو ما تعكسه مؤشرات ترتيب

الألعاب الأعلى تحقيقًا للعائد في السوق المصري، حيث تتصدر ألعاب تعتمد على إنفاق متكرر أو حوافز تنافسية. في هذا المسار، لا يكون الضرر مجرد إسراف مالي، بل قد يتحول إلى نزاعات أسرية وعقاب، أو إلى دفع الطفل لإخفاء الإنفاق، أو إلى تعريضه لمحاولات احتيال داخل مجتمعات اللعب.

وتظهر المشكلات النفسية/التعليمية المرتبطة بالاستخدام الكثيف بوصفها مسارًا محليًا حاضرًا في الدراسات والتقارير الطبية والاجتماعية. توجد بحوث تقيس أنماط الاعتماد/الإدمان للإنترنت بين المراهقين، وترصد ارتباطه بمؤشرات نفسية وسلوكية، بما في ذلك القلق والضغوط وتراجع جوانب من الأداء اليومي. وعلى مستوى الفئة الأكبر سنًا بقليل، ظهرت دراسات عن الاعتماد على الهاتف الذكي بين طلاب الجامعات في مصر، بما يعكس امتداد الظاهرة عبر المراحل العمرية، ويقترح ضرورة التعامل معها كمسار صحة عامة وتربية رقمية لا كملف عقاب ومنع.

خامسًا: الإطار القانوني والمؤسسي في مصر: ما الموجود بالفعل؟ وأين الفجوات؟

1. قوانين ذات صلة من منظور وظيفي

يظهر التحدي الأساسي في السياق المصري في أن أدوات التنظيم المتاحة قانونًا ليست محايدة، لأن جزءًا معتبرًا منها صُمم أصلًا للتعامل مع المخاطر بوصفها جرائم أو تهديدات، لا بوصفها مسارات ضرر تحتاج إلى قواعد سلامة حسب التصميم وتدابير حماية دقيقة. لذلك يصبح من المهم قراءة القوانين القائمة بوصفها مسارات تدخل محتملة قد تُستخدم داخل ملف حماية الأطفال، سواء بطريقة متناسبة أو بطريقة توسّعية تُنتج آثارًا حقوقية جانبية واسعة.

في قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018، تبرز صلاحية حجب المواقع بوصفها أداة تنفيذية عالية الأثر، لأنها تُترجم سريعًا إلى تقييد على مستوى الشبكة، وقد تُستخدم لمعالجة مشكلات شديدة التباين بقرار واحد. ينص القانون على آلية للحجب عندما تُشكّل المواد أو المحتوى المنشور جريمة، مع تنظيم مسار إصدار القرار وما يتصل بتنفيذه وإخطار الجهات المعنية. كما ينص على مسار تظلّم، يتيح لذوي الشأن الاعتراض على قرار الحجب أمام القضاء خلال مدة محددة، وهو عنصر مهم نظريًا لضمان الرقابة القضائية، لكنه لا يكفي وحده إن غابت الشفافية حول معايير الحجب، أو غابت القدرة العملية للمستخدمين على الطعن الفعّال.

في قانون حماية البيانات الشخصية رقم 151 لسنة 2020، تظهر نقطة تماس مباشرة مع أي توجه إلى التحقق من السن، لأن هذه الأدوات لا تعمل دون معالجة بيانات شخصية على نطاق واسع، وقد تنزلق إلى جمع بيانات هوية أو بيانات حساسة بصورة تتجاوز غرض الحماية. القانون يضع متطلبات أكثر صرامة في التعامل مع بيانات الأطفال، ويربط معالجة بياناتهم بموافقة ولي الأمر أو الوصي وبقواعد خاصة تحكم هذا النوع من المعالجة. وتزداد أهمية هذا المسار مع صدور اللائحة التنفيذية (قرار رقم 816 لسنة 2025)، التي تؤكد ضرورة الحصول على موافقة مركز حماية البيانات على الآليات المستخدمة في جمع البيانات وآلية الحصول على موافقة الشخص المعني أو ولي أمره في حالة بيانات الأطفال بوصفها بيانات حساسة. المعنى الوظيفي هنا أن التحقق من السن ليس مجرد إجراء تقني، بل ممارسة تنظيمية ينبغي أن تُقاس بمعايير تقليل البيانات، وأمن المعالجة، وحدود الغرض، وآليات التحقق التي لا تُحوّل الحماية إلى بنية دائمة للتعريف الإجباري بالمستخدمين.

أما قانون الطفل رقم 12 لسنة 1996 وتعديلاته، فهو يوفر مرجعية حقوقية داخلية تُقيّد أي تنظيم جديد من زاوية حقوق الطفل. يتضمن القانون مبادئ ومقاصد تتصل مباشرة ببيئة الطفل الرقمية حتى إن لم يُسمّها نصًا، مثل حق الطفل في الحماية من جميع أشكال العنف والإساءة، وحقه في الحصول على المعلومات وتنمية قدراته، ومبدأ اعتبار مصلحة الطفل الفضلى أساسًا للتعامل معه. كما يتضمن حماية لخصوصية الطفل في سياقات متعددة، بما في ذلك الحظر على نشر أو إذاعة أو عرض ما يؤدي إلى التعرف على الطفل في حالات بعينها، وهو منطق يمكن البناء عليه عند التفكير في سياسات الإبلاغ والتشهير والتداول غير المشروع للصور داخل الفضاء الرقمي.

ويضاف إلى ذلك إطار قانون تنظيم الصحافة والإعلام رقم 180 لسنة 2018، الذي يمنح المجلس الأعلى لتنظيم الإعلام أدوات للتعامل مع محتوى وحسابات ومواقع، بما في ذلك صلاحيات قد تصل إلى الحجب أو المنع في حالات تُقدَّر باعتبارها مخالفة للمعايير القانونية أو المهنية. هذا المسار يهم ملف حماية الأطفال لأن التداخل بين سلامة الطفل وتنظيم المحتوى قد يدفع مؤسسات التنظيم الإعلامي إلى لعب دور مباشر في قرارات تتجاوز التوعية إلى تقييد الوصول أو تقييد الحسابات.

2. الجهات المتداخلة ومسألة الاختصاص

ينشط ملف حماية الأطفال في الفضاء الرقمي عمليًا داخل شبكة مؤسسات، مثل البرلمان الذي يضع الإطار التشريعي، بينما تتحرك الحكومة عبر لجان وسياسات تنفيذية وتوجيهات وزارية. والجهاز القومي لتنظيم الاتصالات يملك موقعًا حاسمًا في أي قرار يتطلب تنفيذًا على مستوى الشبكات أو التزامات على مقدمي الخدمات، بحكم اختصاصه التنظيمي. وفي ملفٍ يتصل بالأطفال، يظهر كذلك المجلس القومي للطفولة والأمومة والجهات التنفيذية المعنية بالحماية الاجتماعية والتعليم والصحة والشباب، إلى جانب جهات إنفاذ القانون والنيابة العامة عند تحويل بعض مسارات الضرر إلى مسارات تجريم.

الخطر العملي يأتي من غموض من يقود تنفيذ السياسات ومن يراجع ويقيّم الأثر التشريعي، لأن هذا الغموض يفتح الباب أمام تضارب اختصاصات أو تبادل أدوار يسهّل اتخاذ قرارات عالية الأثر دون ضمانات كافية. في ملف معقّد مثل حماية الأطفال في الفضاء الرقمي، فإن غياب جهة رقابية مستقلة فعّالة ومعايير علنية لتقييم المخاطر ولقياس الضرورة والتناسب يصبح عاملًا يرفع احتمالات الانزلاق من تدخلات دقيقة إلى تدخلات عامة سهلة التنفيذ.

3. فجوات حاسمة وما يمكن إصلاحه دون قانون جديد

تظهر الفجوة الأولى في غياب سياسة عامة واضحة ومعلنة لحماية بيانات الأطفال بوصفها ملفًا قائمًا بذاته، رغم وجود قانون حماية البيانات واللائحة التنفيذية. القواعد موجودة، لكن تحويلها إلى ممارسات قابلة للقياس يحتاج إرشادات تفصيلية حول أدوات التحقق من السن، ومعايير تقليل البيانات، وحدود الاحتفاظ، وضمانات عدم إعادة استخدام البيانات لأغراض أخرى.

وتظهر الفجوة الثانية في ضعف مسارات التظلم والطعن الفعّال عند تقييد خدمة أو محتوى أو حساب أو عند خطأ في تقدير السن، لأن أثر الخطأ يقع مباشرة على حق الطفل في الوصول والتعلم والمشاركة، وعلى حق الأسرة في إدارة الاستخدام دون أن تُصبح مجبرة على حلول قسرية. وجود نص قانوني او نص لائحي يتيح التظلم في بعض الحالات، مثل تظلمات قرارات الحجب، يظل غير كافٍ إن لم تُبنَ إجراءات سهلة وواضحة للمستخدمين، وإن لم تتوفر شفافية عن أسباب القرار وكيفية مراجعته، ويظهر ذلك على سبيل المثال في آليات الحجب الواردة بقانون تنظيم الصحافة والإعلام والتي يغلب عليها الطابع الإداري في اتخاذ قرار الحجب

دون عرض على جهات قضائية للبحث في مشروعية القرار، وبدون النص صراحة على طريقة التظلم من قرار الحجب ومواعيد الرد على التظلم.

وتظهر الفجوة الثالثة في قابلية التوسع الوظيفي داخل بنية تنظيمية متداخلة. إذ أن أي أداة تُطرح لحماية الطفل يمكن أن تتحول مع الوقت إلى معيار عام لتنظيم الهوية أو تقييد المحتوى أو إعادة ترتيب الوصول، خصوصًا عندما تتقاطع أدوات الحجب في قانون الجرائم التقنية مع سلطات تنظيم الاتصالات والتنظيم الإعلامي.

سادسًا: الاتجاهات السياسية المطروحة في مصر (السيناريوهات المحتملة)

1. نموذج الحظر أو المنع حسب السن

يُشير هذا النموذج على وضع قاعدة عامة تمنع استخدام الهاتف الذكي أو إنشاء حسابات/استخدام منصات بعينها لفئات عمرية محددة. يطرح هذا الاتجاه عادة بوصفه حلًا مباشرًا وسهل وقد ظهر في النقاشات المرتبطة بتوجه تشريعي لضبط استخدام الأطفال للهواتف والمنصات في مصر.

يأخذ هذا النموذج في التطبيق صورًا متعددة مثل منع مطلق لفئة عمرية، أو منع لاستخدامات محددة داخل منصات بعينها، أو منع داخل سياقات معينة. اختلاف الصيغة هنا ليس تفصيلًا، لأن نطاق المنع هو الذي يحدد طبيعة الأثر وإمكانات الإنفاذ.

2. نموذج التحقق أو تأكيد السن الإلزامي

يرتكز هذا النموذج على اشتراط إجراء تحقق من السن قبل الوصول إلى المنصة أو إلى ميزات معينة داخلها، بما يحول العمر من معيار تنظيمي عام إلى شرط تقني دائم. يظهر هذا النموذج عادة كحل وسط بين المنع الكامل وبين ترك الاستخدام دون ضوابط، ويُطرح ضمن حزم تنظيمية تشمل تصنيفًا عمريًا وآليات تحقق وإجراءات تشغيلية أخرى.

و في الممارسة يتدرج هذا الخيار بين تحقق محدود الدقة، وتحقق قوي يتطلب بيانات تعريفية أو وسيطًا موثوقًا، وهو ما يجعله مرتبطًا بنطاق معالجة البيانات والجهات التي ستحتفظ بها، وباحتمالات الخطأ والإقصاء.

3. نموذج حجب منصات أو ألعاب بعينها

يمثل هذا النموذج تدخلًا سريعًا يعتمد على تقييد الوصول إلى خدمة محددة على مستوى الشبكة أو مزودي الخدمة أو قنوات التوزيع. ووجوده في المشهد المصري منتشر، وقد ظهر في قرار حجب لعبة روبلوكس بالتنسيق بين المجلس الأعلى لتنظيم الإعلام والجهاز القومي لتنظيم الاتصالات.

يميل هذا النموذج إلى التعامل مع الخدمة باعتبارها مصدر الخطر، وهو ما يجعله مختلفًا عن التدخلات التي تستهدف خصائص بعينها داخل المنصات أو أنماط تشغيل محددة.

4. نموذج القيود المدرسية على الهاتف

يقوم هذا النموذج على ضبط استخدام الهاتف داخل المدرسة من خلال قواعد انضباط وتدابير تنفيذية وإدارية. هذا الاتجاه حاضر بالفعل في قرارات وتعليمات سابقة لوزارة التربية والتعليم تتعلق بحظر استخدام الهاتف أثناء اليوم الدراسي، كما عاد للظهور في النقاشات السياسية باعتباره محورًا من محاور المعالجة.

يتميز هذا النموذج بأنه يعمل داخل نطاق مؤسسي محدد، ويُفترض أن يوازن بين اعتبارات الانضباط المدرسي ومتطلبات التعلم والسلامة، دون أن يتحول تلقائيًا إلى تنظيم عام للحياة الرقمية خارج المدرسة.

5. نموذج تحميل المنصات مسؤوليات مباشرة

يتمحور هذا النموذج على نقل مركز الثقل من المستخدم إلى مقدم الخدمة عبر التزامات تشغيلية وقانونية. تتضمن هذه الالتزامات، في النقاشات الدائرة، عناصر مثل وجود ممثل قانوني محلي للمنصات، وإجراءات أمان افتراضي، وترتيبات إبلاغ وتعاون، وإطار تنظيمي يُلزم المنصات بتدابير وقائية.

يختلف هذا النموذج جوهريًا عن النماذج السابقة لأنه يعالج بيئة الخدمة وخصائصها بدل الاكتفاء بضبط الدخول، ويخلق مساحة لربط التنظيم بمعايير تصميم وتشغيل قابلة للقياس.

6. نموذج النهج المختلط

يظهر هذا النموذج بوصفه السيناريو الأكثر احتمالًا في الواقع، عبر مزج أدوات متعددة مثل قدر من القيود المدرسية، مع التزامات على المنصات، مع عناصر تحقق عمري أو تصنيف، ومع قابلية اللجوء إلى الحجب كإجراء سريع في حالات بعينها. هذا المزج قد ينتج حزمة عنيفة من القرارات أو مزيجًا متعارضًا يضاعف الأثر السلبي، بحسب ترتيب الأدوات وحدود كل أداة وضمانات تطبيقها.

سابعًا: مخاطر الحظر والتحقق من السن في السياق المصري

يبدو الحظر والتحقق الإلزامي من السن، في الظاهر، كحلول مباشرة لمشكلة مركبة. غير أن كلفتهما في السياق المصري لا تتعلق فقط بإمكان نجاحهما أو فشلهما، بل بطبيعة البنية التي يفرضانها على المجال الرقمي. إذ ستُحوّل -هذه البنية- الهوية إلى شرط للدخول، وتوسع نطاق جمع البيانات، وتفتح أسواقًا جديدة لوسطاء التحقق، ثم تترك آثارًا تراكمية على الخصوصية وحرية التعبير والمساواة وإمكان الحصول على الدعم.

الخطر المركزي هنا أن التدخل لا يشتبك مع مصادر الضرر داخل تصميم المنصات والألعاب بقدر ما يعيد ترتيب بوابات الوصول نفسها، وهو ما يجعل الأثر الحقوقي واسعًا حتى لو كانت النية المعلنة هي حماية الأطفال.

أوسع هذه المخاطر يتصل بالخصوصية وحماية البيانات، لأن التحقق من السن لا يتحقق عمليًا دون درجة ما من جمع البيانات. ومع أي تعريف غامض لما يُعد تحققًا موثوقًا، تميل السياسات إلى الانزلاق نحو طلب وثائق تعريف، أو صور شخصية، أو بيانات اتصال يمكن ربطها بالهوية، وقد يصل الأمر إلى حلول بيومترية بحجة الدقة.

وينقلنا ذلك إلى إشكالية تطبيع القاعدة الجديدة التي تُشير إلى أن الدخول إلى فضاء رقمي يصبح مشروطًا بإثبات هوية أو شبه هوية، ثم تتسع القاعدة تدريجيًا من الأطفال إلى نطاقات أخرى بحكم سهولة الإنفاذ أو رغبة الشركات في اعتماد معيار واحد.

وفي مصر -حيث تتقاطع الأدوات التنظيمية مع ممارسات التقييد السريع- قد يصبح هذا التطبيع مدخلًا واقعيًا لتحول الحماية إلى شرط عام لإدارة الوصول، بما يرفع الكلفة الحقوقية للمشاركة الرقمية على المجتمع كله.

وفي اللحظة التي تصبح فيها بيانات التحقق موجودة، تظهر مشكلة الربط بين الهوية والنشاط حتى لو لم يُعلن ذلك صراحة، لأن الربط يمكن أن يتم عبر معرفات تقنية ثابتة، أو سجلات دخول، أو رموز تحقق قابلة لإعادة الاستخدام، أو مجرد إمكان تجميع البيانات من نقاط مختلفة.

هذا الربط -ولو كان غير مباشر- يكفي لإنتاج أثر شديد الخطورة، والطفل أو المراهق يفقد القدرة على التعلم والبحث وطلب المساعدة في مساحة تحميه من الوصم، ويُعاد تعريف حضوره الرقمي بوصفه أثرًا يمكن تتبعه والرجوع إليه.

تتعقد هذه الصورة أكثر عند دخول وسطاء تحقق السن إلى المشهد. حين تتحول عملية التحقق إلى خدمة تقدمها شركات وسيطة، ينشأ سوق جديد يقوم على جمع بيانات ضخمة لفئات عمرية صغيرة، ثم تقديم هذه الخدمة لمنصات متعددة. وفي سوق كهذا تصبح البيانات موردًا اقتصاديًا بحد ذاته، وتزداد احتمالات الاحتفاظ، أو إعادة الاستخدام.

الأخطر على المراهقين تحديدًا أن هذا كله، قد يضغط على المساحات مجهولة الهوية التي يعتمدون عليها في لحظات هشّة مثل طلب دعم نفسي، أو استشارة حول عنف داخل الأسرة، أو تجنب وصم اجتماعي. وبالتالي فحين يصبح الدخول مشروطًا بآليات يتحكم فيها بالغون أو تُسجل أثرًا تعريفيًا، يتراجع الطلب على الدعم، ويُترك الأكثر هشاشة دون ملاذ آمن.

ومن الخصوصية ينتقل الخطر مباشرة إلى الأمن السيبراني وسرقة الهوية. فالتحقق الإلزامي يوسع سطح الهجوم عبر قواعد بيانات وتكاملات وواجهات وسجلات جديدة، بما يرفع احتمال الاختراق والتسريب وإساءة الوصول الداخلي. وهو ما قد يتحول إلى ابتزاز ووصم واستغلال طويل الأمد، خاصة إذا تعلق بصور أو وثائق أو معلومات تربط قاصرًا بحساب أو شبكة علاقات. ويزداد هذا الخطر مع انتشار تطبيقات رقابة أبوية أو أدوات وسيطة ضعيفة الأمان تحت ضغط الحماية، لأنها غالبًا تطلب صلاحيات واسعة وتجمع أكثر مما يلزم، فتغدو بابًا للاختراق أو أداة تسريب داخل المنزل.

تظهر كذلك آثار مباشرة على حرية التعبير والوصول إلى المعلومات، لأن وجود بوابة تحقق أو شعور بقرب الهوية من النشاط ينتج تأثيرًا يقلل من استعداد المراهق للبحث والتعلم والتجريب المشروع، ويمتد حتى إلى موضوعات تعليمية وصحية ونفسية بسبب الحساسية الاجتماعية. ويضاف إلى ذلك خطر الحجب الزائد والتقييد المفرط، إذ تميل المنصات تحت ضغط الامتثال إلى توسيع المنع لتقليل المسؤولية، فتقيد محتوىً توعويًا أو صحيًا تحت عنوان حماية القُصّر دون تمييز بين ما يضر وما يحمي من الضرر.

وتظل مشكلة عدم الفعالية وسهولة التحايل حاضرة كذلك، لأن الحظر والتحقق يمكن الالتفاف عليهما عبر أدوات شائعة أو حسابات بالغين أو منصات بديلة. وقد تكون النتيجة عكسية حين ينتقل الأطفال إلى مساحات أقل أمانًا وأضعف إشرافًا أو يستخدمون حسابات بالغين تفقدهم أي حماية عمرية داخل المنصات.

وتبلغ المخاطر ذروتها على مستوى الحوكمة، إذ يصبح عنوان حماية الطفل بوابة سهلة لتوسيع الحجب والمنع أو تمديدهما دون مراجعة حقيقية، خاصة مع ضعف مسارات الطعن وتداخل الاختصاصات وغموض المسؤوليات. وعندما يميل الإنفاذ إلى طابع عقابي

يطال المستخدمين والأسر والمدارس بدل إلزام الشركات بتعديل التصميم والتشغيل، تتحول السياسة من حماية إلى إدارة للمخالفة وتضعف فرص تقليل الضرر الحقيقي.

وعلى ذلك ينبغي أن تُصاغ خطوط حمراء لكيفية التعامل مع مسألة حماية الأطفال والمراهقين في الفضاء الرقمي مع الحفاظ الحقوق والحريات الأساسية، والتي يمكن أن تشمل التالي:

- أولًا، رفض أي آلية تحقق من السن تُلزم بتقديم وثائق هوية أو صور وجه أو أي بيانات بيومترية كمدخل عام للخدمة.
- ثانيًا، رفض أي نظام يسمح بالاحتفاظ ببيانات التحقق بعد إتمام الغرض أو يسمح بإعادة استخدامها لأي غرض آخر.
- ثالثًا، رفض أي تصميم تقني يجعل ربط الهوية بالنشاط ممكنًا عبر مُعرّفات ثابتة أو سجلات قابلة للتجميع.
- رابعًا، رفض أي توسع في الحجب أو المنع خارج معايير معلنة ومحددة، دون حق طعن سريع وشفاف ودون مراجعة زمنية تسقط الإجراء تلقائيًا إن لم يثبت أثره.
- خامسًا، رفض أي حزمة تنقل العبء إلى المستخدمين والأسر والمدارس وتترك المنصات دون التزامات قابلة للقياس في السلامة حسب التصميم.
- سادسًا، رفض أي تدابير تُنتج إقصاءً اجتماعيًا أو طبقيًا أو جغرافيًا عبر جعل الحماية مشروطة بأدوات لا يملكها الجميع.

ثامنًا: بدائل حقوقية: من الحظر إلى مساءلة المنصات عبر السلامة حسب التصميم

تقوم البدائل الحقوقية على تحويل مركز الثقل من فكرة منع الدخول إلى فكرة تقليل الضرر داخل الخدمة نفسها، بحيث تُلزم المنصات والألعاب بتدابير أمان افتراضية قابلة للقياس والمراجعة، من دون إنشاء بنية تعريف إجباري أو توسيع جمع البيانات.

جوهر هذا الاتجاه هو أن الطفل لا يواجه المخاطر بسبب وجوده في الفضاء الرقمي بشكل مجرد، بل لأن بيئات رقمية واسعة الانتشار تُدار وفق حوافز تدفع نحو التفاعل المكثف، وتُبقي أبواب التواصل مفتوحة على نحو يسهل إساءة الاستخدام، وتسمح بتدفقات محتوى لا تُراعي الفروق العمرية، وتدمج الاستغلال التجاري داخل التجربة اليومية.

لذلك ينبغي أن تُصمّم البدائل الحقوقية بوصفها حزمة تدخلات دقيقة تستهدف مواضع الضرر، وتحتفظ في الوقت نفسه بضمانات الخصوصية وحرية التعبير وعدم التمييز.

1. التزامات على المنصات بوصفها جوهر البدائل

المدخل الأكثر فاعلية يتمثل في إعادة ضبط الإعدادات الافتراضية لحسابات القُصّر بحيث تكون أكثر أمانًا منذ البداية. وهذا يُقلّل -افتراضيًا وتلقائيًا- قابلية الوصول غير المرغوب، ويحد من انتقال المحتوى الشخصي إلى نطاق عام يصعب التحكم فيه، كما يخفض احتمالات الاستدراج التي تعتمد على البحث عن حسابات مفتوحة. ويتعزز هذا الاتجاه عندما تُعتمد قيود افتراضية على الرسائل الواردة من الغرباء، لأن قدرًا كبيرًا من الأذى يبدأ من قناة تواصل تُفتح بلا عوائق.

وينبغي أن يكون الهدف هنا ليس إغلاق التواصل الاجتماعي، بل إعادة تصميمه وفق قواعد أكثر أمانًا عبر تقليل الرسائل القادمة من خارج الدوائر المعروفة، وتوفير تحكم واضح وسهل في قبول الطلبات، وإدراج تحذيرات مبسطة عند أنماط تواصل عالية الخطورة، مع توجيه المستخدم فورًا إلى خيارات حماية داخل الواجهة نفسها.

وعلى مستوى المحتوى، تزداد الحاجة إلى ضبط التوصيات الخوارزمية للقُصّر من خلال وضع آمن افتراضي لا يُترك لاجتهاد الأسرة أو لوعي الطفل. وينبغي أن يتخذ هذا الضبط شكلًا عمليًا عبر تقليل الدفع نحو المحتوى الحاد أو المثير للصدمة، وخفض مسارات التتابع التي تزيد التعرض المتكرر، والحد من الإشعارات التي تعيد المستخدم إلى التطبيق بصورة متكررة بلا ضرورة.

ويكتمل ذلك بإتاحة أدوات واضحة لإدارة ما يظهر في الصفحة الرئيسية، وتمكين المستخدم من إيقاف توصيات موضوعية بعينها، مع إعطاء وزن أكبر لمحتوى تعليمي وترفيهي أقل قابلية للإيذاء، بما يحافظ على حق الطفل في الوصول والتعلم دون استبداله بمنع عام.

وفي ما يتعلق بالاستغلال الاقتصادي، يشكل تقييد الإعلانات الموجهة للقُصّر وحظر التتبع السلوكي حجر زاوية لأي بديل يحقق الحماية دون مراقبة. القاعدة التي يجب تثبيتها هي أن القُصّر لا يُعاملون كأهداف تسويقية تُبنى عنها ملفات تعريفية.

وبناءً على ذلك تُلزم المنصات بتحويل الإعلانات، إن وُجدت، إلى إعلانات سياقية غير قائمة على التتبع، مع وضوح بصري أكبر يميز الإعلان عن المحتوى، ومع منع أي تصميم يدفع الطفل نحو التفاعل التجاري عبر الإغراءات السريعة أو الرسائل المموهة أو الاستهداف الدقيق.

وتظل أدوات الإبلاغ والاستجابة والدعم عنصرًا حاسمًا يميز بين سياسة شكلية وسياسة تقلل الضرر فعليًا. تقتضي البدائل الحقوقية آليات إبلاغ مناسبة للعمر وسهلة الوصول ومتعددة المسارات، وتوفر حماية فورية مثل كتم الحساب المسيء ومنع تواصله وإخفاء المحتوى. وينبغي أيضًا توفير دعمًا للضحايا يراعي حساسية السن وإجراءات تقلل إعادة الإيذاء، مع قدرة على منع العودة عبر حسابات بديلة عند تكرار الإساءة.

كما تكتسب تقارير الشفافية الدورية أهمية خاصة لأنها تسمح بتقييم الأداء على أساس وقائع قابلة للفحص بدل الاكتفاء بوعود عامة.

وفي الألعاب المتصلة بالإنترنت، تحتاج البدائل إلى قواعد تشغيلية واضحة داخل اللعبة نفسها، لأن مسارات الضرر لا تقع على منصة خارجية فقط. يشمل ذلك ضبط الدردشة النصية والصوتية للقُصّر، وتوفير إعدادات افتراضية تقلل التعرض للتواصل غير المرغوب، وإدارة المجتمعات داخل اللعبة بطريقة تحد من الاستدراج والتحرش.

كما يتطلب المحتوى الذي يصنعه المستخدمون داخل اللعبة إشرافًا أكثر صرامة على المساحات التي يُنشأ فيها هذا المحتوى، مع أدوات إزالة سريعة، ومعايير واضحة، ومسارات اعتراض عادلة تمنع الإفراط في الحذف.

وعلى مستوى المشتريات داخل اللعبة، تبرز ضرورة ضبط التصميم التجاري عبر شفافية أعلى للأسعار، وحدود إنفاق افتراضية مناسبة للعمر، وتقييد الآليات التي تدفع إلى إنفاق متكرر قائم على الاحتمال، حتى لا تتحول المنافسة داخل اللعب إلى ضغط مالي مستمر على الأطفال والأسر.

2. الوقاية والتمكين

لا تُعوض التزامات المنصات وحدها دور المدرسة والأسرة، لأن جزءًا من الحماية يتعلق بالمهارات والقدرة على اتخاذ قرارات أكثر أمانًا. لذلك تُعد مناهج الثقافة الرقمية مدخلًا وقائيًا واقعيًا حين تُصمم بصورة عملية ومناسبة للعمر، وتغطي الخصوصية في الحياة اليومية، ومواجهة التنمر، وفهم أساليب الاستدراج والابتزاز، والتمييز بين المحتوى والإعلان، والتعامل مع التضليل والمعلومات

الزائفة، والحدود الآمنة للتواصل. أي إدماج/رفع مهارات الأطفال بحيث تكون قابلة للتطبيق داخل أنشطة مدرسية وتدريبات محاكاة وحالات واقعية، ليتحول الوعي إلى سلوك.

وفي المدرسة، تُنتج سياسات استخدام الهاتف أثرًا أفضل عندما تكون مرنة ومتصلة بالتعلم والانضباط معًا، بدل أن تتحول إلى حظر أعمى. التنظيم المرن يعني قواعد واضحة لاستخدام الهاتف داخل الحصص وخارجها، مع استثناءات تعليمية محددة، وتدابير تقلل الإلهاء دون مصادرة شاملة، وآلية إنصاف بسيطة عند النزاعات. هذا النهج يمنع تحول إدارة الهاتف إلى ساحة عقاب جماعي، ويجعل المدرسة مساحة لبناء مهارة الانتباه المنظم، وليست مجرد مساحة للمنع.

ويتكامل ذلك مع خطوط مساعدة وإرشاد ودعم نفسي رقمي آمن، لأن كثيرًا من الأذى لا يُعالج عبر الإعدادات فقط، بل عبر وجود مسار سريع وموثوق لطلب المساعدة. هذه الخطوط تحتاج تصميمًا يحمي السرية، ويتيح طلب الدعم دون مخاطر كشف الهوية أو التعرض للوصم، ويربط بين الدعم النفسي والاجتماعي وبين الإحالة إلى جهات حماية عند الضرورة، مع تدريب متخصص للتعامل مع الأطفال والمراهقين.

3. إنفاذ موجّه ضد الجرائم الحقيقية

تُحافظ البدائل الحقوقية على دور إنفاذ القانون، لكنها تعيد توجيهه نحو الجرائم الفعلية ذات الضرر المباشر، بدل توسيع العقاب على المستخدمين أو بناء جمع جماعي للبيانات.

الإنفاذ الموجّه يبدأ بوحدات بلاغات مدربة تستقبل شكاوى الاستدراج والابتزاز وتسريب الصور والتنمر الشديد، وتتعامل معها بمنطق حماية الضحية وتقليل إعادة الإيذاء، مع حساسية خاصة تجاه العمر والجندر وكلفة الوصم الاجتماعي.

ويتطلب ذلك بروتوكولات تعاون منضبطة مع المنصات تقوم على طلبات محددة ومبررة ومقيدة النطاق، تركز على حفظ الأدلة في واقعة بعينها، وليس على إنشاء قنوات دائمة لتجميع البيانات أو الوصول الواسع إلى نشاط المستخدمين.

تاسعًا: إذا فُرض «تأكيد عمر»: شروط حاكمة وضمانات فنية وقانونية

نتعامل هذه الدراسة مع احتمال فرض تأكيد العمر بوصفه واقعًا سياسيًا قد يُدفع إليه سريعًا،وليس بوصفه خيارًا مثاليًا. لذلك يقدّم هذا القسم مواصفة سياسة/حقوقية تضع حدًا أعلى لما يمكن السماح به، وحدًا أدنى لما يجب فرضه من ضمانات، بحيث لا يتحول التنظيم إلى كارثة حقوقية ثم يُطلب من المجتمع التعايش معها.

1. الخطوط الحمراء الحاكمة

- رفض استخدام البيانات البيومترية:: بوصفها الحل الافتراضي أو معيار الامتثال، لأن البيومتريات ترفع حساسية البيانات، وتزيد مخاطر الاختراق، وتخلق قابلية ربط طويلة الأمد لا يمكن سحبها من الحياة الرقمية بعد وقوع الضرر. وأي نظام يسمح بصورة الوجه أو بصمة الصوت أو أي خصائص حيوية كمدخل عام للتأكد من السن يضع المجتمع على مسار يصعب الرجوع عنه، ويحوّل حماية الأطفال إلى مشروع تعريف تقني دائم.

- عدم الاحتفاظ بالبيانات: وظيفة التأكيد، إن فُرضت، يجب أن تكون لحظية ومحدودة للغاية، لا تنتج قواعد بيانات للقُصّر ولا سجلات تحقق قابلة للرجوع إليها. الاحتفاظ، حتى وإن كان تحت عنوان مكافحة التحايل أو المتابعة، يفتح الباب للتوسع الوظيفي، ويحوّل المؤقت إلى دائم، ويجعل التسريب أو إساءة الوصول احتمالًا عالي الكلفة. لذلك يجب أن يُحظر الاحتفاظ بنسخ من وثائق أو صور أو نتائج تحقق قابلة لإعادة الاستخدام، وأن تُفرض آليات إتلاف قابلة للتدقيق.
- عدم الربط: المقصود هنا منع أي تصميم يسمح بربط نتيجة التحقق بسجل النشاط داخل المنصة، سواء عبر معرفات ثابتة أو رموز تحقق قابلة لإعادة الاستخدام أو سجلات فنية يمكن تجميعها. حتى إن لم تُشارك البيانات مع جهة خارجية، فإن الربط الداخلي يكفي لإنتاج أثر مراقبة صامتة وتغيير سلوك المستخدمين، ويحوّل الوصول إلى مساحة رقمية إلى أثر قابل للتتبع.
- عدم المشاركة لأغراض أخرى: يجب أن يُقيد الغرض قانونيًا وتقنيًا بحيث لا تُستخدم البيانات أو "إشارات" التحقق في الإعلانات، أو الاستهداف التجاري، أو التوصية، أو تصنيف المستخدمين، أو أي تعاون موسع لا علاقة له بالتحقق من السن في نطاق محدد. هذا القيد ينبغي أن يكون قابلاً للإنفاذ بعقوبات رادعة، وأن يشمل مزود التحقق والمنصة معًا.
- عدم الإقصاء: لا يجوز أن يتحول تأكيد العمر إلى شرط يَحرم من لا يملك وثائق أو أجهزة حديثة أو اتصالًا مستقرًا، ولا يجوز أن يُبنى التنظيم على افتراضات طبقية. أي نظام لا يتضمن بدائل وصول عادلة سيعيد إنتاج الفجوة الرقمية ويضاعفها، خصوصًا في الخدمات التي تمس التعلم والتواصل والدعم. لذلك يجب أن تُحظر الصيغ التي تجعل "الوثيقة" هي الطريق الوحيد، وأن تُفرض بدائل منخفضة المتطلبات ومناسبة للبيئات الأقل مواردًا.

2. الضمانات الإلزامية التي لا غنى عنها

إذا فُرضت الأداة رغم المخاطر، فلا بد أن تُحاصر بضمانات إلزامية تُصاغ كالتزامات قانونية قابلة للمساءلة. والضمانة الأولى هي تقليل البيانات وفصل الأدوار. تقليل البيانات يعني أن ما يُجمع هو أقل ما يمكن لتحقيق وظيفة محددة، وأن التصميم يُفضل طرقًا لا تنتج بيانات تعريفية أصلًا. وفصل الأدوار يعني أن الجهة التي تقدم تدقيق في السن لا تملك معرفة النشاط داخل المنصة، وأن المنصة لا تحصل إلا على نتيجة محدودة لا تصلح للربط أو لإعادة الاستخدام. ويجب أن يُترجم ذلك إلى متطلبات تقنية واضحة، مع تدقيقات أمنية دورية من جهات مستقلة، واختبارات اختراق، وإخطار إلزامي بحوادث أمن المعلومات، وعقوبات على الإهمال.

الضمانة الثانية هي الشفافية بشأن مزود التحقق وبشأن آلية العمل. فلا يجوز أن يُدار التأكيد عبر وسيط مجهول أو عبر تعاقدات غير معلنة، لأن عدم الشفافية يمنع الرقابة العامة ويجعل المجتمع غير قادر على تقييم المخاطر. الشفافية المطلوبة تشمل اسم مزود التحقق، ونطاق البيانات التي يعالجها، ومكان استضافتها، ومدة الاحتفاظ إن وجدت، والتدابير الأمنية، ونتائج التدقيقات، وسياسات الإتلاف، وعدد الطلبات المنفذة بصورة دورية في تقارير شفافية.

والضمانة الثالثة هي آليات طعن وتظلم فعالة وسريعة. الخطأ في تقدير العمر أو في تنفيذ القيود يجب ألا يتحول إلى حرمان دائم. ينبغي أن يُلزم النظام بمسار اعتراض مبسط ومناسب للأسر وللمراهقين، بزمن استجابة محدد، وبمراجعة بشرية عند النزاعات، وبحق الوصول المؤقت إلى خدمات أساسية عند استمرار النزاع، حتى لا تصبح الأخطاء التقنية عقابًا غير متناسب.

أما الضمانة الرابعة هي تقييم الأثر قبل الإطلاق وبعده. لا يجوز إطلاق نظام واسع دون إجراء تقييم أثر على الحقوق وتقييم أثر

على حماية البيانات، يحدد المخاطر المحتملة، وبدائل أقل تدخلًا، وخطة تخفيف، ومعايير قياس للفعالية. هذه التقييمات لا ينبغي أن تبقى وثائق داخلية، بل يجب نشر خلاصات منها بصورة تسمح برقابة عامة، مع مراجعة دورية تُبقي النظام مشروطًا بنتائج قابلة للقياس، وتسقطه تلقائيًا إن لم يحقق أثرًا وقائيًا واضحًا أو إذا ثبتت كلفته الحقوقية المرتفعة.

3. بدائل أقل انتهاكاً من استخدام الهوية الكاملة

حتى داخل إطار تأكيد العمر الإجباري، توجد تقنيات أقل كشفًا يمكن أن تُحقق الغرض عبر إشارة عمرية محدودة بدل نقل هوية كاملة أو تاريخ ميلاد أو وثائق. الفكرة العملية هنا أن الخدمة تحتاج معرفة تحقق شرط عمري محدد لأجل تقييد بعينه، مثل كون المستخدم فوق 16 أو فوق 18 سنة، لا معرفة من هو المستخدم ولا بناء ملف تعريف عنه؛ لذلك تُعطى الأولوية لآليات إثبات صفة وليس إثبات هوية، وبحيث تكون الإشارة مؤقتة أو للاستخدام مرة واحدة وغير قابلة للربط بين الخدمات.

أحد هذه الآليات هو مسار الاعتمادات الرقمية القابلة للتحقق مع الكشف الانتقائي، حيث تُخزَّن بيانات موثوقة داخل محفظة رقمية لدى المستخدم، ثم يُقدَّم للجهة طالبة التحقق فقط ما يلزم، مثل تأكيد تجاوز سن معيّن دون كشف تاريخ الميلاد أو بيانات تعريفية أخرى. هذا هو منطق نموذج التحقق العمري ضمن محفظة الهوية الرقمية الأوروبية، التي تصف حالة استخدام تتيح إثبات تجاوز عتبة عمرية محددة مع إمكان الكشف الانتقائي بدل الإفصاح الكامل. ويستند هذا المسار إلى بنية (الاعتماد/الحامل/المتحقق) التي تُنظمها مواصفات معيارية مثل نموذج بيانات الاعتمادات القابلة للتحقق لدى W3C، بما يسمح بتمثيل ادعاءات محددة والتحقق من سلامتها دون الحاجة لنسخ وثيقة هوية كاملة داخل كل خدمة.

وتُترجم فكرة الكشف الانتقائي على مستوى البروتوكولات عبر مواصفات مثل OpenID for Verifiable Presentations، التي تُمكّن الجهة المتحققة من طلب الادعاءات اللازمة فقط وتسمح للمحفظة بالكشف عن الحد الأدنى، بما يقلل جمع البيانات ويحد من قابلية الربط. كما تُستخدم صيغ مثل SD-JWT لإخفاء حقول داخل الاعتماد وإظهار ما يلزم عند الطلب فقط، وهو نهج يُقدم نموذجًا عمليًا لكيفية بناء إشارة عمرية بدل مشاركة بيانات تعريفية كاملة.

ويُستكمل ذلك أحيانًا بتقنيات (الإثباتات عديمة المعرفة) التي تسمح للمستخدم بإثبات صحة عبارة مثل تجاوز عمر معين دون كشف أي معلومات إضافية تتجاوز صحة العبارة نفسها، وهو اتجاه تُشير إليه مواصفات تقنية مرتبطة بحلول التحقق العمري الأوروبية بوصفه خيارًا لتعزيز الخصوصية عند تقديم برهان عمر بدل تقديم بيانات عمر مفصلة. ومع ذلك يبقى إدماج هذه التقنيات في سياسة عامة بحاجة إلى حوكمة صارمة حول عدم الربط وعدم الاحتفاظ وعدم تحويل الإشارة إلى معرف ثابت، لأن هذه المخاطر قد تُعيد إنتاج أثر المراقبة حتى مع استخدام أدوات تشفير متقدمة.

كما يُمكن أن يُحصر التأكيد في الوصول إلى محتوى أو ميزات عالية الحساسية بدل تحويله إلى فحص شامل لكل الخدمات. الفكرة أن كثيرًا من المخاطر لا تتطلب بوابة عمر لكل استخدام، بل تتطلب ضوابط دقيقة على نقاط محددة مثل المحتوى شديد الحساسية، أو فتح الرسائل من الغرباء، أو بعض ميزات البث المباشر، أو معاملات الشراء داخل الألعاب. عندما يُربط التأكيد بميزات محددة، يقل نطاق المعالجة، وتقل حوافز الاحتفاظ، وتصبح الأداة أقرب إلى تدخل متناسب عِوضَ أن تكون بنية عامة لإدارة الهوية.

عاشرًا: الرد على الاعتراضات الشائعة

تواجه أي مقاربة حقوقية لحماية الأطفال في الفضاء الرقمي موجة اعتراضات تبدو لأول وهلة بديهية وسهلة التسويق، لأنها تقدم حلولًا سريعة وواضحة الرسالة. غير أن هدف الدراسة يشمل تفكيك هذه الاعتراضات وإظهار أن ما يبدو حاسمًا قد يكون مكلفًا وغير فعال، وأن حماية الأطفال يمكن تحقيقها بوسائل أدق وأقل ضررًا على الحقوق. لذلك يعالج هذا القسم أكثر الاعتراضات تداولًا على نحو يضمن بقاء النقاش في مسار عقلاني قائم على الفعالية والتناسب.

1. الحظر يحمي فورًا

فكرة الحظر تبدو جذابة لأنها توحي بنتيجة فورية، لكنها تتجاهل أن المجال الرقمي لا يعمل كمساحة مغلقة يمكن التحكم في أبوابها بسهولة. فالحظر يخلق حافزًا مباشرًا للتحايل عبر أدوات متاحة، ويحول الوصول إلى نشاط خفي بدل أن يكون استخدامًا يمكن ضبطه بإعدادات أمان وتدخلات تصميمية.

ومع التحايل يفقد الطفل في -كثير أغلب الحالات- طبقات الحماية التي كانت ممكنة داخل المنصات الأكثر استخدامًا، وينتقل إلى مساحات أقل إشرافًا وأضعف أدوات إبلاغ واستجابة، فتتحول النتيجة إلى أثر عكسي يزيد المخاطر بدل أن يقللها.

والأخطر أن الحظر، عندما يُراد له أن يكون قابلاً للإنفاذ، يدفع عادة إلى بناء بوابات تعريف أو مراقبة تجعل الهوية شرطًا للوصول، وهو ما يوسع نطاق الضرر الحقوقي من ملف الأطفال إلى المجتمع كله. وبالتالي فإن الحماية الحقيقية لا تأتي من إغلاق الباب، بل من تقليل المخاطر داخل الخدمة نفسها عبر إعدادات افتراضية آمنة، وتقييد التواصل عالي الخطورة، وضبط التوصيات، وتفعيل استجابة سريعة لحالات الاستدراج والتنمر.

2. الأسرة مسؤولة، وعلى الأسر أن تضبط استخدام الأبناء

دور الأسرة مهم، لكنه لا يمكن أن يُستخدم ذريعة لنقل العبء كله إليها. كثير من الأسر لا تملك أدوات تقنية كافية، ولا وقتًا كافيًا، ولا معرفة مفصلة بكيف تعمل خوارزميات التوصية أو الإعلانات أو تصميمات الألعاب التي تدفع إلى الاستخدام المكثف والإنفاق. تحميل الأسرة المسؤولية وحدها يعني عمليًا تحويل الحماية إلى امتياز طبقي، بحيث أن من يملك موارد ومعرفة سيحصل على حماية أفضل، بينما ستبقى الفئات الأضعف أكثر تعرضًا للأذى.

والأهم أن المنصات والألعاب هي التي تصمم البيئة وتستفيد اقتصاديًا من إبقاء المستخدم أطول، ومن فتح قنوات تواصل واسعة، ومن استهداف تجاري متكرر، ومن دفع سلوكي نحو التفاعل.

لذلك تظل المسؤولية الأساسية على من يملك القدرة على تغيير التصميم والتشغيل، وعلى الدولة بوصفها جهة تنظيم تلزم الشركات بتدابير سلامة قابلة للقياس، ثم يأتي دور الأسرة والمدرسة بوصفه دور دعم وتمكين.

3. التحقق من السن يحل مشكلة الإباحية

الخلط هنا بين هدف مشروع وبين وسيلة واسعة الأثر. فتقليل تعرض القُصّر للمحتوى الجنسي الصريح أو شديد الحساسية يحتاج تدخلات دقيقة على المحتوى نفسه، وعلى تدفقات التوصية، وعلى إعدادات العرض والبحث، وليس على نظام تحقق شامل يحول الإنترنت إلى فضاء مرور عبر بوابة هوية.

والتحقق الشامل لا يضمن النتيجة، لأن التحايل يبقى ممكنًا، ولأن المحتوى قد ينتقل عبر قنوات لا تخضع للتحقق، ولأن المنصات قد تبالغ في المنع فتقيد محتوى ثقيفي وصحي نافع تحت العنوان نفسه.

كما أن بناء نظام تحقق واسع يفتح مخاطر تسريب وابتزاز ووصم أعلى كلفة من المشكلة التي يُراد حلها، خصوصًا في سياق اجتماعي يضاعف أثر أي كشف أو تسريب.

والحل الأكثر اتساقًا هو تقييد الوصول إلى محتوى شديد الحساسية عبر ضوابط وصول محددة، وتحسين كشف المحتوى وإزالته، وضبط التوصية والبحث، وتفعيل آليات تصعيد وإبلاغ سريعة، مع حظر التتبع والاستهداف التجاري للقُصّر، عوضًا عن تحويل الحماية إلى مراقبة شاملة.

4. لا خصوصية للأطفال، والخصوصية رفاهية لا تنطبق عليهم

الخصوصية جزء من الحماية، وليست نقيضًا لها، لأن الطفل والمراهق يحتاجان مساحة آمنة للتعلم والتجربة وطلب الدعم دون خوف من الوصم أو العقاب أو الاستغلال. وتقويض الخصوصية باسم الحماية يخلق بيئة تجعل الأذى أسهل؛ فحين تُجمع البيانات وتتوسع قابلية الربط، تزداد فرص التسريب والابتزاز، وتزداد قابلية استخدام الأدوات داخل الأسرة أو المدرسة كوسيلة سيطرة أو عنف، ويتراجع طلب المساعدة عند الحاجة.

خصوصية المراهقين تحديدًا مرتبطة بمبدأ الاستقلال التدريجي وبالقدرات المتطورة، وهي ما يسمح بانتقالهم من الاعتماد الكامل إلى المسؤولية الذاتية بصورة صحية. والحماية الحقوقية لا تعني ترك الأطفال دون ضمانات، بل تعني ضمانات تحفظه من الاستغلال والعنف، وفي الوقت نفسه تمنع تحويله إلى موضوع مراقبة دائم.

التوصيات

1. التنظيم والحوكمة

ينبغي أن تُبنى السياسة العامة المقترحة على تعريف حماية الأطفال في البيئة الرقمية بوصفها سياسة وقائية دقيقة تستهدف تقليل الضرر داخل تصميم المنصات والألعاب وطريقة تشغيلها، لا بوصفها مدخلًا لتوسيع أدوات الضبط العام للاتصال والمحتوى. ويترجم ذلك في أي إطار تشريعي أو تنظيمي عبر ربط التدخلات بمسارات ضرر قابلة للرصد وفق نموذج 4Cs، وتحويل كل مسار إلى التزامات تشغيلية وقانونية قابلة للقياس والمراجعة، مع إبقاء هدف الحماية منفصلًا عن منطق الرقابة والحجب.

وينبغي أن يُرتّب التدخل وفق اختبار الضرورة والتناسب بوصفه قاعدة تنفيذ، بحيث تُعتمد البدائل الأقل تقييدًا والأقرب لمحركات الضرر أولًا، وتُحاصر الأدوات الأعلى كلفة مثل الحجب والتحقق الشامل داخل نطاقات ضيقة وبشروط صارمة ومراجعات زمنية تُسقط الإجراء تلقائيًا عند غياب أثر وقائي قابل للإثبات.

وينبغي تطوير إطار معياري علني لتقييم المخاطر وقياس الضرورة والتناسب وربطها بآلية رقابة مستقلة فعّالة. ويتضمن الإطار حواجز صريحة ضد التوسع الوظيفي تمنع تحول أدوات حماية الطفل إلى بنية دائمة لإدارة الهوية أو مراقبة الاستخدام أو ضبط المحتوى

على نطاق عام، عبر قواعد غرض محدد ومعلن لكل أداة، وحظر الاستخدامات الثانوية، ومراجعات دورية ملزمة، وشفافية عن قرارات التقييد وأسبابها، ومسارات إنصاف سريعة وفعّالة.

2. حجب الخدمات والمواقع

ينبغي أن تُحاصر صلاحيات الحجب في قانون مكافحة جرائم تقنية المعلومات وقانون تنظيم الصحافة والإعلام، داخل معايير شفافة وأسباب معلنة ومسارات طعن سريعة وواقعية ومراجعة زمنية تسقط الإجراء تلقائيًا إذا لم تثبت ضرورته، لأن مسار التظلم النظري لا يكفي دون قدرة عملية على الاعتراض.

كما يجب أن يُفعّل قانون حماية البيانات ولائحته التنفيذية عبر تحويله إلى سياسة تفصيلية لحماية بيانات الأطفال تشمل إرشادات أدوات التحقق ومعايير تقليل البيانات وحدود الاحتفاظ وضمانات عدم إعادة الاستخدام، مع التعامل مع التحقق بوصفه ممارسة تنظيمية لا مجرد إجراء تقني. ويُستدعى قانون الطفل بوصفه مرجعية حقوقية داخلية تضبط أي تنظيم جديد وتمنع المساس غير المتناسب بحق الطفل في الخصوصية والحماية والوصول إلى المعلومات وتنمية القدرات، مع منع التداخل غير المنضبط بين سلامة الطفل وتنظيم المحتوى العام ضمن إطار تنظيم الصحافة والإعلام.

3. ضمانات غير قابلة للتنازل

عند فرض تأكيد العمر، ينبغي اعتماد خطوط حمراء وضمانات غير قابلة للتنازل. تشمل الخطوط الحمراء رفض البيومتريات كمعيار امتثال أو كمدخل عام للخدمة، ورفض أي نظام ينتج قواعد بيانات أو سجلات تحقق قابلة للرجوع أو يعيد استخدام بيانات التحقق لأي غرض آخر، وحظر الربط بين نتيجة التحقق وسجل النشاط عبر معرفات ثابتة أو رموز قابلة لإعادة الاستخدام أو سجلات قابلة للتجميع، وحظر أي مشاركة أو استخدام إشارات التحقق في الإعلانات أو الاستهداف أو التوصية أو تصنيف المستخدمين، ومنع الإقصاء عبر بدائل وصول عادلة منخفضة المتطلبات لا تفترض وثائق أو أجهزة حديثة أو اتصالًا ثابتًا بوصفها الطريق الوحيد.

وينبغي فرض ضمانات تقليل البيانات وفصل الأدوار بوصفها التزامًا ملزمًا، بحيث لا تملك جهة التحقق معرفة نشاط المستخدم داخل المنصة، ولا تحصل المنصة إلا على نتيجة محدودة لا تصلح للربط أو لإعادة الاستخدام. وتُستكمل الضمانات بتدقيقات أمنية مستقلة واختبارات اختراق وإخطار إلزامي بحوادث أمن المعلومات وعقوبات على الإهمال، مع شفافية كاملة حول مزود التحقق وآلية العمل والاستضافة ومدة الاحتفاظ إن وجدت وسياسات الإتلاف ونتائج التدقيقات وعدد الطلبات المنفذة في تقارير دورية.

وينبغي خلق آليات طعن وتظلم سريعة بمراجعة بشرية عند النزاعات وبحق وصول مؤقت إلى خدمات أساسية عند استمرار النزاع، حتى لا تتحول الأخطاء التقنية إلى عقاب غير متناسب. ويُشترط تقييم أثر على الحقوق وحماية البيانات قبل الإطلاق وبعده مع نشر خلاصات تسمح برقابة عامة وربط استمرار النظام بنتائج قابلة للقياس تسقط الأداة تلقائيًا عند غياب أثر وقائي واضح أو عند ارتفاع الكلفة الحقوقية. وتُفضّل داخل هذا الإطار الإشارات العمرية المحدودة غير القابلة للربط وحصر التأكيد في ميزات عالية الحساسية بدل بوابة عامة، لأن هذا يقلل نطاق المعالجة وحوافز الاحتفاظ ويقرب التدخل من التناسب.

4. التزامات السلامة حسب التصميم

يُصى بوضع مساءلة المنصات والألعاب عبر السلامة حسب التصميم، بما يحوّل الحماية من منطق منع الدخول إلى منطق تقليل الضرر داخل الخدمة نفسها. بحيث تجعل الإعدادات الافتراضية لحسابات القُصّر أكثر حماية منذ البداية، عبر جعل الخصوصية والأمان هما الوضع الابتدائي، بما يقلل قابلية الوصول غير المرغوب، ويحد من انتقال المحتوى الشخصي إلى نطاق عام يصعب التحكم فيه، ويخفض احتمالات الاستدراج المرتبطة بالبحث عن حسابات مفتوحة.

ويُوصى بأن تُقرّ قيودًا افتراضية على الرسائل الواردة من الغرباء، مع إعادة تصميم طلبات التواصل لتقليل فتح قنوات تواصل عالية الخطورة بلا عوائق، وتوفير تحكم واضح وسهل في قبول الطلبات، وإدراج تحذيرات مبسطة عند أنماط تواصل خطرة، وتوجيه المستخدم فورًا إلى خيارات حماية داخل الواجهة.

وتُوصى المنصات بإلتزامات قابلة للاختبار على مستوى المحتوى، عبر وضع آمن افتراضي للقُصّر يضبط التوصيات، ويحد من الدفع نحو المحتوى الحاد أو المثير للصدمة، ويقلل التعرض لمحتوى يطبع الكراهية والوصم، ويخفض مسارات التتابع التي تزيد التعرض المتكرر، ويقيد الإشعارات المصممة لإعادة تدوير الانتباه دون ضرورة. ويكتمل ذلك بتوفير أدوات مفهومة لإدارة ما يظهر في الصفحة الرئيسية، وتمكين إيقاف توصيات موضوعية بعينها، وإعطاء وزن أكبر لمحتوى تعليمي وترفيهي أقل قابلية للإيذاء، بما يحمي حق الطفل في الوصول والتعلم دون استبداله بمنع عام.

ينبغي أن تكون حماية الأطفال من الاستغلال الاقتصادي قاعدة تنظيمية، عبر حظر التتبع السلوكي للقُصّر وتقييد الإعلانات الموجهة لهم، وإعادة صياغة الإعلانات إن وُجدت بوصفها سياقية غير قائمة على ملفات تعريفية، مع تمييز بصري واضح يمنع خلط الإعلان بالمحتوى.

ويُوصى بمعالجة نماذج الربح التي تدمج الاستغلال داخل التجربة اليومية، خصوصًا مسارات التقدم التي تُغري بالدفع لتسريع الإنجاز أو لتجاوز عوائق مصطنعة أو للحصول على عناصر تمنح تمايزًا اجتماعيًا بين اللاعبين، وذلك عبر شفافية أعلى للأسعار، وحدود إنفاق افتراضية مناسبة للعمر، وتقييد الآليات القائمة على الاحتمال والإنفاق المتكرر التي قد تتحول إلى ضغط مالي دائم وتفتح باب نزاعات أسرية أو تحايل أو احتيال داخل مجتمعات اللعب.

5. الإبلاغ والإستجابة

يُوصى بإلزام المنصات والألعاب بواجبات واضحة للإبلاغ والاستجابة والدعم بوصفها معيار الفعالية. تشمل هذه الواجبات آليات إبلاغ مناسبة للعمر وسهلة الوصول ومتعددة المسارات، وإجراءات حماية فورية مثل كتم الحساب المسيء ومنع تواصله وإخفاء المحتوى، واستجابة بزمن محدد لا يُترك لتقدير داخلي غير مرئي، ودعمًا للضحايا يراعي حساسية السن ويقلل إعادة الإيذاء أثناء التعامل مع البلاغ.

ويُوصى كذلك بتوفير قدرة على الحد من عودة المسيء عبر حسابات بديلة عند تكرار الإساءة، وإصدار تقارير شفافية دورية تسمح بتقييم الأداء على أساس وقائع قابلة للفحص. وفي الألعاب المتصلة بالإنترنت تُوصى قواعد تشغيلية داخل اللعبة نفسها تضبط الدردشة النصية والصوتية للقُصّر بإعدادات افتراضية تقلل التعرض للتواصل غير المرغوب، وتدير مجتمعات اللعب بما يحد من الاستدراج والتحرش والتصعيد الجماعي، وتُنظم المحتوى الذي يصنعه المستخدمون بإشراف أكثر صرامة وأدوات إزالة سريعة ومعايير واضحة ومسارات اعتراض عادلة تمنع الإفراط في الحذف.

6. التمكين والوقاية

وتُوصى الدولة بتبني الوقاية والتمكين كمسار موازٍ لا كبديل عن مساءلة الشركات، عبر اعتماد مناهج ثقافة رقمية عملية ومناسبة للعمر تغطي الخصوصية في الحياة اليومية، ومواجهة التنمر، وفهم أساليب الاستدراج والابتزاز، والتمييز بين المحتوى والإعلان، والتعامل مع التضليل، وحدود التواصل الآمن، مع تحويل الوعي إلى سلوك عبر أنشطة مدرسية وتدريبات محاكاة وحالات واقعية.

وأن تكون سياسات الهاتف داخل المدرسة مُصاغة بصورة مرنة ومتصلة بالتعلم والانضباط، بقواعد واضحة للاستخدام مع استثناءات تعليمية وتدابير تقلل الإلهاء دون مصادرة شاملة، وآلية إنصاف بسيطة تمنع تحول التنظيم إلى عقاب جماعي يدفع إلى الإخفاء والتحايل. ويُوصى التعامل مع الاستخدام الكثيف وما يرتبط به من آثار نفسية وتعليمية بوصفه مسار صحة عامة وتربية رقمية، عبر خطوط مساعدة ودعم نفسي رقمي آمن يحمي السرية ويتيح طلب المساعدة دون وصم، مع تدريب متخصص وربط مدروس بجهات حماية عند الضرورة دون تحويل الدعم إلى قناة مراقبة.

ويُوصى بالحفاظ على إنفاذ موجّه ضد الجرائم الحقيقية دون جمع جماعي للبيانات، عبر وحدات بلاغات مدربة لحالات الاستدراج والابتزاز وتسريب الصور والتنمر الشديد بمنطق حماية الضحية وتقليل إعادة الإيذاء، مع حساسية خاصة تجاه العمر والجندر وكلفة الوصم الاجتماعي التي تقلل الإبلاغ.

وأيضًا أن يُدار التعاون مع المنصات عبر طلبات محددة ومبررة ومقيدة النطاق وموجهة لواقعة بعينها لحفظ الأدلة الضرورية، دون إنشاء قنوات دائمة لتجميع البيانات أو الوصول الواسع إلى نشاط المستخدمين، وبما يضمن أن تكون الحماية تنظيمًا يحمّل الجهات القادرة على تغيير التصميم والتشغيل مسؤولية الأمان بدل أن تتحول إلى عقاب ومنع وحجب يدفع الأطفال إلى مساحات أقل أمانًا أو إلى التحايل الذي يبدد طبقات الحماية الممكنة داخل الخدمات الأكثر استخدامًا.