الامن السيبراني ودوره في خفض عنف الطلبة فيما بينهم عبر المنصات الرقمية

مقال _Article

م.م. محمد مالك محمد

ward202020@gmail.com

وزارة التربية/ مديرية تربية محافظة النجف الاشرف

الملخص

في ظل التطورات المتسارعة التي يشهدها العصر الرقمي، أصبح العالم الافتراضي يشكّل بيئة موازية للعالم الواقعي، تؤثر وتتأثر به في مختلف مجالات الحياة، لا سيما في ميدان التعليم. فلم تعد العملية التعليمية محصورة داخل جدران الصفوف الدراسية، بل تجاوزت ذلك إلى الفضاء الإلكتروني، حيث باتت المنصات الرقمية ميدانًا تفاعليًا يتواصل من خلاله الطلبة والمعلمون، ويتبادلون فيه المعلومات والخبرات بصورة آنية ومستمرة. وقد أتاح هذا التحول فرصًا جديدة للتعلم، كما فرض تحديات تستوجب الوقوف عندها وتحليلها، لفهم أبعاد هذه البيئة الرقمية وآثارها على سلوكيات الطلبة، وأساليب التعليم، وفاعلية التفاعل التربوي في العصر الحديث.

الكلمات المفتاحية: الامن السيبراني، المنصات الرقمية.

Cybersecurity and Its Role in Reducing Student-to-Student Violence on Digital Platforms

Mohammed Malik Mohammed

Ministry of Education/ Directorate of Education of Al-Najaf Al-Ashraf Governorate

Abstract

In light of the rapid developments witnessed in the digital age, the virtual world has become a parallel environment to the real world, influencing and being influenced by it in various aspects of life—especially in the field of education. The educational process is no longer confined within classroom walls; rather, it has extended into the digital space, where digital platforms have become an interactive arena through which students and teachers communicate and exchange information and experiences instantly and continuously. This

transformation has opened up new learning opportunities while also posing challenges that require attention and analysis, in order to understand the dimensions of this digital environment and its effects on student behavior, teaching methods, and the effectiveness of educational interaction in the modern era.

Keywords:Cybersecurity and Its Role in Reducing Student-to-Student Violence on Digital Platforms.

لقد أصبح العالم الرقمي اليوم بيئة موازية للواقع المادي الذي يعيش فيه الإنسان، إذ لم تعد حدود المدرسة تتوقف عند أبواب الصفوف الدراسية، بل امتدت إلى الفضاء الإلكتروني، حيث يتفاعل الطلبة مع بعضهم البعض عبر المنصات الرقمية ووسائل التواصل الاجتماعي والتطبيقات التعليمية. ومع هذا التمدد، برزت إشكاليات جديدة تتعلق بممارسات العنف بين الطلبة، والتي لم تقتصر على العنف اللفظي أو الجسدي المباشر فحسب ، بل أخذت صورًا متعددة من أبرزها التنمر الإلكتروني، والتحرش الرقمي، والابتزاز، والتشهير، وغير ذلك من أشكال الاعتداءات الرقمية، ما تتطلب تدخلًا حاسمًا من المؤسسات التربوية والأمنية من خلال تعزيز منظومة الأمن السيبراني وجعلها فاعلة بدرجة كبيرة ، وإن الأمن السيبراني، في جوهره، هو حماية الأنظمة الرقمية والشبكات وقواعد البيانات من الاختراق وسوء الاستخدام، لكنه يتجاوز البعد التقني ليشمل البعد السلوكي والنفسي أيضًا، خاصة عندما يتعلق الأمر بالبيئة التعليمية التي تضم فئة عمرية حساسة كالطلبة. فكلما زادت قدرات المدرسة ومؤسسات الدولة على تأمين الفضاء الإلكتروني، قلّت احتمالات استغلاله كوسيلة للعنف الطلابي، سواء من خلال الوقاية التقنية أو الردع القانوني أو التثقيف السيبراني.

ومن أبرز صور العنف الطلابي في العصر الرقمي ما يعرف بالتنمر الإلكتروني، وهو نوع من العنف يمارسه الطلاب ضد زملائهم عبر الرسائل أو الصور أو منشورات التواصل الاجتماعي، وغالبًا ما يكون غير ظاهر ومخفيًا عن أعين الكبار، لكنه يخلّف آثارًا نفسية عميقة قد تصل إلى الاكتئاب والانتحار في بعض الحالات كما هو مسجل لدى الجهات الرسمية وغير الرسمية . وتشير الدراسات إلى أن نسبة كبيرة من الطلبة يتعرضون لشكل من أشكال التنمر الإلكتروني خلال مسيرتهم الدراسية، مما يزيد من الحاجة إلى تدخلات قائمة على توظيف تقنيات الأمن السيبراني في مراقبة ورصد هذه الحالات والتعامل معها بصورة فعّالة.

ويقوم الأمن السيبراني بدور رئيسي في خفض العنف الطلابي عبر عدة مستويات؛ أولها هو الجانب الوقائي الذي يتمثل في تطوير أنظمة ذكية قادرة على رصد المحتوى المسيء أو العنيف في اللحظة، سواء على مستوى البريد الإلكتروني المؤسسي أو المنصات التعليمية الرسمية.

وتعمل هذه الأنظمة بتقنية الذكاء الاصطناعي وتحليل النصوص للكشف عن التهديدات والأنماط السلوكية الخطيرة. كما توفر بعض المؤسسات التعليمية بوابات خاصة للإبلاغ عن حالات العنف أو التهديد بشكل سري، مما يسمح باتخاذ إجراءات مبكرة للحد من انتشار السلوكيات العنيفة.

أما الجانب الثاني يكمن في التوعية الرقمية، حيث يعد رفع التوعية بأهمية الأمن السيبراني وبمخاطر العنف الإلكتروني جزءًا لا يتجزأ من استراتيجية الوقاية. وتقوم العديد من المدارس بعقد ورش عمل ودورات تدريبية للطلبة والمعلمين حول كيفية الاستخدام الآمن للتكنولوجيا، وطرق حماية الخصوصية، وأخلاقيات التواصل الرقمي. إن إدماج الأمن السيبراني في المناهج الدراسية اصبح ضرورة ملحة ومتطلب أساسي حيث يسهم في بناء ثقافة رقمية مسؤولة تقلل من احتمالات ممارسة أو التعرض للعنف.

ويتجسد البعد الثالث في البعد القانوني والردعي، حيث أصبح من الضروري سنّ تشريعات وقوانين ولوائح واضحة تجرّم العنف السيبراني بكافة أنواعه وتوضح العقوبات المترتبة على ممارسته. كما يجب أن تكون هناك آليات واضحة لتطبيق القانون داخل المدارس بالتعاون مع الجهات الأمنية المختصة، بما يضمن الحماية القانونية للضحايا من جهة، وردع المعتدين من جهة أخرى. وقد أظهرت التجارب أن وجود سياسة صارمة تجاه العنف الإلكتروني في المدرسة ينعكس إيجابًا على سلوك الطلبة ويقلل من الاعتداءات.

وإضافة إلى ما سبق، فإن تفعيل الأمن السيبراني يسهم في تعزيز بيئة تعليمية آمنة ومستقرة، حيث يشعر الطالب بالطمأنينة وعدم التهديد، مما ينعكس على تحصيله الدراسي وصحته النفسية. فوجود رقابة إلكترونية ذكية لا يعني فقط متابعة سلوك الطلبة، بل أيضًا تقديم الدعم النفسي والاستشاري في الحالات التي تستدعي ذلك. وتشير الدراسات الحديثة إلى أن الطلبة الذين يشعرون بالأمان الرقمي أكثر قدرة على التفاعل والمشاركة في الأنشطة التعليمية مقارنة بغيرهم.

ولا بد من الإشارة إلى أن الأمن السيبراني لا يمكن أن يحقق أهدافه بمعزل عن تعاون جميع الأطراف المعنية في البيئة التعليمية، من إدارات المدارس والمعلمين إلى أولياء الأمور والطلبة أنفسهم. فالجميع مسؤول عن بناء منظومة رقمية آمنة، تبدأ من التربية الأسرية وتنتهي بالتشريعات الرسمية. ويجب أن يكون هناك توازن بين حماية حرية التعبير لدى الطلبة ومكافحة الممارسات العنيفة، بما يضمن الحفاظ على القيم التربوية والإنسانية.

وقد بدأت العديد من الدول بتطوير منصات مركزية لإدارة الأمن السيبراني في المؤسسات التعليمية، تتيح مراقبة السلوك الرقمي للطلبة، وتوفير تقارير دورية عن المخاطر المحتملة، مع أدوات تدخل مبكر. وتُستخدم البيانات الضخمة والذكاء الاصطناعي في تحليل أنماط التفاعل

والكشف عن حالات العنف الخفي، مما يسهل عملية التدخل العلاجي أو التأهيلي قبل أن تتفاقم المشكلة. هذه المبادرات التقنية تمثل طفرة في طريقة تعامل المدارس مع العنف الطلابي، إذ تنتقل من رد الفعل إلى الفعل الاستباقي.

ومن الأمثلة الناجحة والتي يمكن لنا ان نستفد منها هي دمج الأمن السيبراني في البيئة التعليمية، تجربة بعض المدارس الأمريكية والبريطانية التي تبنت برامج مراقبة ذكية تستند إلى الذكاء الاصطناعي لتحليل اللغة المستخدمة في المحادثات الرقمية، وقد نجحت هذه البرامج في تقليل حالات التنمر والعنف بنسبة تجاوزت ٣٠% خلال عام دراسي واحد، وفقًا لتقارير مؤسسة (Cyberbullying Research Center) وكما أن منظمة اليونسكو أصدرت دليلًا شاملًا حول كيفية حماية الطلبة من العنف الرقمي، مؤكدة أن الأمن السيبراني ليس ترفًا تقنيًا ولا حاجة ثانوية، بل ضرورة تربوية وأمنية وان الحاجة الى الامن هي من المتطلبات الأساسية التي نادى بها علماء النفس ومنهم(ابراهام ماسلو) حيث جعلها في المرتبة الثانية في هرمه مما يعني الحاجة الى الشعور الامن التحدي الثاني لصحة الفرد وتوافقه النفسي .

وفي السياق العربي، بدأت بعض الدول مثل الإمارات والسعودية والعراق باتخاذ خطوات ملموسة نحو تعزيز الأمن السيبراني في المدارس، من خلال تحديث البنية التحتية الرقمية، وتدريب الكوادر التربوية، وتطوير السياسات الوقائية. ومع أن التحديات ما زالت قائمة، إلا أن الاعتراف بدور الأمن السيبراني في خفض العنف الطلابي يمثل خطوة أولى نحو بناء مدارس أكثر أمنًا وعدالة.

في الختام، يمكن القول إن الأمن السيبراني أصبح ركيزة أساسية في معالجة ظاهرة العنف الطلابي، لما يوفره من أدوات وقائية وتقنية وقانونية تساعد على خلق بيئة تعليمية آمنة. وتزداد أهمية هذا الدور في ظل تزايد اعتماد المدارس على الوسائط الرقمية في التعليم والتواصل، مما يجعل الحاجة إلى استراتيجية شاملة للأمن السيبراني أمرًا لا غنى عنه. إن مواجهة العنف الطلابي لا تقتصر على الإجراءات التربوية التقليدية، بل تتطلب مقاربة جديدة تأخذ بعين الاعتبار التحولات الرقمية والسلوكية في سلوك الطلبة ونقترح مجموعة من التوصيات التي يمكن ان تساهم في خفض العنف السيبراني بين الطلبة

١- التوعية والتثقيف : على الجهات المختصة ادخال مادة او مواضيع معينة ضمن المناهج الدراسية حول مخاطر العنف السيبراني واثارة النفسية والاجتماعية على الطالب

٢- تعزيز الرقابة الاسرية : يمكن تشجيع أولياء الأمور على متابعة نشاطات أبنائهم الالكترونية بشكل متوازن

٣- تطوير وتنمية المهارات الاجتماعية والانفعالية : تدريب الطلبة على حل النزاعات بشكل سلمي ومهارات التواصل الفعال

٤- وضع مدونة سلوك رقمية في المدرسة تشمل السلوكيات الرقمية المقبولة والعقوبات الناتجة على استخدام العنف السيبراني

٥- التعاون مع الجهات ذات العلاقة مثل الشرطة المجتمعية وغيرها لتقديم محاضرات توعوية والتعاون مع منظمات المجتمع المدني لأطلاق حملات توعية للتعريف بخطورة العنف السيبراني

المصادر:.

١. وزارة التربية والتعليم في الإمارات. (٢٠٢٣). دليل الأمن السيبراني في المدارس.

٢. الهيئة الوطنية للأمن السيبراني – السعودية (٢٠٢٢). استراتيجية الأمن السيبراني في القطاع التعليمي.

٣-جامعة الدول العربية (٢٠٢١). التنمر الرقمي والعنف الطلابي: دراسة حالة في المدارس العربية.

4- Hinduja, S. & Patchin, J. W. (2020). Cyberbullying: Identification, Prevention, and Response. Cyberbullying Research Center.

5- UNESCO (2021). Safe to Learn: Ending Violence in and through Schools..

6- Livingstone, S., & Smith, P. K. (2014). Annual Research Review: Harms experienced by child users of online and mobile technologies. Journal of Child Psychology and Psychiatry.