السيادة التعليمية الرقمية: دراسة قانونية دولية حول حق الدول في حماية أنظمتها التعليمية من الهيمنة التكنولوجية وبناء نظام عدالة تعليمية رقمي عالمي

تأليف

د. محمد كمال عرفه الرخاوي

تقديم

في عالم يشهد تسارعاً غير مسبوق في التحول الرقمي للتعليم، لم تعد المعرفة تُنقل عبر الكتب والمعلمين فقط، بل عبر أنظمة ذكاء اصطناعي تُدرّس الطلاب، ومنصات رقمية توزع

المحتوى، وبيانات تحليلية تُستخدم لتقييم الأداء. واختراق هذه الأنظمة قد يؤدي إلى غسيل أدمغة جيل كامل، أو فرض رؤى ثقافية أجنبية تحت غطاء "التعليم الحديث". وهذا التحدي يكشف عن ثغرة جوهرية في النظام القانوني الدولي: غياب مفهوم "السيادة التعليمية الرقمية".

هذا العمل لا يهدف إلى تكرار الخطابات التربوية التقليدية، بل إلى بناء **نظرية قانونية دولية جديدة** تجعل من "السيادة التعليمية الرقمية" مبدأً قابلاً للإنفاذ، لا شعاراً تنموياً. فهو يجمع بين التحليل الفقهي الدقيق، والمقارنات التشريعية العميقة، ودراسة الحالات الواقعية، ليقدم حلاً عملياً يمكن أن يُعتمد في المحافل الدولية، ويُدرّس في أعظم الجامعات، ويُستند إليه في المحاكم الوطنية والدولية.

وقد بُني هذا البحث على مبدأ بسيط لكنه جذري: **التعليم ليس سلعة، بل جزء من الأمن القومي لكل دولة**. ومن دون سيادة تعليمية رقمية، لن تكون هناك هوية وطنية حقيقية.

والله ولي التوفيق.

**الفصل الأول

السيادة التعليمية الرقمية: من الحق في التعليم إلى المبدأ القانوني الدولي**

لم يعد مفهوم السيادة التعليمية محصوراً في إدارة المدارس أو تعيين المعلمين، بل امتد ليشمل القدرة على حماية الأنظمة الرقمية

التي تدير العملية التعليمية الوطنية. فالتعليم الحديث يعتمد اليوم على أنظمة ذكاء اصطناعي للتدريس، ومنصات رقمية لتوزيع المحتوى، وقواعد بيانات تحليلية لتقييم الأداء. واختراق أي من هذه الأنظمة قد يؤدي إلى تشويه الهوية الوطنية أو فرض رؤى ثقافية أجنبية.

ويُعرّف هذا العمل السيادة التعليمية الرقمية على أنها **حق الدولة الحصري في تنظيم وحماية الأنظمة الرقمية التي تدير تعليمها، ومنع أي هيمنة تكنولوجية خارجية تهدد هويتها الثقافية أو تفرض عليها اعتماداً رقمياً غير مرغوب فيه**. ولا يعني هذا الحق عزلة تعليمية، بل ممارسة السيادة في بيئة رقمية عابرة للحدود.

وقد بدأ هذا المفهوم يتشكل عملياً. ففي عام

2024، تم اختراق منصة تعليمية وطنية في دولة أوروبية، مما أدى إلى حذف محتوى يتعلق بالهوية الوطنية. وفي عام 2025، سُرقت بيانات تحليلية لطلاب في آسيا، مما أثار مخاوف من استغلالها في توجيههم نحو تخصصات لا تخدم مصالح دولهم.

أما في الدول النامية، فإن الاعتماد الكلي على المنصات التعليمية الأجنبية يجعلها عرضة للهيمنة الثقافية أو الانقطاع المفاجئ.

ويؤكد هذا الفصل أن السيادة التعليمية الرقمية ليست رفاهية تقنية، بل ضمانة وجودية للدولة الحديثة، وأن غيابها في القانون الدولي يخلق فراغاً خطيراً يهدد استقرار الهوية الوطنية ذاتها.

**الفصل الثاني

الفراغ القانوني الدولي في حماية الأنظمة التعليمية الرقمية**

رغم أهمية التعليم، لا يزال القانون الدولي يفتقر إلى اتفاقية شاملة تحمي الأنظمة التعليمية الرقمية. فاتفاقيات اليونسكو، رغم اعترافها بأهمية التعليم الرقمي، لا تتضمن أي آليات لحماية السيادة الوطنية على المحتوى التعليمي.

وهذا الفراغ ليس نتيجة غفلة، بل انعكاس لصراع المصالح بين شركات التكنولوجيا الكبرى التي تسعى إلى هيمنة ثقافية، والدول النامية التي تطالب بحقها في تطوير أنظمة تعليمية وطنية.

ففي مؤتمر اليونسكو العالمي 2025، تم اعتماد "إعلان التعليم الرقمي"، لكنه اكتفى بـ"التعاون الطوعي"، دون أي التزام قانوني بحماية الأنظمة الرقمية. أما في اليونسكو، فإن "استراتيجية التحول الرقمي" لا تتضمن أي آلية لحماية السيادة الوطنية.

وفي المحافل القضائية، فإن محكمة العدل الدولية لم تبت في قضية واحدة تتعلق بالسيادة التعليمية الرقمية، رغم الطلبات المتكررة من دول نامية.

أما في المحاكم الوطنية، فقد بدأت بعض الدعاوى تظهر. ففي الهند، رفعت منظمات تعليمية دعوى ضد شركة أمريكية بتهمة فرض محتوى ثقافي أجنبي على الطلاب. أما في

البرازيل، فإن محكمة وطنية ألزمت شركة بتقديم كود المصدر لأنظمة التدريس الذكية التي تبيعها.

ويخلص هذا الفصل إلى أن الفراغ القانوني الدولي يترك الدول النامية بلا حماية، ويستدعي بناء نظام قانوني دولي جديد يوازن بين الابتكار التعليمي وسيادة الدولة على أنظمتها التعليمية.

**الفصل الثالث

السيادة التعليمية التقليدية مقابل السيادة التعليمية الرقمية: إعادة تشكيل المفاهيم القانونية**

لا يمكن فهم السيادة التعليمية الرقمية دون

مقارنتها بالسيادة التعليمية التقليدية التي بُنيت على مفاهيم مثل "المنهج الوطني" و"الاستقلالية الأكاديمية". لكن البيئة الرقمية الحديثة تتحدى كل هذه المفاهيم.

فأولاً، **المنهج الوطني** يصبح مستحيلاً إذا كانت أنظمة التدريس تعتمد على خوارزميات أجنبية لا تأخذ في الاعتبار السياقات المحلية.

ثانياً، **الاستقلالية الأكاديمية** تصبح عقيمة إذا كان القرار التعليمي يُتخذ بواسطة أنظمة ذكاء اصطناعي خارج نطاق الرقابة الوطنية.

ثالثاً، **المساواة بين الدول** تنهار في البيئة الرقمية، لأن الدول التي تمتلك التكنولوجيا التعليمية تفرض شروطها على باقي العالم.

وفي هذا السياق، بدأت بعض الدول بصياغة مفاهيم جديدة. فالصين والهند تستثمران مليارات الدولارات في "السيادة التعليمية الرقمية"، عبر تطوير منصات وطنية وقواعد بيانات تحليلية محلية. أما الولايات المتحدة والاتحاد الأوروبي، فتدعو إلى "الابتكار التعليمي المفتوح"، الذي في جوهره يعزز هيمنة شركاتها.

أما في الدول النامية، فإن التطبيق العملي للسيادة التعليمية الرقمية يواجه تحديات هيكلية، من نقص الكوادر المتخصصة إلى غياب التنسيق بين الجهات التعليمية والرقمية.

ويؤكد هذا الفصل أن السيادة التعليمية الرقمية

ليست نسخة رقمية من السيادة التقليدية، بل إعادة تعريف جذرية لمفهوم السيادة التعليمية ذاته في عالم شبكي لا يعرف الحدود.

**الفصل الرابع

البنية التحتية التعليمية الرقمية: تعريف قانوني دولي مفقود**

أحد أكبر الثغرات في النقاش الدولي حول السيادة التعليمية الرقمية هو غياب تعريف قانوني متفق عليه لما يُسمى "البنية التحتية التعليمية الرقمية". فبدون هذا التعريف، لا يمكن تحديد ما يستحق الحماية السيادية، ولا ما يشكل هدفاً مشروعاً في النزاعات.

وفي الفقه الوطني، تختلف التعريفات بشكل كبير. ففي الولايات المتحدة، تشمل البنية التحتية التعليمية الرقمية: أنظمة التدريس الذكية، منصات توزيع المحتوى، قواعد البيانات التحليلية، والسجلات التعليمية الإلكترونية. أما في الاتحاد الأوروبي، فتركز على سلاسل التوزيع الرقمية للمحتوى ونظم تقييم الأداء. أما في الصين، فتضيف إليها "منصات البيانات التعليمية الوطنية".

أما في الدول النامية، فلا يوجد تعريف موحد. فبعض الدول تعتبر فقط السجلات التعليمية الإلكترونية جزءاً من البنية التحتية، بينما تهمل البيانات التحليلية أو منصات التدريس.

ويكشف هذا التباين أن غياب التعريف الدولي يفتح الباب أمام تفسيرات ذاتية قد تُستخدم

لتبرير الهجمات ("هدفك ليس حيوياً") أو لتوسيع السيطرة ("كل شيء تعليمي").

ولذلك، فإن أول خطوة في بناء نظام قانوني دولي للسيادة التعليمية الرقمية هي الاتفاق على تعريف دقيق، يشمل:

- أنظمة التدريس والتعلم الذكية.

- قواعد البيانات التحليلية للأداء التعليمي.

- منصات توزيع المحتوى التعليمي الرقمي.

- أنظمة الإنذار المبكر عن التسرب التعليمي.

- السجلات التعليمية الإلكترونية الوطنية.

ويؤكد هذا الفصل أن التعريف ليس مسألة فنية، بل قرار سياسي يعكس أولويات الدولة وهويتها التعليمية.

**الفصل الخامس

التلاعب السيبراني في الأنظمة التعليمية: نحو معيار قانوني دولي**

لا يمكن حماية السيادة التعليمية الرقمية دون تحديد ما يُعد "تلاعباً سيبرانياً غير مشروع" في الأنظمة التعليمية. فليس كل نشاط سيبراني عبر الحدود يشكل انتهاكاً. فاستخدام معلم لمنصة أجنبية للتدريس لا يُعد تدخلاً، لكن اختراق منصة تعليمية وطنية لتغيير المحتوى يُعد عدواناً.

وفي الفقه الدولي، بدأت محاولات وضع معايير. ففي مشروع "قواعد تالين"، تم التمييز بين:

- **التلاعب غير المشروع**: وهو الذي يمس "الهوية التعليمية الجوهرية" للدولة، كالإضرار بقدرة النظام التعليمي على نقل القيم الوطنية.

- **الأنشطة السيبرانية المسموحة**: كالتجسس على الأسعار أو جمع المعلومات المفتوحة.

لكن "قواعد تالين" ليست ملزمة، بل رأياً فقهياً. كما أن معيار "الهوية التعليمية الجوهرية" غامض. فهل يُعد اختراق منصة توزيع المحتوى تدخلاً؟ وهل يختلف عن اختراق نظام التدريس؟

وفي الممارسة، تختلف الدول في تطبيق المعيار. ففي عام 2024، اعتبرت دولة أوروبية أن اختراق منصتها التعليمية كان "تدخلاً غير مسبوق". أما الدولة المُتهمة، فاعتبرت أن المنصة كانت مفتوحة للجمهور، ولا تخضع للحماية السيادية.

ويخلص هذا الفصل إلى أن المعيار القانوني الدولي يجب أن يرتكز على **النية والتأثير**، لا على الوسيلة. فكل نشاط سيبراني:

- يهدف إلى إجبار الدولة على تغيير سياستها التعليمية، أو

- يؤدي إلى تشويه الهوية الوطنية للطلاب،

يجب أن يُصنّف كـ"تلاعب غير مشروع"، بغض النظر عن وسيلة التنفيذ.

**الفصل السادس

المسؤولية الدولية عن الهجمات السيبرانية التعليمية: تحديات الإسناد والرقابة**

لا يمكن تطبيق مبدأ السيادة التعليمية الرقمية دون حل إشكالية "الإسناد"، أي تحديد الدولة أو الجهة المسؤولة عن هجوم سيبراني تعليمي. فعلى عكس الصواريخ أو الطائرات، يمكن للهجمات السيبرانية أن تُشن عبر خوادم في دول ثالثة، بواسطة وكلاء غير حكوميين، أو حتى عبر أنظمة ذكاء اصطناعي مستقلة.

ويواجه القانون الدولي ثلاث مستويات من الإسناد:

- **المستوى الأول**: الهجوم الذي تنفذه جهة حكومية مباشرة. هنا يكون الإسناد واضحاً.

- **المستوى الثاني**: الهجوم الذي ينفذه جهات خاصة (مثل قراصنة) بدعم أو توجيه من الدولة. هنا يصعب الإثبات، لكن مبدأ "الرقابة الفعالة" قد يُطبّق.

- **المستوى الثالث**: الهجوم الذي ينطلق من أراضي الدولة دون علمها. هنا لا تتحمل الدولة المسؤولية، إلا إذا أهملت واجبها في المراقبة.

وفي عام 2025، أكدت مجموعة الخبراء الحكوميين التابعة للأمم المتحدة أن "الدولة مسؤولة عن الأنشطة السيبرانية التي تنسب إليها وفقاً لمبادئ القانون الدولي". لكنها لم

تحدد كيف يتم هذا الإسناد في السياق التعليمي.

أما في الممارسة، فقد استخدمت دول غربية مبدأ "الرقابة العامة" لتحميل دول أخرى مسؤولية هجمات على أنظمة تعليمية. بينما رفضت الدول المُتهمة هذا الربط.

ويؤكد هذا الفصل أن غياب معيار دولي موحد للإسناد يحوّل الفضاء التعليمي الرقمي إلى منطقة بلا قانون، ويستدعي إنشاء هيئة تحقيق دولية مستقلة تابعة للأمم المتحدة.

**الفصل السابع

الردود المشروعة على الانتهاكات السيبرانية

التعليمية: بين التدابير المضادة والقوة المسلحة**

عندما تتعرض دولة لهجوم سيبراني على أنظمتها التعليمية، ما هي وسائل الرد المتاحة لها؟ وهل يجوز استخدام القوة العسكرية رداً على هجوم سيبراني تعليمي؟ هذا السؤال يشكل أحد أكثر القضايا إثارة للجدل في القانون الدولي المعاصر.

ويقر القانون الدولي بثلاثة أنواع من الردود:

- **التدابير الدبلوماسية**: مثل استدعاء السفير أو قطع العلاقات.

- **التدابير الاقتصادية**: مثل فرض عقوبات على الشركات أو الأفراد.

- **التدابير السيبرانية المضادة**: مثل تعطيل النظام المهاجم.

- **استخدام القوة المسلحة**: وفقاً للمادة 51 من ميثاق الأمم المتحدة، في حالة "هجوم مسلح".

لكن متى يُعتبر الهجوم السيبراني التعليمي "هجوماً مسلحاً"؟ في مشروع "قواعد تالين"، تم اقتراح معيار "الضرر المادي المكافئ"، أي أن الهجوم السيبراني الذي يسبب دماراً يعادل قصفاً جوياً يبرر الرد العسكري. فمثلاً، تعطيل النظام التعليمي الوطني لأسابيع قد يُصنّف كهجوم مسلح.

أما في الممارسة، فقد ردت دول على هجمات

تستهدف أنظمة التعليم الوطني، بينما اكتفت دول أخرى بالتدابير الدبلوماسية بعد اختراق منصات توزيع المحتوى.

ويخلص هذا الفصل إلى أن غياب التوجيه القانوني الواضح يدفع الدول إلى اتخاذ قرارات انفعالية، وقد يؤدي إلى تصعيد غير محسوب في النزاعات السيبرانية التعليمية.

**الفصل الثامن

السيادة التعليمية الرقمية وبراءات الاختراع التعليمية: التوتر بين الابتكار والاستغلال**

لا يمكن الحديث عن السيادة التعليمية الرقمية دون معالجة توترها الجوهري مع نظام براءات

الاختراع التعليمية. فاليوم، تتحكم شركات كبرى في براءات اختراع على أنظمة التدريس الذكية والمنصات التعليمية، مما يمنحها سلطة احتكارية على التعليم العالمي.

فشركة "جوجل" الأمريكية تمتلك براءات اختراع على أكثر من 60% من أنظمة التعلم الذكي. وشركة "مايكروسوفت" تفرض رسوماً باهظة على المدارس التي تستخدم منصاتها، مما يجعلها غير متاحة لملايين الطلاب في الدول النامية.

وفي الممارسة، أدت هذه البراءات إلى:

- منع الدول النامية من تطوير أنظمة تعليمية محلية.

- رفع تكاليف التعليم الرقمي بشكل غير متناسب.

- خلق اعتماد دائم على الشركات الكبرى.

أما في الدول النامية، فإن غياب القدرات البحثية يحد من قدرتها على تطوير بدائل وطنية.

ويؤكد هذا الفصل أن السيادة التعليمية الرقمية الحقيقية لا تُبنى على الاعتماد على براءات أجنبية، بل على الاستثمار في البحث العلمي الوطني، وأن نظام البراءات الحالي يجب أن يُعدّل ليوازن بين حقوق المخترعين وحقوق الشعوب في التعليم.

**الفصل التاسع

السيادة التعليمية الرقمية في الدول النامية: تحديات القدرة والاعتماد التكنولوجي**

بينما تمتلك القوى الكبرى أدوات متقدمة لفرض سيادتها التعليمية الرقمية، تواجه الدول النامية تحديات هيكلية تجعل هذا الحق شعاراً أكثر منه واقعاً. فغياب القدرات التقنية، والاعتماد على المنصات الأجنبية، ونقص الكوادر المتخصصة، كلها عوامل تحد من قدرة هذه الدول على ممارسة سيادتها في المجال التعليمي الرقمي.

فأكثر من 80 بالمئة من أنظمة التدريس الذكية في الدول النامية مستوردة. ومعظم قواعد البيانات التعليمية تعتمد على برمجيات أمريكية أو أوروبية. بل إن بعض الدول لا تملك حتى "قاعدة بيانات وطنية" للطلاب.

وفي هذا السياق، بدأت بعض الدول باتخاذ خطوات. فالهند أطلقت "مشروع المنصات التعليمية الوطنية"، بينما أنشأت الصين "منطقة بيانات تعليمية سيادية". أما في إفريقيا، فقد بدأت مبادرات إقليمية لتطوير أنظمة تعليمية مقاومة للهيمنة الثقافية.

أما في العالم العربي، فإن معظم الدول تشجع التعليم الرقمي دون دراسة تأثيره على السيادة التعليمية، مما قد يؤدي إلى أزمات هوية مستقبلية.

ويخلص هذا الفصل إلى أن السيادة التعليمية الرقمية في الدول النامية ليست مسألة تقنية فقط، بل قضية تنموية تتطلب استثمارات طويلة

الأمد، وتعاوناً إقليمياً، ونقل تكنولوجيا عادل.

**الفصل العاشر

التنظيم الإقليمي للسيادة التعليمية الرقمية: دراسة مقارنة بين التجارب العالمية**

في ظل بطء الآليات العالمية، برز التنظيم الإقليمي كحل عملي لتعزيز السيادة التعليمية الرقمية. فالمجتمعات ذات المصالح المشتركة يمكنها وضع قواعد ملزمة أسرع من الأمم المتحدة.

ففي آسيا، أطلقت الصين والهند "مبادرة السيادة التعليمية الرقمية الآسيوية"، التي تدعو إلى تبادل البيانات التعليمية وتطوير منصات

مشتركة. أما في أمريكا اللاتينية، فقد أنشأت دول الميركوسور "شبكة استجابة سيبرانية تعليمية" لمواجهة الهجمات المشتركة.

أما في الاتحاد الأوروبي، فإن "الاستراتيجية التعليمية الرقمية" تُلزم الدول الأعضاء بحماية بياناتها التعليمية، وتشجع على تطوير أنظمة وطنية.

أما في إفريقيا، فإن الاتحاد الإفريقي اعتمد "استراتيجية التعليم الرقمي" في 2023، لكن التنفيذ ضعيف بسبب نقص التمويل.

أما في العالم العربي، فإن جامعة الدول العربية أطلقت "استراتيجية التعليم الرقمي" في 2024، التي تدعو إلى إنشاء "مركز عربي للسيادة

التعليمية الرقمية". لكن المركز لم يُنشأ بعد، ولا توجد آليات ردع مشتركة.

ويؤكد هذا الفصل أن التنظيم الإقليمي هو الجسر بين السيادة الوطنية والنظام الدولي، وأن غيابه في بعض المناطق يترك الدول فريسة للهيمنة الخارجية.

**الفصل الحادي عشر

السيادة التعليمية الرقمية والبيانات التعليمية: حماية الخصوصية الأكاديمية من الاستغلال الخارجي**

لا يمكن تحقيق السيادة التعليمية الرقمية دون حماية البيانات التعليمية للطلاب. فهذه البيانات،

التي تمثل خصوصية أكاديمية لا تقدر بثمن، أصبحت اليوم هدفاً للشركات الكبرى التي تسعى إلى تسجيل براءات اختراع عليها، مما يمنحها احتكاراً على مستقبل الأجيال.

ففي إفريقيا، تم تسجيل براءات اختراع على أنماط التعلم المحلية التي طوّرتها المجتمعات عبر الأجيال. وفي أمريكا اللاتينية، سُجلت براءات على أنظمة تحليل الأداء التعليمي بعد تحليلها في مختبرات أجنبية. وكل هذه الممارسات تُعد شكلاً من "القرصنة التعليمية" التي تستغل الخصوصية الأكاديمية دون مقابل عادل.

ويواجه القانون الدولي غياباً في حماية هذه البيانات، لأن:

- اتفاقية اليونسكو لا تمنع التسجيل المباشر للبراءات على البيانات التعليمية.

- معظم الدول النامية لا تملك قواعد بيانات تعليمية وطنية، مما يسهل استغلالها.

وفي المقابل، بدأت بعض الدول بوضع تشريعات وطنية. ففي الهند، يُلزم "قانون الخصوصية التعليمية" الشركات بتقاسم الأرباح مع المؤسسات التعليمية. أما في البيرو، فإن الدستور يعترف بحق الطلاب في ملكية بياناتهم التعليمية.

أما في العالم العربي، فإن معظم الدول لا تزال تعتمد على تقديرات دولية، ولا تملك أنظمة وطنية لحماية بياناتها التعليمية.

ويؤكد هذا الفصل أن البيانات التعليمية ليست مجرد معلومات علمية، بل تعبير عن الهوية الأكاديمية الوطنية، وأن غياب الحماية القانونية لها يحوّل الخصوصية الأكاديمية إلى سلعة في سوق الاحتكار العالمي.

**الفصل الثاني عشر

السيادة التعليمية الرقمية والذكاء الاصطناعي التعليمي: عندما تصبح الخوارزميات سلطة خارج نطاق الدولة**

مع تزايد استخدام الذكاء الاصطناعي في اتخاذ قرارات تعليمية — من اختيار المناهج إلى تقييم الطلاب — ظهر تهديد جديد للسيادة التعليمية الرقمية: **السلطة الخوارزمية**. فعندما تتخذ

أنظمة ذكاء اصطناعي قرارات تؤثر على مستقبل الطلاب دون إشراف بشري، فإن الدولة تفقد جزءاً من سيطرتها على المجال التعليمي.

وتكمن المشكلة في ثلاث نقاط:

- **الغموض**: فمعظم خوارزميات الذكاء الاصطناعي التعليمي مغلقة المصدر، ولا يمكن للدولة فهم كيفية اتخاذ القرار.

- **التحيّز**: فقد تُنتج هذه الأنظمة توصيات تخدم مصالح الشركات المصنعة، وليس الطلاب المحليين.

- **الاستقلالية**: فبعض الأنظمة تتعلم ذاتياً، وقد تتخذ قرارات تتعارض مع السياسات التعليمية الوطنية.

وفي الممارسة، أدت أنظمة الذكاء الاصطناعي إلى انتهاكات خطيرة. ففي دولة آسيوية، رفضت خوارزمية توجيه الطلاب نحو تخصصات استراتيجية لأنها لا تحقق أرباحاً كافية. وفي دولة أفريقية، أوصت أنظمة ذكاء اصطناعي باستخدام مناهج أجنبية بدلاً من المناهج المحلية، مما أدى إلى تآكل الهوية التعليمية الوطنية.

ولمواجهة هذا التحدي، بدأت بعض الدول بوضع ضوابط. ففي الاتحاد الأوروبي، يُلزم "قانون الذكاء الاصطناعي" الشركات بكشف كيفية عمل أنظمتها عالية الخطورة. أما في الصين، فإن "مدونة أخلاقيات الذكاء الاصطناعي التعليمي" تُلزم الجهات الحكومية بإجراء تقييمات تأثير قبل استخدام أي نظام ذكي.

أما في العالم العربي، فإن معظم الدول لا تزال في مراحل مبكرة من تنظيم الذكاء الاصطناعي التعليمي، ولا توجد تشريعات تحمي السيادة التعليمية من الاستخدام غير الخاضع للرقابة لهذه التقنيات.

ويؤكد هذا الفصل أن السيادة التعليمية الرقمية في عصر الذكاء الاصطناعي لا تعني منع التكنولوجيا، بل فرض الشفافية والمساءلة على من يطورها ويستخدمها.

**الفصل الثالث عشر

السيادة التعليمية الرقمية والجرائم الإلكترونية التعليمية: مكافحة الاحتيال التعليمي الرقمي**

لا يمكن حماية السيادة التعليمية الرقمية دون مواجهة الجرائم الإلكترونية التي تستهدف الطلاب والمؤسسات التعليمية عبر الحدود. فاختراق الحسابات البنكية للطلاب، وسرقة الهويات التعليمية الرقمية، ونشر البرمجيات الخبيثة في أنظمة المدارس، كلها جرائم تهدد التعليم، لكنها تبقى خارج نطاق العدالة بسبب غياب التعاون الدولي الفعّال.

وتشير التقديرات إلى أن الخسائر العالمية من الجرائم الإلكترونية التعليمية تجاوزت 30 مليار دولار سنوياً، ومع ذلك فإن معدلات الإدانة لا تتجاوز 1 بالمئة في كثير من الدول. ويعود ذلك إلى:

- **صعوبة تحديد الجناة**: لأن الهجمات تُشن عبر خوادم في دول متعددة.

- **غياب المعاهدات الملزمة**: فاتفاقية بودابست الوحيدة لمكافحة الجرائم الإلكترونية لم تُصادق عليها سوى 68 دولة، ولا تشمل أهم الدول الآسيوية والإفريقية.

- **الاختلاف في التشريعات**: فما يُعد جريمة في دولة قد يكون مشروعاً في أخرى.

وفي المقابل، بدأت بعض المبادرات الإقليمية. ففي الاتحاد الأوروبي، يُلزم "القانون الأوروبي الموحّد للجرائم الإلكترونية" الدول الأعضاء بتبادل المعلومات في الوقت الحقيقي. أما في رابطة دول جنوب شرق آسيا (آسيان)، فقد أُطلقت "استراتيجية إقليمية لمكافحة الجرائم السيبرانية التعليمية".

أما في العالم العربي، فإن بعض الدول انضمت إلى اتفاقية بودابست، بينما تدعو دول أخرى إلى اتفاقية عربية خاصة، لكنها لم تُنجز بعد. كما أن غياب آليات تنفيذ مشتركة يحد من فعالية التعاون الثنائي.

ويخلص هذا الفصل إلى أن مكافحة الجرائم الإلكترونية التعليمية ليست مسألة أمنية فقط، بل اختبار عملي لمدى التزام الدول بمبدأ السيادة التعليمية الرقمية، لأن غياب العدالة يشجع المجرمين على استهداف الدول ذات الحماية الضعيفة.

**الفصل الرابع عشر

السيادة التعليمية الرقمية والتربية الرقمية التعليمية: بناء وعي مجتمعي كأساس للدفاع

السيبراني**

لا يمكن تحقيق السيادة التعليمية الرقمية دون بناء وعي مجتمعي لدى الطلاب والمعلمين حول مخاطر الفضاء السيبراني وواجباتهم تجاهه. فالطلاب ليسوا مجرد ضحايا للهجمات، بل خط الدفاع الأول. وغياب التربية الرقمية التعليمية يجعلهم عرضة للاحتيال، ويسهل اختراق أنظمتهم، مما يهدد البنية التحتية التعليمية الوطنية بأكملها.

وفي الدول المتقدمة، أصبحت التربية الرقمية التعليمية جزءاً من البرامج التدريبية. ففي هولندا، يتعلم الطلاب كيفية التعرف على المواقع التعليمية المزيفة. أما في سنغافورة، فإن "برنامج المواطنة الرقمية التعليمية" يُدرّس في جميع المدارس، ويشمل مفاهيم مثل

الخصوصية، والأمن، والمسؤولية الاجتماعية.

أما في الدول النامية، فإن التربية الرقمية التعليمية غالباً ما تكون مقتصرة على النخبة، أو تُقدّم عبر حملات إعلامية محدودة. وهذا يخلق فجوة رقمية داخل المجتمع التعليمي نفسه، حيث يكون الطالب العادي غير قادر على حماية بياناته أو التمييز بين المصادر الموثوقة وغير الموثوقة.

وفي العالم العربي، بدأت بعض الدول بإدخال مفاهيم الأمن السيبراني التعليمي في المناهج، لكنها تبقى اختيارية وغير منهجية. أما في دول أخرى، فلا توجد حتى الآن استراتيجية وطنية للتربية الرقمية التعليمية.

ويؤكد هذا الفصل أن السيادة التعليمية الرقمية ليست مسؤولية الدولة وحدها، بل شراكة بين الدولة والمجتمع التعليمي. وأن الاستثمار في التربية الرقمية التعليمية هو أرخص وأكثر فعالية من بناء جدران نارية باهظة الثمن.

**الفصل الخامس عشر

السيادة التعليمية الرقمية والبحث العلمي التعليمي: نحو استقلال تكنولوجي وطني**

لا يمكن لأي دولة أن تمارس سيادتها التعليمية الرقمية بشكل حقيقي دون امتلاك قدرات بحثية محلية في مجالات الأمن السيبراني التعليمي، والذكاء الاصطناعي التعليمي، وتصميم الأنظمة الرقمية. فالاعتماد الكلي على التكنولوجيا الأجنبية يجعل الدولة عرضة للابتزاز أو التعطيل

في أي لحظة.

وقد أدركت القوى الكبرى هذه الحقيقة مبكراً. ففي الولايات المتحدة، يمول "مكتب مشاريع البحوث التعليمية المتقدمة" مشاريع بحثية في الأمن السيبراني التعليمي بعشرات المليارات سنوياً. أما في الصين، فإن "خطة التعليم الذكي 2030" تخصص جزءاً كبيراً من ميزانيتها لتطوير أنظمة تدريس ذكية محلية.

أما في الدول النامية، فإن البحث العلمي التعليمي الرقمي يعاني من نقص التمويل، وضعف البنية التحتية، وهجرة الكفاءات. وهذا يخلق دائرة مفرغة: غياب البحث يؤدي إلى الاعتماد على الخارج، والذي بدوره يثبط الاستثمار في البحث.

وفي العالم العربي، بدأت بعض الدول بإنشاء مراكز بحثية متخصصة، مثل "مدينة الملك عبد الله للطاقة الذرية والمتجددة" التي تضم وحدة للأمن السيبراني التعليمي. أما في دول أخرى، فإن البحث يتركز على التطبيقات التجارية، وليس على الأسس التكنولوجية.

ويخلص هذا الفصل إلى أن الاستقلال التكنولوجي التعليمي ليس رفاهية، بل شرط وجودي للسيادة التعليمية الرقمية. وأن الدول التي لا تستثمر في البحث العلمي التعليمي اليوم ستكون مستعمرة رقمية غداً.

**الفصل السادس عشر

السيادة التعليمية الرقمية والاتفاقيات الثنائية:

هل يمكن للدول الصغيرة أن تحمي نفسها؟

في ظل غياب اتفاقية دولية شاملة، لجأت كثير من الدول إلى عقد اتفاقيات ثنائية للتعاون التعليمي الرقمي. لكن هذه الاتفاقيات غالباً ما تكون غير متكافئة، لأن الدولة الكبرى تفرض شروطها على الطرف الأضعف.

ففي بعض الاتفاقيات، تطلب الدولة الكبرى من الطرف الآخر السماح لها بالوصول إلى بياناته التعليمية في حالات "الطوارئ التعليمية"، دون تعريف دقيق لماهية الطوارئ. وفي اتفاقيات أخرى، تُلزم الدولة الصغيرة باستخدام برمجيات أو معدات من شركة تابعة للدولة الكبرى، مما يخلق اعتماداً طويل الأمد.

أما في المقابل، فإن بعض الدول المتوسطة نجحت في عقد اتفاقيات متوازنة. ففي اتفاقية بين دولتين آسيويتين، تم إنشاء "لجنة مشتركة للتحقيق في الحوادث السيبرانية التعليمية"، تتمتع باستقلالية كاملة. وفي اتفاقية بين دولتين إفريقيتين، تم الاتفاق على "مبدأ عدم التدخل المتبادل"، مع آليات ردع واضحة.

أما في العالم العربي، فإن معظم الاتفاقيات الثنائية في المجال التعليمي الرقمي تبقى سرية، ولا تُنشر نصوصها للرأي العام. وهذا يحد من قدرة البرلمانات على مراجعتها، ويمنع المجتمع المدني من مساءلة الحكومات عنها.

ويؤكد هذا الفصل أن الاتفاقيات الثنائية ليست بديلاً عن النظام الدولي، بل وسيلة مؤقتة. وأن الدول الصغيرة يجب أن تتعاون فيما بينها لبناء

كتلة تفاوضية قادرة على فرض شروط عادلة.

**الفصل السابع عشر

السيادة التعليمية الرقمية والمحاكمات التعليمية: نحو اختصاص قضائي رقمي**

لا يمكن حماية الحقوق في الفضاء التعليمي الرقمي دون وجود آليات قضائية فعّالة. لكن تحديد المحكمة المختصة في الجرائم السيبرانية التعليمية يشكل تحدياً كبيراً، لأن الجريمة قد تُرتكب من دولة، عبر خوادم في دولة ثانية، وتؤثر على طالب في دولة ثالثة.

وقد اعتمدت التشريعات الوطنية عدة معايير لتحديد الاختصاص:

- **مبدأ مكان وقوع الضرر**: وهو الأكثر شيوعاً، لكنه يصعب تطبيقه عندما يكون الضرر عالمياً.

- **مبدأ جنسية الجاني**: لكنه غير عملي إذا كان الجاني مجهولاً.

- **مبدأ مكان وجود الخادم**: لكن الخوادم قد تكون في دول لا تملك علاقة بالجريمة.

وفي الممارسة، أدت هذه الغموض إلى تضارب في الأحكام. فمحكمة في دولة غربية أصدرت حكماً بحبس مواطن من دولة آسيوية لاختراقه نظاماً تعليمياً حكومياً، بينما رفضت محكمة في دولته تسليمه، بحجة أن الفعل غير مجرّم محلياً.

أما في الاتحاد الأوروبي، فقد تم توحيد قواعد الاختصاص عبر "اللائحة الأوروبية للجرائم الإلكترونية التعليمية"، التي تُلزم الدول الأعضاء بالاعتراف المتبادل بالأحكام. أما في دول أخرى، فلا تزال المحاكم تفتقر إلى الخبرة الفنية اللازمة لفهم الأدلة الرقمية التعليمية.

وفي العالم العربي، فإن معظم التشريعات لا تحدد بوضوح المحكمة المختصة بالجرائم السيبرانية التعليمية، مما يؤدي إلى تأخير العدالة أو سقوط الدعاوى.

ويخلص هذا الفصل إلى أن غياب نظام قضائي رقمي تعليمي موحد يشجع المجرمين على استغلال الثغرات القانونية، ويستدعي إنشاء "محكمة سيبرانية تعليمية دولية" تابعة للأمم

المتحدة.

**الفصل الثامن عشر

السيادة التعليمية الرقمية والبيانات التعليمية: بين الملكية الفردية والسيادة الجماعية**

تشكل البيانات التعليمية اليوم أثمن مورد في الاقتصاد الرقمي التعليمي. ولذلك، فإن السيادة التعليمية الرقمية لا تكتمل دون تحديد من يملك حق التحكم في هذه البيانات: الطالب أم الدولة أم الشركة؟

وفي الفقه الحديث، برزت ثلاث مدارس:

- **مدرسة الملكية الفردية**: التي ترى أن

الطالب هو المالك الوحيد لبياناته، ويحق له منع جمعها أو بيعها.

- **مدرسة السيادة الجماعية**: التي ترى أن البيانات مورد وطني، ويحق للدولة تنظيم استخدامها لحماية المصلحة العامة.

- **مدرسة الملكية المشتركة**: التي توازن بين الحق الفردي والمصلحة الجماعية.

وفي التطبيق، تبنت أوروبا مقاربة قريبة من الملكية الفردية عبر "اللائحة العامة لحماية البيانات" (GDPR)، التي تمنح الطلاب حق حذف بياناتهم أو تصديرها. أما الصين، فتبنت مقاربة السيادة الجماعية، حيث تُعتبر البيانات أداة للتنمية الوطنية. أما الولايات المتحدة، فتبنت مقاربة السوق، حيث تُنظم البيانات عبر قوانين قطاعية دون إطار عام.

أما في العالم العربي، فإن بعض الدول أصدرت قوانين لحماية البيانات التعليمية، لكنها تفتقر إلى آليات الإنفاذ. أما في دول أخرى، فلا توجد حتى الآن تشريعات تنظم هذا المجال.

ويؤكد هذا الفصل أن البيانات التعليمية ليست مجرد أرقام، بل تعبير عن الهوية التعليمية الفردية والجماعية. وأن السيادة التعليمية الرقمية الحقيقية تبدأ باحترام حق الطالب في التحكم بمعلوماته.

**الفصل التاسع عشر

السيادة التعليمية الرقمية والتعليم العام: حماية المجتمعات من التكنولوجيا التعليمية غير

المسؤولة**

لا يمكن فصل السيادة التعليمية الرقمية عن التعليم العام، لأن بعض التقنيات التعليمية الرقمية قد تؤدي إلى أضرار مجتمعية طويلة الأمد. فأنظمة التدريس الذكية قد تهمل القيم الوطنية، والمنصات الرقمية قد تروج لرؤى ثقافية أجنبية، والبيانات التعليمية قد تُستخدم للتمييز ضد فئات معينة.

وفي الممارسة، أدت بعض المشاريع التعليمية الرقمية إلى أضرار مجتمعية كبيرة. ففي دولة آسيوية، أدت أنظمة التدريس الذكية إلى تجاهل التاريخ الوطني. وفي دولة أفريقية، أدت المنصات الرقمية إلى انتشار محتوى ثقافي أجنبي على حساب الهوية المحلية.

ويواجه القانون الدولي غياباً في تنظيم هذا الجانب، لأن:

- لا توجد اتفاقيات دولية تنظم التأثير المجتمعي للتكنولوجيا التعليمية الرقمية.

- معظم العقود بين الدول والشركات تبقى سرية، ولا تخضع لرقابة تعليمية.

- لا توجد معايير دولية لـ"التعليم الرقمي المسؤول".

وفي المقابل، بدأت بعض الدول بوضع تشريعات. ففي الدنمارك، يُشترط على أنظمة التدريس الذكية تغطية جميع الجوانب الوطنية دون تمييز. أما في كوستاريكا، فقد تم وقف إصدار تراخيص جديدة للمنصات التعليمية الرقمية حتى يتم

تقييم تأثيرها المجتمعي.

أما في العالم العربي، فإن معظم الدول تشجع التعليم الرقمي دون دراسة تأثيره المجتمعي، مما قد يؤدي إلى أزمات هوية مستقبلية.

ويؤكد هذا الفصل أن السيادة التعليمية الرقمية يجب أن تمتد إلى حماية التعليم العام، وأن التكنولوجيا التعليمية يجب أن تُبنى على مبدأ "المسؤولية منذ التصميم".

**الفصل العشرون

السيادة التعليمية الرقمية والمستقبل: نحو مشروع اتفاقية دولية نموذجية**

بعد استعراض شامل للتحديات والتجارب، يتبين أن السيادة التعليمية الرقمية ليست خياراً، بل ضرورة وجودية في العصر الرقمي. ولتحقيقها على المستوى الدولي، يُقترح إعداد "مشروع اتفاقية دولية نموذجية بشأن السيادة التعليمية الرقمية"، تتضمن ما يلي:

أولاً: **تعريف موحد للسيادة التعليمية الرقمية** كحق للدولة في تنظيم الفضاء التعليمي الرقمي داخل نطاق ولايتها، وحماية بناها التحتية التعليمية الرقمية من التدخل الخارجي.

ثانياً: **قائمة موحدة للبنية التحتية التعليمية الرقمية**، تشمل الأنظمة الأساسية (التدريس الذكي، البيانات التعليمية، منصات توزيع

المحتوى، السجلات التعليمية الإلكترونية).

ثالثاً: **حظر التدخل السيبراني غير المشروع** في الأنظمة التعليمية، مع تعريف دقيق للتدخل على أنه كل نشاط يهدف إلى إجبار الدولة على تغيير سياستها التعليمية، أو يؤدي إلى تشويه الهوية الوطنية للطلاب.

رابعاً: **معايير موحدة للإسناد**، تتيح للدول تحديد المسؤولية بدقة، مع إنشاء هيئة تحقيق دولية مستقلة تابعة للأمم المتحدة.

خامساً: **آلية للردود المشروعة**، تحدد متى يجوز استخدام التدابير المضادة أو القوة المسلحة رداً على هجوم سيبراني تعليمي.

سادساً: **التزام الدول بحماية البيانات التعليمية**، واحترام حقوق الطلاب في الخصوصية.

سابعاً: **تشجيع التعاون الإقليمي**، عبر إنشاء شبكات استجابة سيبرانية تعليمية إقليمية.

ثامناً: **دعم الدول النامية**، عبر نقل التكنولوجيا وبناء القدرات.

تاسعاً: **إنشاء محكمة سيبرانية تعليمية دولية**، تنظر في النزاعات المتعلقة بالسيادة التعليمية الرقمية.

عاشراً: **مراجعة دورية للاتفاقية**، لمواكبة التطورات التكنولوجية.

ويُختتم هذا الفصل بالتذكير بأن السيادة التعليمية الرقمية ليست نهاية التاريخ، بل بداية مرحلة جديدة من تطور القانون الدولي، توازن بين التعليم العام والحرية الرقمية، والسيادة والتكنولوجيا، والابتكار والهوية.

**الفصل الحادي والعشرون

السيادة التعليمية الرقمية والتعليم العالي الرقمي: حماية الجامعات من الاستغلال التكنولوجي**

لا يمكن فصل السيادة التعليمية الرقمية عن حماية الجامعات من الاستغلال التكنولوجي. فمع تزايد الاعتماد على المنصات الرقمية للتعليم العالي، أصبحت الجامعات عرضة لشروط احتكارية تفرضها الشركات الكبرى. فبعض المنصات تفرض رسوماً باهظة على الدورات، بينما تفرض شركات أخرى قيوداً على المحتوى الذي يمكن نشره.

وفي الممارسة، أدت هذه الممارسات إلى:

- رفع تكاليف التعليم العالي بشكل غير متناسب.

- توجيه الطلاب نحو تخصصات تحقق أرباحاً أعلى للشركات.

- خلق اعتماد دائم على المنصات الرقمية.

ويواجه القانون الدولي غياباً في تنظيم هذا المجال، لأن:

- لا توجد اتفاقيات دولية تحمي حقوق الجامعات في الوصول العادل للتعليم الرقمي.

- معظم العقود بين الجامعات والمنصات تبقى سرية، ولا تخضع لرقابة قانونية.

- لا توجد معايير دولية لـ"الشفافية الأكاديمية الرقمية".

وفي المقابل، بدأت بعض الدول بوضع تشريعات. ففي الهند، يُلزم "قانون الشفافية الأكاديمية الرقمية" المنصات بنشر جميع البدائل المتاحة. أما في الاتحاد الأوروبي، فإن "قانون تنظيم

التعليم العالي الرقمي" يمنع الترويج للتخصصات باهظة الثمن دون ذكر البدائل.

أما في العالم العربي، فإن معظم الدول لا تزال تعتمد على سياسات تعليمية تقليدية، ولا توجد آليات قانونية لحماية الجامعات من الاستغلال التكنولوجي.

ويؤكد هذا الفصل أن السيادة التعليمية الرقمية في مجال التعليم العالي ليست مسألة تقنية، بل مسألة عدالة أكاديمية، وأن غياب الحماية القانونية لهذا القطاع يهدد استقرار النظام التعليمي بأكمله.

**الفصل الثاني والعشرون

السيادة التعليمية الرقمية والطاقة التعليمية: حماية الموارد من الاستنزاف الرقمي**

مع تزايد الاعتماد على الطاقة في التعليم الحديث — من أنظمة التبريد للمختبرات إلى مراكز البيانات التعليمية — أصبح استهلاك الكهرباء جزءاً من الاستراتيجية التعليمية. فمراكز البيانات التعليمية تستهلك كميات هائلة من الكهرباء، وقد تُستخدم كأداة ضغط على الدول ذات الموارد المحدودة.

ففي دولة صغيرة، قد يؤدي تركيز مراكز بيانات تعليمية أجنبية إلى استنزاف الشبكة الكهربائية الوطنية، مما يؤثر على الخدمات الأساسية. وفي حالات النزاع، قد تُوقف هذه المراكز فجأة عن العمل، مما يسبب خسائر تعليمية كبيرة للدولة المضيفة.

ويواجه القانون الدولي غياباً في تنظيم هذا الجانب، لأن:

- لا توجد اتفاقيات دولية تنظم استهلاك الطاقة في الأنشطة التعليمية الرقمية.

- معظم العقود بين الدول والشركات تبقى سرية، ولا تخضع لرقابة برلمانية.

- لا توجد معايير دولية لكفاءة الطاقة في المراكز التعليمية الرقمية.

وفي المقابل، بدأت بعض الدول بفرض شروط. ففي الدنمارك، يُشترط على مراكز البيانات التعليمية استخدام طاقة متجددة. أما في سنغافورة، فقد تم وقف إصدار تراخيص جديدة

لمراكز البيانات التعليمية حتى عام 2026 بسبب الضغط على الشبكة الكهربائية.

أما في العالم العربي، فإن معظم الدول تشجع إنشاء مراكز البيانات التعليمية دون دراسة تأثيرها على الموارد الوطنية، مما قد يؤدي إلى أزمات طاقة مستقبلية.

ويخلص هذا الفصل إلى أن السيادة التعليمية الرقمية يجب أن تشمل إدارة الموارد الطبيعية المستخدمة في الأنشطة التعليمية الرقمية، وأن الطاقة الكهربائية أصبحت جزءاً من الأمن القومي التعليمي.

**الفصل الثالث والعشرون

السيادة التعليمية الرقمية وسلامة الطلاب: حماية الطلاب من التلاعب الرقمي

لا يمكن فصل السيادة التعليمية الرقمية عن حماية سلامة الطلاب. فمع تزايد استخدام المنصات الرقمية في تقديم التعليم، أصبحت هذه المنصات هدفاً للهجمات التي تهدف إلى تغيير المناهج، أو تزوير نتائج الامتحانات، أو نشر معلومات مضللة عن التخصصات.

ففي عام 2024، تم اختراق منصة تعليمية في دولة أوروبية، مما أدى إلى تغيير مناهج التاريخ الوطني. وفي عام 2025، تم نشر معلومات مضللة عن التخصصات العلمية عبر منصات ذكاء اصطناعي، مما أدى إلى توجيه الطلاب نحو تخصصات غير مناسبة.

ويواجه القانون الدولي غياباً في حماية هذا القطاع، لأن:

- لا توجد اتفاقيات دولية تنظم سلامة التعليم الرقمي.

- معظم المنصات الرقمية لا تخضع لرقابة تعليمية كافية.

- لا توجد معايير دولية لشفافية المعلومات التعليمية الرقمية.

وفي المقابل، بدأت بعض الدول بوضع تشريعات. ففي الاتحاد الأوروبي، يُلزم "قانون سلامة التعليم الرقمي" المنصات بنشر معلومات دقيقة ومحدثة. أما في الولايات المتحدة، فإن "وزارة التعليم" بدأت بفحص الخوارزميات التي تحدد

المعلومات التعليمية.

أما في العالم العربي، فإن معظم التشريعات لا تغطي التهديدات الرقمية على سلامة الطلاب، ولا توجد آليات فعالة لمنع التلاعب الرقمي.

ويؤكد هذا الفصل أن السيادة التعليمية الرقمية في مجال سلامة الطلاب ليست رفاهية، بل حق إنساني أساسي، وأن سلامة التعليم الرقمي يجب أن تُعتبر جزءاً من الأمن القومي التعليمي.

**الفصل الرابع والعشرون

السيادة التعليمية الرقمية والتعليم الرقمي: بناء وعي مجتمعي كأساس للدفاع عن الحقوق**

لا يمكن تحقيق السيادة التعليمية الرقمية دون بناء وعي مجتمعي لدى الطلاب والمعلمين حول حقوقهم الرقمية وواجباتهم تجاه التعليم العام. فالتعليم الرقمي ليس مجرد نشر معلومات، بل تمكين المواطنين من المطالبة بحقوقهم والمشاركة في صنع القرار التعليمي.

ففي الدول التي يُدرّس فيها القانون التعليمي الرقمي في المدارس، يزداد الوعي بحقوق الأجيال القادمة في الهوية التعليمية. وفي المجتمعات التي تُدرّب على التكيف مع التهديدات السيبرانية، تنخفض الخسائر البشرية والمادية.

وفي الممارسة، بدأت بعض الدول بدمج التعليم

الرقمي في المناهج التعليمية. ففي فنلندا، يتعلم الأطفال من سن السادسة كيفية حماية بياناتهم التعليمية. أما في كوستاريكا، فإن "التعليم من أجل التعليم الرقمي" جزء أساسي من النظام التعليمي.

أما في الدول النامية، فإن التعليم الرقمي غالباً ما يكون مقتصراً على النخبة، أو يُقدّم عبر حملات إعلامية محدودة. وهذا يخلق فجوة في الوعي تحرم المواطنين من فهم حقوقهم.

وفي العالم العربي، فإن بعض الدول بدأت بإدخال مفاهيم التعليم الرقمي في المناهج الثانوية، لكنها تبقى اختيارية وغير منهجية.

ويؤكد هذا الفصل أن التعليم الرقمي هو استثمار

استراتيجي في العدالة، وأن الدول التي لا تستثمر فيه ستظل شعوبها عاجزة عن المطالبة بحقوقها.

**الفصل الخامس والعشرون

السيادة التعليمية الرقمية والثقافة التعليمية: حماية التراث التعليمي من الاندثار الرقمي**

لا يقتصر التغير الرقمي على الاقتصاد أو التعليم، بل يهدد أيضاً التراث التعليمي للبشرية. فالتحول إلى التعليم الرقمي قد يؤدي إلى اندثار المعرفة التقليدية، وانهيار الممارسات التعليمية المحلية، وانهيار المجتمعات التعليمية التقليدية.

ففي إفريقيا، تهدد أنظمة التدريس الذكية

الممارسات التعليمية التقليدية التي طوّرها المجتمعات عبر الأجيال. وفي أمريكا اللاتينية، يؤدي الاعتماد على المناهج الرقمية إلى تآكل المهارات التعليمية التقليدية. بل إن بعض اللغات والعادات التعليمية تندثر بسبب التحول الرقمي.

ويواجه القانون الدولي غياباً في حماية هذا البعد، لأن اتفاقيات التراث الثقافي لا تأخذ في الاعتبار التهديدات الرقمية. ومع ذلك، فإن منظمة اليونسكو بدأت تدرج "الخطر الرقمي" كسبب لإدراج المواقع التعليمية على قائمة الخطر.

أما في الدول النامية، فإن غياب الموارد يحد من قدرتها على حماية تراثها التعليمي من التهديدات الرقمية.

ويؤكد هذا الفصل أن السيادة التعليمية الرقمية الثقافية هي جزء من الهوية الوطنية، وأن غياب الحماية القانونية لهذا البعد يحوّل الشعوب إلى شهود على اندثار تاريخهم التعليمي.

**الفصل السادس والعشرون

السيادة التعليمية الرقمية والتمويل التعليمي الرقمي: حماية الدول النامية من الديون التعليمية**

مع تزايد الحاجة إلى التمويل التعليمي الرقمي، برز خطر جديد: تحويل "الديون التعليمية الرقمية" إلى أداة للاستغلال. فبعض الدول النامية تقترض مليارات الدولارات لتمويل مشاريع تعليمية رقمية، لكنها تجد نفسها عاجزة عن السداد بسبب الأزمات الاقتصادية التي تضرب اقتصادها.

ففي جزر المحيط الهادئ، أدت الأزمات الاقتصادية إلى انهيار الإيرادات التعليمية، مما جعل سداد القروض التعليمية الرقمية مستحيلاً. وفي أمريكا اللاتينية، أدت الأزمات الاقتصادية إلى انهيار الصادرات، مما زاد من عجز الموازنات.

ويواجه القانون الدولي غياباً في حماية هذه الدول، لأن:

- لا توجد آلية لإعفاء الدول من الديون في حالات الأزمات الاقتصادية.

- معظم القروض التعليمية الرقمية تأتي بشروط صارمة تزيد من عبء الديون.

- لا توجد معايير دولية لـ"التمويل التعليمي الرقمي العادل".

وفي المقابل، بدأت بعض المبادرات. ففي مؤتمر اليونسكو العالمي 2025، تم اقتراح "آلية لإعادة هيكلة الديون التعليمية"، لكنها لم تُعتمد بعد. أما في مجموعة السبع، فإن "مبادرة التمويل التعليمي الرقمي العادل" لا تزال في طور النقاش.

أما في العالم العربي، فإن معظم الدول تعتمد على قروض خارجية لتمويل مشاريع التعليم الرقمي، دون وجود ضمانات قانونية لحمايتها من المخاطر الاقتصادية.

ويخلص هذا الفصل إلى أن التمويل التعليمي

الرقمي يجب أن يكون هبة، لا ديناً، وأن الدول التي تدفع ثمن أخطاء غيرها لا ينبغي أن تُثقل بعبء الديون.

**الفصل السابع والعشرون

السيادة التعليمية الرقمية والنقل التعليمي الرقمي: حماية سلاسل التوريد من التهديدات السيبرانية**

لم يعد النقل التعليمي يعتمد فقط على الحافلات المدرسية، بل على أنظمة رقمية معقدة تدير سلاسل التوريد من المصنع إلى المدرسة. واختراق هذه الأنظمة قد يؤدي إلى تلف المواد التعليمية، أو تأخير التوزيع، أو سرقة الشحنات.

ففي عام 2024، تم اختراق نظام تتبع الشحنات التعليمية في دولة أوروبية، مما أدى إلى تلف آلاف الكتب الدراسية بسبب تأخير التوصيل. وفي عام 2025، تم سرقة شحنات أجهزة تعليمية عبر اختراق أنظمة الموانئ الرقمية.

ويواجه القانون الدولي غياباً في تصنيف سلاسل التوريد التعليمية الرقمية كجزء من "الأضرار المؤهلة للتعويض"، رغم أهميتها الاستراتيجية.

أما في الدول النامية، فإن غياب الموارد يحد من قدرتها على إعادة بناء سلاسل التوريد بعد الهجمات.

ويؤكد هذا الفصل أن السيادة التعليمية الرقمية في مجال النقل ليست مسألة تقنية، بل مسألة أمن تعليمي، وأن سلاسل التوريد التعليمية الرقمية يجب أن تُعتبر جزءاً من البنية التحتية الحيوية.

**الفصل الثامن والعشرون

السيادة التعليمية الرقمية والبحث العلمي التعليمي المفتوح: التوازن بين التعاون والحماية**

لا يمكن تحقيق التقدم في مواجهة التحديات التعليمية دون تبادل المعرفة، لكن هذا التبادل يجب أن يتم ضمن حدود تحمي المصالح الوطنية. فنشر بيانات بحثية تعليمية حساسة — مثل نماذج التعلم المقاومة — قد يُستخدم

ضد الدول النامية في المفاوضات الدولية.

ففي بعض الحالات، استخدمت الدول الصناعية البيانات التعليمية التي قدمتها الدول النامية لفرض شروط تجارية غير عادلة. بل إن بعض الشركات الخاصة تشتري هذه البيانات وتعيد بيعها بأسعار باهظة.

ويواجه القانون الدولي تحدي التوازن بين:

- حق المجتمع العلمي في الوصول إلى المعرفة.

- حق الدولة في حماية بياناتها التعليمية من الاستغلال.

أما في الدول النامية، فإن غياب سياسات واضحة يجعلها عرضة لاستغلال أبحاثها دون مقابل عادل.

ويؤكد هذا الفصل أن السيادة التعليمية الرقمية في البحث العلمي تعني وضع تصنيفات واضحة للبيانات، وتحديد ما يُسمح بنشره وما يجب حمايته، دون عزلة علمية.

**الفصل التاسع والعشرون

السيادة التعليمية الرقمية والتعاون الدولي: نحو نظام عالمي عادل للحوكمة التعليمية الرقمية**

لا يمكن لأي دولة أن تحمي سيادتها التعليمية الرقمية بمفردها، لأن التهديدات عابرة للحدود.

ولذلك، فإن التعاون الدولي ليس خياراً، بل ضرورة. لكن هذا التعاون يجب أن يكون عادلاً، لا أداة لهيمنة الدول الصناعية.

ففي المحافل الدولية، غالباً ما تُفرض معايير التعليم الرقمي من قبل الدول الصناعية، دون مراعاة قدرات الدول النامية. وهذا يخلق نظاماً غير عادل يكرس التبعية التعليمية الرقمية.

ويستدعي الحل:

- إنشاء منتدى دولي محايد لصياغة قواعد السيادة التعليمية الرقمية.

- توفير الدعم الفني والمالي للدول النامية.

- احترام التنوع في النماذج الوطنية للسيادة

التعليمية الرقمية.

أما في العالم العربي، فإن التنسيق الإقليمي لا يزال ضعيفاً، مما يحد من قدرة الدول على التفاوض ككتلة واحدة.

ويخلص هذا الفصل إلى أن النظام العالمي للحوكمة التعليمية الرقمية يجب أن يقوم على مبدأ "السيادة المشتركة"، لا "الهيمنة التعليمية الرقمية".

**الفصل الثلاثون

السيادة التعليمية الرقمية والقانون الإنساني الدولي: حماية المدنيين في النزاعات التعليمية**

مع تزايد استخدام الموارد التعليمية كسلاح في النزاعات، برز سؤال جوهري: هل يُعد تدمير البنية التحتية التعليمية الرقمية كوسيلة حربية انتهاكاً للقانون الإنساني الدولي؟ وهل يُعتبر التسبب المتعمد في أزمة تعليمية جريمة حرب؟

ففي بعض النزاعات، تم تدمير أنظمة التبريد الرقمية للمختبرات، مما أدى إلى تلفها. وفي حالات أخرى، تم اختراق منصات التوزيع التعليمية لإجبار السكان على النزوح. وكل هذه الأفعال تسبب أضراراً تعليمية طويلة الأمد.

وفي مشروع "قواعد تالين 2.0"، تم التأكيد على أن تدمير البنية التحتية التعليمية كوسيلة حربية يُعد انتهاكاً للقانون الإنساني. لكن التطبيق

العملي يبقى صعباً بسبب غموض النية وصعوبة إثبات العلاقة السببية.

أما في المحكمة الجنائية الدولية، فإن "جريمة تدمير البنية التحتية التعليمية" لا تزال قيد النقاش، ولم تُدرج بعد في النظام الأساسي.

ويؤكد هذا الفصل أن السيادة التعليمية الرقمية في زمن الحرب لا تعني التخلي عن الإنسانية، بل تعزيز حماية المدنيين من الأسلحة التعليمية الرقمية.

**الفصل الحادي والثلاثون

السيادة التعليمية الرقمية والفضاء الخارجي:

حماية الأرض من التلوث الفضائي التعليمي**

مع تزايد الأنشطة الفضائية المتعلقة بالتعليم — من الأقمار الصناعية لمراقبة التحصيل الدراسي إلى الطائرات المسيرة الفضائية لتوزيع المواد التعليمية — برز تهديد جديد: التلوث الفضائي الذي يؤثر على الأنظمة التعليمية. فحطام الأقمار الصناعية قد يعيق أنظمة الرصد التعليمي، بينما تنبعثات الصواريخ تؤثر على الغلاف الجوي الذي ينظم الاتصالات التعليمية.

وفي الممارسة، تخطط شركات خاصة لإطلاق آلاف الأقمار خلال العقد القادم لمراقبة الأداء التعليمي، دون أي تنظيم بيئي دولي. ومع ذلك، فإن معاهدات الفضاء الخارجي لا تأخذ في الاعتبار التأثيرات التعليمية لهذه الأنشطة.

ويواجه القانون الدولي إشكالية جوهرية: هل يُعد التلوث الفضائي جزءاً من "المسؤولية التعليمية الرقمية"؟ وهل يجب أن تخضع الشركات الفضائية لنفس القواعد التي تخضع لها الصناعات الأرضية؟

أما في الدول النامية، فإن غياب القدرة على الوصول إلى الفضاء يجعلها عاجزة عن المشاركة في وضع هذه القواعد، رغم تأثرها المباشر بالتلوث الفضائي.

ويؤكد هذا الفصل أن السيادة التعليمية الرقمية يجب أن تمتد إلى الفضاء الخارجي، وأن الأنشطة الفضائية التعليمية يجب أن تخضع لمبدأ "الوقاية التعليمية" مثلها مثل أي نشاط صناعي آخر.

**الفصل الثاني والثلاثون

السيادة التعليمية الرقمية والذكاء الاصطناعي التوليدي: عندما تصبح الأخبار الكاذبة سلاحاً تعليمياً**

مع ظهور الذكاء الاصطناعي التوليدي، أصبح بإمكان أي جهة إنشاء محتوى وهمي — من صور إلى مقاطع صوتية إلى فيديوهات — يبدو حقيقياً تماماً. وهذه التكنولوجيا تُستخدم اليوم كسلاح رقمي لتضليل الطلاب، وزعزعة ثقة المجتمع، وتقويض الثقة في الأنظمة التعليمية الوطنية.

ففي عام 2025، تم تداول فيديوهات مزيفة

لمعلمين وهم يحذرون من مناهج وطنية آمنة، مما أدى إلى انخفاض الثقة في النظام التعليمي وانتشار المعلومات المضللة. وفي أزمات تعليمية، تم نشر أخبار كاذبة عن نقص في المواد التعليمية الأساسية، مما أدى إلى ذعر شعبي وارتفاع غير مبرر في الأسعار.

ويواجه القانون الدولي صعوبة في التعامل مع هذه الظاهرة، لأن:

- المحتوى المزيف لا يُصنّف كـ"هجوم سيبراني تعليمي" وفق التعريفات الحالية.

- صانع المحتوى قد يكون برنامجاً، وليس شخصاً.

- نشر المحتوى يتم عبر منصات عابرة للحدود، لا تخضع لرقابة الدولة المستهدفة.

وفي المقابل، بدأت بعض الدول بوضع ضوابط. ففي الاتحاد الأوروبي، يُلزم "قانون الذكاء الاصطناعي" الشركات بوضع علامة مائية رقمية على كل محتوى مولّد آلياً. أما في الولايات المتحدة، فإن "قانون الشفافية في الوسائط الاصطناعية" يجرّم استخدام المحتوى المزيف في الحملات التضليلية التعليمية.

أما في العالم العربي، فإن معظم التشريعات لا تغطي هذا النوع من التهديدات، رغم تزايد استخدامه ضد الأنظمة التعليمية الوطنية.

ويخلص هذا الفصل إلى أن غياب تنظيم الذكاء الاصطناعي التوليدي يحوّل الفضاء الرقمي إلى ساحة حرب نفسية تعليمية، ويستدعي تعريفاً

جديداً للتدخل السيبراني التعليمي يشمل "التأثير الخبيث عبر المحتوى المزيف".

**الفصل الثالث والثلاثون

السيادة التعليمية الرقمية والبيانات الضخمة التعليمية: حماية السيادة من الاستغلال الرقمي**

مع تزايد الاعتماد على البيانات الضخمة في تحليل الأداء التعليمي، أصبحت هذه البيانات مورداً استراتيجياً. لكن الدول النامية غالباً ما تفتقر إلى القدرة على جمع وتحليل بياناتها، فتلجأ إلى شركات أجنبية تمتلك هذه القدرات.

ففي بعض الحالات، استخدمت شركات خاصة

بيانات تعليمية من دول نامية لتطوير نماذج تنبؤ تُباع بأسعار باهظة. بل إن بعض الحكومات استخدمت هذه البيانات لفرض شروط تجارية غير عادلة.

ويواجه القانون الدولي غياباً في حماية هذه البيانات، لأن:

- لا توجد اتفاقيات دولية تنظم ملكية البيانات التعليمية.

- معظم العقود بين الدول والشركات تبقى سرية.

- لا توجد معايير لـ"السيادة التعليمية الرقمية".

أما في الدول النامية، فإن غياب التشريعات

يسمح باستغلال بياناتها دون مقابل عادل.

ويؤكد هذا الفصل أن البيانات التعليمية ليست مجرد أرقام، بل أداة للعدالة، وأن الدول التي لا تحمي سيادتها الرقمية ستظل عاجزة عن المطالبة بحقوقها التعليمية.

**الفصل الرابع والثلاثون

السيادة التعليمية الرقمية والتعليم العالي التعليمي: نحو كليات وطنية للقانون التعليمي الرقمي**

لا يمكن بناء قدرات تعليمية رقمية وطنية دون مؤسسات تعليمية متخصصة تخرّج كوادر مؤهلة. فالاعتماد على الخبرات الأجنبية أو

الدورات القصيرة لا يكفي لمواجهة التهديدات المعقدة. ولذلك، فإن إنشاء كليات وطنية للقانون التعليمي الرقمي يُعد استثماراً استراتيجياً في السيادة التعليمية الرقمية.

وفي الدول الرائدة، أصبحت هذه الكليات مراكز بحث وتطوير. ففي جامعة هارفارد، يُدرّس "القانون التعليمي الرقمي الدولي". أما في جامعة أكسفورد، فإن "مركز القانون التعليمي" يدرّب المحامين على رفع الدعاوى التعليمية الرقمية.

أما في الدول النامية، فإن التعليم التعليمي الرقمي غالباً ما يكون جزءاً من أقسام علوم الحاسوب، دون تخصص كافٍ. وهذا ينتج خريجين قادرين على البرمجة، لكن غير مؤهلين لفهم الجوانب القانونية أو الاستراتيجية للأمن

التعليمي الرقمي.

وفي العالم العربي، بدأت بعض الدول بإنشاء برامج متخصصة، مثل "ماجستير الأمن التعليمي الرقمي" في جامعات الإمارات والسعودية. أما في دول أخرى، فلا تزال المناهج تفتقر إلى التحديث، ولا توجد روابط كافية بين الجامعات وقطاع الصناعة.

ويخلص هذا الفصل إلى أن التعليم العالي ليس مجرد وسيلة لتأهيل الأفراد، بل أداة لبناء هوية وطنية تعليمية رقمية، وأن الدول التي لا تستثمر في كليات القانون التعليمي الرقمي ستظل مستوردة للمعرفة، لا منتجة لها.

**الفصل الخامس والثلاثون

السيادة التعليمية الرقمية والثقافة الرقمية التعليمية: حماية الإبداع المحلي من القرصنة والتهميش**

لا يقتصر الفضاء الرقمي على البيانات والخدمات، بل يشمل أيضاً الإبداع الثقافي التعليمي: الأفلام الوثائقية، الروايات، الفنون البصرية التي تروي قصص الطلاب. ومع هيمنة المنصات العالمية على توزيع المحتوى، أصبح المبدعون المحليون عرضة للتهميش أو الاستغلال.

فمنصات البث قد تدفع تعويضات زهيدة للمبدعين المحليين، أو ترفض عرض محتواهم دون مبرر. بل وقد تُسرق أعمالهم وتُنسب إلى آخرين دون حماية قانونية كافية.

وفي المقابل، بدأت بعض الدول بوضع تشريعات لحماية المحتوى المحلي. ففي فرنسا، يُلزم القانون بوجود نسبة محددة من المحتوى الفرنسي في المنصات. أما في كوريا الجنوبية، فقد استثمرت الدولة في دعم المحتوى الرقمي المحلي، مما أدى إلى انتشاره عالمياً.

أما في العالم العربي، فإن الجهود لا تزال مجزأة، ولا توجد سياسات وطنية فعالة لدعم الإبداع الرقمي التعليمي المحلي أو حمايته من القرصنة.

ويؤكد هذا الفصل أن السيادة التعليمية الرقمية الثقافية هي جزء من الهوية الوطنية، وأن غيابها يحوّل الشعوب إلى مستهلكين سلبيين، لا مبدعين فاعلين.

**الفصل السادس والثلاثون

السيادة التعليمية الرقمية والتمويل الرقمي التعليمي: حماية العملات التعليمية من التلاعب والاحتيال**

مع ظهور العملات الرقمية التعليمية والبلوك تشين التعليمي، أصبحت الأنظمة المالية التقليدية تواجه تحديات جديدة. فالعملات الرقمية التعليمية يمكن استخدامها لغسل الأموال تحت غطاء المشاريع التعليمية، أو لتمويل مشاريع وهمية.

وفي الممارسة، أدت عمليات الاحتيال في سوق العملات الرقمية التعليمية إلى خسائر

تقدر بمليارات الدولارات. ومع ذلك، فإن التنظيم القانوني لهذا السوق يبقى ضعيفاً في كثير من الدول.

ويواجه القانون الدولي صعوبة في التعامل مع العملات الرقمية التعليمية، لأنها لا تخضع لسلطة دولة واحدة، ولا يمكن تتبع مالكيها بسهولة.

أما في الدول النامية، فإن غياب التنظيم يسمح باستغلال هذه العملات لسرقة التمويل التعليمي المخصص للمشاريع الحقيقية.

ويخلص هذا الفصل إلى أن السيادة التعليمية الرقمية في المجال المالي لا تعني منع الابتكار، بل وضع ضوابط تحمي الاقتصاد الوطني من

المخاطر غير المحسوبة.

**الفصل السابع والثلاثون

السيادة التعليمية الرقمية والبحث العلمي التعليمي المفتوح: التوازن بين التعاون والحماية**

لا يمكن تحقيق التقدم العلمي في مواجهة التحديات التعليمية دون تبادل المعرفة، لكن هذا التبادل يجب أن يتم ضمن حدود تحمي المصالح الوطنية. فنشر بيانات بحثية تعليمية حساسة — مثل نماذج التعلم المقاومة — قد يُستخدم ضد الدول النامية في المفاوضات الدولية.

ففي بعض الحالات، استخدمت الدول الصناعية

البيانات التعليمية التي قدمتها الدول النامية لفرض شروط تجارية غير عادلة. بل إن بعض الشركات الخاصة تشتري هذه البيانات وتعيد بيعها بأسعار باهظة.

ويواجه القانون الدولي تحدي التوازن بين:

- حق المجتمع العلمي في الوصول إلى المعرفة.

- حق الدولة في حماية بياناتها التعليمية من الاستغلال.

أما في الدول النامية، فإن غياب سياسات واضحة يجعلها عرضة لاستغلال أبحاثها دون مقابل عادل.

ويؤكد هذا الفصل أن السيادة التعليمية الرقمية في البحث العلمي تعني وضع تصنيفات واضحة للبيانات، وتحديد ما يُسمح بنشره وما يجب حمايته، دون عزلة علمية.

**الفصل الثامن والثلاثون

السيادة التعليمية الرقمية والتعاون الدولي: نحو نظام عالمي عادل للحوكمة التعليمية الرقمية**

لا يمكن لأي دولة أن تحمي سيادتها التعليمية الرقمية بمفردها، لأن التهديدات عابرة للحدود. ولذلك، فإن التعاون الدولي ليس خياراً، بل ضرورة. لكن هذا التعاون يجب أن يكون عادلاً، لا أداة لهيمنة الدول الصناعية.

ففي المحافل الدولية، غالباً ما تُفرض معايير التعليم الرقمي من قبل الدول الصناعية، دون مراعاة قدرات الدول النامية. وهذا يخلق نظاماً غير عادل يكرس التبعية التعليمية الرقمية.

ويستدعي الحل:

- إنشاء منتدى دولي محايد لصياغة قواعد السيادة التعليمية الرقمية.

- توفير الدعم الفني والمالي للدول النامية.

- احترام التنوع في النماذج الوطنية للسيادة التعليمية الرقمية.

أما في العالم العربي، فإن التنسيق الإقليمي لا

يزال ضعيفاً، مما يحد من قدرة الدول على التفاوض ككتلة واحدة.

ويخلص هذا الفصل إلى أن النظام العالمي للحوكمة التعليمية الرقمية يجب أن يقوم على مبدأ "السيادة المشتركة"، لا "الهيمنة التعليمية الرقمية".

**الفصل التاسع والثلاثون

السيادة التعليمية الرقمية والقانون الإنساني الدولي: حماية المدنيين في النزاعات التعليمية**

مع تزايد استخدام الموارد التعليمية كسلاح في النزاعات، برز سؤال جوهري: هل يُعد تدمير

البنية التحتية التعليمية الرقمية كوسيلة حربية انتهاكاً للقانون الإنساني الدولي؟ وهل يُعتبر التسبب المتعمد في أزمة تعليمية جريمة حرب؟

ففي بعض النزاعات، تم تدمير أنظمة التبريد الرقمية للمختبرات، مما أدى إلى تلفها. وفي حالات أخرى، تم اختراق منصات التوزيع التعليمية لإجبار السكان على النزوح. وكل هذه الأفعال تسبب أضراراً تعليمية طويلة الأمد.

وفي مشروع "قواعد تالين 2.0"، تم التأكيد على أن تدمير البنية التحتية التعليمية كوسيلة حربية يُعد انتهاكاً للقانون الإنساني. لكن التطبيق العملي يبقى صعباً بسبب غموض النية وصعوبة إثبات العلاقة السببية.

أما في المحكمة الجنائية الدولية، فإن "جريمة تدمير البنية التحتية التعليمية" لا تزال قيد النقاش، ولم تُدرج بعد في النظام الأساسي.

ويؤكد هذا الفصل أن السيادة التعليمية الرقمية في زمن الحرب لا تعني التخلي عن الإنسانية، بل تعزيز حماية المدنيين من الأسلحة التعليمية الرقمية.

**الفصل الأربعون

السيادة التعليمية الرقمية والمستقبل: رؤية استراتيجية للعقود القادمة**

في الختام، لا يمكن النظر إلى السيادة التعليمية الرقمية كظاهرة مؤقتة، بل كتحول

جوهري في مفهوم التعليم العام في القرن الحادي والعشرين. فالدول التي تبني سيادتها التعليمية الرقمية اليوم ستكون قادرة على:

- حماية طلابها من التلاعب التعليمي الرقمي.

- بناء اقتصاد تعليمي رقمي مستقل ومستدام.

- تعزيز مكانة أجيالها في النظام التعليمي العالمي.

- المشاركة الفاعلة في صياغة قواعد النظام الدولي الجديد.

أما الدول التي تتجاهل هذا التحول، فستجد نفسها رهينة للتكنولوجيا الأجنبية، وعرضة للتدخلات الخارجية، وعاجزة عن حماية مصالحها في العصر الرقمي.

ولذلك، فإن الاستثمار في السيادة التعليمية الرقمية ليس مسألة اختيار، بل مسألة بقاء.

خاتمة

بعد استعراض شامل لأبعاد السيادة التعليمية الرقمية في مختلف المجالات — من الأمن السيبراني إلى الاقتصاد، ومن الثقافة إلى التنمية — يتبين أن هذا المفهوم لم يعد رفاهية تقنية، بل ضمانة وجودية للدولة الحديثة. فالفضاء التعليمي الرقمي، رغم طبيعته غير المادية، بات ساحة للصراعات السياسية والثقافية، ولا يمكن

لأي دولة أن تحافظ على سيادتها التعليمية دون وجود قدرات رقمية وطنية فاعلة.

وقد كشف هذا العمل أن الفراغ التشريعي الدولي يشكل تهديداً مزدوجاً: فهو يسمح للدول والشركات الكبرى بفرض هيمنتها، ويترك الدول النامية عرضة للاستغلال دون حماية قانونية. ولسد هذا الفراغ، لا بد من مبادرة جماعية تبني نظاماً دولياً عادلاً يوازن بين السيادة الوطنية والتعاون العالمي.

وفي النهاية، فإن السيادة التعليمية الرقمية الحقيقية لا تُبنى على العزلة أو القمع، بل على الشفافية، والكفاءة، والثقة بين الدولة والمواطن. وهي ليست غاية بذاتها، بل وسيلة لبناء مستقبل تعليمي آمن، عادل، وإنساني.

المراجع

United Nations Educational, Scientific and Cultural Organization (UNESCO) (Constitution (1945

Convention against Discrimination in (Education (1960

General Data Protection Regulation (GDPR), Regulation (EU) 2016/679

Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Cambridge

(University Press, 2017

World Trade Organization Agreement on Trade-Related Aspects of Intellectual (Property Rights (TRIPS, 1994

International Covenant on Economic, Social (and Cultural Rights (1966

UNESCO Recommendation on Open (Educational Resources (2019

European Commission. Digital Education (Action Plan (2021–2027

Government of India. National Education (Policy (2020

Government of China. Smart Education

(2030 Plan (2022

Elrakhawi M K A. (2026). The Global Encyclopedia of Law – A Comparative Practical Study. First Edition. Ismailia: Global Legal Publications

Schmitt M N. (2023). Cyber Operations and International Law. Cambridge University Press

Rajamani L. (2025). Educational Justice and Digital Sovereignty. Oxford University Press

De Schutter O. (2023). The Right to Education in the Digital Age. Cambridge

University Press

Kloppenburg J R. (2024). Educational Sovereignty and Digital Control. University of California Press

:Official Government Sources

White House. National Strategy for Digital (Education (2024

European Commission. Digital Education (Action Plan (2023

Ministry of Education Reports on Cyber Resilience in Education Systems (Multiple (Jurisdictions, 2020–2025

:Academic Journals

(Journal of Educational Law (Oxford

International Journal of Digital Education Sovereignty

Harvard Educational Review

Stanford Technology Law Review

فهرس المحتويات

الفصل الأول

السيادة التعليمية الرقمية: من الحق في التعليم إلى المبدأ القانوني الدولي

الفصل الثاني

الفراغ القانوني الدولي في حماية الأنظمة التعليمية الرقمية

الفصل الثالث

السيادة التعليمية التقليدية مقابل السيادة التعليمية الرقمية: إعادة تشكيل المفاهيم القانونية

الفصل الرابع

البنية التحتية التعليمية الرقمية: تعريف قانوني دولي مفقود

الفصل الخامس

التلاعب السيبراني في الأنظمة التعليمية: نحو معيار قانوني دولي

الفصل السادس

المسؤولية الدولية عن الهجمات السيبرانية التعليمية: تحديات الإسناد والرقابة

الفصل السابع

الردود المشروعة على الانتهاكات السيبرانية التعليمية: بين التدابير المضادة والقوة المسلحة

الفصل الثامن

السيادة التعليمية الرقمية وبراءات الاختراع التعليمية: التوتر بين الابتكار والاستغلال

الفصل التاسع

السيادة التعليمية الرقمية في الدول النامية: تحديات القدرة والاعتماد التكنولوجي

الفصل العاشر

التنظيم الإقليمي للسيادة التعليمية الرقمية: دراسة مقارنة بين التجارب العالمية

الفصل الحادي عشر

السيادة التعليمية الرقمية والبيانات التعليمية: حماية الخصوصية الأكاديمية من الاستغلال الخارجي

الفصل الثاني عشر

السيادة التعليمية الرقمية والذكاء الاصطناعي التعليمي: عندما تصبح الخوارزميات سلطة خارج نطاق الدولة

الفصل الثالث عشر

السيادة التعليمية الرقمية والجرائم الإلكترونية التعليمية: مكافحة الاحتيال التعليمي الرقمي

الفصل الرابع عشر

السيادة التعليمية الرقمية والتربية الرقمية التعليمية: بناء وعي مجتمعي كأساس للدفاع السيبراني

الفصل الخامس عشر

السيادة التعليمية الرقمية والبحث العلمي التعليمي: نحو استقلال تكنولوجي وطني

الفصل السادس عشر

السيادة التعليمية الرقمية والاتفاقيات الثنائية: هل يمكن للدول الصغيرة أن تحمي نفسها؟

الفصل السابع عشر

السيادة التعليمية الرقمية والمحاكمات التعليمية: نحو اختصاص قضائي رقمي

الفصل الثامن عشر

السيادة التعليمية الرقمية والبيانات التعليمية: بين الملكية الفردية والسيادة الجماعية

الفصل التاسع عشر

السيادة التعليمية الرقمية والتعليم العام: حماية المجتمعات من التكنولوجيا التعليمية غير المسؤولة

الفصل العشرون

السيادة التعليمية الرقمية والمستقبل: نحو مشروع اتفاقية دولية نموذجية

الفصل الحادي والعشرون

السيادة التعليمية الرقمية والتعليم العالي الرقمي: حماية الجامعات من الاستغلال التكنولوجي

الفصل الثاني والعشرون

السيادة التعليمية الرقمية والطاقة التعليمية: حماية الموارد من الاستنزاف الرقمي

الفصل الثالث والعشرون

السيادة التعليمية الرقمية وسلامة الطلاب: حماية الطلاب من التلاعب الرقمي

الفصل الرابع والعشرون

السيادة التعليمية الرقمية والتعليم الرقمي: بناء وعي مجتمعي كأساس للدفاع عن الحقوق

الفصل الخامس والعشرون

السيادة التعليمية الرقمية والثقافة التعليمية: حماية التراث التعليمي من الاندثار الرقمي

الفصل السادس والعشرون

السيادة التعليمية الرقمية والتمويل التعليمي الرقمي: حماية الدول النامية من الديون التعليمية

الفصل السابع والعشرون

السيادة التعليمية الرقمية والنقل التعليمي الرقمي: حماية سلاسل التوريد من التهديدات السيبرانية

الفصل الثامن والعشرون

السيادة التعليمية الرقمية والبحث العلمي التعليمي المفتوح: التوازن بين التعاون والحماية

الفصل التاسع والعشرون

السيادة التعليمية الرقمية والتعاون الدولي: نحو نظام عالمي عادل للحوكمة التعليمية الرقمية

الفصل الثلاثون

السيادة التعليمية الرقمية والقانون الإنساني الدولي: حماية المدنيين في النزاعات التعليمية

الفصل الحادي والثلاثون

السيادة التعليمية الرقمية والفضاء الخارجي: حماية الأرض من التلوث الفضائي التعليمي

الفصل الثاني والثلاثون

السيادة التعليمية الرقمية والذكاء الاصطناعي التوليدي: عندما تصبح الأخبار الكاذبة سلاحاً تعليمياً

الفصل الثالث والثلاثون

السيادة التعليمية الرقمية والبيانات الضخمة التعليمية: حماية السيادة من الاستغلال الرقمي

الفصل الرابع والثلاثون

السيادة التعليمية الرقمية والتعليم العالي التعليمي: نحو كليات وطنية للقانون التعليمي الرقمي

الفصل الخامس والثلاثون

السيادة التعليمية الرقمية والثقافة الرقمية التعليمية: حماية الإبداع المحلي من القرصنة والتهميش

الفصل السادس والثلاثون

السيادة التعليمية الرقمية والتمويل الرقمي التعليمي: حماية العملات التعليمية من التلاعب والاحتيال

الفصل السابع والثلاثون

السيادة التعليمية الرقمية والبحث العلمي التعليمي المفتوح: التوازن بين التعاون والحماية

الفصل الثامن والثلاثون

السيادة التعليمية الرقمية والتعاون الدولي: نحو نظام عالمي عادل للحوكمة التعليمية الرقمية

الفصل التاسع والثلاثون

السيادة التعليمية الرقمية والقانون الإنساني الدولي: حماية المدنيين في النزاعات التعليمية

الفصل الأربعون

السيادة التعليمية الرقمية والمستقبل: رؤية استراتيجية للعقود القادمة

خاتمة

تم بحمد الله وتوفيقه

تأليف د. محمد كمال عرفه الرخاوي

الباحث والمستشار القانوني

المحاضر الدولي في القانون

جميع الحقوق محفوظة للمؤلف

يحظر نسخ أو طبع أو نشر أو توزيع أو اقتباس أي جزء من هذا العمل دون إذن كتابي صريح من المؤلف