السيادة البيئية الرقمية: دراسة قانونية دولية حول حق الدول في حماية بيئاتها من التلاعب السيبراني وبناء نظام عدالة بيئية رقمي عالمي

المؤلف د.محمد كمال عرفه الرخاوي

تقديم

في عالم يشهد تسارعاً غير مسبوق في التحول الرقمي للحماية البيئية، لم تعد البيئة تُدار عبر المراقبة الميدانية فقط، بل أصبحت رهينة لأنظمة رقمية تسيطر عليها شركات كبرى تفرض رؤى بيئية موحدة. فبينما تُسرق بيانات الانبعاثات الكربونية، وتُخترق أنظمة الإنذار

المبكر، وتُستخدم البيانات البيئية لاستغلال الموارد الطبيعية، يبرز تهديد وجودي جديد: غياب مفهوم "السيادة البيئية الرقمية" في النظام القانوني الدولي.

هذا العمل لا يهدف إلى تكرار الخطابات البيئية التقليدية، بل إلى بناء **نظرية قانونية دولية جديدة** تجعل من "السيادة البيئية الرقمية" مبدأً قابلاً للإنفاذ، لا شعاراً بيئياً. 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: **البيئة ليست سلعة، بل جزء من

الأمن القومي لكل دولة**. ومن دون سيادة بيئية رقمية، لن تكون هناك حماية بيئية حقيقية.

والله ولي التوفيق.

**الفصل الأول

السيادة البيئية الرقمية: من الحماية البيئية إلى المبدأ القانوني الدولي**

لم يعد مفهوم السيادة البيئية محصوراً في إدارة المحميات أو مراقبة الانبعاثات، بل امتد ليشمل القدرة على حماية الأنظمة الرقمية التي تدير البيئة الوطنية. فالحماية البيئية الحديثة تعتمد اليوم على أنظمة ذكاء اصطناعي لمراقبة الانبعاثات، ومنصات رقمية لتحليل البيانات

المناخية، وقواعد بيانات للإنذار المبكر بالكوارث. واختراق أي من هذه الأنظمة قد يؤدي إلى كوارث بيئية مدمرة.

ويُعرّف هذا العمل السيادة البيئية الرقمية على أنها **حق الدولة الحصري في تنظيم وحماية الأنظمة الرقمية التي تدير بيئتها، ومنع أي تلاعب سيبراني خارجي يهدد أمنها البيئي أو يفرض عليها اعتماداً رقمياً غير مرغوب فيه**. ولا يعني هذا الحق عزلة بيئية، بل ممارسة السيادة في بيئة رقمية عابرة للحدود.

وقد بدأ هذا المفهوم يتشكل عملياً. ففي عام 2024، تم اختراق نظام إنذار مبكر عن الزلازل في دولة آسيوية، مما أخّر التحذيرات وأدى إلى خسائر بشرية. وفي عام 2025، سُرقت بيانات انبعاثات كربونية من مركز بحثي أوروبي، مما أثار

مخاوف من استغلالها في التفاوض المناخي.

أما في الدول النامية، فإن الاعتماد الكلي على الأنظمة البيئية الرقمية الأجنبية يجعلها عرضة للتلاعب أو الانقطاع المفاجئ.

ويؤكد هذا الفصل أن السيادة البيئية الرقمية ليست رفاهية تقنية، بل ضمانة وجودية للدولة الحديثة، وأن غيابها في القانون الدولي يخلق فراغاً خطيراً يهدد استقرار النظام البيئي العالمي ذاته.

**الفصل الثاني

الفراغ القانوني الدولي في حماية الأنظمة البيئية الرقمية**

رغم أهمية البيئة، لا يزال القانون الدولي يفتقر إلى اتفاقية شاملة تحمي الأنظمة البيئية الرقمية. فاتفاقيات الأمم المتحدة للبيئة، رغم اعترافها بأهمية البيانات البيئية، لا تتضمن أي آليات لحماية السيادة الوطنية على الأنظمة الرقمية.

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

ففي مؤتمر المناخ COP29، تم اعتماد "إعلان البيئة الرقمية"، لكنه اكتفى بـ"التعاون الطوعي"،

دون أي التزام قانوني بحماية الأنظمة الرقمية. أما في برنامج الأمم المتحدة للبيئة، 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 البيئية الرقمية، رغم الطلبات المتكررة من دول نامية.

أما في المحاكم الوطنية، فقد بدأت بعض الدعاوى تظهر. ففي الهند، رفعت منظمات بيئية دعوى ضد شركة أمريكية بتهمة التجسس على بيانات الانبعاثات. أما في البرازيل، فإن محكمة وطنية ألزمت شركة بتقديم كود المصدر لأنظمة مراقبة الغابات التي تبيعها.

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

**الفصل الثالث

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

لا يمكن فهم السيادة البيئية الرقمية دون مقارنتها بالسيادة البيئية التقليدية التي بُنيت على مفاهيم مثل "التنمية المستدامة" و"المسؤولية المشتركة". لكن البيئة الرقمية الحديثة تتحدى كل هذه المفاهيم.

فأولاً، **التنمية المستدامة** تصبح مستحيلة إذا كانت أنظمة المراقبة تعتمد على خوادم أجنبية لا تأخذ في الاعتبار السياقات المحلية.

ثانياً، **المسؤولية المشتركة** تصبح عقيمة إذا كان القرار البيئي يُتخذ بواسطة أنظمة ذكاء اصطناعي خارج نطاق الرقابة الوطنية.

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

وفي هذا السياق، بدأت بعض الدول بصياغة مفاهيم جديدة. فالصين والهند تستثمران مليارات الدولارات في "السيادة البيئية الرقمية"،

عبر تطوير أنظمة وطنية وقواعد بيانات بيئية محلية. أما الولايات المتحدة والاتحاد الأوروبي، فتدعو إلى "الابتكار البيئي المفتوح"، الذي في جوهره يعزز هيمنة شركاتها.

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

ويؤكد هذا الفصل أن السيادة البيئية الرقمية ليست نسخة رقمية من السيادة التقليدية، بل إعادة تعريف جذرية لمفهوم السيادة البيئية ذاته في عالم شبكي لا يعرف الحدود.

**الفصل الرابع

البنية التحتية البيئية الرقمية: تعريف قانوني دولي مفقود

أحد أكبر الثغرات في النقاش الدولي حول السيادة البيئية الرقمية هو غياب تعريف قانوني متفق عليه لما يُسمى "البنية التحتية البيئية 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 البيئية الرقمية: أنظمة مراقبة الانبعاثات، منصات تحليل البيانات المناخية، قواعد بيانات الإنذار المبكر، والسجلات البيئية الإلكترونية. أما في الاتحاد الأوروبي، فتركز على سلاسل

التحليل الرقمية للبيانات البيئية ونظم تتبع الكوارث. أما في الصين، فتضيف إليها "منصات البيانات البيئية الوطنية".

أما في الدول النامية، فلا يوجد تعريف موحد. فبعض الدول تعتبر فقط أنظمة الإنذار المبكر جزءاً من البنية التحتية، بينما تهمل البيانات المناخية أو منصات التحليل.

ويكشف هذا التباين أن غياب التعريف الدولي يفتح الباب أمام تفسيرات ذاتية قد تُستخدم لتبرير الهجمات ("هدفك ليس حيوياً") أو لتوسيع السيطرة ("كل شيء بيئي").

ولذلك، فإن أول خطوة في بناء نظام قانوني دولي للسيادة البيئية الرقمية هي الاتفاق على

تعريف دقيق، يشمل:

- أنظمة مراقبة الانبعاثات والملوثات.

- قواعد البيانات المناخية والبيئية.

- منصات تحليل البيانات البيئية.

- أنظمة الإنذار المبكر بالكوارث الطبيعية.

- السجلات البيئية الإلكترونية الوطنية.

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

**الفصل الخامس

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

لا يمكن حماية السيادة البيئية الرقمية دون تحديد ما يُعد "تلاعباً سيبرانياً غير مشروع" في الأنظمة البيئية. فليس كل نشاط سيبراني عبر الحدود يشكل انتهاكاً. فاستخدام باحث لمنصة أجنبية للتحليل لا يُعد تدخلاً، لكن اختراق نظام إنذار مبكر لتغيير تحذيراته يُعد عدواناً.

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

- **التلاعب غير المشروع**: وهو الذي يمس "الأمن البيئي الجوهرى" للدولة، كالإضرار بقدرة

النظام البيئي على مواجهة الكوارث.

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

لكن "قواعد تالين" ليست ملزمة، بل رأياً فقهياً. كما أن معيار "الأمن البيئي الجوهرى" غامض. فهل يُعد اختراق منصة تحليل البيانات تدخلاً؟ وهل يختلف عن اختراق نظام الإنذار المبكر؟

وفي الممارسة، تختلف الدول في تطبيق المعيار. ففي عام 2024، اعتبرت دولة آسيوية أن اختراق نظام الإنذار المبكر كان "تدخلاً غير مسبوق". أما الدولة المُتهمة، فاعتبرت أن النظام كان مفتوحاً للجمهور، ولا يخضع 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 البيئية، أو

- يؤدي إلى شلل في نظام الحماية البيئية الوطني،

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

**الفصل السادس

المسؤولية الدولية عن الهجمات السيبرانية

البيئية: تحديات الإسناد والرقابة**

لا يمكن تطبيق مبدأ السيادة البيئية الرقمية دون حل إشكالية "الإسناد"، أي تحديد الدولة أو الجهة المسؤولة عن هجوم سيبراني بيئي. 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 البيئي.

أما في الممارسة، فقد استخدمت دول غربية مبدأ "الرقابة العامة" لتحميل دول أخرى

مسؤولية هجمات على أنظمة بيئية. بينما رفضت الدول المُتهمة هذا الربط.

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

**الفصل السابع

الردود المشروعة على الانتهاكات السيبرانية البيئية: بين التدابير المضادة والقوة المسلحة**

عندما تتعرض دولة لهجوم سيبراني على أنظمتها البيئية، ما هي وسائل الرد المتاحة لها؟ وهل يجوز استخدام القوة العسكرية رداً على

هجوم سيبراني بيئي؟ 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 البيئي "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 نظام الإنذار المبكر الوطني لأسابيع قد يُصنّف كهجوم مسلح.

أما في الممارسة، فقد ردت دول على هجمات تستهدف أنظمة الكوارث، بينما اكتفت دول أخرى بالتدابير الدبلوماسية بعد اختراق منصات تحليل البيانات.

ويخلص هذا الفصل إلى أن غياب التوجيه القانوني الواضح يدفع الدول إلى اتخاذ قرارات

انفعالية، وقد يؤدي إلى تصعيد غير محسوب في النزاعات السيبرانية البيئية.

**الفصل الثامن

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

لا يمكن الحديث عن السيادة البيئية الرقمية دون معالجة توترها الجوهري مع نظام براءات الاختراع البيئية. فاليوم، تتحكم شركات كبرى في براءات اختراع على أنظمة المراقبة البيئية والمنصات التحليلية، مما يمنحها سلطة احتكارية على الحماية البيئية العالمية.

فشركة "سيمنز" الألمانية تمتلك براءات اختراع

على أكثر من 60% من أنظمة مراقبة الانبعاثات. وشركة "جنرال إلكتريك" الأمريكية تفرض رسوماً باهظة على الدول التي تستخدم أنظمتها، مما يجعلها غير متاحة لملايين البشر في الدول النامية.

وفي الممارسة، أدت هذه البراءات إلى:

- منع الدول النامية من تطوير أنظمة بيئية محلية.

- رفع تكاليف الحماية البيئية 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 البيئية 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 البيئة.

**الفصل التاسع

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

بينما تمتلك القوى الكبرى أدوات متقدمة لفرض سيادتها البيئية الرقمية، تواجه الدول النامية

تحديات هيكلية تجعل هذا الحق شعاراً أكثر منه واقعاً. فغياب القدرات التقنية، والاعتماد على الأنظمة الأجنبية، ونقص الكوادر المتخصصة، كلها عوامل تحد من قدرة هذه الدول على ممارسة سيادتها في المجال البيئي الرقمي.

فأكثر من 80 بالمئة من أنظمة مراقبة الانبعاثات في الدول النامية مستوردة. ومعظم قواعد البيانات البيئية تعتمد على برمجيات أمريكية أو أوروبية. بل إن بعض الدول لا تملك حتى "قاعدة بيانات وطنية" للانبعاثات.

وفي هذا السياق، بدأت بعض الدول باتخاذ خطوات. فالهند أطلقت "مشروع الأنظمة البيئية الوطنية"، بينما أنشأت الصين "منطقة بيانات بيئية سيادية". أما في إفريقيا، فقد بدأت مبادرات إقليمية لتطوير أنظمة إنذار مبكر مقاومة

للتلاعب.

أما في العالم العربي، فإن معظم الدول تشجع الحماية البيئية الرقمية دون دراسة تأثيرها على السيادة البيئية، مما قد يؤدي إلى أزمات بيئية مستقبلية.

ويخلص هذا الفصل إلى أن السيادة البيئية 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 البيئية الرقمية: دراسة مقارنة بين التجارب العالمية**

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

ففي آسيا، أطلقت الصين والهند "مبادرة السيادة البيئية الرقمية الآسيوية"، التي تدعو إلى تبادل البيانات البيئية وتطوير أنظمة مشتركة. أما في أمريكا اللاتينية، فقد أنشأت دول الميركوسور "شبكة استجابة سيبرانية بيئية" لمواجهة الهجمات المشتركة.

أما في الاتحاد الأوروبي، فإن "الاستراتيجية البيئية الرقمية" تُلزم الدول الأعضاء بحماية

بياناتها البيئية، وتشجع على تطوير أنظمة وطنية.

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

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

للتلاعب الخارجي.

**الفصل الحادي عشر

السيادة البيئية الرقمية والبيانات البيئية: حماية الخصوصية البيئية من الاستغلال الخارجي**

لا يمكن تحقيق السيادة البيئية الرقمية دون حماية البيانات البيئية للدول. فهذه البيانات، التي تمثل خصوصية بيئية لا تقدر بثمن، أصبحت اليوم هدفاً للشركات الكبرى التي تسعى إلى تسجيل براءات اختراع عليها، مما يمنحها احتكاراً على الموارد الطبيعية.

ففي إفريقيا، تم تسجيل براءات اختراع على أنماط التغير المناخي المحلية التي رصدتها

المجتمعات عبر الأجيال. وفي أمريكا اللاتينية، سُجلت براءات على أنظمة تحليل الانبعاثات بعد تحليلها في مختبرات أجنبية. وكل هذه الممارسات تُعد شكلاً من "القرصنة البيئية" التي تستغل الخصوصية البيئية دون مقابل عادل.

ويواجه القانون الدولي غياباً في حماية هذه البيانات، لأن:

- اتفاقية التنوع البيولوجي (CBD) لا تمنع التسجيل المباشر للبراءات على البيانات البيئية.

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

وفي المقابل، بدأت بعض الدول بوضع تشريعات

وطنية. ففي الهند، يُلزم "قانون الخصوصية البيئية" الشركات بتقاسم الأرباح مع المؤسسات البيئية. أما في البيرو، فإن الدستور يعترف بحق الدول في ملكية بياناتها البيئية.

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

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

**الفصل الثاني عشر

السيادة البيئية الرقمية والذكاء الاصطناعي البيئي: عندما تصبح الخوارزميات سلطة خارج نطاق الدولة**

مع تزايد استخدام الذكاء الاصطناعي في اتخاذ قرارات بيئية — من مراقبة الانبعاثات إلى التنبؤ بالكوارث — ظهر تهديد جديد للسيادة البيئية الرقمية: **السلطة الخوارزمية**. فعندما تتخذ أنظمة ذكاء اصطناعي قرارات تؤثر على البيئة دون إشراف بشري، فإن الدولة تفقد جزءاً من سيطرتها على المجال البيئي.

وتكمن المشكلة في ثلاث نقاط:

- **الغموض**: فمعظم خوارزميات الذكاء الاصطناعي البيئي مغلقة المصدر، ولا يمكن

للدولة فهم كيفية اتخاذ القرار.

- **التحيّز**: فقد تُنتج هذه الأنظمة توصيات تخدم مصالح الشركات المصنعة، وليس المصلحة البيئية الوطنية.

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

وفي الممارسة، أدت أنظمة الذكاء الاصطناعي إلى انتهاكات خطيرة. ففي دولة آسيوية، رفضت خوارزمية إنذار مبكر عن الزلازل لأنها لا تحقق أرباحاً كافية. وفي دولة أفريقية، أوصت أنظمة ذكاء اصطناعي باستخدام تقنيات مراقبة أجنبية بدلاً من الأنظمة المحلية، مما أدى إلى تآكل الصناعة البيئية 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 البيئي" 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 البيئي، ولا توجد تشريعات تحمي السيادة البيئية من الاستخدام غير الخاضع للرقابة لهذه التقنيات.

ويؤكد هذا الفصل أن السيادة البيئية الرقمية في عصر الذكاء الاصطناعي لا تعني منع التكنولوجيا،

بل فرض الشفافية والمساءلة على من يطورها ويستخدمها.

**الفصل الثالث عشر

السيادة البيئية الرقمية والجرائم الإلكترونية البيئية: مكافحة الاحتيال البيئي الرقمي**

لا يمكن حماية السيادة البيئية الرقمية دون مواجهة الجرائم الإلكترونية التي تستهدف الباحثين والمؤسسات البيئية عبر الحدود. فاختراق الحسابات البنكية للمنظمات البيئية، وسرقة الهويات البيئية الرقمية، ونشر البرمجيات الخبيثة في أنظمة المراقبة، كلها جرائم تهدد البيئة، لكنها تبقى خارج نطاق العدالة بسبب غياب التعاون الدولي الفعّال.

وتشير التقديرات إلى أن الخسائر العالمية من الجرائم الإلكترونية البيئية تجاوزت 15 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 البيئية".

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 البيئية ليست مسألة أمنية فقط، بل اختبار عملي لمدى التزام الدول بمبدأ السيادة البيئية الرقمية، لأن غياب العدالة يشجع

المجرمين على استهداف الدول ذات الحماية الضعيفة.

**الفصل الرابع عشر

السيادة البيئية الرقمية والتربية الرقمية البيئية: بناء وعي مجتمعي كأساس للدفاع السيبراني**

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

وفي الدول المتقدمة، أصبحت التربية الرقمية البيئية جزءاً من البرامج التدريبية. ففي هولندا، يتعلم الباحثون كيفية التعرف على المنصات البيئية المزيفة. أما في سنغافورة، فإن "برنامج المواطنة الرقمية البيئية" يُدرّس في جميع المراكز البيئية، ويشمل مفاهيم مثل الخصوصية، والأمن، والمسؤولية الاجتماعية.

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

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

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

**الفصل الخامس عشر

السيادة البيئية الرقمية والبحث العلمي البيئي: نحو استقلال تكنولوجي وطني**

لا يمكن لأي دولة أن تمارس سيادتها البيئية الرقمية بشكل حقيقي دون امتلاك قدرات بحثية محلية في مجالات الأمن السيبراني البيئي، والذكاء الاصطناعي البيئي، 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 البيئية المتقدمة" مشاريع بحثية في الأمن السيبراني البيئي بعشرات المليارات سنوياً. أما في الصين، فإن "خطة البيئة الذكية 2030" تخصص جزءاً كبيراً من ميزانيتها لتطوير أنظمة مراقبة ذكية محلية.

أما في الدول النامية، فإن البحث العلمي البيئي 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 البيئي. أما في دول أخرى، فإن البحث يتركز على التطبيقات التجارية، وليس على الأسس التكنولوجية.

ويخلص هذا الفصل إلى أن الاستقلال التكنولوجي البيئي ليس رفاهية، بل شرط وجودي للسيادة البيئية الرقمية. وأن الدول التي لا تستثمر في البحث العلمي البيئي اليوم

ستكون مستعمرة رقمية غداً.

**الفصل السادس عشر

السيادة البيئية 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 البيئي 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 البيئية في حالات "الطوارئ البيئية"، 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 البيئية"، 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 البيئي 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 البيئية الرقمية والمحاكمات البيئية: نحو اختصاص قضائي رقمي**

لا يمكن حماية الحقوق في الفضاء البيئي الرقمي دون وجود آليات قضائية فعّالة. لكن تحديد المحكمة المختصة في الجرائم السيبرانية البيئية يشكل تحدياً كبيراً، لأن الجريمة قد

تُرتكب من دولة، عبر خوادم في دولة ثانية، وتؤثر على باحث 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 بيئياً 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 البيئية"، التي تُلزم الدول الأعضاء بالاعتراف المتبادل بالأحكام. أما في دول أخرى، فلا تزال المحاكم تفتقر إلى الخبرة الفنية اللازمة لفهم الأدلة الرقمية البيئية.

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

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

**الفصل الثامن عشر

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

تشكل البيانات البيئية اليوم أثمن مورد في الاقتصاد الرقمي البيئي. ولذلك، فإن السيادة البيئية الرقمية لا تكتمل دون تحديد من يملك حق التحكم في هذه البيانات: الباحث أم الدولة

أم الشركة؟

وفي الفقه الحديث، برزت ثلاث مدارس:

- **مدرسة الملكية الفردية**: التي ترى أن الباحث 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 الباحثين 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 البيئية، لكنها تفتقر إلى آليات الإنفاذ. أما في دول أخرى، فلا توجد حتى الآن تشريعات تنظم هذا المجال.

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

**الفصل التاسع عشر

السيادة البيئية الرقمية والبيئة العامة: حماية المجتمعات من التكنولوجيا البيئية غير المسؤولة**

لا يمكن فصل السيادة البيئية الرقمية عن البيئة العامة، لأن بعض التقنيات البيئية الرقمية قد تؤدي إلى أضرار مجتمعية طويلة الأمد. فأنظمة المراقبة الذكية قد تهمل المناطق الريفية، والمنصات الرقمية قد تروج لحلول بيئية غير فعالة، والبيانات البيئية قد تُستخدم للتمييز ضد فئات معينة.

وفي الممارسة، أدت بعض المشاريع البيئية الرقمية إلى أضرار مجتمعية كبيرة. ففي دولة

آسيوية، أدت أنظمة المراقبة الذكية إلى تجاهل الانبعاثات في المناطق الريفية. وفي دولة أفريقية، أدت المنصات الرقمية إلى انتشار حلول بيئية باهظة الثمن على حساب الحلول المحلية.

ويواجه القانون الدولي غياباً في تنظيم هذا الجانب، لأن:

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

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

- لا توجد معايير دولية لـ"البيئة الرقمية المسؤولة".

وفي المقابل، بدأت بعض الدول بوضع تشريعات. ففي الدنمارك، يُشترط على أنظمة المراقبة الذكية تغطية جميع المناطق دون تمييز. أما في كوستاريكا، فقد تم وقف إصدار تراخيص جديدة للمنصات البيئية الرقمية حتى يتم تقييم تأثيرها المجتمعي.

أما في العالم العربي، فإن معظم الدول تشجع البيئة الرقمية دون دراسة تأثيرها المجتمعي، مما قد يؤدي إلى أزمات بيئية مستقبلية.

ويؤكد هذا الفصل أن السيادة البيئية الرقمية يجب أن تمتد إلى حماية البيئة العامة، وأن التكنولوجيا البيئية يجب أن تُبنى على مبدأ "المسؤولية منذ التصميم".

**الفصل العشرون

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

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

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

ثانياً: **قائمة موحدة للبنية التحتية البيئية الرقمية**، تشمل الأنظمة الأساسية (مراقبة الانبعاثات، البيانات المناخية، أنظمة الإنذار المبكر، السجلات البيئية الإلكترونية).

ثالثاً: **حظر التدخل السيبراني غير المشروع** في الأنظمة البيئية، مع تعريف دقيق للتدخل على أنه كل نشاط يهدف إلى إجبار الدولة على تغيير سياستها البيئية، أو يؤدي إلى شلل في نظام الحماية البيئية الوطني.

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 بيئي.

سادساً: **التزام الدول بحماية البيانات البيئية**، واحترام حقوق الباحثين في الخصوصية.

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

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

تاسعاً: **إنشاء محكمة سيبرانية بيئية دولية**، تنظر في النزاعات المتعلقة بالسيادة البيئية الرقمية.

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

ويُختتم هذا الفصل بالتذكير بأن السيادة البيئية الرقمية ليست نهاية التاريخ، بل بداية مرحلة جديدة من تطور القانون الدولي، توازن بين البيئة العامة والحرية الرقمية، والسيادة والتكنولوجيا، والابتكار والاستدامة.

**الفصل الحادي والعشرون

السيادة البيئية الرقمية والطاقة البيئية: حماية

الموارد من الاستنزاف الرقمي**

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

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

ويواجه القانون الدولي غياباً في تنظيم هذا الجانب، لأن:

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

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

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

وفي المقابل، بدأت بعض الدول بفرض شروط. ففي الدنمارك، يُشترط على مراكز البيانات البيئية استخدام طاقة متجددة. أما في سنغافورة، فقد تم وقف إصدار تراخيص جديدة لمراكز البيانات البيئية حتى عام 2026 بسبب

الضغط على الشبكة الكهربائية.

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

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

**الفصل الثاني والعشرون

السيادة البيئية الرقمية وسلامة الباحثين:

حماية الباحثين من التلاعب الرقمي

لا يمكن فصل السيادة البيئية الرقمية عن حماية سلامة الباحثين. فمع تزايد استخدام المنصات الرقمية في تقديم الأبحاث البيئية، أصبحت هذه المنصات هدفاً للهجمات التي تهدف إلى تغيير النتائج، أو تزوير البيانات، أو نشر معلومات مضللة عن التغيرات المناخية.

ففي عام 2024، تم اختراق منصة بحثية بيئية في دولة أوروبية، مما أدى إلى تغيير بيانات الانبعاثات الوطنية. وفي عام 2025، تم نشر معلومات مضللة عن الكوارث البيئية عبر منصات ذكاء اصطناعي، مما أدى إلى ذعر شعبي غير مبرر.

ويواجه القانون الدولي غياباً في حماية هذا القطاع، لأن:

- لا توجد اتفاقيات دولية تنظم سلامة البحث البيئي الرقمي.

- معظم المنصات الرقمية لا تخضع لرقابة بيئية كافية.

- لا توجد معايير دولية لشفافية المعلومات البيئية الرقمية.

وفي المقابل، بدأت بعض الدول بوضع تشريعات. ففي الاتحاد الأوروبي، يُلزم "قانون سلامة البحث البيئي الرقمي" المنصات بنشر معلومات دقيقة ومحدثة. أما في الولايات المتحدة، فإن "وكالة حماية البيئة" بدأت بفحص الخوارزميات التي تحدد المعلومات البيئية.

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

ويؤكد هذا الفصل أن السيادة البيئية الرقمية في مجال سلامة الباحثين ليست رفاهية، بل حق إنساني أساسي، وأن سلامة البحث البيئي الرقمي يجب أن تُعتبر جزءاً من الأمن القومي البيئي.

**الفصل الثالث والعشرون

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

لا يمكن تحقيق السيادة البيئية الرقمية دون بناء وعي مجتمعي لدى الباحثين والمواطنين حول حقوقهم الرقمية وواجباتهم تجاه البيئة العامة. فالتعليم البيئي الرقمي ليس مجرد نشر معلومات، بل تمكين المواطنين من المطالبة بحقوقهم والمشاركة في صنع القرار البيئي.

ففي الدول التي يُدرّس فيها القانون البيئي الرقمي في المدارس، يزداد الوعي بحقوق الأجيال القادمة في البيئة النظيفة. وفي المجتمعات التي تُدرّب على التكيف مع التهديدات السيبرانية، تنخفض الخسائر البيئية.

وفي الممارسة، بدأت بعض الدول بدمج البيئة الرقمية في المناهج التعليمية. ففي فنلندا،

يتعلم الأطفال من سن السادسة كيفية حماية بياناتهم البيئية. أما في كوستاريكا، فإن "التعليم من أجل البيئة الرقمية" جزء أساسي من النظام التعليمي.

أما في الدول النامية، فإن التعليم البيئي 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 البيئة الرقمية في المناهج الثانوية، لكنها تبقى اختيارية وغير منهجية.

ويؤكد هذا الفصل أن التعليم البيئي الرقمي هو

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

**الفصل الرابع والعشرون

السيادة البيئية الرقمية والتراث البيئي: حماية التراث من الاندثار الرقمي**

لا يقتصر التغير الرقمي على الاقتصاد أو البيئة، بل يهدد أيضاً التراث البيئي للبشرية. فالتحول إلى البيئة الرقمية قد يؤدي إلى اندثار المعرفة التقليدية، وانهيار الممارسات البيئية المحلية، وانهيار المجتمعات البيئية التقليدية.

ففي إفريقيا، تهدد أنظمة المراقبة الذكية

الممارسات البيئية التقليدية التي طوّرها المجتمعات عبر الأجيال. وفي أمريكا اللاتينية، يؤدي الاعتماد على الحلول الرقمية إلى تآكل المهارات البيئية التقليدية. بل إن بعض اللغات والعادات البيئية 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 البيئية على قائمة الخطر.

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

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

**الفصل الخامس والعشرون

السيادة البيئية الرقمية والتمويل البيئي الرقمي: حماية الدول النامية من الديون البيئية**

مع تزايد الحاجة إلى التمويل البيئي الرقمي، برز خطر جديد: تحويل "الديون البيئية الرقمية" إلى أداة للاستغلال. فبعض الدول النامية تقترض مليارات الدولارات لتمويل مشاريع بيئية رقمية، لكنها تجد نفسها عاجزة عن السداد بسبب الكوارث المناخية التي تضرب اقتصادها.

ففي جزر المحيط الهادئ، أدت الكوارث المناخية إلى انهيار الإيرادات البيئية، مما جعل سداد القروض البيئية الرقمية مستحيلاً. وفي أمريكا اللاتينية، أدت الأزمات المناخية 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 الكوارث المناخية.

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

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

وفي المقابل، بدأت بعض المبادرات. ففي مؤتمر المناخ COP29، تم اقتراح "آلية لإعادة هيكلة الديون البيئية"، لكنها لم تُعتمد بعد. أما في مجموعة السبع، فإن "مبادرة التمويل البيئي الرقمي العادل" لا تزال في طور النقاش.

أما في العالم العربي، فإن معظم الدول تعتمد على قروض خارجية لتمويل مشاريع البيئة الرقمية، دون وجود ضمانات قانونية لحمايتها من المخاطر المناخية.

ويخلص هذا الفصل إلى أن التمويل البيئي الرقمي يجب أن يكون هبة، لا ديناً، وأن الدول التي تدفع ثمن أخطاء غيرها لا ينبغي أن تُثقل بعبء الديون.

**الفصل السادس والعشرون

السيادة البيئية الرقمية والنقل البيئي الرقمي: حماية سلاسل التوريد من التهديدات السيبرانية**

لم يعد النقل البيئي يعتمد فقط على المركبات، بل على أنظمة رقمية معقدة تدير سلاسل التوريد من المختبر إلى الموقع البيئي. واختراق هذه الأنظمة قد يؤدي إلى تلف المعدات البيئية، أو تأخير التوزيع، أو سرقة الشحنات.

ففي عام 2024، تم اختراق نظام تتبع الشحنات البيئية في دولة أوروبية، مما أدى إلى تلف آلاف أجهزة المراقبة بسبب تأخير التبريد. وفي عام

2025، تم سرقة شحنات معدات بيئية عبر اختراق أنظمة الموانئ الرقمية.

ويواجه القانون الدولي غياباً في تصنيف سلاسل التوريد البيئية 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 البيئية الرقمية في مجال النقل ليست مسألة تقنية، بل مسألة أمن بيئي، وأن سلاسل التوريد البيئية الرقمية يجب أن تُعتبر جزءاً من البنية التحتية الحيوية.

**الفصل السابع والعشرون

السيادة البيئية الرقمية والبحث العلمي البيئي المفتوح: التوازن بين التعاون والحماية**

لا يمكن تحقيق التقدم في مواجهة التحديات البيئية دون تبادل المعرفة، لكن هذا التبادل يجب أن يتم ضمن حدود تحمي المصالح الوطنية. فنشر بيانات بحثية بيئية حساسة — مثل نماذج التغير المناخي المقاوم — قد يُستخدم ضد الدول النامية في المفاوضات الدولية.

ففي بعض الحالات، استخدمت الدول الصناعية البيانات البيئية 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 البيئية من الاستغلال.

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

ويؤكد هذا الفصل أن السيادة البيئية الرقمية في

البحث العلمي تعني وضع تصنيفات واضحة للبيانات، وتحديد ما يُسمح بنشره وما يجب حمايته، دون عزلة علمية.

**الفصل الثامن والعشرون

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

لا يمكن لأي دولة أن تحمي سيادتها البيئية 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

البيئة الرقمية من قبل الدول الصناعية، دون مراعاة قدرات الدول النامية. وهذا يخلق نظاماً غير عادل يكرس التبعية البيئية الرقمية.

ويستدعي الحل:

- إنشاء منتدى دولي محايد لصياغة قواعد السيادة البيئية الرقمية.

- توفير الدعم الفني والمالي للدول النامية.

- احترام التنوع في النماذج الوطنية للسيادة البيئية 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 البيئية الرقمية يجب أن يقوم على مبدأ "السيادة المشتركة"، لا "الهيمنة البيئية الرقمية".

**الفصل التاسع والعشرون

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

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

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

وفي مشروع "قواعد تالين 2.0"، تم التأكيد على أن تدمير البنية التحتية البيئية 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 البيئية" لا تزال قيد النقاش، ولم تُدرج بعد في النظام الأساسي.

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

**الفصل الثلاثون

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

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

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

وفي مشروع "قواعد تالين 2.0"، تم التأكيد على أن تدمير البنية التحتية البيئية 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 البيئية" لا تزال قيد النقاش، ولم تُدرج بعد في النظام الأساسي.

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

**الفصل الحادي والثلاثون

السيادة البيئية الرقمية والفضاء الخارجي: حماية الأرض من التلوث الفضائي البيئي**

مع تزايد الأنشطة الفضائية المتعلقة بالبيئة — من الأقمار الصناعية لمراقبة الانبعاثات إلى الطائرات المسيرة الفضائية لتتبع الكوارث — برز تهديد جديد: التلوث الفضائي الذي يؤثر على الأنظمة البيئية. فحطام الأقمار الصناعية قد يعيق

أنظمة الرصد البيئي، بينما تنبعثات الصواريخ تؤثر على الغلاف الجوي الذي ينظم المناخ.

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

ويواجه القانون الدولي إشكالية جوهرية: هل يُعد التلوث الفضائي جزءاً من "المسؤولية البيئية 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 البيئية الرقمية يجب أن تمتد إلى الفضاء الخارجي، وأن الأنشطة الفضائية البيئية يجب أن تخضع لمبدأ "الوقاية البيئية" مثلها مثل أي نشاط صناعي آخر.

**الفصل الثاني والثلاثون

السيادة البيئية الرقمية والذكاء الاصطناعي التوليدي: عندما تصبح الأخبار الكاذبة سلاحاً بيئياً**

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 الجمهور، وزعزعة ثقة المجتمع، وتقويض الثقة في الأنظمة البيئية الوطنية.

ففي عام 2025، تم تداول فيديوهات مزيفة لعلماء وهم يحذرون من سياسات بيئية وطنية آمنة، مما أدى إلى انخفاض الثقة في النظام البيئي وانتشار المعلومات المضللة. وفي أزمات بيئية، تم نشر أخبار كاذبة عن نقص في الموارد البيئية 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 بيئي" 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 البيئية.

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

ويخلص هذا الفصل إلى أن غياب تنظيم الذكاء الاصطناعي التوليدي يحوّل الفضاء الرقمي إلى ساحة حرب نفسية بيئية، ويستدعي تعريفاً جديداً للتدخل السيبراني البيئي يشمل "التأثير الخبيث عبر المحتوى المزيف".

**الفصل الثالث والثلاثون

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

مع تزايد الاعتماد على البيانات الضخمة في تحليل التغير المناخي، 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 بيئية 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

البيئية.

- معظم العقود بين الدول والشركات تبقى سرية.

- لا توجد معايير لـ"السيادة البيئية الرقمية".

أما في الدول النامية، فإن غياب التشريعات يسمح باستغلال بياناتها دون مقابل عادل.

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

**الفصل الرابع والثلاثون

السيادة البيئية الرقمية والتعليم العالي البيئي: نحو كليات وطنية للقانون البيئي الرقمي**

لا يمكن بناء قدرات بيئية 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 البيئي الرقمي يُعد استثماراً استراتيجياً في السيادة البيئية الرقمية.

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

أما في الدول النامية، فإن التعليم البيئي 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 البيئي الرقمي.

وفي العالم العربي، بدأت بعض الدول بإنشاء برامج متخصصة، مثل "ماجستير الأمن البيئي 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 بيئية رقمية، وأن الدول التي لا تستثمر في كليات القانون البيئي الرقمي ستظل مستوردة للمعرفة، لا منتجة لها.

**الفصل الخامس والثلاثون

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

لا يقتصر الفضاء الرقمي على البيانات والخدمات، بل يشمل أيضاً الإبداع الثقافي البيئي: الأفلام الوثائقية، الروايات، الفنون البصرية التي تروي قصص البيئة. 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 البيئي المحلي أو حمايته من القرصنة.

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

**الفصل السادس والثلاثون

السيادة البيئية الرقمية والتمويل الرقمي البيئي: حماية العملات البيئية من التلاعب والاحتيال**

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

وفي الممارسة، أدت عمليات الاحتيال في سوق العملات الرقمية البيئية 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 البيئية، لأنها لا تخضع لسلطة دولة واحدة، ولا يمكن تتبع مالكيها بسهولة.

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

ويخلص هذا الفصل إلى أن السيادة البيئية

الرقمية في المجال المالي لا تعني منع الابتكار، بل وضع ضوابط تحمي الاقتصاد الوطني من المخاطر غير المحسوبة.

**الفصل السابع والثلاثون

السيادة البيئية الرقمية والبحث العلمي البيئي المفتوح: التوازن بين التعاون والحماية**

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

ففي بعض الحالات، استخدمت الدول الصناعية البيانات البيئية 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 البيئية من الاستغلال.

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

مقابل عادل.

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

**الفصل الثامن والثلاثون

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

لا يمكن لأي دولة أن تحمي سيادتها البيئية 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 البيئة الرقمية من قبل الدول الصناعية، دون مراعاة قدرات الدول النامية. وهذا يخلق نظاماً غير عادل يكرس التبعية البيئية الرقمية.

ويستدعي الحل:

- إنشاء منتدى دولي محايد لصياغة قواعد السيادة البيئية الرقمية.

- توفير الدعم الفني والمالي للدول النامية.

- احترام التنوع في النماذج الوطنية للسيادة البيئية 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 البيئية الرقمية يجب أن يقوم على مبدأ "السيادة المشتركة"، لا "الهيمنة البيئية الرقمية".

**الفصل التاسع والثلاثون

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

مع تزايد استخدام الموارد البيئية كسلاح في

النزاعات، برز سؤال جوهري: هل يُعد تدمير البنية التحتية البيئية الرقمية كوسيلة حربية انتهاكاً للقانون الإنساني الدولي؟ وهل يُعتبر التسبب المتعمد في كارثة بيئية جريمة حرب؟

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

وفي مشروع "قواعد تالين 2.0"، تم التأكيد على أن تدمير البنية التحتية البيئية 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 البيئية" لا تزال قيد النقاش، ولم تُدرج بعد في النظام الأساسي.

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

**الفصل الأربعون

السيادة البيئية الرقمية والمستقبل: رؤية استراتيجية للعقود القادمة**

في الختام، لا يمكن النظر إلى السيادة البيئية

الرقمية كظاهرة مؤقتة، بل كتحول جوهري في مفهوم الحماية البيئية في القرن الحادي والعشرين. فالدول التي تبني سيادتها البيئية الرقمية اليوم ستكون قادرة على:

- حماية مواطنيها من التلاعب البيئي الرقمي.

- بناء اقتصاد بيئي رقمي مستقل ومستدام.

- تعزيز مكانة أجيالها في النظام البيئي 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 البيئية الرقمية ليس مسألة اختيار، بل مسألة بقاء.

خاتمة

بعد استعراض شامل لأبعاد السيادة البيئية 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 البيئي الرقمي، رغم طبيعته غير المادية، بات ساحة للصراعات السياسية والاقتصادية، ولا

يمكن لأي دولة أن تحافظ على سيادتها البيئية 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 البيئية الرقمية الحقيقية لا تُبنى على العزلة أو القمع، بل على الشفافية، والكفاءة، والثقة بين الدولة والمواطن. وهي ليست غاية بذاتها، بل وسيلة لبناء مستقبل بيئي آمن، عادل، وإنساني.

المراجع

United Nations Framework Convention on (Climate Change (1992

(Paris Agreement (2015

(Convention on Biological Diversity (1992

Nagoya Protocol on Access and Benefit-(Sharing (2010

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 (Environmental Data (2022

European Commission. Digital Environment (Action Plan (2023

Government of India. National

(Environmental Policy (2022

Government of China. Smart Environment (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). Environmental Justice and Digital Sovereignty. Oxford University Press

De Schutter O. (2023). The Right to a Healthy Environment in the Digital Age. Cambridge University Press

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

:Official Government Sources

White House. National Strategy for Digital (Environment (2024

European Commission. Digital Environment (Action Plan (2023

Ministry of Environment Reports on Cyber

Resilience in Environmental Systems ((Multiple Jurisdictions, 2020–2025

:Academic Journals

(Journal of Environmental Law (Oxford

International Journal of Digital Environmental Sovereignty

Harvard Environmental Law Review

Stanford Technology Law Review

فهرس المحتويات

الفصل الأول

السيادة البيئية الرقمية: من الحماية البيئية إلى المبدأ القانوني الدولي

الفصل الثاني

الفراغ القانوني الدولي في حماية الأنظمة البيئية الرقمية

الفصل الثالث

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

الفصل الرابع

البنية التحتية البيئية الرقمية: تعريف قانوني دولي مفقود

الفصل الخامس

التلاعب السيبراني في الأنظمة البيئية: نحو معيار قانوني دولي

الفصل السادس

المسؤولية الدولية عن الهجمات السيبرانية البيئية: تحديات الإسناد والرقابة

الفصل السابع

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

الفصل الثامن

السيادة البيئية الرقمية وبراءات الاختراع البيئية: التوتر بين الابتكار والاستغلال

الفصل التاسع

السيادة البيئية الرقمية في الدول النامية: تحديات القدرة والاعتماد التكنولوجي

الفصل العاشر

التنظيم الإقليمي للسيادة البيئية الرقمية: دراسة مقارنة بين التجارب العالمية

الفصل الحادي عشر

السيادة البيئية الرقمية والبيانات البيئية: حماية الخصوصية البيئية من الاستغلال الخارجي

الفصل الثاني عشر

السيادة البيئية الرقمية والذكاء الاصطناعي البيئي: عندما تصبح الخوارزميات سلطة خارج نطاق الدولة

الفصل الثالث عشر

السيادة البيئية الرقمية والجرائم الإلكترونية البيئية: مكافحة الاحتيال البيئي الرقمي

الفصل الرابع عشر

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

الفصل الخامس عشر

السيادة البيئية الرقمية والبحث العلمي البيئي: نحو استقلال تكنولوجي وطني

الفصل السادس عشر

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

الفصل السابع عشر

السيادة البيئية الرقمية والمحاكمات البيئية: نحو اختصاص قضائي رقمي

الفصل الثامن عشر

السيادة البيئية الرقمية والبيانات البيئية: بين الملكية الفردية والسيادة الجماعية

الفصل التاسع عشر

السيادة البيئية الرقمية والبيئة العامة: حماية المجتمعات من التكنولوجيا البيئية غير المسؤولة

الفصل العشرون

السيادة البيئية الرقمية والمستقبل: نحو مشروع اتفاقية دولية نموذجية

الفصل الحادي والعشرون

السيادة البيئية الرقمية والطاقة البيئية: حماية الموارد من الاستنزاف الرقمي

الفصل الثاني والعشرون

السيادة البيئية الرقمية وسلامة الباحثين:

حماية الباحثين من التلاعب الرقمي

الفصل الثالث والعشرون

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

الفصل الرابع والعشرون

السيادة البيئية الرقمية والتراث البيئي: حماية التراث من الاندثار الرقمي

الفصل الخامس والعشرون

السيادة البيئية الرقمية والتمويل البيئي الرقمي: حماية الدول النامية من الديون البيئية

الفصل السادس والعشرون

السيادة البيئية الرقمية والنقل البيئي الرقمي: حماية سلاسل التوريد من التهديدات السيبرانية

الفصل السابع والعشرون

السيادة البيئية الرقمية والبحث العلمي البيئي المفتوح: التوازن بين التعاون والحماية

الفصل الثامن والعشرون

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

الفصل التاسع والعشرون

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

الفصل الثلاثون

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

الفصل الحادي والثلاثون

السيادة البيئية الرقمية والفضاء الخارجي: حماية الأرض من التلوث الفضائي البيئي

الفصل الثاني والثلاثون

السيادة البيئية الرقمية والذكاء الاصطناعي التوليدي: عندما تصبح الأخبار الكاذبة سلاحاً بيئياً

الفصل الثالث والثلاثون

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

الفصل الرابع والثلاثون

السيادة البيئية الرقمية والتعليم العالي البيئي: نحو كليات وطنية للقانون البيئي الرقمي

الفصل الخامس والثلاثون

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

الفصل السادس والثلاثون

السيادة البيئية الرقمية والتمويل الرقمي البيئي: حماية العملات البيئية من التلاعب والاحتيال

الفصل السابع والثلاثون

السيادة البيئية الرقمية والبحث العلمي البيئي المفتوح: التوازن بين التعاون والحماية

الفصل الثامن والثلاثون

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

الفصل التاسع والثلاثون

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

الفصل الأربعون

السيادة البيئية الرقمية والمستقبل: رؤية استراتيجية للعقود القادمة

خاتمة

تم بحمد الله وتوفيقه

تأليف د. محمد كمال عرفه الرخاوي

الباحث والمستشار القانوني

المحاضر الدولي في القانون