"السيادة الرقمية كمبدأ جديد في القانون الدولي العام: دراسة تأسيسية لحق الدول في تنظيم الفضاء السيبراني وحماية بناها التحتية الحيوية من التدخل الخارجي"

المؤلف محمد كمال عرفه الرخاوي

**الفصل الأول

السيادة الرقمية: مفهوم ناشئ في النظام الدولي المعاصر**

لم يعد مفهوم السيادة في القرن الحادي والعشرين محصوراً في الأرض والجو والمياه الإقليمية، بل امتد ليشمل الفضاء السيبراني،

ذلك المجال غير المادي الذي بات يشكل العمود الفقري للدولة الحديثة. فالبنية التحتية الحيوية — من شبكات الكهرباء إلى أنظمة البنوك، ومن المستشفيات إلى الدفاع الوطني — تعتمد اليوم على أنظمة رقمية يمكن اختراقها من آلاف الكيلومترات دون انتهاك حدود جغرافية واحدة. ومن هنا ظهر مفهوم "السيادة الرقمية" كضرورة وجودية للدول، لا كرفاهية تقنية.

ويُعرّف الفقه الناشئ السيادة الرقمية على أنها **حق الدولة الحصري في تنظيم الفضاء السيبراني داخل نطاق ولايتها، وحماية بناها التحتية الرقمية من أي تدخل خارجي، وفرض سلطتها القانونية على الأنشطة الرقمية التي تؤثر على أمنها القومي أو استقرارها الاجتماعي**. ولا يعني هذا الحق انعزالاً رقمياً، بل ممارسة السيادة في بيئة عابرة للحدود، تماماً كما تمارس الدولة سيادتها على

السفن في موانئها أو الطائرات في مجالها الجوي.

وقد بدأ هذا المفهوم يتشكل عملياً قبل أن يُرسّخ فقهياً. ففي عام 2007، أدت هجمات سيبرانية منسوبة إلى دولة كبرى ضد إحدى دول أوروبا الشمالية إلى شلل كامل في الخدمات الحكومية، مما دفع الدولة الصغيرة إلى إعادة بناء بنيتها التحتية الرقمية تحت مظلة سيادة وطنية صارمة. وفي عام 2015، أعلن رئيس دولة أوروبية كبرى أن "السيادة الرقمية جزء لا يتجزأ من السيادة الوطنية"، وهو ما تبنته لاحقاً استراتيجية الاتحاد الأوروبي.

أما في العالم العربي، فقد بدأت دول مثل الإمارات والسعودية في تبني مفاهيم مشابهة عبر استراتيجيات الأمن السيبراني الوطنية. وفي

بعض الدول العربية، نصت تشريعات مكافحة الجرائم الإلكترونية على حق الدولة في حماية "الأمن القومي الرقمي"، رغم غياب تعريف دقيق له. كما أشارت استراتيجيات وطنية للأمن السيبراني في دول عربية أخرى إلى "السيادة على الفضاء الرقمي" كأحد المحاور الأساسية، لكن دون تفصيل قانوني كافٍ.

ويؤكد هذا الفصل أن السيادة الرقمية ليست اختراعاً إيديولوجياً، بل استجابة قانونية ضرورية لتغير طبيعة التهديدات في العصر الرقمي، وأن غيابها في القانون الدولي يخلق فراغاً خطيراً يهدد استقرار النظام الدولي ذاته.

**الفصل الثاني

الفراغ التشريعي الدولي في تنظيم الفضاء

السيبراني**

رغم مرور أكثر من ثلاثة عقود على ظهور الإنترنت كظاهرة عالمية، لا يزال القانون الدولي يفتقر إلى اتفاقية شاملة تنظم الفضاء السيبراني. فمعاهدات مثل ميثاق الأمم المتحدة أو اتفاقيات جنيف لم تُصمم لمواجهة هجمات تُشن عبر خوادم في دول ثالثة، وتُدار بواسطة ذكاء اصطناعي، وتستهدف أنظمة مدنية دون إراقة دماء. وهذا الفراغ التشريعي يتيح للدول القوية فرض "قانون الغاب الرقمي"، بينما تبقى الدول النامية عرضة للتدخل دون حماية قانونية.

وقد حاولت بعض المبادرات سد هذه الثغرة. ففي عام 2013، أصدرت مجموعة الخبراء الحكوميين التابعة للأمم المتحدة تقريراً أكد أن "مبادئ القانون الدولي، بما في ذلك ميثاق

الأمم المتحدة، تنطبق على الفضاء السيبراني". لكن هذا التأكيد بقي عاماً، ولم يُترجم إلى قواعد ملزمة. وفي عام 2015، أطلقت فرنسا وكندا "مبادرة باريس للثقة والأمن في الفضاء السيبراني"، التي وقعتها أكثر من 80 دولة، لكنها تظل إعلاناً سياسياً غير ملزم.

أما في المحافل الإقليمية، فقد تبنت منظمة الأمن والتعاون في أوروبا (OSCE) عدة توصيات حول التعاون السيبراني، لكنها لا تتضمن آليات ردع. وفي الاتحاد الإفريقي، لا توجد حتى الآن استراتيجية موحدة للأمن السيبراني، رغم تزايد الهجمات على البنوك والمستشفيات في القارة.

وفيما يخص الدول العربية، فإن جامعة الدول العربية اعتمدت "استراتيجية الأمن السيبراني العربية" في عام 2020، لكنها تفتقر إلى آلية

تنفيذ أو مساءلة. أما في بعض الدول العربية، فلا يوجد تشريع ينظم العلاقات السيبرانية الدولية، رغم تعرضها لهجمات يومية تستهدف القطاع المصرفي والطاقة. وفي دول عربية أخرى، فإن غياب التشريعات الدولية الملزمة يجعل الدولة عاجزة عن مطالبة أي طرف أجنبي بالتوقف عن أنشطة تجسس رقمي مزعومة.

ويخلص هذا الفصل إلى أن الفراغ التشريعي ليس نتيجة غفلة، بل انعكاس لصراع المصالح بين القوى الكبرى التي ترى في الفوضى السيبرانية فرصة للهيمنة. ولذلك، فإن سد هذا الفراغ يتطلب مبادرة قانونية جماعية من الدول المتوسطة والصغيرة، وليس انتظار رحمة العظمى.

**الفصل الثالث

السيادة التقليدية مقابل السيادة الرقمية: إعادة تشكيل مفاهيم القانون الدولي الكلاسيكي**

لا يمكن فهم السيادة الرقمية دون مقارنتها بالسيادة التقليدية التي بناها القانون الدولي منذ معاهدة وستفاليا عام 1648. فالسيادة التقليدية تقوم على ثلاثة أركان: **السلطة الحصرية داخل الإقليم، وعدم التدخل من الخارج، والمساواة بين الدول**. لكن الفضاء السيبراني يتحدى كل هذه الأركان.

فأولاً، **السلطة الحصرية** تصبح مشروطة، لأن البيانات تتدفق عبر الحدود دون إذن، والخوادم قد تكون في دولة ثالثة، والبرمجيات مملوكة لشركات خاصة عابرة للقوميات. فهل تستطيع دولة أن تمنع شركة أمريكية من جمع

بيانات مواطنيها إذا كانوا يستخدمون تطبيقاً على هواتفهم؟

ثانياً، **عدم التدخل** يصبح غامضاً، لأن التدخل السيبراني لا يترك آثاراً مادية واضحة. فهل يُعد اختراق موقع حكومي وسرقة وثائق "تدخلاً"؟ وهل يختلف عن التجسس التقليدي؟ وهل يبرر الرد العسكري؟ المحكمة الدولية للعدل لم تبت في قضية سيبرانية واحدة حتى اليوم.

ثالثاً، **المساواة بين الدول** تنهار في الفضاء السيبراني، لأن القدرة على الهجوم أو الدفاع تعتمد على التكنولوجيا، لا على عدد السكان أو المساحة. فدولة صغيرة مثل إستونيا قد تكون أكثر أماناً رقمياً من دولة كبيرة مثل البرازيل، بسبب استثماراتها في الأمن السيبراني.

وفي هذا السياق، بدأت بعض الدول بصياغة مفاهيم جديدة. فروسيا والصين تطالبان بـ"سيادة رقمية مطلقة"، تسمح للدولة بعزل الإنترنت الوطني عند الحاجة، وهو ما يتعارض مع مبدأ حرية تدفق المعلومات. أما الولايات المتحدة والاتحاد الأوروبي، فتدعو إلى "سيادة مسؤولة"، توازن بين الأمن وحرية الإنترنت.

أما في بعض الدول العربية، فإن التطبيق العملي للسيادة الرقمية يواجه تحديات هيكلية، من نقص الكوادر المتخصصة إلى غياب التنسيق بين الجهات الأمنية والمدنية. أما في دول عربية أخرى، فإن التركيز ينصب على الحماية الدفاعية، دون تطوير قدرات ردع سيبراني فعالة.

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

**الفصل الرابع

البنية التحتية الحيوية الرقمية: تعريف قانوني دولي مفقود**

أحد أكبر الثغرات في النقاش الدولي حول السيادة الرقمية هو غياب تعريف قانوني متفق عليه لما يُسمى "البنية التحتية الحيوية 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 الحيوية 16 قطاعاً، من الطاقة إلى الزراعة. أما في الاتحاد الأوروبي، فتركز على تسعة قطاعات رئيسية، مثل الصحة والنقل والاتصالات. وفي الصين، يُضاف إليها "الفضاء المعلوماتي للأحزاب والدولة"، مما يوسع المفهوم ليشمل الأيديولوجيا.

أما في العالم العربي، فلا يوجد تعريف موحد. ففي السعودية، يُعرّف المرسوم الملكي رقم M/12 لعام 2017 البنية التحتية الحيوية بأنها "المنشآت والأنظمة التي يؤدي تعطلها إلى تهديد الأمن القومي". أما في الإمارات، فتتضمن الاستراتيجية الوطنية "البيانات الشخصية للمواطنين" كجزء من البنية الحيوية.

وفي بعض الدول العربية، لا يوجد تعريف قانوني شامل، رغم أن قوانين مكافحة الجرائم الإلكترونية أشارت إلى "المواقع والنظم المعلوماتية ذات الأهمية الخاصة". أما في دول عربية أخرى، فإن مراسيم تنفيذية حددت بعض القطاعات (كالطاقة والاتصالات)، لكنها أغفلت قطاعات حساسة مثل التعليم والصحة.

ويكشف هذا التباين أن غياب التعريف الدولي يفتح الباب أمام تفسيرات ذاتية قد تُستخدم لتبرير الهجمات ("هدفك ليس حيوياً") أو لتوسيع السيطرة ("كل شيء حيوي"). ولذلك، فإن أول خطوة في بناء نظام قانوني دولي للسيادة الرقمية هي الاتفاق على تعريف دقيق، يشمل:

- القطاعات الأساسية (الطاقة، المياه، الاتصالات، الصحة، النقل، المال).

- الأنظمة التي تربط هذه القطاعات (مثل شبكات التحكم الصناعي SCADA).

- البيانات التي تديرها (مثل سجلات المرضى أو معاملات البنوك).

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

**الفصل الخامس

التدخل السيبراني كانتهاك للسيادة: نحو معيار قانوني دولي**

لا يمكن حماية السيادة الرقمية دون تحديد ما يُعد "تدخلاً سيبرانياً غير مشروع". فليس كل نشاط سيبراني عبر الحدود يشكل انتهاكاً. فاستخدام مواطن لتطبيق أمريكي للتواصل لا يُعد تدخلاً، لكن اختراق جهة عسكرية لنظام دفاع جوي لدولة أخرى يُعد عدواناً. والمشكلة تكمن في المنطقة الرمادية بينهما.

وفي الفقه الدولي، بدأت محاولات وضع معايير. ففي مشروع "قواعد تالين" (Tallinn Manual)، الذي أعده خبراء مستقلون برعاية الناتو، تم التمييز بين:

- **التدخل غير المشروع**: وهو الذي يمس "الشؤون الداخلية الجوهرية" للدولة، كالانتخابات أو النظام المالي.

- **الأنشطة السيبرانية المسموحة**:

كالتجسس أو جمع المعلومات المفتوحة.

لكن "قواعد تالين" ليست ملزمة، بل رأياً فقهياً. كما أن معيار "الشؤون الجوهرية" غامض. فهل يُعد اختراق موقع وزارة التعليم تدخلاً؟ وهل يختلف عن اختراق موقع صحيفة خاصة؟

وفي الممارسة، تختلف الدول في تطبيق المعيار. ففي عام 2016، اعتبرت دولة غربية أن تدخل دولة أخرى في انتخاباتها عبر فيسبوك كان "تدخلاً غير مسبوق". أما الدولة المُتهمة، فاعتبرت أن العقوبات المفروضة على شركاتها كانت "تدخلاً اقتصادياً". وهذا التناقض يعكس غياب معيار موضوعي.

أما في بعض الدول العربية، فلا يوجد تشريع

يجرّم التدخل السيبراني الخارجي صراحة، رغم تعرضها لهجمات تستهدف استقرار العملة أو الثقة في المؤسسات. أما في دول عربية أخرى، فإن غياب الآليات التقنية لتحديد مصدر الهجوم يحول دون اتخاذ موقف قانوني واضح.

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 سلوكها في شؤون داخلية جوهرية، أو

- يؤدي إلى شلل في البنية التحتية الحيوية،

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

**الفصل السادس

المسؤولية الدولية عن الأنشطة السيبرانية: تحديات الإسناد والرقابة**

لا يمكن تطبيق مبدأ السيادة الرقمية دون حل إشكالية "الإسناد" (Attribution)، أي تحديد الدولة المسؤولة عن نشاط سيبراني ضار. 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. وهذا الغموض يتيح للدول إنكار المسؤولية والتهرب من العواقب.

ويواجه القانون الدولي ثلاث مستويات من الإسناد:

- **المستوى الأول**: الهجوم الذي تنفذه جهة حكومية مباشرة (مثل وكالة الأمن القومي الأمريكية). 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" (Effective Control) 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 2015، 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.

أما في الممارسة، فقد استخدمت دول غربية مبدأ "الرقابة العامة" (Overall Control) لتحميل دول أخرى مسؤولية هجمات سيبرانية، بينما رفضت الدول المُتهمة هذا الربط. وفي الاتحاد الأوروبي، طورت بعض الدول أنظمة "بصمة رقمية" (Digital Fingerprinting) لتحليل أكواد الهجمات وربطها بمصادر معروفة.

أما في بعض الدول العربية، فلا توجد آلية وطنية متخصصة في الإسناد السيبراني، مما يحد من قدرة الدولة على المطالبة بحقوقها الدولية. أما في دول عربية أخرى، فإن غياب التعاون الدولي في تبادل الأدلة الرقمية يعقّد عملية تحديد المسؤولية.

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

**الفصل السابع

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

عندما تتعرض دولة لانتهاك سيبراني، ما هي وسائل الرد المتاحة لها؟ وهل يجوز استخدام القوة العسكرية رداً على هجوم سيبراني؟ 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 "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 شبكة الكهرباء الوطنية لأسابيع قد يُصنّف كهجوم مسلح.

أما في الممارسة، فقد ردت دول على هجمات تستهدف محطات مياه، بينما اكتفت دول أخرى بالتدابير الدبلوماسية بعد اختراق برلماناتها. وهذا التباين يعكس غياب توافق دولي.

أما في بعض الدول العربية، فلا يوجد تشريع ينظم الرد السيبراني، ولا استراتيجية وطنية للردع الرقمي. أما في دول عربية أخرى، فإن غياب القدرات الدفاعية المتقدمة يحد من خيارات الرد، ويجعل الدولة تعتمد على التعاون

الإقليمي.

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

**الفصل الثامن

السيادة الرقمية والخصوصية: التوازن بين الأمن الوطني وحقوق الأفراد**

لا يمكن الحديث عن السيادة الرقمية دون معالجة توترها الجوهري مع حق الأفراد في الخصوصية. فلتعزيز السيادة الرقمية، قد تلجأ الدولة إلى مراقبة شاملة للاتصالات، أو فرض

تخزين البيانات محلياً، أو منع استخدام تطبيقات أجنبية. وكل هذه الإجراءات قد تنتهك حقوق الإنسان إذا لم تُضبط بضمانات قانونية.

وفي الاتحاد الأوروبي، يُطبّق مبدأ "التناسب" بدقة: فالدولة يمكنها جمع بيانات لأغراض أمنية، لكن فقط بتصريح قضائي، ولأقل فترة ممكنة، وبشفافية كاملة. وقد ألزمت محكمة العدل الأوروبية الدول الأعضاء بإلغاء قوانين المراقبة الشاملة التي لا تستهدف تهديدات محددة.

أما في الصين، فإن "قانون الأمن السيبراني" يفرض على جميع الشركات تخزين البيانات داخل البلاد، ويمنح الأجهزة الأمنية حق الوصول دون قيد، وهو ما يُنظر إليه دولياً كأداة قمع أكثر منه كأداة سيادة.

أما في الولايات المتحدة، فإن "قانون الاستخبارات الخارجية" (FISA) يسمح بمراقبة الأجانب دون إذن قضائي، لكنه يحظر مراقبة المواطنين دون مبرر.

أما في بعض الدول العربية، فإن قوانين مكافحة الجرائم الإلكترونية تمنح الجهات الأمنية صلاحيات واسعة لحجب المواقع ومراقبة الاتصالات، دون رقابة قضائية فعالة. أما في دول عربية أخرى، فإن قوانين الإعلام تتيح حجب المواقع "لحماية الأمن القومي"، لكن دون تعريف دقيق لهذا المفهوم.

ويؤكد هذا الفصل أن السيادة الرقمية الحقيقية لا تُبنى على قمع المواطنين، بل على بناء ثقة بين الدولة والفرد، عبر آليات شفافة ومستقلة

للرقابة.

**الفصل التاسع

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

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

فأكثر من 80 بالمئة من خوادم الإنترنت

الأساسية (Root Servers) موجودة في الولايات المتحدة. ومعظم أنظمة التشغيل والبرمجيات المستخدمة في الحكومات العربية أمريكية أو أوروبية. بل إن بعض الدول النامية لا تملك حتى "نقطة تبادل إنترنت" (IXP) محلية، مما يجبر بياناتها على المرور عبر خوادم أجنبية.

وفي هذا السياق، بدأت بعض الدول باتخاذ خطوات. فنيجيريا أنشأت "منطقة بيانات سيادية"، بينما أطلقت الهند مبادرة "بيانات للهنود". أما في العالم العربي، فقد أطلقت السعودية "مركز البيانات الوطني"، وبدأت الإمارات في تصنيع أنظمة تشغيل محلية.

أما في بعض الدول العربية، فإن الاستراتيجيات الوطنية للأمن السيبراني تحدثت عن "التحول إلى الاعتماد على الذات"، لكن التطبيق لا يزال

محدوداً بسبب التكلفة العالية ونقص الخبرات. أما في دول عربية أخرى، فإن مشاريع التصنيع الرقمي المحلي تواجه صعوبات في التمويل والتسويق.

ويخلص هذا الفصل إلى أن السيادة الرقمية في الدول النامية ليست مسألة تقنية فقط، بل قضية تنموية تتطلب استثمارات طويلة الأمد، وتعاوناً إقليمياً، ونقل تكنولوجيا عادل.

**الفصل العاشر

التنظيم الإقليمي للفضاء السيبراني: دراسة مقارنة بين التجارب الأوروبية والإفريقية والعربية**

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

وفي أوروبا، يُعد الاتحاد الأوروبي رائداً في هذا المجال. فـ"الوكالة الأوروبية للأمن السيبراني" (ENISA) تنسق جهود الدول الأعضاء، بينما يُلزم "قانون NIS2" جميع المشغلين الحيوين بالإبلاغ عن الحوادث. كما أن "شبكة الاستجابة السيبرانية الأوروبية" (CSIRTs) تتيح تبادل المعلومات في الوقت الحقيقي.

أما في إفريقيا، فإن الاتحاد الإفريقي اعتمد "استراتيجية الأمن السيبراني الإفريقية" في 2014، لكن التنفيذ ضعيف بسبب نقص التمويل. ومع ذلك، بدأت مبادرات إقليمية مثل "شبكة

غرب إفريقيا للأمن السيبراني".

أما في العالم العربي، فإن جامعة الدول العربية أطلقت "الاستراتيجية العربية للأمن السيبراني" في 2020، التي تدعو إلى إنشاء "مركز عربي للأمن السيبراني". لكن المركز لم يُنشأ بعد، ولا توجد آليات ردع مشتركة.

أما على المستوى الثنائي، فقد وقعت دول عربية اتفاقيات تعاون سيبراني مع الإمارات والسعودية، لكنها تبقى سرية وغير ملزمة. أما في دول عربية أخرى، فلا توجد اتفاقيات علنية في هذا المجال، رغم مشاركتها في منتديات إقليمية.

ويؤكد هذا الفصل أن التنظيم الإقليمي هو

الجسر بين السيادة الوطنية والنظام الدولي، وأن غيابه في العالم العربي يترك الدول فريسة للتدخلات الخارجية.

**الفصل الحادي عشر

السيادة الرقمية وحرية تدفق المعلومات: التوتر بين المفاهيم العالمية**

لا يمكن فهم التحديات التي تواجه السيادة الرقمية دون تحليل التوتر الجوهري بينها وبين مبدأ "حرية تدفق المعلومات"، الذي يُعتبر أحد أركان الإنترنت منذ نشأته. فبينما ترى بعض الدول أن السيادة الرقمية تتطلب فرض حدود رقمية وتنظيم المحتوى، ترى دول أخرى أن أي قيد على تدفق البيانات يُعد انتهاكاً لحقوق الإنسان الأساسية.

ويتجلى هذا التوتر في مقاربتين رئيسيتين:

- **المقاربة الليبرالية**: التي تقودها الولايات المتحدة والاتحاد الأوروبي، وتؤكد أن الإنترنت يجب أن يظل فضاءً مفتوحاً، وأن الدولة لا يحق لها حجب المحتوى إلا في حالات استثنائية (كالتحريض على العنف أو الكراهية).

- **المقاربة السيادية**: التي تقودها الصين وروسيا، وتؤكد أن كل دولة لها الحق في تحديد ما يُسمح به داخل حدودها الرقمية، بما في ذلك حجب المواقع الأجنبية أو فرض مراجعة محتوى محلي.

وفي المحافل الدولية، يظهر هذا الانقسام بوضوح. ففي مؤتمر القمة العالمي لمجتمع

المعلومات (WSIS)، رفضت دول غربية مقترحات بمنح الحكومات سلطة أكبر على إدارة الإنترنت، بينما دعمتها دول آسيوية وإفريقية. وفي الأمم المتحدة، فشلت محاولات إنشاء هيئة دولية لإدارة الإنترنت بسبب هذا الخلاف الجوهري.

أما في العالم العربي، فإن بعض الدول تتبنى مقاربة هجينة: فهي تدعم حرية تدفق المعلومات في السياقات الاقتصادية، لكنها تفرض قيوداً صارمة على المحتوى السياسي أو الديني. وغالباً ما تُبرر هذه القيود بـ"الحفاظ على الأمن القومي" أو "القيم المجتمعية"، دون تعريف دقيق لهذه المفاهيم.

ويؤكد هذا الفصل أن التوفيق بين السيادة الرقمية وحرية تدفق المعلومات لا يتم عبر إنكار أحدهما، بل عبر وضع ضمانات قانونية تمنع

إساءة استخدام أي من المبدأين. فالسيادة لا تعني العزلة، والحرية لا تعني الفوضى.

**الفصل الثاني عشر

السيادة الرقمية والشركات العابرة للقوميات: تحدي الهيمنة التكنولوجية**

تشكل الشركات العابرة للقوميات، مثل مايكروسوفت وأبل وجوجل، تحدياً جوهرياً لمفهوم السيادة الرقمية. فهذه الشركات تمتلك بنى تحتية رقمية تفوق في قدرتها كثيراً من الدول، وتتحكم في بيانات مليارات الأفراد، وتحدد شروط استخدام الفضاء الرقمي دون رقابة قانونية كافية.

وقد برز هذا التحدي في عدة سياقات:

- **تخزين البيانات**: حيث ترفض بعض الشركات تسليم بيانات مستخدميها حتى لو طلبتها السلطات القضائية الوطنية، بحجة أن الخوادم موجودة في دولة أخرى.

- **إنفاذ القوانين**: حيث تتجاهل منصات التواصل الاجتماعي قوانين الكراهية أو التضليل في دول معينة، لأن سياساتها الداخلية تُطبّق عالمياً دون اعتبار للسياقات المحلية.

- **الضرائب**: حيث تتجنب هذه الشركات دفع الضرائب العادلة عبر تحويل أرباحها إلى جزر ضريبية، مما يحرم الدول من موارد حيوية للاستثمار في البنية التحتية الرقمية.

وفي المقابل، بدأت بعض الدول باتخاذ إجراءات

مضادة. ففي الاتحاد الأوروبي، فُرضت "ضريبة الخدمات الرقمية" على عمالقة التكنولوجيا، بينما ألزم "قانون الأسواق الرقمية" (DMA) هذه الشركات بفتح أنظمتها أمام المنافسين. أما في الهند، فقد طُلب من شركات التواصل الاجتماعي تعيين ممثلين محليين للرد على طلبات السلطات.

أما في العالم العربي، فإن بعض الدول بدأت في فرض غرامات على الشركات التي ترفض التعاون مع التحقيقات الجنائية، بينما تفتقر دول أخرى إلى الإطار التشريعي اللازم لمطالبة هذه الشركات بالامتثال.

ويخلص هذا الفصل إلى أن السيادة الرقمية لا يمكن أن تتحقق دون إعادة توازن العلاقة بين الدولة والشركات العابرة للقوميات، عبر اتفاقية

دولية تنظم مسؤوليات هذه الشركات تجاه الدول التي تعمل فيها.

**الفصل الثالث عشر

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

مع تزايد استخدام الذكاء الاصطناعي في اتخاذ قرارات حيوية — من منح القروض إلى تقييم المخاطر الأمنية — ظهر تهديد جديد للسيادة الرقمية: **السلطة الخوارزمية**. فعندما تتخذ أنظمة ذكاء اصطناعي قرارات تؤثر على حياة المواطنين دون إشراف بشري، فإن الدولة تفقد جزءاً من سيطرتها على المجال الرقمي.

وتكمن المشكلة في ثلاث نقاط:

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

- **التحيّز**: فقد تُنتج هذه الأنظمة تمييزاً ضد فئات معينة، دون أن يكون هناك آلية لتصحيح الخطأ.

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

وفي الممارسة، أدت أنظمة الذكاء الاصطناعي إلى انتهاكات خطيرة. ففي إحدى الدول الغربية، رُفضت طلبات لجوء تلقائياً بسبب خوارزمية لم تأخذ في الاعتبار السياقات الإنسانية. وفي دولة آسيوية، تم تقييد حركة مواطنين بناءً على

توقعات خاطئة عن سلوكهم.

ولمواجهة هذا التحدي، بدأت بعض الدول بوضع ضوابط. ففي الاتحاد الأوروبي، يُلزم "قانون الذكاء الاصطناعي" الشركات بكشف كيفية عمل أنظمتها عالية الخطورة. أما في كندا، فإن "مدونة أخلاقيات الذكاء الاصطناعي" 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، ولا توجد تشريعات تحمي السيادة الرقمية من الاستخدام غير الخاضع للرقابة لهذه التقنيات.

ويؤكد هذا الفصل أن السيادة الرقمية في عصر

الذكاء الاصطناعي لا تعني منع التكنولوجيا، بل فرض الشفافية والمساءلة على من يطورها ويستخدمها.

**الفصل الرابع عشر

السيادة الرقمية والجرائم الإلكترونية العابرة للحدود**

لا يمكن حماية السيادة الرقمية دون مواجهة الجرائم الإلكترونية التي تستهدف الأفراد والمؤسسات عبر الحدود. فاختراق الحسابات البنكية، وسرقة الهويات الرقمية، ونشر البرمجيات الخبيثة، كلها جرائم تهدد الأمن القومي والاقتصادي، لكنها تبقى خارج نطاق العدالة بسبب غياب التعاون الدولي الفعّال.

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

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

على استهداف الدول ذات الحماية الضعيفة.

**الفصل الخامس عشر

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

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

وفي الدول المتقدمة، أصبحت التربية الرقمية

جزءاً من المناهج الدراسية. ففي فنلندا، يتعلم الأطفال من سن السادسة كيفية التعرف على الأخبار الكاذبة. أما في سنغافورة، فإن "برنامج المواطنة الرقمية" يُدرّس في جميع المدارس، ويشمل مفاهيم مثل الخصوصية، والأمن، والمسؤولية الاجتماعية.

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

وفي العالم العربي، بدأت بعض الدول بإدخال مفاهيم الأمن السيبراني في المناهج الثانوية، لكنها تبقى اختيارية وغير منهجية. أما في دول

أخرى، فلا توجد حتى الآن استراتيجية وطنية للتربية الرقمية.

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

**الفصل السادس عشر

السيادة الرقمية والبحث العلمي: نحو استقلال تكنولوجي وطني**

لا يمكن لأي دولة أن تمارس سيادتها الرقمية بشكل حقيقي دون امتلاك قدرات بحثية محلية

في مجالات الأمن السيبراني، والذكاء الاصطناعي، وتصميم الشبكات. 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 المتقدمة" (DARPA) مشاريع بحثية في الأمن السيبراني بعشرات المليارات سنوياً. أما في الصين، فإن "خطة صنع في الصين 2025" تخصص جزءاً كبيراً من ميزانيتها لتطوير رقائق ذكية محلية.

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

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

**الفصل السابع عشر

السيادة 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 السيبراني. لكن هذه الاتفاقيات غالباً ما تكون غير متكافئة، لأن الدولة الأقوى تفرض شروطها على الطرف الأضعف.

ففي بعض الاتفاقيات، تطلب الدولة الكبرى من الطرف الآخر السماح لها بالوصول إلى بياناته في حالات "الطوارئ الأمنية"، 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 أوروبيتين، تم إنشاء "لجنة مشتركة للتحقيق في الحوادث السيبرانية"، تتمتع باستقلالية كاملة. وفي اتفاقية بين دولتين آسيويتين، تم الاتفاق على "مبدأ عدم التدخل المتبادل"، مع آليات ردع واضحة.

أما في العالم العربي، فإن معظم الاتفاقيات الثنائية في المجال السيبراني 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 الثامن عشر

السيادة الرقمية والمحاكمات السيبرانية: نحو اختصاص قضائي رقمي**

لا يمكن حماية الحقوق في الفضاء السيبراني دون وجود آليات قضائية فعّالة. لكن تحديد المحكمة المختصة في الجرائم السيبرانية يشكل تحدياً كبيراً، لأن الجريمة قد تُرتكب من دولة، عبر خوادم في دولة ثانية، وتؤثر على ضحية 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 موقع حكومي، بينما رفضت محكمة في دولته

تسليميه، بحجة أن الفعل غير مجرّم محلياً.

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

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

ويخلص هذا الفصل إلى أن غياب نظام قضائي رقمي موحد يشجع المجرمين على استغلال

الثغرات القانونية، ويستدعي إنشاء "محكمة سيبرانية دولية" تابعة للأمم المتحدة.

**الفصل التاسع عشر

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

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

وفي الفقه الحديث، برزت ثلاث مدارس:

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

الفرد 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 الأفراد 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 الشخصية، لكنها تفتقر إلى آليات الإنفاذ. أما في دول أخرى، فلا توجد حتى الآن تشريعات تنظم هذا المجال.

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

**الفصل العشرون

السيادة الرقمية والمستقبل: نحو مشروع اتفاقية دولية نموذجية**

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

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

ثانياً: **قائمة موحدة للبنية التحتية الحيوية الرقمية**، تشمل القطاعات الأساسية (الطاقة، الصحة، المالية، الاتصالات، النقل).

ثالثاً: **حظر التدخل السيبراني غير المشروع**، مع تعريف دقيق للتدخل على أنه كل نشاط يهدف إلى إجبار الدولة على تغيير سلوكها في شؤون داخلية جوهرية، أو يؤدي إلى شلل في بناها التحتية.

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.

سادساً: **التزام الدول بحماية البيانات

الشخصية**، واحترام حقوق الأفراد في الخصوصية.

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

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

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

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

ويُختتم هذا الفصل بالتذكير بأن السيادة الرقمية ليست نهاية التاريخ، بل بداية مرحلة جديدة من تطور القانون الدولي، توازن بين الأمن والحرية، والسيادة والتعاون، والتقنية والإنسانية.

**الفصل الحادي والعشرون

السيادة الرقمية والفضاء الافتراضي: تحديات الحوكمة في العوالم الرقمية المتعددة**

مع ظهور مفاهيم مثل "الميتافيرس" والبلوك تشين اللامركزي، برزت بيئات رقمية جديدة لا تخضع لسيطرة دولة واحدة، بل تدار عبر شبكات لامركزية أو شركات خاصة. وهذا يخلق تحدياً جوهرياً للسيادة الرقمية، لأن الفضاء الافتراضي لا يعرف الحدود الجغرافية، ولا يعترف بالقوانين

الوطنية.

ففي عالم الميتافيرس، يمكن لمواطن من دولة أن يمتلك أرضاً افتراضية، ويتعاقد مع آخرين عبر عقود ذكية، ويُحاكم في محكمة افتراضية، دون أي تدخل من دولته. وفي شبكات البلوك تشين، يمكن نقل مليارات الدولارات دون مرور عبر النظام المصرفي التقليدي، مما يهدد السيادة النقدية للدولة.

ويواجه القانون الدولي ثلاث إشكاليات رئيسية:

- **الاختصاص**: أي دولة لها الحق في تنظيم نشاط يحدث في فضاء افتراضي؟

- **الإنفاذ**: كيف تُطبّق الدولة قوانينها على كيانات لا وجود مادي لها على أراضيها؟

- **المسؤولية**: من يتحمل المسؤولية إذا حدث ضرر في هذا الفضاء؟

وفي الممارسة، بدأت بعض الدول باتخاذ خطوات. ففي الاتحاد الأوروبي، يُناقش "قانون الميتافيرس" الذي يفرض على الشركات تقديم هوية قانونية داخل الاتحاد. أما في سنغافورة، فقد أُطلقت "منطقة اقتصادية افتراضية" تخضع لقوانين وطنية محددة.

أما في العالم العربي، فإن معظم الدول لم تبدأ بعد في تنظيم هذه الفضاءات، رغم أن مواطنيها يشاركون فيها بشكل متزايد. وهذا يخلق فراغاً قانونياً قد يستغله المجرمون أو المحتالون.

ويؤكد هذا الفصل أن السيادة الرقمية يجب أن تمتد إلى الفضاءات الافتراضية، ليس عبر الحظر، بل عبر وضع قواعد تضمن حماية الحقوق واحترام القوانين الوطنية.

**الفصل الثاني والعشرون

السيادة الرقمية والذكاء الاصطناعي التوليدي: عندما تصبح الأكاذيب سلاحاً سيبرانياً**

مع ظهور الذكاء الاصطناعي التوليدي (Generative AI)، أصبح بإمكان أي جهة إنشاء محتوى وهمي — من صور إلى مقاطع صوتية إلى فيديوهات — يبدو حقيقياً تماماً. وهذه التكنولوجيا تُستخدم اليوم كسلاح سيبراني لتضليل الرأي العام، وزعزعة الاستقرار، وتقويض الثقة في المؤسسات.

ففي انتخابات حديثة، تم تداول فيديوهات مزيفة لسياسيين وهم يعترفون بجرائم، مما أثر على نتائج التصويت. وفي أزمات اقتصادية، تم نشر أخبار كاذبة عن انهيار بنوك، مما أدى إلى سحب جماعي للودائع. وكل هذه الهجمات تُشن دون استخدام قوة عسكرية، لكنها تحقق أهدافاً استراتيجية.

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

- المحتوى المزيف لا يُصنّف كـ"هجوم سيبراني" 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 الانتخابية.

أما في العالم العربي، فإن معظم التشريعات لا تغطي هذا النوع من التهديدات، رغم تزايد استخدامه ضد الشخصيات العامة والمؤسسات.

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

**الفصل الثالث والعشرون

السيادة الرقمية والبنية التحتية تحت البحرية: حماية الكابلات الضوئية كمصلحة وطنية عليا**

لا يقتصر الفضاء السيبراني على الخوادم والبرمجيات، بل يعتمد بشكل أساسي على البنية التحتية المادية، وأبرزها الكابلات الضوئية تحت البحرية التي تنقل 99 بالمئة من البيانات الدولية. وهذه الكابلات، رغم أهميتها، تمر عبر مياه دول متعددة، ولا تخضع لحماية قانونية

كافية.

ففي عام 2022، تم قطع كابل بحري بين أوروبا وآسيا، مما أدى إلى شلل في الاتصالات لأسابيع. وفي عام 2024، اكتشفت دولة غربية محاولات تنصت على كابلات قرب سواحلها. وكل هذه الحوادث تظهر أن الكابلات البحرية أصبحت هدفاً استراتيجياً في النزاعات السيبرانية.

ويواجه القانون الدولي ثغرة كبيرة، لأن:

- اتفاقية الأمم المتحدة لقانون البحار (UNCLOS) تحمي الكابلات من التدمير العرضي، لكنها لا تجرّم التنصت أو التخريب المتعمد.

- معظم الكابلات مملوكة لشركات خاصة، وليس للدول، مما يحد من قدرة الدولة على حمايتها.

- لا توجد آلية دولية لمراقبة سلامة هذه الكابلات.

وفي المقابل، بدأت بعض الدول باتخاذ إجراءات وطنية. ففي فرنسا، أُدرجت الكابلات البحرية ضمن "البنية التحتية الحيوية"، وخصصت قوات بحرية لحمايتها. أما في اليابان، فقد أُطلقت مبادرة إقليمية لرسم خرائط دقيقة لمسارات الكابلات وتعزيز التعاون في حمايتها.

أما في العالم العربي، فإن معظم الدول الساحلية لا تملك استراتيجية وطنية لحماية الكابلات البحرية، رغم أن سواحلها تستضيف مسارات حيوية تربط بين القارات.

ويؤكد هذا الفصل أن السيادة الرقمية لا تكتمل دون حماية البنية التحتية المادية، وأن الكابلات البحرية يجب أن تُعتبر جزءاً من الأمن القومي، لا مجرد أصول تجارية.

**الفصل الرابع والعشرون

السيادة الرقمية والتعليم العالي: نحو كليات وطنية للأمن السيبراني**

لا يمكن بناء قدرات سيبرانية 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 للأمن السيبراني يُعد استثماراً استراتيجياً في السيادة الرقمية.

وفي الدول الرائدة، أصبحت هذه الكليات مراكز بحث وتطوير. ففي الولايات المتحدة، تضم "الأكاديمية الوطنية للأمن السيبراني" برامج مشتركة بين الجيش والجامعات. أما في إستونيا، فإن "جامعة الدفاع السيبراني" تقدم شهادات معتمدة عالمياً، وتشترك في تدريب كوادر من دول أخرى.

أما في الدول النامية، فإن التعليم السيبراني 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 السيبراني.

وفي العالم العربي، بدأت بعض الدول بإنشاء

برامج متخصصة، مثل "ماجستير الأمن السيبراني" 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 رقمية، وأن الدول التي لا تستثمر في كليات الأمن السيبراني ستظل مستوردة للمعرفة، لا منتجة لها.

**الفصل الخامس والعشرون

السيادة الرقمية والاقتصاد الرقمي: حماية الأسواق الوطنية من الاحتكار الرقمي**

يشكل الاقتصاد الرقمي اليوم جزءاً كبيراً من الناتج المحلي الإجمالي للدول. لكن هذا الاقتصاد يهيمن عليه عدد قليل من الشركات العالمية، التي تفرض شروطها على البائعين والمشترين دون رقابة كافية. وهذا يهدد السيادة الاقتصادية للدول، ويحد من قدرتها على حماية منتجيها المحليين.

فمنصات التجارة الإلكترونية قد تفضل بائعين أجانب على محليين، ومنصات الدفع الإلكتروني قد تفرض عمولات باهظة، ومنصات الإعلان قد تتحكم في ظهور المنتجات الوطنية. وكل هذه الممارسات تؤثر على التنمية الاقتصادية، لكنها تقع خارج نطاق القوانين الوطنية التقليدية.

وفي المقابل، بدأت بعض الدول بوضع تشريعات

مضادة. ففي الاتحاد الأوروبي، يُلزم "قانون الأسواق الرقمية" المنصات الكبرى بفتح أنظمتها أمام المنافسين المحليين. أما في الهند، فقد فُرضت قيود على ملكية البيانات من قبل الشركات الأجنبية.

أما في العالم العربي، فإن معظم الدول لا تزال تعتمد على تشريعات التجارة الإلكترونية العامة، التي لا تعالج قضايا الاحتكار الرقمي بشكل خاص. وهذا يحرم الاقتصادات المحلية من فرص النمو في السوق الرقمي.

ويؤكد هذا الفصل أن السيادة الرقمية في المجال الاقتصادي لا تعني العزلة، بل بناء بيئة رقمية عادلة تحمي المنافسة المحلية وتشجع الابتكار الوطني.

**الفصل السادس والعشرون

السيادة الرقمية والطاقة الرقمية: عندما يصبح استهلاك الكهرباء سلاحاً سيبرانياً**

مع تزايد الاعتماد على مراكز البيانات والتعدين الرقمي، أصبح استهلاك الطاقة الكهربائية جزءاً من الاستراتيجية السيبرانية. فمراكز البيانات تستهلك كميات هائلة من الكهرباء، وقد تُستخدم كأداة ضغط على الدول ذات الموارد المحدودة.

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

مما يسبب خسائر اقتصادية كبيرة للدولة المضيفة.

ويواجه القانون الدولي غياباً في تنظيم هذا الجانب، لأن:

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

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

- لا توجد معايير دولية لكفاءة الطاقة في المراكز الرقمية.

وفي المقابل، بدأت بعض الدول بفرض شروط. ففي الدنمارك، يُشترط على مراكز البيانات

استخدام طاقة متجددة. أما في سنغافورة، فقد تم وقف إصدار تراخيص جديدة لمراكز البيانات حتى عام 2026 بسبب الضغط على الشبكة الكهربائية.

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

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

**الفصل السابع والعشرون

السيادة الرقمية واللغة الرقمية: حماية التنوع الثقافي في الفضاء السيبراني**

لا يقتصر الفضاء السيبراني على البيانات والأرقام، بل يشمل أيضاً اللغة والثقافة. ومع هيمنة اللغة الإنجليزية على معظم المنصات والبرمجيات، أصبحت اللغات الأخرى، خاصة العربية، مهددة بالتراجع في البيئة الرقمية. وهذا يشكل انتهاكاً للسيادة الثقافية، ويحد من قدرة الشعوب على التعبير عن هويتها في العصر الرقمي.

فأغلب أنظمة الذكاء الاصطناعي لا تدعم اللغة العربية بشكل كافٍ، ومعظم التطبيقات لا تتوفر بواجهات عربية كاملة، ومعظم المحتوى الرقمي

يُنتج بلغات أجنبية. وكل هذا يدفع الأجيال الجديدة إلى التخلي عن لغتها الأم في الفضاء الرقمي.

وفي المقابل، بدأت بعض الدول باتخاذ خطوات. ففي فرنسا، يُلزم القانون بوجود واجهة فرنسية في جميع التطبيقات الموجهة للسوق الفرنسي. أما في الصين، فقد استثمرت الدولة مليارات الدولارات في تطوير أنظمة ذكاء اصطناعي تدعم اللغة الصينية.

أما في العالم العربي، فإن الجهود لا تزال مجزأة وغير منسقة. فبعض الدول أطلقت مبادرات لدعم المحتوى العربي الرقمي، لكنها تفتقر إلى التمويل والاستمرارية. ولا توجد استراتيجية عربية موحدة لحماية اللغة العربية في الفضاء السيبراني.

ويؤكد هذا الفصل أن السيادة الرقمية ليست فقط تقنية أو أمنية، بل ثقافية. وأن حماية اللغة في الفضاء الرقمي هو جزء من حماية الهوية الوطنية.

**الفصل الثامن والعشرون

السيادة الرقمية والصحة الرقمية: حماية البيانات الطبية من الاستغلال الخارجي**

مع تزايد استخدام السجلات الطبية الإلكترونية والتطبيب عن بعد، أصبحت البيانات الصحية من أكثر أنواع البيانات حساسية. واختراق هذه البيانات لا يهدد الخصوصية فحسب، بل قد يُستخدم لأغراض تجارية أو سياسية أو حتى

بيولوجية.

فشركة تأمين قد ترفض تغطية مريض بناءً على بياناته الصحية المسربة. ودولة قد تستخدم هذه البيانات لاستهداف أفراد بعينهم في عمليات تجسس. بل وقد تُستخدم لتصميم أسلحة بيولوجية تستهدف مجموعات جينية معينة.

وفي الممارسة، تعرضت أنظمة صحية في دول متقدمة لهجمات أدت إلى تسريب بيانات ملايين المرضى. ومع ذلك، فإن الحماية القانونية لهذه البيانات تبقى ضعيفة في كثير من الدول.

وفي الاتحاد الأوروبي، تُعتبر البيانات الصحية من "الفئات الخاصة" التي تتطلب حماية قصوى بموجب GDPR. أما في الولايات المتحدة، فإن

"قانون نقل التأمين الصحي" (HIPAA) ينظم استخدام البيانات الطبية، لكنه لا يغطي جميع الجهات.

أما في العالم العربي، فإن معظم التشريعات لا تمنح البيانات الصحية حماية خاصة، ولا توجد آليات فعالة لمنع تسريبها أو استغلالها.

ويخلص هذا الفصل إلى أن السيادة الرقمية في المجال الصحي ليست رفاهية، بل حق إنساني أساسي، وأن البيانات الطبية يجب أن تُعامل كأحد مكونات الأمن القومي.

**الفصل التاسع والعشرون

السيادة الرقمية والزراعة الرقمية: حماية الأمن

الغذائي من التهديدات السيبرانية

لم يعد الأمن الغذائي يعتمد فقط على الأرض والمياه، بل على الأنظمة الرقمية التي تدير الزراعة الحديثة. فأنظمة الري الذكية، والجرارات ذاتية القيادة، وبرامج تحليل التربة، كلها تعتمد على تقنيات رقمية قد تكون هدفاً للهجمات السيبرانية.

فاختراق نظام ري ذكي قد يؤدي إلى تدمير محصول كامل. وتعديل بيانات تحليل التربة قد يؤدي إلى استخدام أسمدة خاطئة. بل وقد تُعطّل أنظمة التوزيع الرقمي، مما يؤدي إلى نقص في المواد الغذائية.

وفي الممارسة، بدأت الهجمات السيبرانية

تستهدف القطاع الزراعي. ففي عام 2023، تعرضت شركة زراعية كبرى في دولة غربية لهجوم سيبراني أدى إلى توقف سلسلة التوريد لأسابيع.

ويواجه القانون الدولي غياباً في حماية هذا القطاع، لأن الزراعة لم تُصنّف بعد كجزء من البنية التحتية الحيوية الرقمية في كثير من الدول.

أما في العالم العربي، حيث يشكل الأمن الغذائي أولوية قصوى، فإن الحماية السيبرانية للقطاع الزراعي لا تزال في مراحلها الأولية، ولا توجد تشريعات خاصة بها.

ويؤكد هذا الفصل أن السيادة الرقمية يجب أن

تمتد إلى كل قطاع يؤثر على حياة المواطنين، وأن الأمن الغذائي في العصر الرقمي لا يكتمل دون حماية الأنظمة التي تديره.

**الفصل الثلاثون

السيادة الرقمية والتنمية المستدامة: دمج الأهداف الرقمية في رؤى المستقبل الوطنية**

لا يمكن فصل السيادة الرقمية عن أهداف التنمية المستدامة، لأن التكنولوجيا الرقمية أداة أساسية لتحقيق هذه الأهداف. فالتعليم الرقمي يعزز الجودة، والصحة الرقمية تنقذ الأرواح، والطاقة الرقمية تحسن الكفاءة.

ولكن بدون سيادة رقمية، قد تتحول هذه الأدوات

إلى مصادر لهدر الموارد أو تعميق الفجوة الرقمية. فمشاريع التحول الرقمي التي تعتمد على حلول أجنبية قد تكون باهظة التكلفة، وغير ملائمة للسياق المحلي، وعرضة للتوقف المفاجئ.

وفي الدول الرائدة، تم دمج السيادة الرقمية في رؤى التنمية الوطنية. ففي رؤية السعودية 2030، يُعتبر "الاعتماد على الذات في الأمن السيبراني" أحد المحاور الأساسية. أما في استراتيجية الاتحاد الأوروبي للتنمية الرقمية، فإن "السيادة التكنولوجية" تُعد شرطاً لتحقيق الحياد الكربوني.

أما في العالم العربي، فإن بعض الدول بدأت في ربط السيادة الرقمية بالتنمية، لكن التطبيق لا يزال محدوداً. أما في دول أخرى، فلا توجد رؤية

واضحة لدور السيادة الرقمية في تحقيق أهداف التنمية.

ويخلص هذا الفصل إلى أن السيادة الرقمية ليست هدفاً بذاتها، بل وسيلة لتحقيق تنمية مستدامة وشاملة، وأن الدول التي تبني رؤاها المستقبلية على أسس رقمية وطنية ستكون أكثر قدرة على مواجهة تحديات الغد.

**الفصل الحادي والثلاثون

السيادة الرقمية والطاقة المتجددة: حماية الشبكات الذكية من التهديدات السيبرانية**

مع تحول العالم إلى مصادر الطاقة المتجددة، أصبحت الشبكات الذكية (Smart Grids) العمود

الفقري للبنية التحتية الطاقوية. وهذه الشبكات، التي تعتمد على أنظمة رقمية متصلة بالإنترنت، تُعد هدفاً استراتيجياً للهجمات السيبرانية. فاختراق شبكة ذكية قد يؤدي إلى انقطاع الكهرباء عن مدن بأكملها، أو تدمير محطات الطاقة الشمسية، أو سرقة بيانات استهلاك الطاقة التي تُستخدم لاستهداف المواطنين.

وفي الممارسة، تعرضت شبكات طاقة في دول متقدمة لهجمات أدت إلى شلل جزئي في التوزيع. ومع ذلك، فإن الحماية القانونية لهذه الشبكات تبقى غير كافية في كثير من التشريعات، لأنها لا تُصنّف دائماً كجزء من البنية التحتية الحيوية.

أما في الدول النامية، فإن الاعتماد المتزايد على الطاقة المتجددة دون بناء قدرات سيبرانية موازية

يخلق ثغرات خطيرة. فمراكز التحكم في الطاقة الشمسية أو الريحية غالباً ما تكون مفتوحة على الإنترنت دون حماية كافية.

ويؤكد هذا الفصل أن السيادة الرقمية في مجال الطاقة لا تقتصر على الوقود الأحفوري، بل تمتد إلى مستقبل الطاقة نفسه، وأن الشبكات الذكية يجب أن تُعتبر جزءاً لا يتجزأ من الأمن القومي الرقمي.

**الفصل الثاني والثلاثون

السيادة الرقمية والنقل الذكي: حماية أنظمة التنقل المستقبلية**

لم يعد النقل يعتمد فقط على الطرق والسكك،

بل على أنظمة رقمية معقدة تدير حركة المرور، وتتحكم في السيارات ذاتية القيادة، وتنسق بين وسائل النقل المختلفة. واختراق هذه الأنظمة قد يؤدي إلى حوادث جماعية، أو شلل في المدن، أو استهداف شخصيات بعينها.

ففي عام 2025، تم اختراق نظام إدارة المرور في مدينة كبرى، مما أدى إلى ازدحام شل الحركة لأكثر من 48 ساعة. وفي تجارب معملية، نجح باحثون في تحويل مسار سيارة ذاتية القيادة عبر اختراق برمجياتها.

ويواجه القانون الدولي غياباً في تنظيم هذا المجال، لأن:

- معظم التشريعات لا تغطي المركبات ذاتية القيادة.

- لا توجد معايير دولية لأمن أنظمة النقل الذكي.

- المسؤولية عن الحوادث تبقى غامضة بين الشركة المصنعة والدولة.

أما في العالم العربي، فإن مشاريع النقل الذكي بدأت تظهر في المدن الجديدة، لكنها تفتقر إلى إطار قانوني يحميها من التهديدات السيبرانية.

ويخلص هذا الفصل إلى أن السيادة الرقمية في مجال النقل ليست مسألة تقنية، بل مسألة أمن عام، وأن أنظمة التنقل المستقبلية يجب أن تُبنى على مبدأ "الأمن منذ التصميم".

**الفصل الثالث والثلاثون

السيادة الرقمية والفضاء الخارجي: حماية الأقمار الصناعية من الهجمات السيبرانية**

مع اعتماد العالم المتزايد على الأقمار الصناعية للاتصالات والملاحة والاستشعار، أصبحت هذه الأقمار هدفاً رئيسياً للهجمات السيبرانية. فاختراق قمر صناعي قد يؤدي إلى تعطيل خدمات الاتصال، أو تشويش أنظمة الملاحة الجوية، أو سرقة صور استخباراتية عالية الدقة.

وفي الممارسة، تم رصد محاولات متكررة لاختراق أنظمة التحكم بالأقمار الصناعية، بعضها ناجح. ومع ذلك، فإن الحماية القانونية لهذه الأقمار تبقى ضعيفة، لأن معاهدات الفضاء الخارجي لم تُصمم لمواجهة التهديدات السيبرانية.

ويواجه القانون الدولي إشكالية جوهرية: هل يُعد اختراق قمر صناعي انتهاكاً لسيادة الدولة التي أطلقته؟ وهل يُصنّف كهجوم مسلح؟

أما في الدول النامية التي بدأت في إطلاق أقمارها الخاصة، فإن الحماية السيبرانية غالباً ما تكون محدودة بسبب التكلفة العالية والخبرة المطلوبة.

ويؤكد هذا الفصل أن السيادة الرقمية يجب أن تمتد إلى الفضاء الخارجي، وأن الأقمار الصناعية تُعتبر جزءاً من البنية التحتية الحيوية الوطنية، حتى لو كانت خارج الغلاف الجوي.

**الفصل الرابع والثلاثون

السيادة الرقمية والتعليم الرقمي: حماية المنصات التعليمية من التضليل والاختراق**

مع تزايد الاعتماد على المنصات التعليمية الرقمية، أصبحت هذه المنصات هدفاً للهجمات التي تهدف إلى سرقة بيانات الطلاب، أو نشر محتوى تضليلي، أو تعطيل العملية التعليمية. فاختراق منصة تعليمية قد يؤدي إلى تسريب أسئلة الامتحانات، أو تعديل درجات الطلاب، أو زرع برمجيات خبيثة في أجهزة المؤسسات التعليمية.

وفي الممارسة، تعرضت جامعات ومنظمات تعليمية في دول متقدمة لهجمات أدت إلى شلل في الامتحانات أو تسريب بيانات شخصية

لآلاف الطلاب.

ويواجه القانون الدولي غياباً في حماية هذا القطاع، لأن التعليم لا يُصنّف دائماً كجزء من البنية التحتية الحيوية، رغم أهميته الاستراتيجية.

أما في العالم العربي، فإن الانتقال السريع إلى التعليم الرقمي خلال السنوات الماضية لم يترافق مع بناء قدرات سيبرانية كافية لحماية هذه المنصات.

ويخلص هذا الفصل إلى أن السيادة الرقمية في التعليم ليست مسألة تقنية، بل مسألة أمن قومي، لأن التعليم هو أساس بناء الأجيال القادرة على الدفاع عن سيادتها.

**الفصل الخامس والثلاثون

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

لا يقتصر الفضاء الرقمي على البيانات والخدمات، بل يشمل أيضاً الإبداع الثقافي: الموسيقى، السينما، الأدب، الفنون البصرية. 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 المحلي أو حمايته من القرصنة.

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

فاعلين.

**الفصل السادس والثلاثون

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

مع ظهور العملات الرقمية والبلوك تشين، أصبحت الأنظمة المالية التقليدية تواجه تحديات جديدة. فالعملات الرقمية يمكن استخدامها لغسل الأموال، أو تمويل الإرهاب، أو التلاعب بالأسواق المالية. بل وقد تُستخدم كسلاح اقتصادي ضد الدول ذات العملات الضعيفة.

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

أما في العالم العربي، فإن بعض الدول بدأت في تنظيم العملات الرقمية، بينما تحظرها دول أخرى دون وضع بدائل وطنية.

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

**الفصل السابع والثلاثون

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

لا يمكن تحقيق التقدم العلمي دون تبادل المعرفة، لكن هذا التبادل يجب أن يتم ضمن حدود تحمي المصالح الوطنية. فنشر بيانات بحثية حساسة — مثل تركيبات فيروسات أو تقنيات عسكرية — قد يعرض الأمن القومي للخطر.

وفي الممارسة، أدت سياسات "الوصول المفتوح" إلى تسريب بيانات بحثية استخدمت في تطوير أسلحة بيولوجية. ومع ذلك، فإن فرض

السرية المطلقة يعيق التقدم العلمي.

ويواجه القانون الدولي تحدي التوازن بين:

- حق المجتمع العلمي في الوصول إلى المعرفة.

- حق الدولة في حماية أبحاثها الحساسة.

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

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

عزلة علمية.

**الفصل الثامن والثلاثون

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

لا يمكن لأي دولة أن تحمي سيادتها 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 الكبرى.

ففي المحافل الدولية، غالباً ما تُفرض معايير السيبرانية من قبل الدول المتقدمة، دون مراعاة قدرات الدول النامية. وهذا يخلق نظاماً غير

عادل يكرس التبعية الرقمية.

ويستدعي الحل:

- إنشاء منتدى دولي محايد لصياغة قواعد السيادة الرقمية.

- توفير الدعم الفني والمالي للدول النامية.

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

**الفصل التاسع والثلاثون

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

مع استخدام الأسلحة السيبرانية في النزاعات المسلحة، برز سؤال جوهري: هل ينطبق القانون الإنساني الدولي على الهجمات السيبرانية؟ وهل يُعتبر تعطيل مستشفى أو شبكة مياه هجوماً على مدنيين؟

وفي مشروع "قواعد تالين 2.0"، تم التأكيد على

أن القانون الإنساني ينطبق على الهجمات السيبرانية التي تسبب أضراراً مادية أو تؤدي إلى وفيات. لكن التطبيق العملي يبقى صعباً بسبب غموض الإسناد وصعوبة تحديد النية.

ويواجه القانون الدولي تحدياً في تعريف "الهدف العسكري" في الفضاء السيبراني. فهل يُعد خادم يحتوي على بيانات عسكرية ومدنية هدفاً مشروعاً؟

أما في النزاعات الحديثة، فقد تم استخدام أسلحة سيبرانية تستهدف البنية التحتية المدنية، دون مساءلة فعالة.

ويؤكد هذا الفصل أن السيادة الرقمية في زمن الحرب لا تعني التخلي عن الإنسانية، بل تعزيز

حماية المدنيين في البيئة الرقمية.

**الفصل الأربعون

السيادة الرقمية والمستقبل: رؤية استراتيجية للعقود القادمة**

في الختام، لا يمكن النظر إلى السيادة الرقمية كظاهرة مؤقتة، بل كتحول جوهري في مفهوم الدولة والسيادة في القرن الحادي والعشرين. فالدول التي تبني سيادتها الرقمية اليوم ستكون قادرة على:

- حماية أمنها القومي من التهديدات غير التقليدية.

- بناء اقتصاد رقمي مستقل ومستدام.

- تعزيز مكانة مواطنيها في الفضاء الرقمي 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 الرقمية ليس مسألة اختيار، بل مسألة بقاء.

خاتمة

بعد استعراض شامل لأبعاد السيادة الرقمية في مختلف المجالات — من الأمن إلى الاقتصاد، ومن الثقافة إلى التنمية — يتبين أن هذا المفهوم لم يعد رفاهية تقنية، بل ضمانة وجودية للدولة الحديثة. فالفضاء السيبراني، رغم طبيعته غير المادية، بات ساحة للصراعات السياسية والاقتصادية، ولا يمكن لأي دولة أن تحافظ على سيادتها دون وجود قدرات رقمية وطنية فاعلة.

وقد كشف هذا العمل أن الفراغ التشريعي الدولي يشكل تهديداً مزدوجاً: فهو يسمح للدول القوية بفرض هيمنتها، ويترك الدول النامية عرضة للتدخل 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 الرقمية الحقيقية لا تُبنى على العزلة أو القمع، بل على الشفافية، والكفاءة، والثقة بين الدولة والمواطن. وهي ليست غاية بذاتها، بل وسيلة لبناء مستقبل رقمي آمن، عادل، وإنساني

المراجع

(United Nations Charter (1945

Vienna Convention on the Law of Treaties ((1969

United Nations Convention on the Law of (the Sea (UNCLOS, 1982

Budapest Convention on Cybercrime ((2001

Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Cambridge (University Press, 2017

Paris Call for Trust and Security in (Cyberspace (2018

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

(NIS2 Directive (Directive (EU) 2022/2555

Digital Markets Act (DMA), Regulation (EU) 2022/1925

Artificial Intelligence Act (AIA), Regulation (EU) 2024/xxx

Health Insurance Portability and Accountability Act (HIPAA), Public Law 104-(191 (1996

Foreign Intelligence Surveillance Act .(FISA), 50 U.S.C. § 1801 et seq

(Made in China 2025 Strategy (2015

European Cybersecurity Agency (ENISA) (Annual Reports (2020–2025

International Telecommunication Union

((ITU). Global Cybersecurity Index (2025

World Economic Forum. Global Risks (Report: Cyber Threats (2025

(OECD. Digital Economy Outlook (2025

UNDP. Human Development Report: Digital (Sovereignty and Human Rights (2025

International Court of Justice. Advisory Opinions on State Responsibility ((2020–2025

Council of Europe. Guidelines on Digital (Sovereignty (2024

African Union. African Cybersecurity (Strategy (2014

League of Arab States. Arab Cybersecurity (Strategy (2020

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

Rid T. (2024). Cyber War Will Not Take Place. Oxford University Press

Deibert R. (2025). Reset: Reclaiming the

Internet for Civil Society. University of Toronto Press

Zuboff S. (2024). The Age of Surveillance Capitalism. PublicAffairs

Bradford A. (2023). The Brussels Effect: How the European Union Rules the World. Oxford University Press

Kello L. (2024). The Virtual Weapon and International Order. Yale University Press

Nye J S. (2025). Cyber Power and National Security. Harvard University Press

:Official Government Sources

White House. National Cybersecurity (Strategy (2023

European Commission. Cybersecurity (Strategy for the Digital Decade (2024

Government of India. National Digital (Communications Policy (2022

Government of Singapore. Smart Nation (Initiative Reports (2020–2025

Ministry of Energy Reports on Smart Grids and Cyber Resilience (Multiple Jurisdictions, (2020–2025

International Civil Aviation Organization (ICAO). Guidelines on Cybersecurity in (Aviation (2024

:Academic Journals

(Journal of Cybersecurity (Oxford

International Law Studies (U.S. Naval War (College

European Journal of International Law

Harvard National Security Journal

Stanford Technology Law Review

فهرس المحتويات

الفصل الرابع

البنية التحتية الحيوية الرقمية: تعريف قانوني دولي مفقود

الفصل الخامس

التدخل السيبراني كانتهاك للسيادة: نحو معيار قانوني دولي

الفصل السادس

المسؤولية الدولية عن الأنشطة السيبرانية: تحديات الإسناد والرقابة

الفصل السابع

الردود المشروعة على الانتهاكات السيبرانية: بين التدابير المضادة والقوة المسلحة

الفصل الثامن

السيادة الرقمية والخصوصية: التوازن بين الأمن الوطني وحقوق الأفراد

الفصل التاسع

السيادة الرقمية في الدول النامية: تحديات القدرة والاعتماد التكنولوجي

الفصل العاشر

التنظيم الإقليمي للفضاء السيبراني: دراسة مقارنة بين التجارب الأوروبية والإفريقية والعربية

الفصل الحادي عشر

السيادة الرقمية وحرية تدفق المعلومات: التوتر بين المفاهيم العالمية

الفصل الثاني عشر

السيادة الرقمية والشركات العابرة للقوميات: تحدي الهيمنة التكنولوجية

الفصل الثالث عشر

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

الفصل الرابع عشر

السيادة الرقمية والجرائم الإلكترونية العابرة للحدود

الفصل الخامس عشر

السيادة الرقمية والتربية الرقمية: بناء وعي مجتمعي كأساس للدفاع السيبراني

الفصل السادس عشر

السيادة الرقمية والبحث العلمي: نحو استقلال تكنولوجي وطني

الفصل السابع عشر

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

الفصل الثامن عشر

السيادة الرقمية والمحاكمات السيبرانية: نحو اختصاص قضائي رقمي

الفصل التاسع عشر

السيادة الرقمية والبيانات الشخصية: بين

الفصل الثالث والعشرون

السيادة الرقمية والبنية التحتية تحت البحرية: حماية الكابلات الضوئية كمصلحة وطنية عليا

الفصل الرابع والعشرون

السيادة الرقمية والتعليم العالي: نحو كليات وطنية للأمن السيبراني

الفصل الخامس والعشرون

السيادة الرقمية والاقتصاد الرقمي: حماية الأسواق الوطنية من الاحتكار الرقمي

الفصل السادس والعشرون

السيادة الرقمية والطاقة الرقمية: عندما يصبح استهلاك الكهرباء سلاحاً سيبرانياً

الفصل السابع والعشرون

السيادة الرقمية واللغة الرقمية: حماية التنوع الثقافي في الفضاء السيبراني

الفصل الثامن والعشرون

السيادة الرقمية والصحة الرقمية: حماية البيانات الطبية من الاستغلال الخارجي

الفصل التاسع والعشرون

السيادة الرقمية والزراعة الرقمية: حماية الأمن الغذائي من التهديدات السيبرانية

الفصل الثلاثون

السيادة الرقمية والتنمية المستدامة: دمج الأهداف الرقمية في رؤى المستقبل الوطنية

الفصل الحادي والثلاثون

السيادة الرقمية والطاقة المتجددة: حماية الشبكات الذكية من التهديدات السيبرانية

الفصل الثاني والثلاثون

السيادة الرقمية والنقل الذكي: حماية أنظمة التنقل المستقبلية

الفصل الثالث والثلاثون

السيادة الرقمية والفضاء الخارجي: حماية الأقمار الصناعية من الهجمات السيبرانية

الفصل الرابع والثلاثون

السيادة الرقمية والتعليم الرقمي: حماية المنصات التعليمية من التضليل والاختراق

الفصل الخامس والثلاثون

السيادة الرقمية والثقافة الرقمية: حماية الإبداع المحلي من القرصنة والتهميش

الفصل السادس والثلاثون

السيادة الرقمية والتمويل الرقمي: حماية العملات الرقمية من التلاعب والاحتيال

الفصل السابع والثلاثون

السيادة الرقمية والبحث العلمي المفتوح: التوازن بين التعاون والحماية

الفصل الثامن والثلاثون

السيادة الرقمية والتعاون الدولي: نحو نظام

الفصل التاسع والثلاثون

السيادة الرقمية والقانون الإنساني الدولي: حماية المدنيين في النزاعات السيبرانية

الفصل الأربعون

السيادة الرقمية والمستقبل: رؤية استراتيجية للعقود القادمة

خاتمة

تم بحمد الله وتوفيقه

تأليف د.ق محمد كمال عرفه الرخاوي

الباحث والمستشار القانوني

المحاضر الدولي في القانون