السيادة الصحية الرقمية: دراسة قانونية دولية حول حق الدول في حماية بياناتها الصحية من الاستغلال الخارجي وبناء نظام عدالة صحية رقمي عالمي

تأليف

د. محمد كمال عرفه الرخاوي

تقديم

في عالم يشهد تسارعاً غير مسبوق في التحول الرقمي للقطاع الصحي، لم تعد البيانات الصحية مجرد معلومات سريرية، بل أصبحت

سلعة استراتيجية تُتداول في أسواق عالمية بلا رقابة. فبينما تمتلك شركات التكنولوجيا الكبرى قواعد بيانات جينية لمئات الملايين من البشر، تفتقر الدول النامية إلى الحد الأدنى من الحماية القانونية لبيانات مواطنيها. وهذا التفاوت الصارخ يكشف عن ثغرة جوهرية في النظام القانوني الدولي: غياب مفهوم "السيادة الصحية الرقمية".

هذا العمل لا يهدف إلى تكرار الخطابات الطبية التقليدية، بل إلى بناء **نظرية قانونية دولية جديدة** تجعل من "السيادة الصحية الرقمية" مبدأً قابلاً للإنفاذ، لا شعاراً إنسانياً. 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: **البيانات الصحية ليست ملكاً للشركات، بل جزء من الأمن القومي لكل دولة**. ومن دون سيادة صحية رقمية، لن تكون هناك عدالة صحية حقيقية.

والله ولي التوفيق.

**الفصل الأول

السيادة الصحية الرقمية: من الخصوصية الفردية إلى المبدأ القانوني الدولي**

لم يعد مفهوم السيادة الصحية محصوراً في

إدارة المستشفيات أو توفير الأدوية، بل امتد ليشمل القدرة على حماية الأنظمة الرقمية التي تدير البيانات الصحية الوطنية. فالطب الحديث يعتمد اليوم على أنظمة ذكاء اصطناعي للتشخيص، ومنصات رقمية لتوزيع الأدوية، وقواعد بيانات جينية لتطوير العلاجات. واختراق أي من هذه الأنظمة قد يؤدي إلى كوارث صحية وطنية.

ويُعرّف هذا العمل السيادة الصحية الرقمية على أنها **حق الدولة الحصري في تنظيم وحماية الأنظمة الرقمية التي تدير بياناتها الصحية، ومنع أي استغلال خارجي لهذه البيانات يهدد أمنها الصحي أو يفرض عليها اعتماداً تكنولوجياً غير مرغوب فيه**. ولا يعني هذا الحق عزلة صحية، بل ممارسة السيادة في بيئة رقمية عابرة للحدود.

وقد بدأ هذا المفهوم يتشكل عملياً. ففي عام 2024، تم اختراق نظام صحي وطني في دولة أوروبية، مما أدى إلى تسريب بيانات 10 ملايين مريض. وفي عام 2025، سُرقت بيانات لقاحات استراتيجية من مركز بحثي في آسيا، مما أثار مخاوف من استغلالها في تطوير أسلحة بيولوجية.

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

ويؤكد هذا الفصل أن السيادة الصحية الرقمية ليست رفاهية تقنية، بل ضمانة وجودية للدولة الحديثة، وأن غيابها في القانون الدولي يخلق فراغاً خطيراً يهدد استقرار النظام الصحي

العالمي ذاته.

**الفصل الثاني

الفراغ القانوني الدولي في حماية الأنظمة الصحية الرقمية**

رغم أهمية الصحة العامة، لا يزال القانون الدولي يفتقر إلى اتفاقية شاملة تحمي الأنظمة الصحية الرقمية. فاتفاقيات منظمة الصحة العالمية، رغم اعترافها بأهمية الصحة الرقمية، لا تتضمن أي آليات لحماية السيادة الوطنية على البيانات الصحية.

وهذا الفراغ ليس نتيجة غفلة، بل انعكاس لصراع المصالح بين الشركات الكبرى التي تسعى إلى

هيمنة تكنولوجية، والدول النامية التي تطالب بحقها في تطوير أنظمة صحية وطنية.

ففي مؤتمر الصحة العالمي 2025، تم اعتماد "إعلان الصحة الرقمية"، لكنه اكتفى بـ"التعاون الطوعي"، دون أي التزام قانوني بحماية الأنظمة الرقمية. أما في منظمة الصحة العالمية، 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 الصحية الرقمية، رغم الطلبات المتكررة من دول نامية.

أما في المحاكم الوطنية، فقد بدأت بعض

الدعاوى تظهر. ففي الهند، رفعت منظمات صحية دعوى ضد شركة أمريكية بتهمة استغلال بيانات المرضى دون موافقة. أما في البرازيل، فإن محكمة وطنية ألزمت شركة بتقديم كود المصدر لأنظمة التشخيص الذكية التي تبيعها.

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

**الفصل الثالث

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

لا يمكن فهم السيادة الصحية الرقمية دون مقارنتها بالسيادة الصحية التقليدية التي بُنيت على مفاهيم مثل "الرعاية الصحية الشاملة" و"الاستقلالية الطبية". لكن البيئة الرقمية الحديثة تتحدى كل هذه المفاهيم.

فأولاً، **الرعاية الصحية الشاملة** تصبح مستحيلة إذا كانت أنظمة التشخيص تعتمد على خوارزميات أجنبية لا تأخذ في الاعتبار السياقات المحلية.

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

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

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

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

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

**الفصل الرابع

البنية التحتية الصحية الرقمية: تعريف قانوني دولي مفقود**

أحد أكبر الثغرات في النقاش الدولي حول السيادة الصحية الرقمية هو غياب تعريف قانوني متفق عليه لما يُسمى "البنية التحتية الصحية 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 الصحية الرقمية: أنظمة التشخيص الذكية، منصات توزيع الأدوية، قواعد البيانات الجينية، والسجلات الصحية الإلكترونية. أما في الاتحاد الأوروبي، فتركز على سلاسل التوريد الرقمية للأدوية ونظم تتبع الأمراض. أما في الصين، فتضيف إليها "منصات البيانات الصحية الوطنية".

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

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

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

- أنظمة التشخيص والعلاج الذكية.

- قواعد البيانات الجينية والسريرية.

- منصات توزيع الأدوية والتتبع الرقمي.

- أنظمة الإنذار المبكر عن الأوبئة.

- السجلات الصحية الإلكترونية الوطنية.

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

**الفصل الخامس

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

لا يمكن حماية السيادة الصحية الرقمية دون تحديد ما يُعد "تلاعباً سيبرانياً غير مشروع" في الأنظمة الصحية. فليس كل نشاط سيبراني عبر الحدود يشكل انتهاكاً. فاستخدام طبيب لمنصة أجنبية للتشخيص لا يُعد تدخلاً، لكن

اختراق نظام صحي وطني لتغيير نتائج الفحوصات يُعد عدواناً.

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

- **التلاعب غير المشروع**: وهو الذي يمس "الأمن الصحي الجوهرى" للدولة، كالإضرار بقدرة النظام الصحي على مواجهة الأوبئة.

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

لكن "قواعد تالين" ليست ملزمة، بل رأياً فقهياً. كما أن معيار "الأمن الصحي الجوهرى" غامض. فهل يُعد اختراق منصة توزيع الأدوية تدخلاً؟

وهل يختلف عن اختراق نظام التشخيص؟

وفي الممارسة، تختلف الدول في تطبيق المعيار. ففي عام 2024، اعتبرت دولة أوروبية أن اختراق نظامها الصحي 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 الصحية، أو

- يؤدي إلى شلل في النظام الصحي الوطني،

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

**الفصل السادس

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

لا يمكن تطبيق مبدأ السيادة الصحية الرقمية دون حل إشكالية "الإسناد"، أي تحديد الدولة أو الجهة المسؤولة عن هجوم سيبراني صحي. 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 الصحي.

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

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

**الفصل السابع

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

عندما تتعرض دولة لهجوم سيبراني على أنظمتها الصحية، ما هي وسائل الرد المتاحة لها؟ وهل يجوز استخدام القوة العسكرية رداً على هجوم سيبراني صحي؟ 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 الصحي "هجوماً مسلحاً"؟ في مشروع "قواعد تالين"، تم اقتراح معيار "الضرر المادي المكافئ"، أي أن الهجوم السيبراني الذي يسبب دماراً يعادل قصفاً جوياً يبرر الرد العسكري. فمثلاً، تعطيل النظام الصحي الوطني لأسابيع قد يُصنّف كهجوم مسلح.

أما في الممارسة، فقد ردت دول على هجمات تستهدف أنظمة الأوبئة، بينما اكتفت دول أخرى بالتدابير الدبلوماسية بعد اختراق منصات توزيع الأدوية.

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

**الفصل الثامن

السيادة الصحية الرقمية وبراءات الاختراع الطبية: التوتر بين الابتكار والاستغلال**

لا يمكن الحديث عن السيادة الصحية الرقمية دون معالجة توترها الجوهري مع نظام براءات الاختراع الطبية. فاليوم، تتحكم شركات كبرى في براءات اختراع على الأدوية واللقاحات والتقنيات التشخيصية، مما يمنحها سلطة احتكارية على الصحة العالمية.

فشركة "فايزر" الأمريكية تمتلك براءات اختراع على أكثر من 70% من اللقاحات الحديثة. وشركة "نوفارتيس" السويسرية تفرض رسوماً باهظة على الأدوية الأساسية، مما يجعلها غير متاحة لملايين المرضى في الدول النامية.

وفي الممارسة، أدت هذه البراءات إلى:

- منع الدول النامية من تطوير أدوية محلية.

- رفع تكاليف الرعاية الصحية 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 الصحية 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 الصحة.

**الفصل التاسع

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

بينما تمتلك القوى الكبرى أدوات متقدمة لفرض سيادتها الصحية 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 الصحي الرقمي.

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

وفي هذا السياق، بدأت بعض الدول باتخاذ خطوات. فالهند أطلقت "مشروع البيانات الصحية الوطنية"، بينما أنشأت الصين "منطقة بيانات صحية سيادية". أما في إفريقيا، فقد بدأت مبادرات إقليمية لتطوير أنظمة تشخيص مقاومة للأوبئة.

أما في العالم العربي، فإن معظم الدول تشجع الصحة الرقمية دون دراسة تأثيرها على السيادة الصحية، مما قد يؤدي إلى أزمات صحية مستقبلية.

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

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

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

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

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

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

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

الصحية 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 للاستغلال الخارجي.

**الفصل الحادي عشر

السيادة الصحية الرقمية والبيانات الجينية: حماية الخصوصية الوراثية من الاستغلال الخارجي**

لا يمكن تحقيق السيادة الصحية الرقمية دون حماية البيانات الجينية للمواطنين. فهذه البيانات،

التي تمثل خصوصية وراثية لا تقدر بثمن، أصبحت اليوم هدفاً للشركات الكبرى التي تسعى إلى تسجيل براءات اختراع عليها، مما يمنحها احتكاراً على العلاجات المستقبلية.

ففي إفريقيا، تم تسجيل براءات اختراع على جينات مقاومة للملاريا طوّرتها المجتمعات المحلية عبر الأجيال. وفي أمريكا اللاتينية، سُجلت براءات على جينات فريدة بعد تحليلها في مختبرات أجنبية. وكل هذه الممارسات تُعد شكلاً من "القرصنة الجينية" التي تستغل الخصوصية الوراثية دون مقابل عادل.

ويواجه القانون الدولي غياباً في حماية هذه البيانات، لأن:

- اتفاقية التنوع البيولوجي (CBD) تدعو إلى

"تقاسم المنافع"، لكنها لا تمنع التسجيل المباشر للبراءات.

- بروتوكول ناغويا ينظم الوصول إلى الموارد الجينية، لكنه لا يغطي البيانات الرقمية المشتقة منها.

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

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

أما في العالم العربي، فإن معظم الدول لا تزال

تعتمد على تقديرات دولية، ولا تملك أنظمة وطنية لحماية بياناتها الجينية.

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

**الفصل الثاني عشر

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

مع تزايد استخدام الذكاء الاصطناعي في اتخاذ

قرارات طبية — من التشخيص إلى وصف العلاجات — ظهر تهديد جديد للسيادة الصحية الرقمية: **السلطة الخوارزمية**. فعندما تتخذ أنظمة ذكاء اصطناعي قرارات تؤثر على حياة المرضى دون إشراف بشري، فإن الدولة تفقد جزءاً من سيطرتها على المجال الصحي.

وتكمن المشكلة في ثلاث نقاط:

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

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

- **الاستقلالية**: فبعض الأنظمة تتعلم ذاتياً،

وقد تتخذ قرارات تتعارض مع السياسات الصحية الوطنية.

وفي الممارسة، أدت أنظمة الذكاء الاصطناعي إلى انتهاكات خطيرة. ففي دولة آسيوية، رفضت خوارزمية تشخيص أمراض نادرة لأنها لا تحقق أرباحاً كافية. وفي دولة أفريقية، أوصت أنظمة ذكاء اصطناعي باستخدام أدوية مستوردة بدلاً من الأدوية المحلية، مما أدى إلى تآكل الصناعة الدوائية 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 الطبي" 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 الطبي، ولا توجد تشريعات تحمي السيادة الصحية من الاستخدام غير الخاضع للرقابة لهذه التقنيات.

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

**الفصل الثالث عشر

السيادة الصحية الرقمية والجرائم الإلكترونية

الصحية: مكافحة الاحتيال الصحي الرقمي**

لا يمكن حماية السيادة الصحية الرقمية دون مواجهة الجرائم الإلكترونية التي تستهدف الأفراد والمؤسسات الصحية عبر الحدود. فاختراق الحسابات البنكية للمرضى، وسرقة الهويات الصحية الرقمية، ونشر البرمجيات الخبيثة في أنظمة المستشفيات، كلها جرائم تهدد الصحة العامة، لكنها تبقى خارج نطاق العدالة بسبب غياب التعاون الدولي الفعّال.

وتشير التقديرات إلى أن الخسائر العالمية من الجرائم الإلكترونية الصحية تجاوزت 100 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 الصحية".

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 الصحية ليست مسألة أمنية فقط، بل اختبار عملي لمدى التزام الدول بمبدأ السيادة الصحية الرقمية، لأن غياب العدالة يشجع المجرمين على استهداف الدول ذات الحماية الضعيفة.

**الفصل الرابع عشر

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

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

وفي الدول المتقدمة، أصبحت التربية الرقمية الصحية جزءاً من البرامج التدريبية. ففي هولندا، يتعلم المرضى كيفية التعرف على المواقع الطبية المزيفة. أما في سنغافورة، فإن "برنامج

المواطنة الرقمية الصحية" يُدرّس في جميع مراكز التدريب الصحي، ويشمل مفاهيم مثل الخصوصية، والأمن، والمسؤولية الاجتماعية.

أما في الدول النامية، فإن التربية الرقمية الصحية غالباً ما تكون مقتصرة على النخبة، أو تُقدّم عبر حملات إعلامية محدودة. وهذا يخلق فجوة رقمية داخل المجتمع الصحي 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 الصحي في برامج التدريب، لكنها تبقى اختيارية وغير منهجية. أما في دول أخرى، فلا توجد حتى الآن استراتيجية وطنية للتربية الرقمية الصحية.

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

**الفصل الخامس عشر

السيادة الصحية الرقمية والبحث العلمي الصحي: نحو استقلال تكنولوجي وطني**

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

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

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

**الفصل السادس عشر

السيادة الصحية 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 الصحي 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 الصحية في حالات "الطوارئ الصحية"، 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 الصحية"، 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 الصحي 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 الصحية الرقمية والمحاكمات الصحية: نحو اختصاص قضائي رقمي**

لا يمكن حماية الحقوق في الفضاء الصحي الرقمي دون وجود آليات قضائية فعّالة. لكن تحديد المحكمة المختصة في الجرائم السيبرانية الصحية يشكل تحدياً كبيراً، لأن الجريمة قد تُرتكب من دولة، عبر خوادم في دولة ثانية، وتؤثر على مريض 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 صحياً 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 الصحية"، التي تُلزم الدول الأعضاء بالاعتراف المتبادل بالأحكام. أما في دول أخرى، فلا تزال المحاكم تفتقر إلى الخبرة الفنية اللازمة لفهم الأدلة الرقمية الصحية.

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

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

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

**الفصل الثامن عشر

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

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

وفي الفقه الحديث، برزت ثلاث مدارس:

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

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

**الفصل التاسع عشر

السيادة الصحية الرقمية والصحة العامة: حماية المجتمعات من التكنولوجيا الصحية غير المسؤولة**

لا يمكن فصل السيادة الصحية الرقمية عن الصحة العامة، لأن بعض التقنيات الصحية الرقمية قد تؤدي إلى أضرار مجتمعية طويلة الأمد. فأنظمة التشخيص الذكية قد تهمل الأمراض النادرة، والمنصات الرقمية قد تروج لأدوية غير فعالة، والبيانات الجينية قد تُستخدم للتمييز ضد فئات معينة.

وفي الممارسة، أدت بعض المشاريع الصحية الرقمية إلى أضرار مجتمعية كبيرة. ففي دولة آسيوية، أدت أنظمة التشخيص الذكية إلى تجاهل أمراض المناطق الريفية. وفي دولة أفريقية، أدت المنصات الرقمية إلى انتشار أدوية

مزيفة بسبب غياب الرقابة.

ويواجه القانون الدولي غياباً في تنظيم هذا الجانب، لأن:

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

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

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

وفي المقابل، بدأت بعض الدول بوضع تشريعات. ففي الدنمارك، يُشترط على أنظمة التشخيص الذكية تغطية جميع الأمراض دون تمييز. أما في

كوستاريكا، فقد تم وقف إصدار تراخيص جديدة للمنصات الصحية الرقمية حتى يتم تقييم تأثيرها المجتمعي.

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

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

**الفصل العشرون

السيادة الصحية الرقمية والمستقبل: نحو

مشروع اتفاقية دولية نموذجية**

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

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

ثانياً: **قائمة موحدة للبنية التحتية الصحية الرقمية**، تشمل الأنظمة الأساسية

(التشخيص الذكي، البيانات الجينية، منصات توزيع الأدوية، السجلات الصحية الإلكترونية).

ثالثاً: **حظر التدخل السيبراني غير المشروع** في الأنظمة الصحية، مع تعريف دقيق للتدخل على أنه كل نشاط يهدف إلى إجبار الدولة على تغيير سياستها الصحية، أو يؤدي إلى شلل في النظام الصحي 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 صحي.

سادساً: **التزام الدول بحماية البيانات الصحية**، واحترام حقوق المرضى في الخصوصية.

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

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

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

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

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

**الفصل الحادي والعشرون

السيادة الصحية الرقمية والصيدلة الرقمية: حماية المرضى من الاستغلال التكنولوجي**

لا يمكن فصل السيادة الصحية الرقمية عن

حماية المرضى من الاستغلال التكنولوجي في قطاع الصيدلة. فمع تزايد الاعتماد على المنصات الرقمية لتوزيع الأدوية، أصبح المريض عرضة لشروط احتكارية تفرضها الشركات الكبرى. فبعض المنصات تروج لأدوية باهظة الثمن بدلاً من البدائل الأرخص، بينما تفرض شركات أخرى رسوماً إضافية على التوصيل السريع للمرضى في حالات الطوارئ.

وفي الممارسة، أدت هذه الممارسات إلى:

- رفع تكاليف الرعاية الصحية بشكل غير متناسب.

- توجيه المرضى نحو أدوية تحقق أرباحاً أعلى للشركات.

- خلق اعتماد دائم على المنصات الرقمية.

ويواجه القانون الدولي غياباً في تنظيم هذا المجال، لأن:

- لا توجد اتفاقيات دولية تحمي حقوق المرضى في الوصول العادل للأدوية الرقمية.

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

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

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

تنظيم الصيدلة الرقمية" يمنع الترويج للأدوية باهظة الثمن دون ذكر البدائل.

أما في العالم العربي، فإن معظم الدول لا تزال تعتمد على سياسات صحية تقليدية، ولا توجد آليات قانونية لحماية المرضى من الاستغلال التكنولوجي في الصيدلة الرقمية.

ويؤكد هذا الفصل أن السيادة الصحية الرقمية في مجال الصيدلة ليست مسألة تقنية، بل مسألة عدالة اجتماعية، وأن غياب الحماية القانونية لهذا القطاع يهدد استقرار النظام الصحي بأكمله.

**الفصل الثاني والعشرون

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

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

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

ويواجه القانون الدولي غياباً في تنظيم هذا الجانب، لأن:

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

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

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

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

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

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

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

**الفصل الثالث والعشرون

السيادة الصحية الرقمية وسلامة المرضى: حماية المرضى من التلاعب الرقمي

لا يمكن فصل السيادة الصحية الرقمية عن حماية سلامة المرضى. فمع تزايد استخدام المنصات الرقمية في تقديم الرعاية الصحية، أصبحت هذه المنصات هدفاً للهجمات التي تهدف إلى تغيير جرعات الأدوية، أو تزوير نتائج الفحوصات، أو نشر معلومات مضللة عن العلاجات.

ففي عام 2024، تم اختراق منصة طبية في دولة أوروبية، مما أدى إلى تغيير جرعات أدوية لمرضى السكري، وتسبب في حالات تسمم جماعي. وفي عام 2025، تم نشر معلومات مضللة عن علاجات السرطان عبر منصات ذكاء اصطناعي، مما أدى إلى رفض المرضى

للعلاجات الفعالة.

ويواجه القانون الدولي غياباً في حماية هذا القطاع، لأن:

- لا توجد اتفاقيات دولية تنظم سلامة الرعاية الصحية الرقمية.

- معظم المنصات الرقمية لا تخضع لرقابة صحية كافية.

- لا توجد معايير دولية لشفافية المعلومات الصحية الرقمية.

وفي المقابل، بدأت بعض الدول بوضع تشريعات. ففي الاتحاد الأوروبي، يُلزم "قانون سلامة الرعاية الصحية الرقمية" المنصات بنشر معلومات

دقيقة ومحدثة. أما في الولايات المتحدة، فإن "إدارة الغذاء والدواء" بدأت بفحص الخوارزميات التي تحدد المعلومات العلاجية.

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

ويؤكد هذا الفصل أن السيادة الصحية الرقمية في مجال سلامة المرضى ليست رفاهية، بل حق إنساني أساسي، وأن سلامة الرعاية الصحية الرقمية يجب أن تُعتبر جزءاً من الأمن القومي الصحي.

**الفصل الرابع والعشرون

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

لا يمكن تحقيق السيادة الصحية الرقمية دون بناء وعي مجتمعي لدى المرضى ومقدمي الخدمة حول حقوقهم الرقمية وواجباتهم تجاه الصحة العامة. فالتعليم الصحي الرقمي ليس مجرد نشر معلومات، بل تمكين المواطنين من المطالبة بحقوقهم والمشاركة في صنع القرار الصحي.

ففي الدول التي يُدرّس فيها القانون الصحي الرقمي في المدارس، يزداد الوعي بحقوق الأجيال القادمة في الخصوصية الصحية. وفي المجتمعات التي تُدرّب على التكيف مع التهديدات السيبرانية، تنخفض الخسائر البشرية

والمادية.

وفي الممارسة، بدأت بعض الدول بدمج الصحة الرقمية في المناهج التعليمية. ففي فنلندا، يتعلم الأطفال من سن السادسة كيفية حماية بياناتهم الصحية. أما في كوستاريكا، فإن "التعليم من أجل الصحة الرقمية" جزء أساسي من النظام التعليمي.

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

ويؤكد هذا الفصل أن التعليم الصحي الرقمي هو استثمار استراتيجي في العدالة، وأن الدول التي لا تستثمر فيه ستظل شعوبها عاجزة عن المطالبة بحقوقها.

**الفصل الخامس والعشرون

السيادة الصحية الرقمية والثقافة الصحية: حماية التراث الصحي من الاندثار الرقمي**

لا يقتصر التغير الرقمي على الاقتصاد أو الصحة، بل يهدد أيضاً التراث الصحي للبشرية. فالتحول إلى الطب الرقمي قد يؤدي إلى اندثار المعرفة

التقليدية، وانهيار الممارسات العلاجية المحلية، وانهيار المجتمعات الصحية التقليدية.

ففي إفريقيا، تهدد أنظمة التشخيص الذكية الممارسات العلاجية التقليدية التي طوّرها المجتمعات عبر الأجيال. وفي أمريكا اللاتينية، يؤدي الاعتماد على الأدوية الرقمية إلى تآكل المهارات العلاجية التقليدية. بل إن بعض اللغات والعادات الصحية 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 الصحية على قائمة الخطر.

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

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

**الفصل السادس والعشرون

السيادة الصحية الرقمية والتمويل الصحي الرقمي: حماية الدول النامية من الديون الصحية**

مع تزايد الحاجة إلى التمويل الصحي الرقمي،

برز خطر جديد: تحويل "الديون الصحية الرقمية" إلى أداة للاستغلال. فبعض الدول النامية تقترض مليارات الدولارات لتمويل مشاريع صحية رقمية، لكنها تجد نفسها عاجزة عن السداد بسبب الأزمات الصحية التي تضرب اقتصادها.

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

ويواجه القانون الدولي غياباً في حماية هذه الدول، لأن:

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

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

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

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

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

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

**الفصل السابع والعشرون

السيادة الصحية الرقمية والنقل الصحي الرقمي: حماية سلاسل التوريد من التهديدات السيبرانية**

لم يعد النقل الصحي يعتمد فقط على الطرق والسكك، بل على أنظمة رقمية معقدة تدير سلاسل التوريد من المصنع إلى المريض. واختراق هذه الأنظمة قد يؤدي إلى تلف الأدوية،

أو تأخير التوزيع، أو سرقة الشحنات.

ففي عام 2024، تم اختراق نظام تتبع الشحنات الصحية في دولة أوروبية، مما أدى إلى تلف آلاف الجرعات من اللقاحات بسبب تأخير التبريد. وفي عام 2025، تم سرقة شحنات أدوية أساسية عبر اختراق أنظمة الموانئ الرقمية.

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

**الفصل الثامن والعشرون

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

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

ضد الدول النامية في المفاوضات الدولية.

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

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

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

**الفصل التاسع والعشرون

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

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

ويستدعي الحل:

- إنشاء منتدى دولي محايد لصياغة قواعد السيادة الصحية الرقمية.

- توفير الدعم الفني والمالي للدول النامية.

- احترام التنوع في النماذج الوطنية للسيادة

الصحية 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 الصحية الرقمية يجب أن يقوم على مبدأ "السيادة المشتركة"، لا "الهيمنة الصحية الرقمية".

**الفصل الثلاثون

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

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

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

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

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

**الفصل الحادي والثلاثون

السيادة الصحية الرقمية والفضاء الخارجي: حماية الأرض من التلوث الفضائي الصحي**

مع تزايد الأنشطة الفضائية المتعلقة بالصحة — من الأقمار الصناعية لمراقبة الأوبئة إلى الطائرات المسيرة الفضائية لتوزيع اللقاحات — برز تهديد جديد: التلوث الفضائي الذي يؤثر على الأنظمة الصحية. فحطام الأقمار الصناعية قد يعيق أنظمة الرصد الصحي، بينما تنبعثات الصواريخ تؤثر على الغلاف الجوي الذي ينظم انتشار الأمراض.

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

ويواجه القانون الدولي إشكالية جوهرية: هل يُعد التلوث الفضائي جزءاً من "المسؤولية

الصحية 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 الصحية الرقمية يجب أن تمتد إلى الفضاء الخارجي، وأن الأنشطة الفضائية الصحية يجب أن تخضع لمبدأ "الوقاية الصحية" مثلها مثل أي نشاط صناعي آخر.

**الفصل الثاني والثلاثون

السيادة الصحية الرقمية والذكاء الاصطناعي التوليدي: عندما تصبح الأخبار الكاذبة سلاحاً صحياً

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 الصحية الوطنية.

ففي عام 2025، تم تداول فيديوهات مزيفة لأطباء وهم يحذرون من لقاحات آمنة، مما أدى إلى انخفاض معدلات التطعيم وانتشار الأوبئة. وفي أزمات صحية، تم نشر أخبار كاذبة عن نقص

في الأدوية 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 صحي" 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 الصحية.

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

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

**الفصل الثالث والثلاثون

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

مع تزايد الاعتماد على البيانات الضخمة في تحليل الصحة العامة، 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 صحية 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 الصحية.

- معظم العقود بين الدول والشركات تبقى سرية.

- لا توجد معايير لـ"السيادة الصحية الرقمية".

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

ويؤكد هذا الفصل أن البيانات الصحية ليست

مجرد أرقام، بل أداة للعدالة، وأن الدول التي لا تحمي سيادتها الرقمية ستظل عاجزة عن المطالبة بحقوقها الصحية.

**الفصل الرابع والثلاثون

السيادة الصحية الرقمية والتعليم العالي الصحي: نحو كليات وطنية للقانون الصحي الرقمي**

لا يمكن بناء قدرات صحية 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 الصحي الرقمي يُعد استثماراً استراتيجياً في السيادة الصحية الرقمية.

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

أما في الدول النامية، فإن التعليم الصحي 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 الصحي الرقمي.

وفي العالم العربي، بدأت بعض الدول بإنشاء برامج متخصصة، مثل "ماجستير الأمن الصحي

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 صحية رقمية، وأن الدول التي لا تستثمر في كليات القانون الصحي الرقمي ستظل مستوردة للمعرفة، لا منتجة لها.

**الفصل الخامس والثلاثون

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

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

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

**الفصل السادس والثلاثون

السيادة الصحية الرقمية والتمويل الرقمي الصحي: حماية العملات الصحية من التلاعب

والاحتيال**

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

وفي الممارسة، أدت عمليات الاحتيال في سوق العملات الرقمية الصحية 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 الصحية، لأنها لا تخضع لسلطة

دولة واحدة، ولا يمكن تتبع مالكيها بسهولة.

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

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

**الفصل السابع والثلاثون

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

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

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

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

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

**الفصل الثامن والثلاثون

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

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

ويستدعي الحل:

- إنشاء منتدى دولي محايد لصياغة قواعد السيادة الصحية الرقمية.

- توفير الدعم الفني والمالي للدول النامية.

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

**الفصل التاسع والثلاثون

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

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

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

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

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

**الفصل الأربعون

السيادة الصحية الرقمية والمستقبل: رؤية استراتيجية للعقود القادمة**

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

- حماية مواطنيها من التلاعب الصحي الرقمي.

- بناء اقتصاد صحي رقمي مستقل ومستدام.

- تعزيز مكانة أجيالها في النظام الصحي 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 الصحية الرقمية ليس مسألة اختيار، بل مسألة بقاء.

خاتمة

بعد استعراض شامل لأبعاد السيادة الصحية 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 الصحي الرقمي، رغم طبيعته غير المادية، بات ساحة للصراعات السياسية والاقتصادية، ولا يمكن لأي دولة أن تحافظ على سيادتها الصحية 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 الصحية الرقمية الحقيقية لا تُبنى على العزلة أو القمع، بل على الشفافية، والكفاءة، والثقة بين الدولة والمواطن. وهي ليست غاية بذاتها، بل وسيلة لبناء مستقبل صحي آمن، عادل، وإنساني.

المراجع

World Health Organization Constitution ((1946

(International Health Regulations (2005

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

(Convention on Biological Diversity (1992

Nagoya Protocol on Access and Benefit-(Sharing (2010

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

United Nations Human Rights Council.

Resolution on the Right to Privacy in the (Digital Age (2023

European Commission. European Health (Data Space Regulation (2024

Government of India. National Digital (Health Mission (2023

Government of China. Smart Health 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). Health Justice and Digital Sovereignty. Oxford University Press

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

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

:Official Government Sources

White House. National Strategy for Digital (Health (2024

European Commission. Digital Health Action (Plan (2023

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

:Academic Journals

(Journal of Health Law (Oxford

International Journal of Digital Health Sovereignty

Harvard Health Law Review

فهرس المحتويات

الفصل السادس

المسؤولية الدولية عن الهجمات السيبرانية الصحية: تحديات الإسناد والرقابة

الفصل السابع

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

الفصل الثامن

السيادة الصحية الرقمية وبراءات الاختراع الطبية: التوتر بين الابتكار والاستغلال

الفصل التاسع

السيادة الصحية الرقمية في الدول النامية: تحديات القدرة والاعتماد التكنولوجي

الفصل العاشر

التنظيم الإقليمي للسيادة الصحية الرقمية: دراسة مقارنة بين التجارب العالمية

الفصل الحادي عشر

السيادة الصحية الرقمية والبيانات الجينية: حماية الخصوصية الوراثية من الاستغلال الخارجي

الفصل الثاني عشر

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

الفصل الثالث عشر

السيادة الصحية الرقمية والجرائم الإلكترونية الصحية: مكافحة الاحتيال الصحي الرقمي

الفصل الرابع عشر

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

السيبراني

الفصل الخامس عشر

السيادة الصحية الرقمية والبحث العلمي الصحي: نحو استقلال تكنولوجي وطني

الفصل السادس عشر

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

الفصل السابع عشر

السيادة الصحية الرقمية والمحاكمات الصحية: نحو اختصاص قضائي رقمي

الفصل الثامن عشر

السيادة الصحية الرقمية والبيانات الصحية: بين الملكية الفردية والسيادة الجماعية

الفصل التاسع عشر

السيادة الصحية الرقمية والصحة العامة: حماية المجتمعات من التكنولوجيا الصحية غير المسؤولة

الفصل العشرون

السيادة الصحية الرقمية والمستقبل: نحو مشروع اتفاقية دولية نموذجية

الفصل الحادي والعشرون

السيادة الصحية الرقمية والصيدلة الرقمية: حماية المرضى من الاستغلال التكنولوجي

الفصل الثاني والعشرون

السيادة الصحية الرقمية والطاقة الصحية: حماية الموارد من الاستنزاف الرقمي

الفصل الثالث والعشرون

السيادة الصحية الرقمية وسلامة المرضى: حماية المرضى من التلاعب الرقمي

الفصل الرابع والعشرون

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

الفصل الخامس والعشرون

السيادة الصحية الرقمية والثقافة الصحية: حماية التراث الصحي من الاندثار الرقمي

الفصل السادس والعشرون

السيادة الصحية الرقمية والتمويل الصحي الرقمي: حماية الدول النامية من الديون الصحية

الفصل السابع والعشرون

السيادة الصحية الرقمية والنقل الصحي الرقمي: حماية سلاسل التوريد من التهديدات السيبرانية

الفصل الثامن والعشرون

السيادة الصحية الرقمية والبحث العلمي الصحي المفتوح: التوازن بين التعاون والحماية

الفصل التاسع والعشرون

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

الفصل الثلاثون

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

الفصل الحادي والثلاثون

السيادة الصحية الرقمية والفضاء الخارجي: حماية الأرض من التلوث الفضائي الصحي

الفصل الثاني والثلاثون

السيادة الصحية الرقمية والذكاء الاصطناعي التوليدي: عندما تصبح الأخبار الكاذبة سلاحاً صحياً

الفصل الثالث والثلاثون

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

الفصل الرابع والثلاثون

السيادة الصحية الرقمية والتعليم العالي الصحي: نحو كليات وطنية للقانون الصحي الرقمي

الفصل الخامس والثلاثون

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

الفصل السادس والثلاثون

السيادة الصحية الرقمية والتمويل الرقمي الصحي: حماية العملات الصحية من التلاعب والاحتيال

الفصل السابع والثلاثون

السيادة الصحية الرقمية والبحث العلمي الصحي المفتوح: التوازن بين التعاون والحماية

الفصل الثامن والثلاثون

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

الفصل التاسع والثلاثون

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

الفصل الأربعون

السيادة الصحية الرقمية والمستقبل: رؤية استراتيجية للعقود القادمة

خاتمة

تم بحمد الله وتوفيقه

تأليف د محمد كمال عرفه الرخاوي

الباحث والمستشار القانوني

المحاضر الدولي في القانون