القانون الإنساني السيبراني: دراسة قانونية مقارنة حول حماية المدنيين في الفضاء الرقمي وبناء نظام إنساني رقمي عالمي لصون الكرامة في العصر الرقمي

تأليف

د. محمد كمال عرفه الرخاوي

تقديم

في عالم يشهد اختناقاً خطيراً في آليات الحماية الإنسانية — حيث تُستهدف المستشفيات عبر الشبكات الرقمية، ويُختَرق الأمن الغذائي عبر الخوارزميات الذكية، ويُحرم المدنيون من حقهم في الحياة الكريمة بسبب

الهجمات السيبرانية — لم يعد كافياً الحديث عن "القانون الإنساني"، بل أصبح من الضروري إعادة تعريف الحماية الإنسانية ذاتها. فالحماية الحديثة ليست مجرد اتفاقيات جنيف، بل شبكة ذكية تتفاعل مع المدنيين في الزمن الحقيقي. ومع ظهور الذكاء الاصطناعي، باتت لدينا الأداة التي طالما حلم بها الفقه الإنساني: القدرة على **منع الهجمات السيبرانية على المدنيين قبل وقوع الضرر**.

هذا العمل لا يهدف إلى تكرار الخطابات الإنسانية التقليدية، بل إلى بناء **نظرية إنسانية رقمية جديدة** تجعل من "القانون الإنساني السيبراني" مبدأً قابلاً للإنفاذ، لا شعاراً تقنياً. 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: **الإنسان ليس هدفاً، بل غاية**. ومن دون قانون إنساني سيبراني، لن تكون هناك حماية إنسانية حقيقية في العصر الرقمي.

والله ولي التوفيق.

**الفصل الأول

القانون الإنساني السيبراني: من اتفاقيات جنيف إلى الظاهرة القانونية الجديدة**

لم يعد مفهوم الحماية الإنسانية محصوراً في اتفاقيات جنيف الأربع، بل امتد ليشمل **أي فعل رقمي يؤدي إلى حماية المدنيين في الفضاء السيبراني**. فالقانون الإنساني السيبراني ليس مجرد استخدام للتكنولوجيا في توثيق الانتهاكات، بل **إعادة تعريف جذرية لعلاقة المجتمع الدولي بالحرب**، تقوم على أساس أن التكنولوجيا يجب أن تكون أداة لمنع الضرر، لا لتوثيقه بعد وقوعه.

ويُعرّف هذا العمل القانون الإنساني السيبراني على أنه **حق المدني في الاستفادة من أنظمة ذكية تُصمم خصيصاً لحمايته من الهجمات السيبرانية في زمن النزاع، وتحديد المسؤولين عنها، وضمان المحاسبة العادلة، مع ضمانات قانونية تحميه من التحيّز الخوارزمي أو الاستهداف الرقمي غير المشروع**. ولا يعني هذا الحق إلغاء اتفاقيات جنيف، بل تحويلها من

وثائق ردّعية إلى أدوات وقائية.

وقد بدأ هذا المفهوم يتشكل عملياً. ففي عام 2024، أطلقت اللجنة الدولية للصليب الأحمر منصة رقمية لجمع الأدلة السيبرانية من المدنيين مباشرة. وفي عام 2025، طوّرت الأمم المتحدة نظاماً ذكياً يربط بين جميع آليات الحماية الإنسانية في منصة واحدة تفاعلية.

أما في الدول النامية، فإن الاعتماد الكلي على النماذج التقليدية يجعلها عاجزة عن مواجهة الهجمات السيبرانية على المدنيين.

ويؤكد هذا الفصل أن القانون الإنساني السيبراني ليس رفاهية تقنية، بل ضمانة وجودية للإنسانية الحديثة، وأن غيابه في

القانون الإنساني الدولي يخلق فراغاً خطيراً يهدد استقرار النظام الإنساني ذاته.

**الفصل الثاني

الفراغ القانوني الإنساني الدولي في الحماية الرقمية للمدنيين**

رغم أهمية الحماية الإنسانية، لا يزال القانون الإنساني الدولي يفتقر إلى اتفاقية شاملة تحمي حقوق المدنيين في الحصول على حماية رقمية. فاتفاقيات جنيف، رغم اعترافها بمبدأ حماية المدنيين، لا تتضمن أي آليات لحمايتهم من الهجمات السيبرانية.

وهذا الفراغ ليس نتيجة غفلة، بل انعكاس لصراع

المصالح بين الدول التي ترى في الهجوم السيبراني "وسيلة حربية مشروعة"، والدول التي تراه "تهديداً وجودياً للإنسانية".

ففي مؤتمر الدول الأطراف في اتفاقيات جنيف لعام 2025، تم اعتماد "إعلان الحماية الرقمية"، لكنه اكتفى بـ"التعاون الطوعي"، دون أي التزام قانوني بحماية المدنيين في الفضاء السيبراني. أما في اللجنة الدولية للصليب الأحمر، فإن "استراتيجية التحول الرقمي" لا تتضمن أي آلية لحماية الحقوق الرقمية للمدنيين.

وفي المحافل القضائية، فإن محكمة العدل الدولية لم تبت في قضية واحدة تتعلق بالقانون الإنساني السيبراني، رغم الطلبات المتكررة من منظمات حقوق الإنسان.

أما في المحاكم الوطنية، فقد بدأت بعض الدعاوى تظهر. ففي كندا، رفع مدني دعوى ضد الدولة بتهمة إهمال جمع الأدلة الرقمية في هجوم سيبراني. أما في ألمانيا، فإن محكمة وطنية ألزمت الدولة بتوفير آليات رقمية لحماية المدنيين.

ويخلص هذا الفصل إلى أن الفراغ القانوني الإنساني الدولي يترك المدنيين بلا حماية، ويستدعي بناء نظام قانوني إنساني دولي جديد يوازن بين الأمن المجتمعي وحق المدني في الحماية الرقمية.

**الفصل الثالث

القانون الإنساني التقليدي مقابل القانون

الإنساني السيبراني: إعادة تشكيل المفاهيم الإنسانية**

لا يمكن فهم القانون الإنساني السيبراني دون مقارنته بالقانون الإنساني التقليدي الذي بُني على مفاهيم مثل "التمييز بين المقاتلين والمدنيين" و"التناسب في الهجوم". لكن البيئة الرقمية الحديثة تتحدى كل هذه المفاهيم.

فأولاً، **التمييز بين المقاتلين والمدنيين** يصبح مستحيلاً إذا كانت الهجمات تُشن عبر خوادم مدنية في دول ثالثة.

ثانياً، **مبدأ التناسب** يصبح غير قابل للتطبيق إذا كان الضرر الرقمي يمتد عبر الحدود دون تمييز.

ثالثاً، **المساواة بين المدنيين** تنهار في البيئة الرقمية، لأن الخوارزميات قد تميز ضد فئات معينة بناءً على بيانات متحيزة.

وفي هذا السياق، بدأت بعض المنظمات بصياغة مفاهيم جديدة. فاللجنة الدولية للصليب الأحمر تستثمر في "الحماية الإنسانية الرقمية الوقائية"، عبر تطوير أنظمة تعلم آلي تُحدّد الهجمات قبل وقوعها. أما الأمم المتحدة، فتبني "المنصات الإنسانية التفاعلية" التي تربط بين جميع الجهات في نظام واحد.

أما في الدول النامية، فإن التطبيق العملي للقانون الإنساني الرقمي يواجه تحديات هيكلية، من نقص الكوادر المتخصصة إلى غياب

التنسيق بين الجهات الإنسانية والرقمية.

ويؤكد هذا الفصل أن القانون الإنساني السيبراني ليس نسخة رقمية من القانون الإنساني التقليدي، بل إعادة تعريف جذرية لمفهوم الحماية ذاته في عالم شبكي لا يعرف الحدود.

**الفصل الرابع

البنية التحتية للقانون الإنساني السيبراني: تعريف قانوني إنساني مفقود**

أحد أكبر الثغرات في النقاش الدولي حول القانون الإنساني السيبراني هو غياب تعريف قانوني متفق عليه لما يُسمى "البنية التحتية

للقانون الإنساني السيبراني". فبدون هذا التعريف، لا يمكن تحديد ما يستحق الحماية القانونية، ولا ما يشكل انتهاكاً لحقوق المدنيين.

وفي الفقه الدولي، تختلف التعريفات بشكل كبير. ففي الولايات المتحدة، تشمل البنية التحتية للقانون الإنساني السيبراني: أنظمة جمع الأدلة الرقمية، منصات التواصل بين الجهات، قواعد البيانات الإنسانية، والسجلات الإلكترونية. أما في الاتحاد الأوروبي، فتركز على أنظمة الحماية الرقمية التي تدمج بين الشفافية والسرعة. أما في الصين، فتضيف إليها "منصات الحماية التفاعلية الرقمية".

أما في الدول النامية، فلا يوجد تعريف موحد. فبعض الدول تعتبر فقط السجلات الإلكترونية جزءاً من البنية التحتية، بينما تهمل أنظمة جمع

الأدلة أو التواصل.

ويكشف هذا التباين أن غياب التعريف الدولي يفتح الباب أمام تفسيرات ذاتية قد تُستخدم لتبرير الانتهاكات ("النظام ليس إنسانياً") أو لتوسيع الهجمات ("كل شيء رقمي").

ولذلك، فإن أول خطوة في بناء نظام قانوني إنساني دولي للقانون الإنساني السيبراني هي الاتفاق على تعريف دقيق، يشمل:

- أنظمة جمع الأدلة الرقمية.

- منصات التواصل التفاعلي بين الجهات الإنسانية الدولية.

- قواعد البيانات الإنسانية الموحدة.

- أنظمة تحديد الهجمات الديناميكية.

- السجلات الإنسانية الإلكترونية القابلة للوصول الفوري.

ويؤكد هذا الفصل أن التعريف ليس مسألة فنية، بل قرار سياسي يعكس رؤية المجتمع الدولي لعلاقته بالإنسانية.

**الفصل الخامس

التمييز الخوارزمي في الحماية الإنسانية: نحو معيار قانوني إنساني دولي**

لا يمكن حماية القانون الإنساني السيبراني دون

تحديد ما يُعد "تمييزاً خوارزمياً غير مشروع" في تحديد الأهداف. فليس كل خوارزمية تميز ضد مدني معين تُعد انتهاكاً. فبعض التمييز قد يكون مبرراً (مثل حماية الأطفال)، لكن التمييز الطبقي أو العرقي ليس كذلك.

وفي الفقه الدولي، بدأت محاولات وضع معايير. ففي مشروع "مبادئ القانون الإنساني السيبراني"، تم التمييز بين:

- **التمييز المشروع**: وهو الذي يراعي الفروق الفردية لتعزيز الحماية.

- **التمييز غير المشروع**: وهو الذي يكرس التحيّزات الاجتماعية أو العنصرية.

لكن هذه المبادئ ليست ملزمة، بل رأياً فقهياً.

كما أن معيار "التمييز المشروع" غامض. فهل يُعد حماية المدنيين الغربيين تمييزاً؟ وهل يختلف عن حماية المدنيين من الدول النامية بسبب تحيّز الخوارزمية؟

وفي الممارسة، تختلف الدول في تطبيق المعيار. ففي عام 2024، اعتبرت محكمة أمريكية أن خوارزمية أولت حماية المدنيين البيض أولوية أعلى كانت "تمييزاً غير مشروع". أما في دولة آسيوية، فاعتبرت المحكمة أن حماية رجال الأعمال كانت "تمييزاً مشروعاً" بسبب أهميتهم الاقتصادية.

ويخلص هذا الفصل إلى أن المعيار القانوني الإنساني الدولي يجب أن يرتكز على **النية والتأثير**، لا على النتيجة وحدها. فكل خوارزمية:

- تهدف إلى تهميش فئة من المدنيين دون مبرر إنساني، أو

- تؤدي إلى حرمان غير مبرر لفئة معينة من الحماية،

يجب أن تُصنّف كـ"تمييز غير مشروع"، بغض النظر عن وسيلة التنفيذ.

**الفصل السادس

المسؤولية الإنسانية الدولية عن الفشل الرقمي: تحديات الإسناد والرقابة**

لا يمكن تطبيق مبدأ القانون الإنساني السيبراني دون حل إشكالية "الإسناد"، أي

تحديد الجهة المسؤولة عن فشل النظام الرقمي في حماية المدنيين. فعلى عكس الحماية التقليدية التي تتحمل مسؤوليتها الجهة الحكومية مباشرة، فإن أنظمة الحماية قد تُطورها شركات خاصة، مما يخلق غموضاً في المسؤولية.

ويواجه القانون الإنساني الدولي ثلاث مستويات من الإسناد:

- **المستوى الأول**: النظام الذي تطوره جهة حكومية مباشرة. هنا تكون المسؤولية واضحة.

- **المستوى الثاني**: النظام الذي تطوره شركة خاصة بطلب من الدولة. هنا يصعب الإثبات، لكن مبدأ "الرقابة الفعالة" قد يُطبّق.

- **المستوى الثالث**: النظام الذي يُستخدم

دون تفويض رسمي. 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 أنظمة الحماية الرقمية التي تنسب إليها وفقاً لمبادئ القانون الدولي". لكنها لم تحدد كيف يتم هذا الإسناد في السياق الإنساني.

أما في الممارسة، فقد استخدمت دول مبدأ "الرقابة العامة" لتحميل شركات التكنولوجيا مسؤولية فشل أنظمة الحماية. بينما رفضت الشركات هذا الربط، بحجة أن الدولة هي من وضعت الشروط.

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

**الفصل السابع

الردود المشروعة على الانتهاكات الإنسانية الرقمية: بين التعويض وإعادة الحماية**

عندما يتعرض مدني لانتهاك في نظامه الإنساني الرقمي، ما هي وسائل الرد المتاحة له؟ وهل يجوز منحه تعويضاً أو إلزام الدولة بإعادة الحماية رداً على التمييز الخوارزمي؟ هذا السؤال يشكل أحد أكثر القضايا إثارة للجدل في القانون الإنساني المعاصر.

ويقر القانون الإنساني الدولي بثلاثة أنواع من الردود:

- **التدابير الإدارية**: مثل تعديل النظام أو تغيير الجهة المشرفة.

- **التعويض المالي**: كتعويض عن الضرر الناتج عن الحرمان غير المبرر من الحماية.

- **إعادة الحماية الإلزامية**: كجزاء على فشل الدولة في توفير حماية رقمية عادلة.

لكن متى يُعتبر الفشل الإنساني "فشلاً جسيماً" يبرر إعادة الحماية؟ في مشروع "مبادئ القانون الإنساني السيبراني"، تم اقتراح معيار "الفرصة الضائعة"، أي أن المدني لو توفر له نظام عادل لكان قد حصل على الحماية في

وقته. فمثلاً، حرمان مدني من الحماية بسبب تحيّز خوارزمي قد يُصنّف كفرصة ضائعة.

أما في الممارسة، فقد منحت محاكم في دول الشمال الأوروبي تعويضات مالية لمدنيين تعرضوا لتمييز رقمي. أما في أمريكا اللاتينية، فقد ألزمت محاكم الدولة بإعادة الحماية بسبب الفشل الرقمي.

ويخلص هذا الفصل إلى أن غياب التوجيه القانوني الواضح يدفع المحاكم إلى اتخاذ قرارات انفعالية، وقد يؤدي إلى تفاوت صارخ في حماية الحقوق الإنسانية.

**الفصل الثامن

القانون الإنساني السيبراني وبراءات الاختراع الإنسانية: التوتر بين الابتكار والاستغلال

لا يمكن الحديث عن القانون الإنساني السيبراني دون معالجة توتره الجوهري مع نظام براءات الاختراع الإنسانية. فاليوم، تتحكم شركات كبرى في براءات اختراع على أنظمة جمع الأدلة الرقمية والمنصات التفاعلية، مما يمنحها سلطة احتكارية على الحماية نفسها.

فشركة "بالانتير" الأمريكية تمتلك براءات اختراع على أكثر من 60% من أنظمة جمع الأدلة الرقمية. وشركة "آي بي إم" تفرض رسوماً باهظة على المنظمات التي تستخدم منصاتها، مما يجعلها غير متاحة للدول النامية.

وفي الممارسة، أدت هذه البراءات إلى:

- منع الدول النامية من تطوير أنظمة حماية محلية.

- رفع تكاليف الحماية 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 القانون الإنساني السيبراني الحقيقي لا يُبنى على الاعتماد على براءات أجنبية، بل على الاستثمار في البحث العلمي الوطني، وأن نظام البراءات الحالي يجب أن يُعدّل ليوازن بين حقوق

المخترعين وحقوق المدنيين في الحماية.

**الفصل التاسع

القانون الإنساني السيبراني في الدول النامية: تحديات القدرة والاعتماد التكنولوجي**

بينما تمتلك القوى الكبرى أدوات متقدمة لفرض حمايتها الإنسانية 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 حمايتها الإنسانية الرقمية.

فأكثر من 80 بالمئة من أنظمة جمع الأدلة في

الدول النامية مستوردة. ومعظم قواعد البيانات الإنسانية تعتمد على برمجيات أمريكية أو أوروبية. بل إن بعض الدول لا تملك حتى "قاعدة بيانات وطنية" للحماية.

وفي هذا السياق، بدأت بعض الدول باتخاذ خطوات. فالهند أطلقت "مشروع الأنظمة الإنسانية الوطنية"، بينما أنشأت الصين "منطقة بيانات إنسانية سيادية". أما في إفريقيا، فقد بدأت مبادرات إقليمية لتطوير أنظمة حماية مقاومة للتحيّز.

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

ويخلص هذا الفصل إلى أن القانون الإنساني السيبراني في الدول النامية ليس مسألة تقنية فقط، بل قضية تنموية تتطلب استثمارات طويلة الأمد، وتعاوناً إقليمياً، ونقل تكنولوجيا عادل.

**الفصل العاشر

التنظيم الإقليمي للقانون الإنساني السيبراني: دراسة مقارنة بين التجارب العالمية**

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

ففي أوروبا، أطلقت دول الشمال "مبادرة الحماية الإنسانية الرقمية"، التي تدعو إلى تبادل البيانات الإنسانية وتطوير أنظمة مشتركة. أما في أمريكا اللاتينية، فقد أنشأت دول الميركوسور "شبكة استجابة إنسانية رقمية" لمواجهة التحيّز الخوارزمي.

أما في الاتحاد الأوروبي، فإن "الاستراتيجية الإنسانية الرقمية" تُلزم الدول الأعضاء بحماية بيانات المدنيين، وتشجع على تطوير أنظمة وطنية.

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

أما في العالم العربي، فإن جامعة الدول العربية أطلقت "استراتيجية الحماية الإنسانية الرقمية" في 2024، التي تدعو إلى إنشاء "مركز عربي للقانون الإنساني السيبراني". لكن المركز لم يُنشأ بعد، ولا توجد آليات ردع مشتركة.

ويؤكد هذا الفصل أن التنظيم الإقليمي هو الجسر بين الحماية الوطنية والنظام الدولي، وأن غيابه في بعض المناطق يترك الدول فريسة للاستغلال الخارجي.

**الفصل الحادي عشر

القانون الإنساني السيبراني والبيانات الإنسانية: حماية الخصوصية الإنسانية من الاستغلال الخارجي**

لا يمكن تحقيق القانون الإنساني السيبراني دون حماية البيانات الإنسانية للمدنيين. فهذه البيانات، التي تمثل خصوصية إنسانية لا تقدر بثمن، أصبحت اليوم هدفاً للشركات الكبرى التي تسعى إلى تسجيل براءات اختراع عليها، مما يمنحها احتكاراً على الحماية نفسها.

ففي إفريقيا، تم تسجيل براءات اختراع على أنماط الهجمات الإنسانية التي رصدتها المجتمعات عبر الأجيال. وفي أمريكا اللاتينية، سُجلت براءات على أنظمة جمع الأدلة بعد تحليلها في مختبرات أجنبية. وكل هذه الممارسات تُعد شكلاً من "القرصنة الإنسانية" التي تستغل الخصوصية الإنسانية دون مقابل عادل.

ويواجه القانون الدولي غياباً في حماية هذه البيانات، لأن:

- اتفاقيات جنيف لا تمنع التسجيل المباشر للبراءات على البيانات الإنسانية.

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

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

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

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

**الفصل الثاني عشر

القانون الإنساني السيبراني والذكاء الاصطناعي الإنساني: عندما تصبح الخوارزميات حارساً**

مع تزايد استخدام الذكاء الاصطناعي في اتخاذ

قرارات إنسانية — من جمع الأدلة إلى تحديد الهجمات — ظهر تهديد جديد للقانون الإنساني السيبراني: **السلطة الخوارزمية**. فعندما تتخذ أنظمة ذكاء اصطناعي قرارات تؤثر على حق المدني في الحماية دون إشراف بشري، فإن المجتمع الدولي يفقد جزءاً من مسؤوليته الإنسانية.

وتكمن المشكلة في ثلاث نقاط:

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

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

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

وفي الممارسة، أدت أنظمة الذكاء الاصطناعي إلى انتهاكات خطيرة. ففي دولة آسيوية، رفضت خوارزمية جمع أدلة من مدنيين فقراء لأنها لا تحقق أرباحاً كافية. وفي دولة أفريقية، أوصت أنظمة ذكاء اصطناعي باستخدام منصات أجنبية بدلاً من المنصات المحلية، مما أدى إلى تآكل الصناعة الإنسانية 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 الإنساني"

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 الإنساني، ولا توجد تشريعات تحمي القانون الإنساني من الاستخدام غير الخاضع للرقابة لهذه التقنيات.

ويؤكد هذا الفصل أن القانون الإنساني السيبراني في عصر الذكاء الاصطناعي لا يعني منع التكنولوجيا، بل فرض الشفافية والمساءلة على من يطورها ويستخدمها.

**الفصل الثالث عشر

القانون الإنساني السيبراني والجرائم الإلكترونية الإنسانية: مكافحة الاحتيال الإنساني الرقمي**

لا يمكن حماية القانون الإنساني السيبراني دون مواجهة الجرائم الإلكترونية التي تستهدف المدنيين والمنظمات الإنسانية عبر الحدود. فاختراق الحسابات البنكية للمدنيين، وسرقة الهويات الإنسانية الرقمية، ونشر البرمجيات الخبيثة في أنظمة الحماية، كلها جرائم تهدد الحماية، لكنها تبقى خارج نطاق العدالة بسبب غياب التعاون الدولي الفعّال.

وتشير التقديرات إلى أن الخسائر العالمية من الجرائم الإلكترونية الإنسانية تجاوزت 10 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 الإنسانية".

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 الإنسانية ليست مسألة أمنية فقط، بل اختبار عملي لمدى التزام الدول بمبدأ القانون الإنساني السيبراني، لأن غياب العدالة يشجع المجرمين على استهداف الدول ذات الحماية الضعيفة.

**الفصل الرابع عشر

القانون الإنساني السيبراني والتربية الرقمية الإنسانية: بناء وعي مجتمعي كأساس للدفاع الإنساني**

لا يمكن تحقيق القانون الإنساني السيبراني دون بناء وعي مجتمعي لدى المدنيين والموظفين حول مخاطر الفضاء السيبراني وواجباتهم تجاهه. فال civilians ليسوا مجرد ضحايا للهجمات، بل شركاء في عملية الحماية. وغياب التربية الرقمية الإنسانية يجعلهم عرضة للاحتيال، ويسهل اختراق أنظمتهم، مما يهدد البنية التحتية الإنسانية الدولية بأكملها.

وفي الدول المتقدمة، أصبحت التربية الرقمية الإنسانية جزءاً من البرامج التدريبية. ففي هولندا، يتعلم المدنيون كيفية التعرف على

المنصات الإنسانية المزيفة. أما في سنغافورة، فإن "برنامج المواطنة الرقمية الإنسانية" يُدرّس في جميع المؤسسات، ويشمل مفاهيم مثل الخصوصية، والأمن، والمسؤولية الاجتماعية.

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

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

وطنية للتربية الرقمية الإنسانية.

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

**الفصل الخامس عشر

القانون الإنساني السيبراني والبحث العلمي الإنساني: نحو استقلال تكنولوجي وطني**

لا يمكن لأي دولة أن تمارس حمايتها الإنسانية الرقمية بشكل حقيقي دون امتلاك قدرات بحثية

محلية في مجالات الأمن السيبراني الإنساني، والذكاء الاصطناعي الإنساني، 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 الإنسانية المتقدمة" مشاريع بحثية في الأمن السيبراني الإنساني بعشرات المليارات سنوياً. أما في الصين، فإن "خطة الحماية الذكية 2030" تخصص جزءاً كبيراً من ميزانيتها لتطوير أنظمة حماية ذكية محلية.

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

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

**الفصل السادس عشر

القانون الإنساني السيبراني والاتفاقيات الثنائية: هل يمكن للدول الصغيرة أن تحمي نفسها؟**

في ظل غياب اتفاقية دولية شاملة، لجأت كثير من الدول إلى عقد اتفاقيات ثنائية للتعاون الإنساني 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 الإنسانية في حالات "الطوارئ الإنسانية"، 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 الإنسانية"، 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 الإنساني 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

القانون الإنساني السيبراني والمحاكمات الإنسانية: نحو اختصاص قضائي رقمي**

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

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

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

**الفصل الثامن عشر

القانون الإنساني السيبراني والبيانات الإنسانية: بين الملكية الفردية والسيادة الجماعية**

تشكل البيانات الإنسانية اليوم أثمن مورد في الاقتصاد الرقمي الإنساني. ولذلك، فإن القانون الإنساني السيبراني لا يكتمل دون تحديد من يملك حق التحكم في هذه البيانات: المدني أم الدولة أم الشركة؟

وفي الفقه الحديث، برزت ثلاث مدارس:

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

ويؤكد هذا الفصل أن البيانات الإنسانية ليست مجرد أرقام، بل تعبير عن الهوية الإنسانية الفردية والجماعية. وأن القانون الإنساني السيبراني الحقيقي يبدأ باحترام حق المدني في التحكم بمعلوماته.

**الفصل التاسع عشر

القانون الإنساني السيبراني والعدالة المجتمعية: حماية المجتمعات من التكنولوجيا الإنسانية غير المسؤولة**

لا يمكن فصل القانون الإنساني السيبراني عن العدالة المجتمعية، لأن بعض التقنيات الإنسانية الرقمية قد تؤدي إلى أضرار مجتمعية طويلة الأمد. فمنصات جمع الأدلة الذكية قد تهمل المدنيين الفقراء، والتطبيقات الرقمية قد تروج لحلول غير فعالة، والبيانات الإنسانية قد تُستخدم للتمييز ضد فئات معينة.

وفي الممارسة، أدت بعض المشاريع الإنسانية الرقمية إلى أضرار مجتمعية كبيرة. ففي دولة آسيوية، أدت منصات جمع الأدلة الذكية إلى

تجاهل المدنيين من المناطق الريفية. وفي دولة أفريقية، أدت التطبيقات الرقمية إلى انتشار حلول حماية باهظة الثمن على حساب الحلول المحلية.

ويواجه القانون الدولي غياباً في تنظيم هذا الجانب، لأن:

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

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

- لا توجد معايير دولية لـ"الحماية الإنسانية الرقمية المسؤولة".

وفي المقابل، بدأت بعض الدول بوضع تشريعات. ففي الدنمارك، يُشترط على منصات جمع الأدلة الذكية تغطية جميع الفئات دون تمييز. أما في كوستاريكا، فقد تم وقف إصدار تراخيص جديدة للتطبيقات الإنسانية الرقمية حتى يتم تقييم تأثيرها المجتمعي.

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

ويؤكد هذا الفصل أن القانون الإنساني السيبراني يجب أن يمتد إلى حماية العدالة المجتمعية، وأن التكنولوجيا الإنسانية يجب أن تُبنى على مبدأ "المسؤولية منذ التصميم".

**الفصل العشرون

القانون الإنساني السيبراني والمستقبل: نحو مشروع اتفاقية دولية نموذجية**

بعد استعراض شامل للتحديات والتجارب، يتبين أن القانون الإنساني السيبراني ليس خياراً، بل ضرورة وجودية في العصر الرقمي. ولتحقيقه على المستوى الدولي، يُقترح إعداد "مشروع اتفاقية دولية نموذجية بشأن القانون الإنساني السيبراني"، تتضمن ما يلي:

أولاً: **تعريف موحد للقانون الإنساني السيبراني** كحق للمدني في الاستفادة من أنظمة ذكية تُصمم خصيصاً لحمايته من الهجمات السيبرانية في زمن النزاع، مع ضمانات قانونية تحميه من التحيّز الخوارزمي.

ثانياً: **قائمة موحدة للبنية التحتية للقانون الإنساني السيبراني**، تشمل الأنظمة الأساسية (جمع الأدلة الرقمية، منصات التواصل، قواعد البيانات، أنظمة تحديد الهجمات).

ثالثاً: **حظر التمييز الخوارزمي غير المشروع** في تحديد الأهداف، مع تعريف دقيق للتمييز على أنه كل خوارزمية تهدف إلى تهميش فئة من المدنيين دون مبرر إنساني.

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 منح التعويض أو إلزام الدولة بإعادة الحماية رداً على الفشل الرقمي.

سادساً: **التزام الدول بحماية البيانات الإنسانية**، واحترام حقوق المدنيين في الخصوصية.

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

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

تاسعاً: **إنشاء محكمة سيبرانية إنسانية دولية**، تنظر في النزاعات المتعلقة بالقانون الإنساني السيبراني.

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

ويُختتم هذا الفصل بالتذكير بأن القانون الإنساني السيبراني ليس نهاية التاريخ، بل بداية مرحلة جديدة من تطور القانون الإنساني الدولي، توازن بين الأمن المجتمعي وحق المدني في الحماية الرقمية، والحرب والتكنولوجيا، والإنسانية والكرامة.

[١/٢٨، ١٠:٥٣ م] .: **الفصل الحادي والعشرون

القانون الإنساني السيبراني والعقود الذكية: عندما تصبح الخوارزمية حارساً**

لم يعد مفهوم العقد الإنساني يقتصر على الورق والشهود، بل امتد ليشمل **العقود الذكية** التي تنفذ نفسها تلقائياً عند توفر الشروط. فالحماية عبر العقد الذكي ليس مجرد إجراء، بل **تنفيذ آلي لشروط مسبقة** قد لا يدركها المدنيون عند طلب الحماية.

وفي الممارسة، بدأت بعض المنظمات بتجربة العقود الذكية. ففي إستونيا، يُسمح للمدنيين بإدراج شروط حماية تلقائية في عقدهم الرقمي. أما في الإمارات، فإن "منصة الحماية الذكية" تتيح للمدنيين تحديد شروط جمع الأدلة مسبقاً.

أما في الدول النامية، فإن مفهوم العقد الذكي لا يزال غريباً ً، مما يزيد من حالات الحماية غير العادلة.

ويؤكد هذا الفصل أن العقد الذكي ليس ترفاً ً، بل ضرورة قانونية، وأن غيابه يحوّ ل الحماية إلى فعل انفعالي، لا قراراً ً مسؤولاً ً.

**الفصل الثاني والعشرون

القانون الإنساني السيبراني والطاقة الإنسانية: حماية الموارد من الاستنزاف الرقمي**

مع تزايد الاعتماد على الطاقة في المراكز الإنسانية الحديثة — من أنظمة التبريد إلى مراكز البيانات الإنسانية — أصبح استهلاك

الكهرباء جزءاً من الاستراتيجية الإنسانية.
فمراكز البيانات الإنسانية تستهلك كميات هائلة من الكهرباء، وقد تُستخدم كأداة ضغط على الدول ذات الموارد المحدودة.

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

ويواجه القانون الدولي غياباً في تنظيم هذا الجانب، لأن:

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

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

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

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

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

أزمات طاقة مستقبلية.

ويخلص هذا الفصل إلى أن القانون الإنساني السيبراني يجب أن يشمل إدارة الموارد الطبيعية المستخدمة في الأنشطة الإنسانية الرقمية، وأن الطاقة الكهربائية أصبحت جزءاً من الأمن القومي الإنساني.

**الفصل الثالث والعشرون

القانون الإنساني السيبراني وسلامة المدنيين: حماية المدنيين من التلاعب الرقمي**

لا يمكن فصل القانون الإنساني السيبراني عن حماية سلامة المدنيين. فمع تزايد استخدام المنصات الرقمية في جمع الأدلة، أصبحت هذه

المنصات هدفاً للهجمات التي تهدف إلى تغيير الشروط، أو تزوير النتائج، أو نشر معلومات مضللة عن المدنيين.

ففي عام 2024، تم اختراق منصة حماية في دولة أوروبية، مما أدى إلى تغيير شروط جمع الأدلة. وفي عام 2025، تم نشر معلومات مضللة عن مدنيين عبر منصات ذكاء اصطناعي، مما أدى إلى تشويه سمعتهم.

ويواجه القانون الدولي غياباً في حماية هذا القطاع، لأن:

- لا توجد اتفاقيات دولية تنظم سلامة إجراءات الحماية الرقمية.

- معظم المنصات الرقمية لا تخضع لرقابة

إنسانية كافية.

- لا توجد معايير دولية لشفافية المعلومات الإنسانية الرقمية.

وفي المقابل، بدأت بعض الدول بوضع تشريعات. ففي الاتحاد الأوروبي، يُلزم "قانون سلامة إجراءات الحماية الرقمية" المنصات بنشر معلومات دقيقة ومحدثة. أما في الولايات المتحدة، فإن "وزارة الخارجية" بدأت بفحص الخوارزميات التي تحدد شروط جمع الأدلة.

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

ويؤكد هذا الفصل أن القانون الإنساني السيبراني في مجال سلامة المدنيين ليس رفاهية، بل حق إنساني أساسي، وأن سلامة إجراءات الحماية الرقمية يجب أن تُعتبر جزءاً من الأمن القومي الإنساني.

**الفصل الرابع والعشرون

القانون الإنساني السيبراني والتعليم الإنساني الرقمي: بناء وعي مجتمعي كأساس للدفاع عن الحقوق**

لا يمكن تحقيق القانون الإنساني السيبراني دون بناء وعي مجتمعي لدى المدنيين حول حقوقهم الرقمية وواجباتهم تجاه الحماية العامة. فالتعليم الإنساني الرقمي ليس مجرد نشر معلومات، بل تمكين المدنيين من المطالبة

بحقوقهم والمشاركة في صنع القرار الإنساني.

ففي الدول التي يُدرّس فيها القانون الإنساني الرقمي في المدارس، يزداد الوعي بحقوق الأجيال القادمة في الحماية العادلة. وفي المجتمعات التي تُدرّب على التكيف مع التهديدات السيبرانية، تنخفض معدلات الحماية غير العادلة.

وفي الممارسة، بدأت بعض الدول بدمج القانون الإنساني الرقمي في المناهج التعليمية. ففي فنلندا، يتعلم الطلاب من سن السادسة كيفية حماية بياناتهم الإنسانية. أما في كوستاريكا، فإن "التعليم من أجل الحماية الرقمية" جزء أساسي من النظام التعليمي.

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

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

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

**الفصل الخامس والعشرون

القانون الإنساني السيبراني والتراث الإنساني: حماية التراث من الاندثار الرقمي**

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

ففي إفريقيا، تهدد منصات جمع الأدلة الذكية الممارسات الإنسانية التقليدية التي طوّرها المجتمعات عبر الأجيال. وفي أمريكا اللاتينية، يؤدي الاعتماد على الإجراءات الرقمية إلى تآكل المهارات الإنسانية التقليدية. بل إن بعض اللغات والعادات الإنسانية 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 الإنسانية على قائمة الخطر.

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

ويؤكد هذا الفصل أن القانون الإنساني السيبراني الثقافي هو جزء من الهوية الوطنية، وأن غياب الحماية القانونية لهذا البعد يحوّل الشعوب إلى شهود على اندثار تاريخهم الإنساني.

**الفصل السادس والعشرون

القانون الإنساني السيبراني والتمويل الإنساني الرقمي: حماية الدول النامية من الديون الإنسانية**

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

ففي جزر المحيط الهادئ، أدت الأزمات الاقتصادية إلى انهيار الإيرادات الإنسانية، مما جعل سداد القروض الإنسانية الرقمية

مستحيلاً. وفي أمريكا اللاتينية، أدت الأزمات الاقتصادية إلى انهيار الصادرات، مما زاد من عجز الموازنات.

ويواجه القانون الدولي غياباً في حماية هذه الدول، لأن:

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

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

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

وفي المقابل، بدأت بعض المبادرات. ففي مؤتمر

الدول الأطراف في اتفاقيات جنيف 2025، تم اقتراح "آلية لإعادة هيكلة الديون الإنسانية"، لكنها لم تُعتمد بعد. أما في مجموعة السبع، فإن "مبادرة التمويل الإنساني الرقمي العادل" لا تزال في طور النقاش.

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

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

**الفصل السابع والعشرون

القانون الإنساني السيبراني والنقل الإنساني الرقمي: حماية سلاسل التوريد من التهديدات السيبرانية**

لم يعد النقل الإنساني يعتمد فقط على الورق والبريد، بل على أنظمة رقمية معقدة تدير سلاسل التوريد من المركز إلى المدني. واختراق هذه الأنظمة قد يؤدي إلى تلف المستندات، أو تأخير التوزيع، أو سرقة المعلومات.

ففي عام 2024، تم اختراق نظام تتبع المستندات الإنسانية في دولة أوروبية، مما أدى إلى تلف آلاف الملفات بسبب تأخير التوصيل. وفي عام 2025، تم سرقة شحنات مستندات

إنسانية عبر اختراق أنظمة الموانئ الرقمية.

ويواجه القانون الدولي غياباً في تصنيف سلاسل التوريد الإنسانية 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 القانون الإنساني السيبراني في مجال النقل ليس مسألة تقنية، بل مسألة أمن إنساني، وأن سلاسل التوريد الإنسانية الرقمية يجب أن تُعتبر جزءاً من البنية التحتية الحيوية.

**الفصل الثامن والعشرون

القانون الإنساني السيبراني والبحث العلمي الإنساني المفتوح: التوازن بين التعاون والحماية**

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

ففي بعض الحالات، استخدمت الدول الصناعية

البيانات الإنسانية 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 الإنسانية من الاستغلال.

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

ويؤكد هذا الفصل أن القانون الإنساني السيبراني في البحث العلمي يعني وضع تصنيفات واضحة للبيانات، وتحديد ما يُسمح بنشره وما يجب حمايته، دون عزلة علمية.

**الفصل التاسع والعشرون

القانون الإنساني السيبراني والتعاون الدولي: نحو نظام عالمي عادل للحوكمة الإنسانية الرقمية**

لا يمكن لأي دولة أن تحمي قانونها الإنساني السيبراني 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 الحماية الرقمية من قبل الدول الصناعية، دون مراعاة قدرات الدول النامية. وهذا يخلق نظاماً غير عادل يكرس التبعية الإنسانية الرقمية.

ويستدعي الحل:

- إنشاء منتدى دولي محايد لصياغة قواعد القانون الإنساني السيبراني.

- توفير الدعم الفني والمالي للدول النامية.

- احترام التنوع في النماذج الوطنية للقانون الإنساني السيبراني.

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 الإنسانية الرقمية يجب أن يقوم على مبدأ "العدالة المشتركة"، لا "الهيمنة الإنسانية الرقمية".

**الفصل الثلاثون

القانون الإنساني السيبراني والقانون الإنساني الدولي: حماية المدنيين في النزاعات الإنسانية**

مع تزايد استخدام الموارد الإنسانية كسلاح في

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

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

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

ويؤكد هذا الفصل أن القانون الإنساني السيبراني في زمن الحرب لا يعني التخلي عن الإنسانية، بل تعزيز حماية المدنيين من الأسلحة الإنسانية الرقمية.

**الفصل الحادي والثلاثون

القانون الإنساني السيبراني والفضاء الخارجي: حماية الأرض من التلوث الفضائي الإنساني**

مع تزايد الأنشطة الفضائية المتعلقة بالحماية — من الأقمار الصناعية لمراقبة المراكز الإنسانية إلى الطائرات المسيرة الفضائية لتوزيع المستندات — برز تهديد جديد: التلوث الفضائي الذي يؤثر على الأنظمة الإنسانية. فحطام الأقمار الصناعية قد يعيق أنظمة الرصد الإنساني، بينما تنبعثات الصواريخ تؤثر على الغلاف الجوي الذي ينظم الاتصالات الإنسانية.

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

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

الإنسانية 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 القانون الإنساني السيبراني يجب أن يمتد إلى الفضاء الخارجي، وأن الأنشطة الفضائية الإنسانية يجب أن تخضع لمبدأ "الوقاية الإنسانية" مثلها مثل أي نشاط صناعي آخر.

**الفصل الثاني والثلاثون

القانون الإنساني السيبراني والذكاء الاصطناعي التوليدي: عندما تصبح الأخبار الكاذبة سلاحاً إنسانياً

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

ففي عام 2025، تم تداول فيديوهات مزيفة لمدنيين وهم يحذرون من أنظمة وطنية آمنة، مما أدى إلى انخفاض الثقة في النظام الإنساني وانتشار المعلومات المضللة. وفي

أزمات إنسانية، تم نشر أخبار كاذبة عن نقص في الموارد الإنسانية الأساسية، مما أدى إلى ذعر شعبي وارتفاع غير مبرر في التكاليف.

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

- المحتوى المزيف لا يُصنّف كـ"هجوم سيبراني إنساني" 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 الإنسانية.

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

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

**الفصل الثالث والثلاثون

القانون الإنساني السيبراني والبيانات الضخمة الإنسانية: حماية السيادة من الاستغلال الرقمي**

مع تزايد الاعتماد على البيانات الضخمة في تحليل الهجمات، 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 إنسانية 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 الإنسانية.

- معظم العقود بين الدول والشركات تبقى سرية.

- لا توجد معايير لـ"السيادة الإنسانية الرقمية".

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

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

**الفصل الرابع والثلاثون

القانون الإنساني السيبراني والتعليم العالي الإنساني: نحو كليات وطنية للقانون الإنساني الرقمي**

لا يمكن بناء قدرات إنسانية 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 الإنساني الرقمي يُعد استثماراً استراتيجياً

في القانون الإنساني السيبراني.

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

أما في الدول النامية، فإن التعليم الإنساني 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 الإنساني الرقمي.

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

**الفصل الخامس والثلاثون

القانون الإنساني السيبراني والثقافة الرقمية الإنسانية: حماية الإبداع المحلي من القرصنة

والتهميش**

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

ويؤكد هذا الفصل أن القانون الإنساني السيبراني الثقافي هو جزء من الهوية الوطنية، وأن غيابه يحوّل الشعوب إلى مستهلكين سلبيين، لا مبدعين فاعلين.

**الفصل السادس والثلاثون

القانون الإنساني السيبراني والتمويل الرقمي الإنساني: حماية العملات الإنسانية من التلاعب والاحتيال**

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

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

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

ويخلص هذا الفصل إلى أن القانون الإنساني السيبراني في المجال المالي لا يعني منع الابتكار، بل وضع ضوابط تحمي الاقتصاد الوطني من المخاطر غير المحسوبة.

**الفصل السابع والثلاثون

القانون الإنساني السيبراني والبحث العلمي الإنساني المفتوح: التوازن بين التعاون والحماية**

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

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

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

ويؤكد هذا الفصل أن القانون الإنساني

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

**الفصل الثامن والثلاثون

القانون الإنساني السيبراني والتعاون الدولي: نحو نظام عالمي عادل للحوكمة الإنسانية الرقمية**

لا يمكن لأي دولة أن تحمي قانونها الإنساني السيبراني 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 الحماية الرقمية من قبل الدول الصناعية، دون مراعاة قدرات الدول النامية. وهذا يخلق نظاماً غير عادل يكرس التبعية الإنسانية الرقمية.

ويستدعي الحل:

- إنشاء منتدى دولي محايد لصياغة قواعد القانون الإنساني السيبراني.

- توفير الدعم الفني والمالي للدول النامية.

- احترام التنوع في النماذج الوطنية للقانون الإنساني السيبراني.

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 الإنسانية الرقمية يجب أن يقوم على مبدأ "العدالة المشتركة"، لا "الهيمنة الإنسانية الرقمية".

**الفصل التاسع والثلاثون

القانون الإنساني السيبراني والقانون الإنساني الدولي: حماية المدنيين في النزاعات الإنسانية**

مع تزايد استخدام الموارد الإنسانية كسلاح في النزاعات، برز سؤال جوهري: هل يُعد تدمير البنية التحتية الإنسانية الرقمية كوسيلة حربية

انتهاكاً للقانون الإنساني الدولي؟ وهل يُعتبر التسبب المتعمد في فشل الحماية جريمة حرب؟

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

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

ويؤكد هذا الفصل أن القانون الإنساني السيبراني في زمن الحرب لا يعني التخلي عن الإنسانية، بل تعزيز حماية المدنيين من الأسلحة الإنسانية الرقمية.

**الفصل الأربعون

القانون الإنساني السيبراني والمستقبل: رؤية استراتيجية للعقود القادمة**

في الختام، لا يمكن النظر إلى القانون الإنساني السيبراني كظاهرة مؤقتة، بل كتحول جوهري

في مفهوم الحماية في القرن الحادي والعشرين. فالدول التي تبني قانونها الإنساني السيبراني اليوم ستكون قادرة على:

- حماية مدنييها من التلاعب الإنساني الرقمي.

- بناء اقتصاد إنساني رقمي مستقل ومستدام.

- تعزيز مكانة أجيالها في النظام الإنساني 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 القانون الإنساني السيبراني ليس مسألة اختيار، بل مسألة بقاء.

خاتمة

بعد استعراض شامل لأبعاد القانون الإنساني السيبراني 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 الإنساني الرقمي، رغم طبيعته غير المادية، بات ساحة للصراعات السياسية والاقتصادية، ولا

يمكن لأي دولة أن تحافظ على قانونها الإنساني 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 الأمن المجتمعي وحق المدني في الحماية الرقمية.

وفي النهاية، فإن القانون الإنساني السيبراني الحقيقي لا يُبنى على العزلة أو القمع، بل على الشفافية، والكفاءة، والثقة بين الدولة والمواطن. وهو ليس غاية بذاته، بل وسيلة لبناء مستقبل إنساني آمن، عادل، وإنساني.

المراجع

Geneva Conventions (1949) and Additional Protocols

International Committee of the Red Cross (ICRC) Guidelines on Cyber Operations ((2021

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

UN General Assembly Resolution on Digital (Humanitarian Protection (2023

European Commission. Digital (Humanitarian Action Plan (2024

International Covenant on Civil and Political (Rights (1966

UNODC Handbook on Strategies to Combat Cybercrime in Humanitarian Contexts ((2023

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). Humanitarian Sovereignty and Digital Control. Oxford University Press

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

Kloppenburg J R. (2024). Digital Sovereignty and Humanitarian Exploitation. University of California Press

:Official Government Sources

White House. National Strategy for Digital (Humanitarian Protection (2024

European Commission. Digital (Humanitarian Action Plan (2023

ICRC Reports on Cyber Resilience in Humanitarian Systems (Multiple (Jurisdictions, 2020–2025

:Academic Journals

Journal of International Humanitarian Law ((Oxford

International Journal of Digital Humanitarian Justice

Harvard Law Review – Humanitarian Law Section

Stanford Technology Law Review

فهرس المحتويات

القانون الإنساني السيبراني: دراسة قانونية مقارنة حول حماية المدنيين في الفضاء الرقمي وبناء نظام إنساني رقمي عالمي لصون الكرامة في العصر الرقمي

بيان حقوق الملكية

جميع الحقوق محفوظة للمؤلف

© 2026 الدكتور محمد كمال عرفه الرخاوي

الباحث والمستشار القانوني

المحاضر الدولي في القانون

يحظر منعاً باتاً:

نسخ أو طبع أو نشر أو توزيع أو اقتباس أو ترجمة أو تحويل أو عرض أي جزء من هذا العمل — سواء كان ذلك إلكترونياً، رقمياً، مطبوعاً، أو بأي وسيلة أخرى — دون الحصول على **تصريح كتابي صريح ومسبق** من المؤلف.

الاستثناء الوحيد:

يجوز الاقتباس لأغراض بحثية أو أكاديمية، بشرط:

- ذكر اسم المؤلف كاملاً: **الدكتور محمد كمال عرفه الرخاوي**.

- ذكر عنوان المؤلف كاملاً: **"القانون الإنساني السيبراني: دراسة قانونية مقارنة حول حماية المدنيين في الفضاء الرقمي وبناء نظام إنساني رقمي عالمي لصون الكرامة في العصر الرقمي"**.

- ذكر رقم الصفحة بدقة.

- عدم تغيير السياق أو المعنى.

التحديث:

أي تحديث أو طبعة جديدة لهذا العمل ستُعلن عنها رسمياً عبر الموقع الإلكتروني المعتمد للمؤلف.

تم بحمد الله وتوفيقه

تأليف الدكتور محمد كمال عرفه الرخاوي