العدالة السيبرانية: دراسة قانونية مقارنة حول مكافحة الجرائم الإلكترونية وبناء نظام جنائي رقمي إنساني عالمي

تأليف

د.محمد كمال عرفه الرخاوي

تقديم

في عالم يشهد اختناقاً خطيراً في آليات العدالة الجنائية — حيث تُرتكب جرائم ضد الإنسانية عبر الشبكات الرقمية، ويُفلت مرتكبوها بسبب غياب الإطار القانوني، ويُحرم الضحايا من حقهم في العدالة بسبب بطء الإجراءات — لم يعد كافياً الحديث عن "القانون

الجنائي"، بل أصبح من الضروري إعادة تعريف العدالة الجنائية ذاتها. فالعدالة الحديثة ليست مجرد محكمة في لاهاي، بل شبكة ذكية تتفاعل مع الضحايا في الزمن الحقيقي. ومع ظهور الذكاء الاصطناعي، باتت لدينا الأداة التي طالما حلم بها الفقه الجنائي: القدرة على **تعقب الجرائم الإلكترونية في الفضاء السيبراني قبل وقوع الضرر**.

هذا العمل لا يهدف إلى تكرار الخطابات الجنائية التقليدية، بل إلى بناء **نظرية جنائية رقمية جديدة** تجعل من "العدالة السيبرانية" 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: **العدالة ليست غاية، بل وسيلة لحماية الضحية من الجريمة الرقمية**. ومن دون عدالة سيبرانية، لن تكون هناك عدالة جنائية حقيقية في العصر الرقمي.

والله ولي التوفيق.

**الفصل الأول

العدالة السيبرانية: من المحكمة إلى الظاهرة القانونية الجديدة**

لم يعد مفهوم العدالة الجنائية محصوراً في

المحكمة الجنائية الدولية أو لجان التحقيق، بل امتد ليشمل **أي فعل رقمي يؤدي إلى تعقب الجرائم الإلكترونية في الفضاء السيبراني**. فالعدالة السيبرانية ليست مجرد استخدام للتكنولوجيا في التحقيق، بل **إعادة تعريف جذرية لعلاقة المجتمع الدولي بالجريمة**، تقوم على أساس أن التكنولوجيا يجب أن تكون أداة لمنع الجريمة، لا لمعاقبتها بعد وقوعها.

ويُعرّف هذا العمل العدالة السيبرانية على أنها **حق الضحية في الاستفادة من أنظمة ذكية تُصمم خصيصاً لتعقب الجرائم الإلكترونية في الفضاء السيبراني، وتحديد المسؤولين عنها، وضمان المحاكمة العادلة، مع ضمانات قانونية تحمي حقوق المتهم من التحيّز الخوارزمي**. ولا يعني هذا الحق إلغاء المحكمة، بل تحويلها من ردّعي إلى وقائي.

وقد بدأ هذا المفهوم يتشكل عملياً. ففي عام 2024، أطلقت المحكمة الجنائية الدولية منصة رقمية لجمع الأدلة السيبرانية من الضحايا مباشرة. وفي عام 2025، طوّرت الأمم المتحدة نظاماً ذكياً يربط بين جميع آليات العدالة الجنائية في منصة واحدة تفاعلية.

أما في الدول النامية، فإن الاعتماد الكلي على النماذج التقليدية يجعلها عاجزة عن مواجهة الجرائم الإلكترونية.

ويؤكد هذا الفصل أن العدالة السيبرانية ليست رفاهية تقنية، بل ضمانة وجودية للعدالة الحديثة، وأن غيابها في القانون الجنائي الدولي يخلق فراغاً خطيراً يهدد استقرار النظام العدلي ذاته.

**الفصل الثاني

الفراغ القانوني الجنائي الدولي في الحماية الرقمية للضحايا**

رغم أهمية العدالة، لا يزال القانون الجنائي الدولي يفتقر إلى اتفاقية شاملة تحمي حقوق الضحايا في الحصول على عدالة رقمية.
فاتفاقيات روما الأساسية، رغم اعترافها بمبدأ حماية الضحايا، لا تتضمن أي آليات لحمايتهم من الجرائم الإلكترونية.

وهذا الفراغ ليس نتيجة غفلة، بل انعكاس لصراع المصالح بين الدول التي ترى في الجريمة "حدثاً فردياً"، والدول التي تراها "تهديداً جماعياً".

ففي مؤتمر الدول الأطراف في نظام روما الأساسي لعام 2025، تم اعتماد "إعلان العدالة الرقمية"، لكنه اكتفى بـ"التعاون الطوعي"، دون أي التزام قانوني بحماية الضحايا في الفضاء السيبراني. أما في مكتب المدعي العام للمحكمة الجنائية الدولية، فإن "استراتيجية التحول الرقمي" لا تتضمن أي آلية لحماية الحقوق الرقمية للضحايا.

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

أما في المحاكم الوطنية، فقد بدأت بعض

الدعاوى تظهر. ففي كندا، رفع ضحية دعوى ضد الدولة بتهمة إهمال جمع الأدلة الرقمية في جريمة إلكترونية. أما في ألمانيا، فإن محكمة وطنية ألزمت الدولة بتوفير آليات رقمية لحماية الضحايا.

ويخلص هذا الفصل إلى أن الفراغ القانوني الجنائي الدولي يترك الضحايا بلا حماية، ويستدعي بناء نظام قانوني جنائي دولي جديد يوازن بين الأمن المجتمعي وحق الضحية في العدالة الرقمية.

**الفصل الثالث

العدالة الجنائية التقليدية مقابل العدالة السيبرانية: إعادة تشكيل المفاهيم الجنائية**

لا يمكن فهم العدالة السيبرانية دون مقارنتها بالعدالة الجنائية التقليدية التي بُنيت على مفاهيم مثل "الأدلة المادية" و"الشهود العيان". لكن البيئة الرقمية الحديثة تتحدى كل هذه المفاهيم.

فأولاً، **الأدلة المادية** تصبح غير كافية إذا كانت الجريمة تُرتكب عبر خوادم في دول متعددة.

ثانياً، **الشهود العيان** يصبحون غير ذي جدوى إذا كانت الجريمة تُرتكب عبر برامج ذكية لا تترك أثراً بشرياً.

ثالثاً، **المساواة بين الضحايا** تنهار في

البيئة الرقمية، لأن الخوارزميات قد تميز ضد ضحايا معينين بناءً على بيانات متحيزة.

وفي هذا السياق، بدأت بعض الدول بصياغة مفاهيم جديدة. ففنلندا وهولندا تستثمران في "العدالة الجنائية الرقمية الوقائية"، عبر تطوير أنظمة تعلم آلي تُحدّد الجرائم قبل وقوعها. أما سنغافورة، فتبني "المنصات الجنائية التفاعلية" التي تربط بين جميع الجهات في نظام واحد.

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

ويؤكد هذا الفصل أن العدالة السيبرانية ليست

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

**الفصل الرابع

البنية التحتية للعدالة السيبرانية: تعريف قانوني جنائي مفقود**

أحد أكبر الثغرات في النقاش الدولي حول العدالة السيبرانية هو غياب تعريف قانوني متفق عليه لما يُسمى "البنية التحتية للعدالة السيبرانية". فبدون هذا التعريف، لا يمكن تحديد ما يستحق الحماية القانونية، ولا ما يشكل انتهاكاً لحقوق الضحية.

وفي الفقه الوطني، تختلف التعريفات بشكل كبير. ففي الولايات المتحدة، تشمل البنية التحتية للعدالة السيبرانية: أنظمة جمع الأدلة الرقمية، منصات التواصل بين الجهات، قواعد البيانات الجنائية، والسجلات الإلكترونية. أما في الاتحاد الأوروبي، فتركز على أنظمة العدالة الرقمية التي تدمج بين الشفافية والسرعة. أما في الصين، فتضيف إليها "منصات العدالة 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 جنائياً") أو لتوسيع الرقابة ("كل شيء رقمي").

ولذلك، فإن أول خطوة في بناء نظام قانوني جنائي دولي للعدالة السيبرانية هي الاتفاق على تعريف دقيق، يشمل:

- أنظمة جمع الأدلة الرقمية.

- منصات التواصل التفاعلي بين الجهات الجنائية الدولية.

- قواعد البيانات الجنائية الموحدة.

- أنظمة تحديد الجناة الديناميكية.

- السجلات الجنائية الإلكترونية القابلة للوصول الفوري.

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

**الفصل الخامس

التمييز الخوارزمي في العدالة السيبرانية: نحو معيار قانوني جنائي دولي**

لا يمكن حماية العدالة السيبرانية دون تحديد ما يُعد "تمييزاً خوارزمياً غير مشروع" في تحديد الجناة. فليس كل خوارزمية تميز ضد جانٍ معين تُعد انتهاكاً. فبعض التمييز قد يكون مبرراً (مثل تسريع التحقيق مع الجناة الخطرين)، لكن التمييز العنصري أو الطبقي ليس كذلك.

وفي الفقه الدولي، بدأت محاولات وضع معايير. ففي مشروع "مبادئ العدالة السيبرانية"، تم التمييز بين:

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

- **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 تسريع التحقيق مع الجناة الغربيين تمييزاً؟ وهل يختلف عن تسريع التحقيق مع الجناة من الدول النامية بسبب تحيّز الخوارزمية؟

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

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

- تهدف إلى تهميش فئة من الجناة دون مبرر جنائي، أو

- تؤدي إلى حرمان غير مبرر لفئة معينة من

العدالة،

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

**الفصل السادس

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

لا يمكن تطبيق مبدأ العدالة السيبرانية دون حل إشكالية "الإسناد"، أي تحديد الجهة المسؤولة عن فشل النظام الرقمي في جمع الأدلة أو تحديد الجناة. فعلى عكس العدالة التقليدية التي تتحمل مسؤوليتها المحكمة مباشرة، فإن أنظمة العدالة قد تُطورها شركات خاصة، مما يخلق غموضاً في المسؤولية.

ويواجه القانون الجنائي 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 العدالة الرقمية التي تنسب إليها وفقاً لمبادئ القانون الدولي". لكنها لم تحدد كيف يتم هذا الإسناد في السياق الجنائي.

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

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

**الفصل السابع

الردود المشروعة على الانتهاكات الجنائية الرقمية: بين التعويض وإعادة المحاكمة**

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

ويقر القانون الجنائي 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 العدالة.

- **إعادة المحاكمة**: كجزاء على فشل الدولة في توفير عدالة رقمية عادلة.

لكن متى يُعتبر الفشل الجنائي "فشلاً جسيماً" يبرر إعادة المحاكمة؟ في مشروع "مبادئ العدالة السيبرانية"، تم اقتراح معيار "الفرصة الضائعة"، أي أن الضحية لو توفر له نظام عادل لكان قد حصل على العدالة في وقته. فمثلاً، حرمان ضحية من جمع أدلة رقمية بسبب تحيّز خوارزمي قد يُصنّف كفرصة ضائعة.

أما في الممارسة، فقد منحت محاكم في دول

الشمال الأوروبي تعويضات مالية لضحايا تعرضوا لتمييز رقمي. أما في أمريكا اللاتينية، فقد ألزمت محاكم الدولة بإعادة المحاكمات 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 الجنائية.

**الفصل الثامن

العدالة السيبرانية وبراءات الاختراع الجنائية: التوتر بين الابتكار والاستغلال**

لا يمكن الحديث عن العدالة السيبرانية دون

معالجة توترها الجوهري مع نظام براءات الاختراع الجنائية. فاليوم، تتحكم شركات كبرى في براءات اختراع على أنظمة جمع الأدلة الرقمية والمنصات التفاعلية، مما يمنحها سلطة احتكارية على العدالة نفسها.

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

وفي الممارسة، أدت هذه البراءات إلى:

- منع الدول النامية من تطوير أنظمة عدالة محلية.

- رفع تكاليف العدالة 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 العدالة السيبرانية 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 الضحايا في العدالة.

**الفصل التاسع

العدالة السيبرانية في الدول النامية: تحديات

القدرة والاعتماد التكنولوجي**

بينما تمتلك القوى الكبرى أدوات متقدمة لفرض عدالتها الجنائية 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 عدالتها الجنائية الرقمية.

فأكثر من 80 بالمئة من أنظمة جمع الأدلة في الدول النامية مستوردة. ومعظم قواعد البيانات الجنائية تعتمد على برمجيات أمريكية أو أوروبية. بل إن بعض الدول لا تملك حتى "قاعدة بيانات وطنية" للجرائم.

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

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

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

**الفصل العاشر

التنظيم الإقليمي للعدالة السيبرانية: دراسة مقارنة بين التجارب العالمية**

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

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

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

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

أما في العالم العربي، فإن جامعة الدول العربية أطلقت "استراتيجية العدالة الجنائية الرقمية" في 2024، التي تدعو إلى إنشاء "مركز عربي للعدالة الجنائية الرقمية". لكن المركز لم يُنشأ بعد، ولا توجد آليات ردع مشتركة.

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

**الفصل الحادي عشر

العدالة السيبرانية والبيانات الجنائية: حماية الخصوصية الجنائية من الاستغلال الخارجي**

لا يمكن تحقيق العدالة السيبرانية دون حماية البيانات الجنائية للضحايا. فهذه البيانات، التي تمثل خصوصية جنائية لا تقدر بثمن، أصبحت اليوم هدفاً للشركات الكبرى التي تسعى إلى تسجيل براءات اختراع عليها، مما يمنحها احتكاراً على العدالة نفسها.

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

ويواجه القانون الدولي غياباً في حماية هذه البيانات، لأن:

- اتفاقيات حقوق الإنسان لا تمنع التسجيل المباشر للبراءات على البيانات الجنائية.

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

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

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

ويؤكد هذا الفصل أن البيانات الجنائية ليست مجرد معلومات علمية، بل تعبير عن الهوية الجنائية للضحية، وأن غياب الحماية القانونية لها يحوّل الخصوصية الجنائية إلى سلعة في سوق

الاحتكار العالمي.

**الفصل الثاني عشر

العدالة السيبرانية والذكاء الاصطناعي الجنائي: عندما تصبح الخوارزميات قاضياً**

مع تزايد استخدام الذكاء الاصطناعي في اتخاذ قرارات جنائية — من جمع الأدلة إلى تحديد الجناة — ظهر تهديد جديد للعدالة السيبرانية: **السلطة الخوارزمية**. فعندما تتخذ أنظمة ذكاء اصطناعي قرارات تؤثر على حق الضحية في العدالة دون إشراف بشري، فإن المجتمع الدولي يفقد جزءاً من مسؤوليته الجنائية.

وتكمن المشكلة في ثلاث نقاط:

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

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

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

وفي الممارسة، أدت أنظمة الذكاء الاصطناعي إلى انتهاكات خطيرة. ففي دولة آسيوية، رفضت خوارزمية جمع أدلة من ضحايا 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 الجنائية 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 الجنائي" 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 الجنائي، ولا توجد تشريعات تحمي العدالة الجنائية من الاستخدام غير الخاضع للرقابة لهذه التقنيات.

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

**الفصل الثالث عشر

العدالة السيبرانية والجرائم الإلكترونية الجنائية: مكافحة الاحتيال الجنائي الرقمي**

لا يمكن حماية العدالة السيبرانية دون مواجهة الجرائم الإلكترونية التي تستهدف الضحايا والمؤسسات الجنائية عبر الحدود. فاختراق الحسابات البنكية للضحايا، وسرقة الهويات الجنائية الرقمية، ونشر البرمجيات الخبيثة في أنظمة المحكمة، كلها جرائم تهدد العدالة، لكنها

تبقى خارج نطاق العدالة بسبب غياب التعاون الدولي الفعّال.

وتشير التقديرات إلى أن الخسائر العالمية من الجرائم الإلكترونية الجنائية تجاوزت 15 مليار دولار سنوياً، ومع ذلك فإن معدلات الإدانة لا تتجاوز 1 بالمئة في كثير من الدول. ويعود ذلك إلى:

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

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

- **الاختلاف في التشريعات**: فما يُعد جريمة

في دولة قد يكون مشروعاً في أخرى.

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

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

**الفصل الرابع عشر

العدالة السيبرانية والتربية الرقمية الجنائية: بناء وعي مجتمعي كأساس للدفاع الجنائي**

لا يمكن تحقيق العدالة السيبرانية دون بناء وعي مجتمعي لدى الضحايا والموظفين حول مخاطر الفضاء السيبراني وواجباتهم تجاهه. فالضحايا ليسوا مجرد ضحايا للهجمات، بل شركاء في عملية العدالة. وغياب التربية الرقمية الجنائية يجعلهم عرضة للاحتيال، ويسهل اختراق

أنظمتهم، مما يهدد البنية التحتية الجنائية الدولية بأكملها.

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

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

الموثوقة.

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

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

**الفصل الخامس عشر

العدالة السيبرانية والبحث العلمي الجنائي: نحو استقلال تكنولوجي وطني**

لا يمكن لأي دولة أن تمارس عدالتها الجنائية الرقمية بشكل حقيقي دون امتلاك قدرات بحثية محلية في مجالات الأمن السيبراني الجنائي، والذكاء الاصطناعي الجنائي، 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 الجنائية المتقدمة" مشاريع بحثية في الأمن السيبراني الجنائي بعشرات المليارات سنوياً. أما في الصين، فإن "خطة العدالة الذكية 2030" تخصص جزءاً كبيراً من ميزانيتها لتطوير

أنظمة عدالة ذكية محلية.

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

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

**الفصل السادس عشر

العدالة السيبرانية والاتفاقيات الثنائية: هل يمكن للدول الصغيرة أن تحمي نفسها؟**

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

العدالة السيبرانية والمحاكمات الجنائية: نحو اختصاص قضائي رقمي**

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

وقد اعتمدت التشريعات الوطنية عدة معايير لتحديد الاختصاص:

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

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

- **مبدأ مكان وجود الخادم**: لكن الخوادم قد

تكون في دول لا تملك علاقة بالجريمة.

وفي الممارسة، أدت هذه الغموض إلى تضارب في الأحكام. فمحكمة في دولة غربية أصدرت حكماً بحبس مواطن من دولة آسيوية لاختراقه نظاماً جنائياً 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 الجنائية"، التي تُلزم الدول الأعضاء بالاعتراف المتبادل بالأحكام. أما في دول أخرى، فلا تزال المحاكم تفتقر إلى الخبرة الفنية اللازمة لفهم الأدلة الرقمية الجنائية.

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

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

**الفصل الثامن عشر

العدالة السيبرانية والبيانات الجنائية: بين الملكية الفردية والسيادة الجماعية**

تشكل البيانات الجنائية اليوم أثمن مورد في الاقتصاد الرقمي الجنائي. ولذلك، فإن العدالة السيبرانية لا تكتمل دون تحديد من يملك حق التحكم في هذه البيانات: الضحية أم الدولة أم الشركة؟

وفي الفقه الحديث، برزت ثلاث مدارس:

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

ويؤكد هذا الفصل أن البيانات الجنائية ليست

مجرد أرقام، بل تعبير عن الهوية الجنائية الفردية والجماعية. وأن العدالة السيبرانية الحقيقية تبدأ باحترام حق الضحية في التحكم بمعلوماته.

**الفصل التاسع عشر

العدالة السيبرانية والعدالة المجتمعية: حماية المجتمعات من التكنولوجيا الجنائية غير المسؤولة**

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

وفي الممارسة، أدت بعض المشاريع الجنائية الرقمية إلى أضرار مجتمعية كبيرة. ففي دولة آسيوية، أدت منصات جمع الأدلة الذكية إلى تجاهل الضحايا من المناطق الريفية. وفي دولة أفريقية، أدت التطبيقات الرقمية إلى انتشار حلول عدالة باهظة الثمن على حساب الحلول المحلية.

ويواجه القانون الدولي غياباً في تنظيم هذا الجانب، لأن:

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

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

- لا توجد معايير دولية لـ"العدالة الجنائية 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 الجنائية الرقمية حتى يتم تقييم تأثيرها المجتمعي.

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

ويؤكد هذا الفصل أن العدالة السيبرانية يجب أن

تمتد إلى حماية العدالة المجتمعية، وأن التكنولوجيا الجنائية يجب أن تُبنى على مبدأ "المسؤولية منذ التصميم".

**الفصل العشرون

العدالة السيبرانية والمستقبل: نحو مشروع اتفاقية دولية نموذجية**

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

أولاً: **تعريف موحد للعدالة السيبرانية** كحق للضحية في الاستفادة من أنظمة ذكية تُصمم خصيصاً لتعقب الجرائم الإلكترونية في الفضاء السيبراني، مع ضمانات قانونية تحمي حقوق المتهم من التحيّز الخوارزمي.

ثانياً: **قائمة موحدة للبنية التحتية للعدالة السيبرانية**، تشمل الأنظمة الأساسية (جمع الأدلة الرقمية، منصات التواصل، قواعد البيانات، أنظمة تحديد الجناة).

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

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 المحكمة بإعادة المحاكمة رداً على الفشل الرقمي.

سادساً: **التزام الدول بحماية البيانات الجنائية**، واحترام حقوق الضحايا في الخصوصية.

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

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

تاسعاً: **إنشاء محكمة سيبرانية جنائية دولية**، تنظر في النزاعات المتعلقة بالعدالة السيبرانية.

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

ويُختتم هذا الفصل بالتذكير بأن العدالة السيبرانية ليست نهاية التاريخ، بل بداية مرحلة جديدة من تطور القانون الجنائي الدولي، توازن بين الأمن المجتمعي وحق الضحية في العدالة الرقمية، والجريمة والتكنولوجيا، والعقاب والكرامة

الإنسانية.

**الفصل الحادي والعشرون

العدالة السيبرانية والعقود الذكية: عندما تصبح الخوارزمية قاضياً وشاهداً**

لم يعد مفهوم العقد الجنائي يقتصر على الورق والشهود، بل امتد ليشمل **العقود الذكية** التي تنفذ نفسها تلقائياً عند توفر الشروط. فالعدالة عبر العقد الذكي ليس مجرد إجراء، بل **تنفيذ آلي لشروط مسبقة** قد لا يدركها الضحايا عند تقديم الأدلة.

وفي الممارسة، بدأت بعض الدول بتجربة العقود الذكية. ففي إستونيا، يُسمح للضحايا بإدراج

شروط عدالة تلقائية في عقدهم الرقمي. أما في الإمارات، فإن "منصة العدالة الذكية" تتيح للضحايا تحديد شروط جمع الأدلة مسبقاً.

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

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

**الفصل الثاني والعشرون

العدالة السيبرانية والطاقة الجنائية: حماية الموارد من الاستنزاف الرقمي**

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

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

ويواجه القانون الدولي غياباً في تنظيم هذا الجانب، لأن:

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

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

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

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

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

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

**الفصل الثالث والعشرون

العدالة السيبرانية وسلامة الضحايا: حماية الضحايا من التلاعب الرقمي**

لا يمكن فصل العدالة السيبرانية عن حماية سلامة الضحايا. 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 الضحايا.

ففي عام 2024، تم اختراق منصة عدالة في دولة أوروبية، مما أدى إلى تغيير شروط جمع الأدلة. وفي عام 2025، تم نشر معلومات مضللة عن ضحايا 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 العدالة الرقمية.

- معظم المنصات الرقمية لا تخضع لرقابة جنائية كافية.

- لا توجد معايير دولية لشفافية المعلومات الجنائية الرقمية.

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

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

ويؤكد هذا الفصل أن العدالة السيبرانية في مجال سلامة الضحايا ليس رفاهية، بل حق إنساني أساسي، وأن سلامة إجراءات العدالة الرقمية يجب أن تُعتبر جزءاً من الأمن القومي الجنائي.

**الفصل الرابع والعشرون

العدالة السيبرانية والتعليم الجنائي الرقمي: بناء وعي مجتمعي كأساس للدفاع عن الحقوق**

لا يمكن تحقيق العدالة السيبرانية دون بناء وعي

مجتمعي لدى الضحايا حول حقوقهم الرقمية وواجباتهم تجاه العدالة العامة. فالتعليم الجنائي الرقمي ليس مجرد نشر معلومات، بل تمكين الضحايا من المطالبة بحقوقهم والمشاركة في صنع القرار الجنائي.

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

وفي الممارسة، بدأت بعض الدول بدمج العدالة الرقمية في المناهج التعليمية. ففي فنلندا، يتعلم الطلاب من سن السادسة كيفية حماية بياناتهم الجنائية. أما في كوستاريكا، فإن

"التعليم من أجل العدالة الرقمية" جزء أساسي من النظام التعليمي.

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

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

ويؤكد هذا الفصل أن التعليم الجنائي الرقمي هو استثمار استراتيجي في العدالة، وأن الدول التي لا تستثمر فيه ستظل ضحاياها عاجزين عن

المطالبة بحقوقهم.

**الفصل الخامس والعشرون

العدالة السيبرانية والتراث الجنائي: حماية التراث من الاندثار الرقمي**

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

ففي إفريقيا، تهدد منصات جمع الأدلة الذكية الممارسات الجنائية التقليدية التي طوّرها المجتمعات عبر الأجيال. وفي أمريكا اللاتينية،

يؤدي الاعتماد على الإجراءات الرقمية إلى تآكل المهارات الجنائية التقليدية. بل إن بعض اللغات والعادات الجنائية 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 الجنائية على قائمة الخطر.

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

ويؤكد هذا الفصل أن العدالة السيبرانية الثقافية هي جزء من الهوية الوطنية، وأن غياب الحماية

القانونية لهذا البعد يحوّل الشعوب إلى شهود على اندثار تاريخهم الجنائي.

**الفصل السادس والعشرون

العدالة السيبرانية والتمويل الجنائي الرقمي: حماية الدول النامية من الديون الجنائية**

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

ففي جزر المحيط الهادئ، أدت الأزمات

الاقتصادية إلى انهيار الإيرادات الجنائية، مما جعل سداد القروض الجنائية 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 الجنائية الرقمية تأتي بشروط صارمة تزيد من عبء الديون.

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

وفي المقابل، بدأت بعض المبادرات. ففي مؤتمر الدول الأطراف في نظام روما الأساسي 2025، تم اقتراح "آلية لإعادة هيكلة الديون الجنائية"، لكنها لم تُعتمد بعد. أما في مجموعة السبع، فإن "مبادرة التمويل الجنائي الرقمي العادل" لا تزال في طور النقاش.

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

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

**الفصل السابع والعشرون

العدالة السيبرانية والنقل الجنائي الرقمي: حماية سلاسل التوريد من التهديدات السيبرانية**

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

ففي عام 2024، تم اختراق نظام تتبع المستندات الجنائية في دولة أوروبية، مما أدى إلى تلف آلاف الملفات بسبب تأخير التوصيل.

وفي عام 2025، تم سرقة شحنات مستندات جنائية عبر اختراق أنظمة الموانئ الرقمية.

ويواجه القانون الدولي غياباً في تصنيف سلاسل التوريد الجنائية 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 العدالة السيبرانية في مجال النقل ليس مسألة تقنية، بل مسألة أمن جنائي، وأن سلاسل التوريد الجنائية الرقمية يجب أن تُعتبر جزءاً من البنية التحتية الحيوية.

**الفصل الثامن والعشرون

العدالة السيبرانية والبحث العلمي الجنائي المفتوح: التوازن بين التعاون والحماية**

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

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

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

ويؤكد هذا الفصل أن العدالة السيبرانية في

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

**الفصل التاسع والعشرون

العدالة السيبرانية والتعاون الدولي: نحو نظام عالمي عادل للحوكمة الجنائية الرقمية**

لا يمكن لأي دولة أن تحمي عدالتها الجنائية 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

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

ويستدعي الحل:

- إنشاء منتدى دولي محايد لصياغة قواعد العدالة الجنائية الرقمية.

- توفير الدعم الفني والمالي للدول النامية.

- احترام التنوع في النماذج الوطنية للعدالة الجنائية 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 الجنائية الرقمية يجب أن يقوم على مبدأ "العدالة المشتركة"، لا "الهيمنة الجنائية الرقمية".

**الفصل الثلاثون

العدالة السيبرانية والقانون الإنساني الدولي: حماية المدنيين في النزاعات الجنائية**

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

حرب؟

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

وفي مشروع "قواعد تالين 2.0"، تم التأكيد على أن تدمير البنية التحتية الجنائية 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 الجنائية" لا تزال قيد

النقاش، ولم تُدرج بعد في النظام الأساسي.

ويؤكد هذا الفصل أن العدالة السيبرانية في زمن الحرب لا يعني التخلي عن الإنسانية، بل تعزيز حماية المدنيين من الأسلحة الجنائية الرقمية.

**الفصل الحادي والثلاثون

العدالة السيبرانية والفضاء الخارجي: حماية الأرض من التلوث الفضائي الجنائي**

مع تزايد الأنشطة الفضائية المتعلقة بالعدالة — من الأقمار الصناعية لمراقبة المحاكم إلى الطائرات المسيرة الفضائية لتوزيع المستندات — برز تهديد جديد: التلوث الفضائي الذي يؤثر على الأنظمة الجنائية. فحطام الأقمار الصناعية قد

يعيق أنظمة الرصد الجنائي، بينما تنبعثات الصواريخ تؤثر على الغلاف الجوي الذي ينظم الاتصالات الجنائية.

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

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

**الفصل الثاني والثلاثون

العدالة السيبرانية والذكاء الاصطناعي التوليدي: عندما تصبح الأخبار الكاذبة سلاحاً جنائياً**

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 الجنائية الوطنية.

ففي عام 2025، تم تداول فيديوهات مزيفة لضحايا وهم يحذرون من أنظمة وطنية آمنة، مما أدى إلى انخفاض الثقة في النظام الجنائي وانتشار المعلومات المضللة. وفي أزمات جنائية، تم نشر أخبار كاذبة عن نقص في الموارد الجنائية 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 جنائي" 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 الجنائية.

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

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

**الفصل الثالث والثلاثون

العدالة السيبرانية والبيانات الضخمة الجنائية: حماية السيادة من الاستغلال الرقمي**

مع تزايد الاعتماد على البيانات الضخمة في تحليل الجرائم، 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 جنائية 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 الجنائية.

- معظم العقود بين الدول والشركات تبقى سرية.

- لا توجد معايير لـ"السيادة الجنائية الرقمية".

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

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

**الفصل الرابع والثلاثون

العدالة السيبرانية والتعليم العالي الجنائي: نحو كليات وطنية للقانون الجنائي الرقمي**

لا يمكن بناء قدرات جنائية 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 الجنائي الرقمي يُعد استثماراً استراتيجياً في العدالة السيبرانية.

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

أما في الدول النامية، فإن التعليم الجنائي 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 الجنائي الرقمي.

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

**الفصل الخامس والثلاثون

العدالة السيبرانية والثقافة الرقمية الجنائية: حماية الإبداع المحلي من القرصنة والتهميش**

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

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

**الفصل السادس والثلاثون

العدالة السيبرانية والتمويل الرقمي الجنائي: حماية العملات الجنائية من التلاعب والاحتيال**

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

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

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

ويخلص هذا الفصل إلى أن العدالة السيبرانية

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

**الفصل السابع والثلاثون

العدالة السيبرانية والبحث العلمي الجنائي المفتوح: التوازن بين التعاون والحماية**

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

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

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

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

**الفصل الثامن والثلاثون

العدالة السيبرانية والتعاون الدولي: نحو نظام عالمي عادل للحوكمة الجنائية الرقمية**

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

ويستدعي الحل:

- إنشاء منتدى دولي محايد لصياغة قواعد العدالة الجنائية الرقمية.

- توفير الدعم الفني والمالي للدول النامية.

- احترام التنوع في النماذج الوطنية للعدالة الجنائية 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 الجنائية الرقمية يجب أن يقوم على مبدأ "العدالة المشتركة"، لا "الهيمنة الجنائية الرقمية".

**الفصل التاسع والثلاثون

العدالة السيبرانية والقانون الإنساني الدولي: حماية المدنيين في النزاعات الجنائية**

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

البنية التحتية الجنائية الرقمية كوسيلة حربية انتهاكاً للقانون الإنساني الدولي؟ وهل يُعتبر التسبب المتعمد في فشل العدالة جريمة حرب؟

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

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

ويؤكد هذا الفصل أن العدالة السيبرانية في زمن الحرب لا يعني التخلي عن الإنسانية، بل تعزيز حماية المدنيين من الأسلحة الجنائية الرقمية.

**الفصل الأربعون

العدالة السيبرانية والمستقبل: رؤية استراتيجية للعقود القادمة**

في الختام، لا يمكن النظر إلى العدالة السيبرانية كظاهرة مؤقتة، بل كتحول جوهري

في مفهوم العدالة في القرن الحادي والعشرين. فالدول التي تبني عدالتها الجنائية الرقمية اليوم ستكون قادرة على:

- حماية ضحاياها من التلاعب الجنائي الرقمي.

- بناء اقتصاد جنائي رقمي مستقل ومستدام.

- تعزيز مكانة أجيالها في النظام الجنائي 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 العدالة السيبرانية ليس مسألة اختيار، بل مسألة بقاء.

خاتمة

بعد استعراض شامل لأبعاد العدالة السيبرانية 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 الجنائي الرقمي، رغم طبيعته غير المادية، بات ساحة للصراعات السياسية والاقتصادية، ولا يمكن لأي

دولة أن تحافظ على عدالتها الجنائية 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 الضحية في العدالة الرقمية.

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

المراجع

Rome Statute of the International Criminal Court (1998)

Convention on the Prevention and Punishment of the Crime of Genocide ((1948

Geneva Conventions (1949) and Additional Protocols

General Data Protection Regulation

(GDPR), Regulation (EU) 2016/679

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

International Covenant on Civil and Political (Rights (1966

UNODC Handbook on Strategies to Combat (Cybercrime (2023

European Commission. Digital Justice (Action Plan (2024

Government of Estonia. Smart Court (Initiative Report (2023

Government of Singapore. Digital Justice

(Framework (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). International Criminal Justice and Digital Sovereignty. Oxford University Press

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

Press

Kloppenburg J R. (2024). Digital Sovereignty and International Criminal Law. University of California Press

:Official Government Sources

White House. National Strategy for Digital (Justice (2024

European Commission. Digital Justice (Action Plan (2023

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

:Academic Journals

Journal of International Criminal Justice ((Oxford

International Journal of Digital Criminal Justice

Harvard Law Review – Criminal Justice Section

Stanford Technology Law Review

فهرس المحتويات

العدالة السيبرانية: دراسة قانونية مقارنة حول مكافحة الجرائم الإلكترونية وبناء نظام جنائي رقمي إنساني عالمي

بيان حقوق الملكية

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: **"العدالة

السيبرانية: دراسة قانونية مقارنة حول مكافحة الجرائم الإلكترونية وبناء نظام جنائي رقمي إنساني عالمي"**.

- 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