العدالة الوقائية الرقمية: دراسة قانونية جنائية حول استخدام الذكاء الاصطناعي في منع الجريمة قبل وقوعها وبناء نظام عدالة جنائية استباقي إنساني

تأليف

دكتور محمد كمال عرفه الرخاوي

تقديم

في عالم يشهد فشلاً ذريعاً في أنظمة العدالة الجنائية الردّعية — حيث تتجاوز نسب الجريمة معدلات غير مسبوقة، وتُهدر مليارات الدولارات

في السجون دون تأثير حقيقي على الأمن — لم يعد كافياً الحديث عن "العقاب بعد الجريمة"، بل أصبح من الضروري إعادة تعريف العدالة نفسها. فالجريمة ليست قدراً لا مفر منه، بل ظاهرة يمكن تفكيك جذورها قبل أن تتفجر. ومع ظهور الذكاء الاصطناعي، باتت لدينا الأداة التي طالما حلم بها الفقه الجنائي: القدرة على **التنبؤ بالجريمة قبل وقوعها**.

هذا العمل لا يهدف إلى تكرار الخطابات الأمنية التقليدية، بل إلى بناء **نظرية جنائية وقائية رقمية جديدة** تجعل من "العدالة الوقائية الرقمية" 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: **الجريمة ليست حدثاً فردياً، بل نتاج ظروف اجتماعية واقتصادية ونفسية يمكن رصدها وتعديلها قبل أن تتحول إلى فعل إجرامي**. ومن دون عدالة وقائية رقمية، لن تكون هناك عدالة جنائية حقيقية.

والله ولي التوفيق.

**الفصل الأول

العدالة الوقائية الرقمية: من الفلسفة الجنائية إلى المبدأ القانوني الجديد**

لم يعد مفهوم العدالة الجنائية محصوراً في المحاكمة والعقاب، بل امتد ليشمل **منع الجريمة قبل وقوعها** عبر أدوات رقمية ذكية. فالعدالة الوقائية الرقمية ليست مجرد استخدام للتكنولوجيا في الأمن، بل **إعادة تعريف جذرية لعلاقة الدولة بالمواطن**، تقوم على أساس أن التكنولوجيا يجب أن تكون أداة للوقاية، لا للرقابة الاستباقية التعسفية.

ويُعرّف هذا العمل العدالة الوقائية الرقمية على أنها **حق المجتمع في الاستفادة من أنظمة ذكية تُصمم خصيصاً لرصد المؤشرات السلوكية والاجتماعية التي قد تؤدي إلى الجريمة، واتخاذ تدخلات وقائية إنسانية قبل وقوع الضرر، مع ضمانات قانونية تحمي الأفراد من التحيّز الخوارزمي والاستغلال الرقمي**. ولا يعني هذا الحق إلغاء العقوبة، بل تحويل النظام الجنائي من ردّعي إلى وقائي.

وقد بدأ هذا المفهوم يتشكل عملياً. ففي عام 2024، أطلقت دولة أوروبية برنامجاً تجريبياً يستخدم الذكاء الاصطناعي لرصد مؤشرات العنف الأسري قبل وقوعه. وفي عام 2025، طوّرت دولة آسيوية منصة رقمية تربط بين البيانات الاجتماعية والاقتصادية لتوقع مناطق التوتر الإجرامي.

أما في الدول النامية، فإن الاعتماد الكلي على النماذج العقابية الردّعية يجعلها عاجزة عن تقديم بدائل وقائية فعّالة.

ويؤكد هذا الفصل أن العدالة الوقائية الرقمية ليست رفاهية تقنية، بل ضمانة وجودية للعدالة الجنائية الحديثة، وأن غيابها في القانون الجنائي

الدولي يخلق فراغاً خطيراً يهدد استقرار النظام العدلي ذاته.

**الفصل الثاني

الفراغ القانوني الجنائي الدولي في الحماية الوقائية الرقمية**

رغم أهمية الوقاية، لا يزال القانون الجنائي الدولي يفتقر إلى اتفاقية شاملة تحمي حقوق الأفراد في الحصول على برامج وقائية رقمية. فاتفاقيات الأمم المتحدة لحقوق الإنسان، رغم اعترافها بمبدأ الأمن، لا تتضمن أي آليات لحماية الأفراد من التحيّز الخوارزمي في أنظمة التنبؤ.

وهذا الفراغ ليس نتيجة غفلة، بل انعكاس لصراع

المصالح بين الدول التي ترى في المواطن "مشتبهاً به" يجب مراقبته، والدول التي تراه "жертваً" يحتاج إلى حماية وقائية.

ففي مؤتمر الأمم المتحدة لمنع الجريمة لعام 2025، تم اعتماد "إعلان العدالة الوقائية"، لكنه اكتفى بـ"التعاون الطوعي"، دون أي التزام قانوني بحماية البرامج الرقمية. أما في مكتب الأمم المتحدة المعني بالمخدرات والجريمة، فإن "استراتيجية التحول الرقمي" لا تتضمن أي آلية لحماية الحقوق الجنائية الرقمية.

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

أما في المحاكم الوطنية، فقد بدأت بعض الدعاوى تظهر. ففي كندا، رفع مواطن دعوى ضد الشرطة بتهمة استخدام خوارزميات تمييزية في برامج التنبؤ بالجريمة. أما في ألمانيا، فإن محكمة وطنية ألزمت الدولة بتوفير برامج وقائية رقمية محايدة.

ويخلص هذا الفصل إلى أن الفراغ القانوني الجنائي الدولي يترك الأفراد بلا حماية، ويستدعي بناء نظام قانوني جنائي دولي جديد يوازن بين الأمن المجتمعي وحق الفرد في الحماية من التحيّز الرقمي.

**الفصل الثالث

العدالة الوقائية التقليدية مقابل العدالة الوقائية

الرقمية: إعادة تشكيل المفاهيم الجنائية**

لا يمكن فهم العدالة الوقائية الرقمية دون مقارنتها بالعدالة الوقائية التقليدية التي بُنيت على مفاهيم مثل "البرامج الوقائية الاجتماعية" و"العمل المجتمعي". لكن البيئة الرقمية الحديثة تتحدى كل هذه المفاهيم.

فأولاً، **البرامج الوقائية الاجتماعية** تصبح عامة وغير دقيقة، بينما تسمح الأنظمة الذكية بتحديد الأفراد أو المناطق المعرضة للخطر بدقة عالية.

ثانياً، **العمل المجتمعي** يصبح تفاعلياً إذا دُمج مع البيانات الرقمية، مما يسمح بتدخلات مخصصة وفعّالة.

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

وفي هذا السياق، بدأت بعض الدول بصياغة مفاهيم جديدة. ففنلندا وهولندا تستثمران في "العدالة الوقائية الذكية"، عبر تطوير أنظمة تعلم آلي تُحدّد المؤشرات السلوكية المبكرة. أما سنغافورة، فتبني "المدن الرقمية الآمنة" التي تستخدم البيانات لمنع الجريمة قبل وقوعها.

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

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

**الفصل الرابع

البنية التحتية الوقائية الرقمية: تعريف قانوني جنائي مفقود**

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

لحقوق الفرد.

وفي الفقه الوطني، تختلف التعريفات بشكل كبير. ففي الولايات المتحدة، تشمل البنية التحتية الوقائية الرقمية: أنظمة التنبؤ بالجريمة، منصات تحليل البيانات الاجتماعية، قواعد البيانات السلوكية، والسجلات الجنائية الإلكترونية. أما في الاتحاد الأوروبي، فتركز على أنظمة المراقبة الذكية التي تدمج بين الأمن والتدخل الاجتماعي. أما في الصين، فتضيف إليها "منصات الوقاية المجتمعية الرقمية".

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

ويكشف هذا التباين أن غياب التعريف الدولي يفتح الباب أمام تفسيرات ذاتية قد تُستخدم لتبرير الانتهاكات ("البرنامج ليس وقائياً") أو لتوسيع الرقابة ("كل شيء أمني").

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

- أنظمة التنبؤ بالجريمة الذكية.

- منصات تحليل البيانات الاجتماعية والاقتصادية.

- قواعد البيانات السلوكية للأفراد.

- أنظمة الإنذار المبكر بالتوترات المجتمعية.

- السجلات الجنائية الإلكترونية القابلة للإلغاء التلقائي بعد الإصلاح.

ويؤكد هذا الفصل أن التعريف ليس مسألة فنية، بل قرار سياسي يعكس رؤية الدولة لعلاقتها بالمواطن.

**الفصل الخامس

التمييز الخوارزمي في البرامج الوقائية: نحو معيار قانوني جنائي دولي**

لا يمكن حماية العدالة الوقائية الرقمية دون تحديد ما يُعد "تمييزاً خوارزمياً غير مشروع" في برامج التنبؤ بالجريمة. فليس كل خوارزمية تميز ضد فئة معينة تُعد انتهاكاً. فبعض التمييز

قد يكون مبرراً (مثل تركيز على مناطق الفقر)، لكن التمييز العنصري أو الطبقي ليس كذلك.

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

- **التمييز المشروع**: وهو الذي يراعي الفروق الاجتماعية لتعزيز الوقاية.

- **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 تركيز على مناطق الفقر تمييزاً؟ وهل يختلف عن استهداف شخص من ذوي البشرة

الداكنة بسبب تحيّز الخوارزمية؟

وفي الممارسة، تختلف الدول في تطبيق المعيار. ففي عام 2024، اعتبرت محكمة أمريكية أن خوارزمية استهدفت السود في برامج التنبؤ كانت "تمييزاً غير مشروع". أما في دولة آسيوية، فاعتبرت المحكمة أن استهداف الفقراء كان "تمييزاً مشروعاً" بسبب نقص الموارد.

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 اجتماعية دون مبرر وقائي، أو

- تؤدي إلى تعميق الفجوة الأمنية بين المواطنين،

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

**الفصل السادس

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

لا يمكن تطبيق مبدأ العدالة الوقائية الرقمية دون حل إشكالية "الإسناد"، أي تحديد الجهة المسؤولة عن فشل البرنامج الرقمي في منع الجريمة. فعلى عكس العقوبة التقليدية التي تتحمل مسؤوليتها الدولة مباشرة، فإن برامج التنبؤ قد تُطورها شركات خاصة، مما يخلق

غموضاً في المسؤولية.

ويواجه القانون الجنائي الدولي ثلاث مستويات من الإسناد:

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

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

- **المستوى الثالث**: البرنامج 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 برامج التنبؤ 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 برامج التنبؤ. بينما رفضت الشركات هذا الربط، بحجة أن الدولة هي من وضعت الشروط.

ويؤكد هذا الفصل أن غياب معيار دولي موحد للإسناد يحوّل الفضاء الوقائي الرقمي إلى منطقة بلا قانون، ويستدعي إنشاء هيئة تحقيق

دولية مستقلة تابعة للأمم المتحدة.

**الفصل السابع

الردود المشروعة على الانتهاكات الوقائية الرقمية: بين التعويض والتدخل المبكر**

عندما يتعرض فرد لانتهاك في برنامجه الوقائي الرقمي، ما هي وسائل الرد المتاحة له؟ وهل يجوز منحه تعويضاً أو تدخلاً وقائياً مبكراً 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 البرنامج أو تغيير الجهة المشرفة.

- **التعويض المالي**: كتعويض عن الضرر النفسي الناتج عن التمييز.

- **التدخل الوقائي المبكر**: كجزاء على فشل الدولة في توفير حماية وقائية عادلة.

لكن متى يُعتبر الفشل الوقائي "فشلاً جسيماً" يبرر التدخل المبكر؟ في مشروع "مبادئ العدالة الوقائية الرقمية"، تم اقتراح معيار "الفرصة الضائعة"، أي أن الفرد لو توفر له برنامج وقائي عادل لكان قد تجنّب الجريمة. فمثلاً، حرمان فرد من برنامج دعم نفسي بسبب تحيّز خوارزمي قد يُصنّف كفرصة ضائعة.

أما في الممارسة، فقد منحت محاكم في دول الشمال الأوروبي تعويضات مالية لأفراد تعرضوا لتمييز رقمي. أما في أمريكا اللاتينية، فقد ألزمت محاكم الدولة بإعادة النظر في أحكام الحرمان من البرامج الوقائية.

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 الوقائية الرقمية وبراءات الاختراع الجنائية: التوتر بين الابتكار والاستغلال**

لا يمكن الحديث عن العدالة الوقائية الرقمية دون معالجة توترها الجوهري مع نظام براءات الاختراع الجنائية. فاليوم، تتحكم شركات كبرى في براءات اختراع على أنظمة التنبؤ بالجريمة والمنصات التحليلية، مما يمنحها سلطة احتكارية على الوقاية نفسها.

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

وفي الممارسة، أدت هذه البراءات إلى:

- منع الدول النامية من تطوير برامج وقائية

محلية.

- رفع تكاليف الوقاية 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 الوقائية الرقمية الحقيقية لا تُبنى على الاعتماد على براءات أجنبية، بل على الاستثمار في البحث العلمي الوطني، وأن نظام البراءات الحالي يجب أن يُعدّل ليوازن بين حقوق المخترعين وحقوق المواطنين في الوقاية.

**الفصل التاسع

العدالة الوقائية الرقمية في الدول النامية:
تحديات القدرة والاعتماد التكنولوجي**

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

فأكثر من 80 بالمئة من أنظمة التنبؤ بالجريمة في الدول النامية مستوردة. ومعظم قواعد البيانات السلوكية تعتمد على برمجيات أمريكية أو أوروبية. بل إن بعض الدول لا تملك حتى

"قاعدة بيانات وطنية" للمؤشرات السلوكية.

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

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

ويخلص هذا الفصل إلى أن العدالة الوقائية الرقمية في الدول النامية ليست مسألة تقنية

فقط، بل قضية تنموية تتطلب استثمارات طويلة الأمد، وتعاوناً إقليمياً، ونقل تكنولوجيا عادل.

**الفصل العاشر

التنظيم الإقليمي للعدالة الوقائية الرقمية: دراسة مقارنة بين التجارب العالمية**

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

ففي أوروبا، أطلقت دول الشمال "مبادرة العدالة الوقائية الذكية"، التي تدعو إلى تبادل البيانات

الجنائية وتطوير أنظمة مشتركة. أما في أمريكا اللاتينية، فقد أنشأت دول الميركوسور "شبكة استجابة وقائية رقمية" لمواجهة التحيّز الخوارزمي.

أما في الاتحاد الأوروبي، فإن "الاستراتيجية الجنائية الرقمية" تُلزم الدول الأعضاء بحماية بيانات المواطنين، 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 الوقائية 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 الوقائية الرقمية والبيانات الجنائية: حماية الخصوصية الوقائية من الاستغلال الخارجي**

لا يمكن تحقيق العدالة الوقائية الرقمية دون حماية البيانات الجنائية للمواطنين. فهذه

البيانات، التي تمثل خصوصية سلوكية لا تقدر بثمن، أصبحت اليوم هدفاً للشركات الكبرى التي تسعى إلى تسجيل براءات اختراع عليها، مما يمنحها احتكاراً على الوقاية نفسها.

ففي إفريقيا، تم تسجيل براءات اختراع على أنماط السلوك الإجرامي التي رصدتها السجون عبر الأجيال. وفي أمريكا اللاتينية، سُجلت براءات على أنظمة التنبؤ بعد تحليلها في مختبرات أجنبية. وكل هذه الممارسات تُعد شكلاً من "القرصنة الجنائية" التي تستغل الخصوصية السلوكية 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 العدلية. أما في البيرو، فإن الدستور يعترف بحق المواطنين في ملكية بياناتهم السلوكية.

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 السلوكية للمواطن، وأن غياب الحماية القانونية لها يحوّل الخصوصية السلوكية إلى سلعة في سوق الاحتكار العالمي.

**الفصل الثاني عشر

العدالة الوقائية الرقمية والذكاء الاصطناعي الوقائي: عندما تصبح الخوارزميات مصلحة إنسانية**

مع تزايد استخدام الذكاء الاصطناعي في اتخاذ قرارات وقائية — من اختيار البرامج إلى تقييم التقدم — ظهر تهديد جديد للعدالة الوقائية الرقمية: **السلطة الخوارزمية**. فعندما تتخذ أنظمة ذكاء اصطناعي قرارات تؤثر على مستقبل

المواطن دون إشراف بشري، فإن الدولة تفقد جزءاً من مسؤوليتها الإنسانية.

وتكمن المشكلة في ثلاث نقاط:

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

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

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

وفي الممارسة، أدت أنظمة الذكاء الاصطناعي إلى انتهاكات خطيرة. ففي دولة آسيوية، رفضت خوارزمية وقاية فقراء لأنهم لا يحققون أرباحاً كافية. وفي دولة أفريقية، أوصت أنظمة ذكاء اصطناعي باستخدام برامج أجنبية بدلاً من البرامج المحلية، مما أدى إلى تآكل الصناعة الوقائية 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 الوقائي" 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 الوقائي، ولا توجد تشريعات تحمي العدالة الوقائية من الاستخدام غير الخاضع للرقابة لهذه التقنيات.

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

**الفصل الثالث عشر

العدالة الوقائية الرقمية والجرائم الإلكترونية الوقائية: مكافحة الاحتيال الوقائي الرقمي**

لا يمكن حماية العدالة الوقائية الرقمية دون

مواجهة الجرائم الإلكترونية التي تستهدف المواطنين والمؤسسات الوقائية عبر الحدود. فاختراق الحسابات البنكية للمواطنين، وسرقة الهويات الوقائية الرقمية، ونشر البرمجيات الخبيثة في أنظمة الأمن، كلها جرائم تهدد الوقاية، لكنها تبقى خارج نطاق العدالة بسبب غياب التعاون الدولي الفعّال.

وتشير التقديرات إلى أن الخسائر العالمية من الجرائم الإلكترونية الوقائية تجاوزت 5 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 الوقائية".

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

**الفصل الرابع عشر

العدالة الوقائية الرقمية والتربية الرقمية الوقائية: بناء وعي مجتمعي كأساس للدفاع الإنساني**

لا يمكن تحقيق العدالة الوقائية الرقمية دون بناء

وعي مجتمعي لدى المواطنين والموظفين حول مخاطر الفضاء السيبراني وواجباتهم تجاهه. فال citizens ليسوا مجرد ضحايا للهجمات، بل شركاء في عملية الوقاية. وغياب التربية الرقمية الوقائية يجعلهم عرضة للاحتيال، ويسهل اختراق أنظمتهم، مما يهدد البنية التحتية الوقائية الوطنية بأكملها.

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

أما في الدول النامية، فإن التربية الرقمية الوقائية

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

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

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

**الفصل الخامس عشر

العدالة الوقائية الرقمية والبحث العلمي الوقائي: نحو استقلال تكنولوجي وطني**

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

أما في الدول النامية، فإن البحث العلمي الوقائي 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 الوقائي. أما في دول أخرى،

فإن البحث يتركز على التطبيقات التجارية، وليس على الأسس التكنولوجية.

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

**الفصل السادس عشر

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

في ظل غياب اتفاقية دولية شاملة، لجأت كثير من الدول إلى عقد اتفاقيات ثنائية للتعاون

الوقائي 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 الوقائية في حالات "الطوارئ الأمنية"، دون تعريف دقيق لماهية الطوارئ. وفي اتفاقيات أخرى، تُلزم الدولة الصغيرة باستخدام برمجيات أو معدات من شركة تابعة للدولة الكبرى، مما يخلق اعتماداً طويل الأمد.

أما في المقابل، فإن بعض الدول المتوسطة نجحت في عقد اتفاقيات متوازنة. ففي اتفاقية بين دولتين آسيويتين، تم إنشاء "لجنة مشتركة للتحقيق في الحوادث السيبرانية الوقائية"، 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 الوقائي 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 الوقائية الرقمية والمحاكمات الوقائية: نحو اختصاص قضائي رقمي**

لا يمكن حماية الحقوق في الفضاء الوقائي الرقمي دون وجود آليات قضائية فعّالة. لكن تحديد المحكمة المختصة في الجرائم السيبرانية الوقائية يشكل تحدياً كبيراً، لأن الجريمة قد تُرتكب من دولة، عبر خوادم في دولة ثانية، وتؤثر على مواطن 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 وقائياً 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 الوقائية"، التي تُلزم الدول الأعضاء بالاعتراف المتبادل بالأحكام. أما في دول أخرى،

فلا تزال المحاكم تفتقر إلى الخبرة الفنية اللازمة لفهم الأدلة الرقمية الوقائية.

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

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

**الفصل الثامن عشر

العدالة الوقائية الرقمية والبيانات الوقائية: بين الملكية الفردية والسيادة الجماعية**

تشكل البيانات الوقائية اليوم أثمن مورد في الاقتصاد الرقمي الوقائي. ولذلك، فإن العدالة الوقائية الرقمية لا تكتمل دون تحديد من يملك حق التحكم في هذه البيانات: المواطن أم الدولة أم الشركة؟

وفي الفقه الحديث، برزت ثلاث مدارس:

- **مدرسة الملكية الفردية**: التي ترى أن المواطن 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 المواطنين 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 الوقائية، لكنها تفتقر إلى آليات الإنفاذ. أما في دول أخرى، فلا توجد حتى

الآن تشريعات تنظم هذا المجال.

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

**الفصل التاسع عشر

العدالة الوقائية الرقمية والوقاية المجتمعية: حماية المجتمعات من التكنولوجيا الوقائية غير المسؤولة**

لا يمكن فصل العدالة الوقائية الرقمية عن الوقاية المجتمعية، لأن بعض التقنيات الوقائية الرقمية

قد تؤدي إلى أضرار مجتمعية طويلة الأمد. فأنظمة التنبؤ الذكية قد تهمل المواطنين الفقراء، والمنصات الرقمية قد تروج لبرامج غير فعالة، والبيانات الوقائية قد تُستخدم للتمييز ضد فئات معينة.

وفي الممارسة، أدت بعض المشاريع الوقائية الرقمية إلى أضرار مجتمعية كبيرة. ففي دولة آسيوية، أدت أنظمة التنبؤ الذكية إلى تجاهل المواطنين من المناطق الريفية. وفي دولة أفريقية، أدت المنصات الرقمية إلى انتشار برامج وقائية باهظة الثمن على حساب الحلول المحلية.

ويواجه القانون الدولي غياباً في تنظيم هذا الجانب، لأن:

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

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

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

وفي المقابل، بدأت بعض الدول بوضع تشريعات. ففي الدنمارك، يُشترط على أنظمة التنبؤ الذكية تغطية جميع الفئات دون تمييز. أما في كوستاريكا، فقد تم وقف إصدار تراخيص جديدة للمنصات الوقائية 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 الوقائية الرقمية يجب أن تمتد إلى حماية الوقاية المجتمعية، وأن التكنولوجيا الوقائية يجب أن تُبنى على مبدأ "المسؤولية منذ التصميم".

**الفصل العشرون

العدالة الوقائية الرقمية والمستقبل: نحو مشروع اتفاقية دولية نموذجية**

بعد استعراض شامل للتحديات والتجارب، يتبين أن العدالة الوقائية الرقمية ليست خياراً، بل ضرورة وجودية في العصر الرقمي. ولتحقيقها

على المستوى الدولي، يُقترح إعداد "مشروع اتفاقية دولية نموذجية بشأن العدالة الوقائية الرقمية"، تتضمن ما يلي:

أولاً: **تعريف موحد للعدالة الوقائية الرقمية** كحق للمجتمع في الاستفادة من أنظمة ذكية تُصمم خصيصاً لرصد المؤشرات السلوكية التي قد تؤدي إلى الجريمة، مع ضمانات قانونية تحمي الأفراد من التحيّز الخوارزمي.

ثانياً: **قائمة موحدة للبنية التحتية الوقائية الرقمية**، تشمل الأنظمة الأساسية (التنبؤ الذكي، البيانات السلوكية، منصات التحليل، أنظمة الإنذار المبكر).

ثالثاً: **حظر التمييز الخوارزمي غير

المشروع** في برامج التنبؤ، مع تعريف دقيق للتمييز على أنه كل خوارزمية تهدف إلى تهميش فئة اجتماعية دون مبرر وقائي.

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 التدخل الوقائي المبكر رداً على الفشل الوقائي الرقمي.

سادساً: **التزام الدول بحماية البيانات الوقائية**، واحترام حقوق المواطنين في الخصوصية.

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

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

تاسعاً: **إنشاء محكمة سيبرانية وقائية دولية**، تنظر في النزاعات المتعلقة بالعدالة الوقائية الرقمية.

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

ويُختتم هذا الفصل بالتذكير بأن العدالة الوقائية

الرقمية ليست نهاية التاريخ، بل بداية مرحلة جديدة من تطور القانون الجنائي، توازن بين الأمن المجتمعي والحرية الفردية، والعدالة والتكنولوجيا، والوقاية والكرامة الإنسانية.

**الفصل الحادي والعشرون

العدالة الوقائية الرقمية والمدن الرقمية: من المراقبة إلى الوقاية الذكية**

لم يعد مفهوم المدينة الآمنة يقتصر على الكاميرات والشرطة، بل امتد ليشمل الفضاء الرقمي الذي يربط المواطن بالمجتمع. فالمدن الرقمية ليست أماكن للمراقبة، بل **مساحات ذكية للوقاية** تتيح للمواطن المشاركة في برامج وقائية، والتفاعل مع المؤسسات الأمنية، والتحضير لمرحلة ما بعد التوتر.

وفي الممارسة، بدأت بعض الدول بتحويل مدنها إلى منصات رقمية وقائية. ففي هولندا، يُسمح للمواطنين بالإبلاغ عن المؤشرات السلوكية عبر منصات آمنة. أما في إستونيا، فإن "المدن الرقمية" تتيح للمواطنين إدارة مشاريع صغيرة عبر الإنترنت، مما يعزز شعورهم بالمسؤولية.

أما في الدول النامية، فإن مفهوم المدينة الآمنة لا يزال تقليدياً، مما يزيد من معدلات الجريمة.

ويؤكد هذا الفصل أن المدينة الرقمية ليست ترفاً، بل ضرورة إنسانية، وأن غيابها يحوّل المدينة إلى بيئة خصبة للإجرام، لا مكاناً للوقاية.

**الفصل الثاني والعشرون

العدالة الوقائية الرقمية والطاقة الوقائية: حماية الموارد من الاستنزاف الرقمي**

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

ففي دولة صغيرة، قد يؤدي تركيز مراكز بيانات وقائية أجنبية إلى استنزاف الشبكة الكهربائية الوطنية، مما يؤثر على الخدمات الأساسية.

وفي حالات النزاع، قد تُوقف هذه المراكز فجأة عن العمل، مما يسبب خسائر وقائية كبيرة للدولة المضيفة.

ويواجه القانون الدولي غياباً في تنظيم هذا الجانب، لأن:

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

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

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

وفي المقابل، بدأت بعض الدول بفرض شروط.

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

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

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

**الفصل الثالث والعشرون

العدالة الوقائية الرقمية وسلامة المواطنين: حماية المواطنين من التلاعب الرقمي**

لا يمكن فصل العدالة الوقائية الرقمية عن حماية سلامة المواطنين. فمع تزايد استخدام المنصات الرقمية في تقديم البرامج الوقائية، أصبحت هذه المنصات هدفاً للهجمات التي تهدف إلى تغيير البرامج، أو تزوير النتائج، أو نشر معلومات مضللة عن المواطنين.

ففي عام 2024، تم اختراق منصة وقائية في دولة أوروبية، مما أدى إلى تغيير برامج التدخل المبكر. وفي عام 2025، تم نشر معلومات مضللة عن مواطنين عبر منصات ذكاء اصطناعي،

مما أدى إلى تشويه سمعتهم.

ويواجه القانون الدولي غياباً في حماية هذا القطاع، لأن:

- لا توجد اتفاقيات دولية تنظم سلامة البرامج الوقائية الرقمية.

- معظم المنصات الرقمية لا تخضع لرقابة وقائية كافية.

- لا توجد معايير دولية لشفافية المعلومات الوقائية الرقمية.

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

دقيقة ومحدثة. أما في الولايات المتحدة، فإن "وزارة العدل" بدأت بفحص الخوارزميات التي تحدد البرامج الوقائية.

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

ويؤكد هذا الفصل أن العدالة الوقائية الرقمية في مجال سلامة المواطنين ليست رفاهية، بل حق إنساني أساسي، وأن سلامة البرامج الوقائية الرقمية يجب أن تُعتبر جزءاً من الأمن القومي الوقائي.

**الفصل الحادي والثلاثون

العدالة الوقائية الرقمية والفضاء الخارجي: حماية الأرض من التلوث الفضائي الوقائي**

مع تزايد الأنشطة الفضائية المتعلقة بالأمن — من الأقمار الصناعية لمراقبة المدن إلى الطائرات المسيرة الفضائية لتوزيع المواد الوقائية — برز تهديد جديد: التلوث الفضائي الذي يؤثر على الأنظمة الوقائية. فحطام الأقمار الصناعية قد يعيق أنظمة الرصد الوقائي، بينما تنبعثات الصواريخ تؤثر على الغلاف الجوي الذي ينظم الاتصالات الوقائية.

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

الاعتبار التأثيرات الوقائية لهذه الأنشطة.

ويواجه القانون الدولي إشكالية جوهرية: هل يُعد التلوث الفضائي جزءاً من "المسؤولية الوقائية 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 الوقائية الرقمية يجب أن تمتد إلى الفضاء الخارجي، وأن الأنشطة الفضائية الوقائية يجب أن تخضع لمبدأ

"الوقاية الأمنية" مثلها مثل أي نشاط صناعي آخر.

**الفصل الثاني والثلاثون

العدالة الوقائية الرقمية والذكاء الاصطناعي التوليدي: عندما تصبح الأخبار الكاذبة سلاحاً وقائياً**

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 الوقائية الوطنية.

ففي عام 2025، تم تداول فيديوهات مزيفة لمواطنين وهم يحذرون من برامج وطنية آمنة، مما أدى إلى انخفاض الثقة في النظام الوقائي وانتشار المعلومات المضللة. وفي أزمات وقائية، تم نشر أخبار كاذبة عن نقص في المواد الوقائية الأساسية، مما أدى إلى ذعر شعبي وارتفاع غير مبرر في الأسعار.

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

- المحتوى المزيف لا يُصنّف كـ"هجوم سيبراني وقائي" 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 الوقائية.

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

ويخلص هذا الفصل إلى أن غياب تنظيم الذكاء

الاصطناعي التوليدي يحوّل الفضاء الرقمي إلى ساحة حرب نفسية وقائية، ويستدعي تعريفاً جديداً للتدخل السيبراني الوقائي يشمل "التأثير الخبيث عبر المحتوى المزيف".

**الفصل الثالث والثلاثون

العدالة الوقائية الرقمية والبيانات الضخمة الوقائية: حماية السيادة من الاستغلال الرقمي**

مع تزايد الاعتماد على البيانات الضخمة في تحليل السلوك المجتمعي، 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 وقائية 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 الوقائية.

- معظم العقود بين الدول والشركات تبقى سرية.

- لا توجد معايير لـ"السيادة الوقائية الرقمية".

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

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

**الفصل الرابع والثلاثون

العدالة الوقائية الرقمية والتعليم العالي الوقائي: نحو كليات وطنية للقانون الوقائي الرقمي**

لا يمكن بناء قدرات وقائية 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 الوقائي الرقمي يُعد استثماراً استراتيجياً في العدالة الوقائية الرقمية.

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

أما في الدول النامية، فإن التعليم الوقائي 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 الوقائي

الرقمي.

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

**الفصل الخامس والثلاثون

العدالة الوقائية الرقمية والثقافة الرقمية الوقائية: حماية الإبداع المحلي من القرصنة والتهميش

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

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

**الفصل السادس والثلاثون

العدالة الوقائية الرقمية والتمويل الرقمي الوقائي: حماية العملات الوقائية من التلاعب والاحتيال**

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

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

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

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

**الفصل السابع والثلاثون

العدالة الوقائية الرقمية والبحث العلمي الوقائي المفتوح: التوازن بين التعاون والحماية**

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

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

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

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

حمايته، دون عزلة علمية.

**الفصل الثامن والثلاثون

العدالة الوقائية الرقمية والتعاون الدولي: نحو نظام عالمي عادل للحوكمة الوقائية الرقمية**

لا يمكن لأي دولة أن تحمي عدالتها الوقائية 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 الوقاية الرقمية من قبل الدول الصناعية، دون مراعاة قدرات الدول النامية. وهذا يخلق نظاماً

غير عادل يكرس التبعية الوقائية الرقمية.

ويستدعي الحل:

- إنشاء منتدى دولي محايد لصياغة قواعد العدالة الوقائية الرقمية.

- توفير الدعم الفني والمالي للدول النامية.

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

**الفصل التاسع والثلاثون

العدالة الوقائية الرقمية والقانون الإنساني الدولي: حماية المدنيين في النزاعات الوقائية**

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

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

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

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

**الفصل الأربعون

العدالة الوقائية الرقمية والمستقبل: رؤية استراتيجية للعقود القادمة**

في الختام، لا يمكن النظر إلى العدالة الوقائية الرقمية كظاهرة مؤقتة، بل كتحول جوهري في مفهوم العدالة الجنائية في القرن الحادي والعشرين. فالدول التي تبني عدالتها الوقائية الرقمية اليوم ستكون قادرة على:

- حماية مواطنيها من التلاعب الوقائي الرقمي.

- بناء اقتصاد وقائي رقمي مستقل ومستدام.

- تعزيز مكانة أجيالها في النظام العدلي 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 الوقائية الرقمية ليس مسألة اختيار، بل مسألة بقاء.

خاتمة

بعد استعراض شامل لأبعاد العدالة الوقائية الرقمية في مختلف المجالات — من الأمن السيبراني إلى الاقتصاد، ومن الثقافة إلى التنمية — يتبين أن هذا المفهوم لم يعد رفاهية تقنية، بل ضمانة وجودية للدولة الحديثة. فالفضاء الوقائي الرقمي، رغم طبيعته غير المادية، بات ساحة للصراعات السياسية والاقتصادية، ولا يمكن لأي دولة أن تحافظ على عدالتها الوقائية 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 العدالة الوطنية والتعاون العالمي.

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

المراجع

United Nations Standard Minimum Rules for the Prevention of Crime (Nelson Mandela (Rules, 2015

Convention on the Rights of Persons (Deprived of Liberty (OAS, 1990

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 Reduce (Recidivism (2023

European Commission. Digital Justice (Action Plan (2024

Government of Estonia. Smart City (Initiative Report (2023

Government of Singapore. Digital (Prevention 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). Preventive Justice and Digital Sovereignty. Oxford University Press

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

Kloppenburg J R. (2024). Preventive Sovereignty and Digital Control. 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 Preventive Systems (Multiple (Jurisdictions, 2020–2025

:Academic Journals

Journal of Criminal Law and Criminology ((Northwestern

International Journal of Digital Preventive Justice

Harvard Law Review – Criminal Justice Section

Stanford Technology Law Review

فهرس المحتويات

الفراغ القانوني الجنائي الدولي في الحماية الوقائية الرقمية

الفصل الثالث

العدالة الوقائية التقليدية مقابل العدالة الوقائية الرقمية: إعادة تشكيل المفاهيم الجنائية

الفصل الرابع

البنية التحتية الوقائية الرقمية: تعريف قانوني جنائي مفقود

الفصل الخامس

التمييز الخوارزمي في البرامج الوقائية: نحو معيار قانوني جنائي دولي

الفصل السادس

المسؤولية الجنائية الدولية عن الفشل الوقائي الرقمي: تحديات الإسناد والرقابة

الفصل السابع

الردود المشروعة على الانتهاكات الوقائية الرقمية: بين التعويض والتدخل المبكر

الفصل الثامن

العدالة الوقائية الرقمية وبراءات الاختراع الجنائية:

الفصل الثاني عشر

العدالة الوقائية الرقمية والذكاء الاصطناعي الوقائي: عندما تصبح الخوارزميات مصلحة إنسانية

الفصل الثالث عشر

العدالة الوقائية الرقمية والجرائم الإلكترونية الوقائية: مكافحة الاحتيال الوقائي الرقمي

الفصل الرابع عشر

العدالة الوقائية الرقمية والتربية الرقمية الوقائية: بناء وعي مجتمعي كأساس للدفاع الإنساني

الفصل الخامس عشر

العدالة الوقائية الرقمية والبحث العلمي الوقائي: نحو استقلال تكنولوجي وطني

الفصل السادس عشر

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

الفصل السابع عشر

العدالة الوقائية الرقمية والمحاكمات الوقائية: نحو اختصاص قضائي رقمي

الفصل الثامن عشر

العدالة الوقائية الرقمية والبيانات الوقائية: بين الملكية الفردية والسيادة الجماعية

الفصل التاسع عشر

العدالة الوقائية الرقمية والوقاية المجتمعية: حماية المجتمعات من التكنولوجيا الوقائية غير المسؤولة

الفصل العشرون

العدالة الوقائية الرقمية والمستقبل: نحو مشروع اتفاقية دولية نموذجية

الفصل الحادي والعشرون

العدالة الوقائية الرقمية والمدن الرقمية: من المراقبة إلى الوقاية الذكية

الفصل الثاني والعشرون

العدالة الوقائية الرقمية والطاقة الوقائية: حماية الموارد من الاستنزاف الرقمي

الفصل الثالث والعشرون

العدالة الوقائية الرقمية وسلامة المواطنين: حماية المواطنين من التلاعب الرقمي

الفصل الرابع والعشرون

العدالة الوقائية الرقمية والتعليم الوقائي الرقمي: بناء وعي مجتمعي كأساس للدفاع عن الحقوق

الفصل الخامس والعشرون

العدالة الوقائية الرقمية والتراث الوقائي: حماية التراث من الاندثار الرقمي

الفصل السادس والعشرون

العدالة الوقائية الرقمية والتمويل الوقائي الرقمي: حماية الدول النامية من الديون الوقائية

الفصل السابع والعشرون

العدالة الوقائية الرقمية والنقل الوقائي الرقمي: حماية سلاسل التوريد من التهديدات السيبرانية

الفصل الثامن والعشرون

العدالة الوقائية الرقمية والبحث العلمي الوقائي المفتوح: التوازن بين التعاون والحماية

الفصل التاسع والعشرون

العدالة الوقائية الرقمية والتعاون الدولي: نحو نظام عالمي عادل للحوكمة الوقائية الرقمية

الفصل الثلاثون

العدالة الوقائية الرقمية والقانون الإنساني الدولي: حماية المدنيين في النزاعات الوقائية

الفصل الحادي والثلاثون

العدالة الوقائية الرقمية والفضاء الخارجي: حماية الأرض من التلوث الفضائي الوقائي

الفصل الثاني والثلاثون

العدالة الوقائية الرقمية والذكاء الاصطناعي التوليدي: عندما تصبح الأخبار الكاذبة سلاحاً وقائياً

الفصل الثالث والثلاثون

العدالة الوقائية الرقمية والبيانات الضخمة الوقائية: حماية السيادة من الاستغلال الرقمي

الفصل الرابع والثلاثون

العدالة الوقائية الرقمية والتعليم العالي الوقائي: نحو كليات وطنية للقانون الوقائي الرقمي

الفصل الخامس والثلاثون

العدالة الوقائية الرقمية والثقافة الرقمية الوقائية: حماية الإبداع المحلي من القرصنة والتهميش

الفصل السادس والثلاثون

العدالة الوقائية الرقمية والتمويل الرقمي الوقائي: حماية العملات الوقائية من التلاعب والاحتيال

الفصل السابع والثلاثون

العدالة الوقائية الرقمية والبحث العلمي الوقائي المفتوح: التوازن بين التعاون والحماية

الفصل الثامن والثلاثون

العدالة الوقائية الرقمية والتعاون الدولي: نحو نظام عالمي عادل للحوكمة الوقائية الرقمية

الفصل التاسع والثلاثون

العدالة الوقائية الرقمية والقانون الإنساني الدولي: حماية المدنيين في النزاعات الوقائية

الفصل الأربعون

العدالة الوقائية الرقمية والمستقبل: رؤية استراتيجية للعقود القادمة

خاتمة

تم بحمد الله وتوفيقه

تأليف د.محمد كمال عرفه الرخاوي

الباحث والمستشار القانوني

المحاضر الدولي في القانون