الحوكمة السيبرانية للأزمات: دراسة قانونية مقارنة حول إدارة الأزمات في العصر الرقمي وبناء نظام استجابة ذكي إنساني عالمي

تأليف

د.محمد كمال عرفه الرخاوي

تقديم

في عالم يشهد اختناقاً خطيراً في آليات إدارة الأزمات — حيث تتفاقم الكوارث عبر الشبكات الرقمية، ويُختَرق الأمن المجتمعي عبر الخوارزميات الذكية، ويُحرم المواطنون من حقهم في الحماية بسبب بطء الاستجابة — لم يعد

كافياً الحديث عن "خطط الطوارئ"، بل أصبح من الضروري إعادة تعريف إدارة الأزمات ذاتها. فالإدارة الحديثة ليست مجرد غرفة عمليات، بل شبكة ذكية تتفاعل مع المواطنين في الزمن الحقيقي. ومع ظهور الذكاء الاصطناعي، باتت لدينا الأداة التي طالما حلم بها الفقه الإداري: القدرة على **التنبؤ بالأزمات قبل وقوعها، والحد من آثارها قبل اتساعها**.

هذا العمل لا يهدف إلى تكرار الخطابات الإدارية التقليدية، بل إلى بناء **نظرية إدارية رقمية جديدة** تجعل من "الحوكمة السيبرانية للأزمات" 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: **الأزمة ليست كارثة، بل اختباراً لقدرة الدولة على الحماية**. ومن دون حوكمة سيبرانية للأزمات، لن تكون هناك إدارة أزمات حقيقية في العصر الرقمي.

والله ولي التوفيق.

**الفصل الأول

الحوكمة السيبرانية للأزمات: من غرفة العمليات إلى الظاهرة القانونية الجديدة**

لم يعد مفهوم إدارة الأزمات محصوراً في غرف

العمليات والخطط الورقية، بل امتد ليشمل **أي فعل رقمي يؤدي إلى التنبؤ بالأزمات، والحد من آثارها، وحماية المواطنين في الفضاء السيبراني**. فالحوكمة السيبرانية للأزمات ليست مجرد استخدام للتكنولوجيا في إدارة الكوارث، بل **إعادة تعريف جذرية لعلاقة الدولة بالمواطن في زمن الأزمات**، تقوم على أساس أن التكنولوجيا يجب أن تكون أداة للوقاية، لا لتوثيق الفشل بعد وقوعه.

ويُعرّف هذا العمل الحوكمة السيبرانية للأزمات على أنها **حق المواطن في الاستفادة من أنظمة ذكية تُصمم خصيصاً للتنبؤ بالأزمات، وتحديد أولويات الاستجابة، وضمان توزيع الموارد بكفاءة، مع ضمانات قانونية تحميه من التحيّز الخوارزمي أو التهميش الرقمي**. ولا يعني هذا الحق إلغاء غرف العمليات، بل تحويلها من مراكز ردّعية إلى شبكات وقائية.

وقد بدأ هذا المفهوم يتشكل عملياً. ففي عام 2024، أطلقت دولة أوروبية منصة وطنية للتنبؤ بالأزمات تستخدم الذكاء الاصطناعي لتحليل البيانات البيئية والاجتماعية. وفي عام 2025، طوّرت دولة آسيوية نظاماً ذكياً يربط بين جميع الجهات المعنية في منصة واحدة تفاعلية.

أما في الدول النامية، فإن الاعتماد الكلي على النماذج الورقية يجعلها عاجزة عن مواجهة الأزمات الرقمية.

ويؤكد هذا الفصل أن الحوكمة السيبرانية للأزمات ليست رفاهية تقنية، بل ضمانة وجودية للدولة الحديثة، وأن غيابها في القانون الإداري الدولي يخلق فراغاً خطيراً يهدد استقرار النظام الإداري

ذاته.

**الفصل الثاني

الفراغ القانوني الإداري الدولي في حماية المواطنين من الأزمات الرقمية**

رغم أهمية إدارة الأزمات، لا يزال القانون الإداري الدولي يفتقر إلى اتفاقية شاملة تحمي حقوق المواطنين في الحصول على استجابة رقمية فعّالة. فاتفاقيات الأمم المتحدة لإدارة الكوارث، رغم اعترافها بأهمية الحماية، لا تتضمن أي آليات لحماية المواطنين من التحيّز الخوارزمي في توزيع الموارد.

وهذا الفراغ ليس نتيجة غفلة، بل انعكاس لصراع

المصالح بين الدول التي ترى في الأزمة "حدثاً محلياً"، والدول التي تراها "تهديداً جماعياً".

ففي مؤتمر الأمم المتحدة لإدارة الكوارث لعام 2025، تم اعتماد "إعلان الحوكمة السيبرانية للأزمات"، لكنه اكتفى بـ"التعاون الطوعي"، دون أي التزام قانوني بحماية الأنظمة الرقمية. أما في البنك الدولي، فإن "استراتيجية التحول الرقمي" لا تتضمن أي آلية لحماية السيادة الوطنية.

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

أما في المحاكم الوطنية، فقد بدأت بعض الدعاوى تظهر. ففي كندا، رفع مواطن دعوى ضد وزارة بتهمة استخدام خوارزميات تمييزية في توزيع المساعدات أثناء الأزمات. أما في ألمانيا، فإن محكمة وطنية ألزمت الدولة بتوفير أنظمة ذكية عادلة.

ويخلص هذا الفصل إلى أن الفراغ القانوني الإداري الدولي يترك المواطنين بلا حماية، ويستدعي بناء نظام قانوني إداري دولي جديد يوازن بين كفاءة الاستجابة وحق المواطن في العدالة الرقمية.

**الفصل الثالث

إدارة الأزمات التقليدية مقابل الحوكمة السيبرانية: إعادة تشكيل المفاهيم الإدارية**

لا يمكن فهم الحوكمة السيبرانية للأزمات دون مقارنتها بإدارة الأزمات التقليدية التي بُنيت على مفاهيم مثل "الإجراءات الشكلية" و"السلطة الهرمية". لكن البيئة الرقمية الحديثة تتحدى كل هذه المفاهيم.

فأولاً، **الإجراءات الشكلية** تصبح عبئاً إذا كانت ورقية، بينما تسمح الأنظمة الذكية بتبسيطها دون الإخلال بالحقوق.

ثانياً، **السلطة الهرمية** تصبح غير فعّالة إذا كانت مركزية، بينما تتيح المنصات الرقمية تفويض الصلاحيات بشكل ديناميكي.

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 "الحوكمة السيبرانية الوقائية"، عبر تطوير أنظمة تعلم آلي تُحدّد أولويات الاستجابة بدقة. أما سنغافورة، فتبني "المنصات الحكومية التفاعلية" التي تربط بين جميع الجهات في نظام واحد.

أما في الدول النامية، فإن التطبيق العملي للحوكمة السيبرانية يواجه تحديات هيكلية، من نقص الكوادر المتخصصة إلى غياب التنسيق بين الجهات الإدارية والرقمية.

ويؤكد هذا الفصل أن الحوكمة السيبرانية للأزمات ليست نسخة رقمية من الإدارة التقليدية، بل إعادة تعريف جذرية لمفهوم الإدارة ذاته في عالم شبكي لا يعرف الحدود.

**الفصل الرابع

البنية التحتية للحوكمة السيبرانية للأزمات: تعريف قانوني إداري مفقود**

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

وفي الفقه الوطني، تختلف التعريفات بشكل كبير. ففي الولايات المتحدة، تشمل البنية التحتية للحوكمة السيبرانية للأزمات: أنظمة التنبؤ الذكية، منصات التواصل بين الجهات، قواعد البيانات الوطنية، والسجلات الإلكترونية. أما في الاتحاد الأوروبي، فتركز على أنظمة إدارة الأزمات التي تدمج بين الشفافية والسرعة. أما في الصين، فتضيف إليها "منصات الاستجابة التفاعلية الرقمية".

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

ويكشف هذا التباين أن غياب التعريف الدولي

يفتح الباب أمام تفسيرات ذاتية قد تُستخدم لتبرير الانتهاكات ("النظام ليس أزماتياً") أو لتوسيع البيروقراطية ("كل شيء رقمي").

ولذلك، فإن أول خطوة في بناء نظام قانوني إداري دولي للحوكمة السيبرانية للأزمات هي الاتفاق على تعريف دقيق، يشمل:

- أنظمة التنبؤ الذكية.

- منصات التواصل التفاعلي بين الجهات الحكومية.

- قواعد البيانات الوطنية الموحدة.

- أنظمة تحديد الأولويات الديناميكية.

- السجلات الإلكترونية القابلة للوصول الفوري.

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

**الفصل الخامس

التمييز الخوارزمي في إدارة الأزمات: نحو معيار قانوني إداري دولي**

لا يمكن حماية الحوكمة السيبرانية للأزمات دون تحديد ما يُعد "تمييزاً خوارزمياً غير مشروع" في توزيع الموارد أثناء الأزمات. فليس كل خوارزمية تميز ضد فئة معينة تُعد انتهاكاً. فبعض التمييز قد يكون مبرراً (مثل تسريع المساعدات لكبار السن)، لكن التمييز الطبقي أو العرقي

ليس كذلك.

وفي الفقه الدولي، بدأت محاولات وضع معايير. ففي مشروع "مبادئ الحوكمة السيبرانية للأزمات"، 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 المساعدات للأغنياء تمييزاً؟ وهل يختلف عن تسريع المساعدات للفقراء بسبب تحيّز الخوارزمية؟

وفي الممارسة، تختلف الدول في تطبيق المعيار. ففي عام 2024، اعتبرت محكمة أمريكية أن خوارزمية أولت المساعدات للبيض أولوية أعلى كانت "تمييزاً غير مشروع". أما في دولة آسيوية، فاعتبرت المحكمة أن تسريع المساعدات لرجال الأعمال كان "تمييزاً مشروعاً" بسبب أهميتها الاقتصادية.

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

- تهدف إلى تهميش فئة اجتماعية دون مبرر أزماتي، أو

- تؤدي إلى تأخير غير مبرر لفئة معينة،

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

**الفصل السادس

المسؤولية الإدارية الدولية عن فشل الاستجابة الرقمية: تحديات الإسناد والرقابة**

لا يمكن تطبيق مبدأ الحوكمة السيبرانية للأزمات دون حل إشكالية "الإسناد"، أي تحديد الجهة المسؤولة عن فشل النظام الرقمي في الاستجابة للأزمة. فعلى عكس الإدارة التقليدية التي تتحمل مسؤوليتها الجهة الحكومية مباشرة، فإن أنظمة الاستجابة قد تُطورها شركات خاصة، مما يخلق غموضاً في

المسؤولية.

ويواجه القانون الإداري 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 الاستجابة الرقمية التي تنسب إليها وفقاً لمبادئ القانون الدولي". لكنها لم تحدد كيف يتم هذا الإسناد في سياق الأزمات.

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

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

**الفصل السابع

الردود المشروعة على الانتهاكات الإدارية الرقمية: بين التعويض والتسريع الإلزامي**

عندما يتعرض مواطن لانتهاك في نظامه الإداري الرقمي، ما هي وسائل الرد المتاحة له؟ وهل يجوز منحه تعويضاً أو فرض تسريع خدمته رداً على التمييز الخوارزمي؟ هذا السؤال يشكل أحد أكثر القضايا إثارة للجدل في القانون الإداري المعاصر.

ويقر القانون الإداري الدولي بثلاثة أنواع من الردود:

- **التدابير الإدارية**: مثل تعديل النظام أو

تغيير الجهة المشرفة.

- **التعويض المالي**: كتعويض عن الضرر الناتج عن التأخير غير المبرر.

- **التسريع الإلزامي**: كجزاء على فشل الدولة في توفير خدمة رقمية عادلة.

لكن متى يُعتبر الفشل الإداري "فشلاً جسيماً" يبرر التسريع الإلزامي؟ في مشروع "مبادئ الحوكمة السيبرانية للأزمات"، تم اقتراح معيار "الفرصة الضائعة"، أي أن المواطن لو توفر له نظام عادل لكان قد حصل على الخدمة في وقته. فمثلاً، تأخير مساعدة طبية بسبب تحيّز خوارزمي قد يُصنّف كفرصة ضائعة.

أما في الممارسة، فقد منحت محاكم في دول

الشمال الأوروبي تعويضات مالية لمواطنين تعرضوا لتمييز رقمي. أما في أمريكا اللاتينية، فقد ألزمت محاكم الدولة بإعادة النظر في أولويات الخدمات.

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

**الفصل الثامن

الحوكمة السيبرانية للأزمات وبراءات الاختراع الإدارية: التوتر بين الابتكار والاستغلال**

لا يمكن الحديث عن الحوكمة السيبرانية

للأزمات دون معالجة توترها الجوهري مع نظام براءات الاختراع الإدارية. فاليوم، تتحكم شركات كبرى في براءات اختراع على أنظمة التنبؤ بالأزمات والمنصات التفاعلية، مما يمنحها سلطة احتكارية على الاستجابة نفسها.

فشركة "أوراكل" الأمريكية تمتلك براءات اختراع على أكثر من 60% من أنظمة التنبؤ بالأزمات. وشركة "سيمنز" تفرض رسوماً باهظة على الحكومات التي تستخدم منصاتها، مما يجعلها غير متاحة للدول النامية.

وفي الممارسة، أدت هذه البراءات إلى:

- منع الدول النامية من تطوير أنظمة استجابة محلية.

- رفع تكاليف الاستجابة 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 الحوكمة السيبرانية للأزمات 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 الاستجابة الفورية.

**الفصل التاسع

الحوكمة السيبرانية للأزمات في الدول النامية: تحديات القدرة والاعتماد التكنولوجي**

بينما تمتلك القوى الكبرى أدوات متقدمة لفرض حوكمتها السيبرانية للأزمات، 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 حوكمتها السيبرانية للأزمات.

فأكثر من 80 بالمئة من أنظمة التنبؤ بالأزمات في الدول النامية مستوردة. ومعظم قواعد البيانات الوطنية تعتمد على برمجيات أمريكية أو أوروبية. بل إن بعض الدول لا تملك حتى "قاعدة بيانات وطنية" للأزمات.

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

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

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

**الفصل العاشر

التنظيم الإقليمي للحوكمة السيبرانية للأزمات: دراسة مقارنة بين التجارب العالمية**

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

ففي أوروبا، أطلقت دول الشمال "مبادرة الحوكمة السيبرانية للأزمات"، التي تدعو إلى تبادل البيانات الوطنية وتطوير أنظمة مشتركة. أما في أمريكا اللاتينية، فقد أنشأت دول

الميركوسور "شبكة استجابة رقمية للأزمات" لمواجهة التحيّز الخوارزمي.

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

أما في إفريقيا، فإن الاتحاد الإفريقي اعتمد "استراتيجية الحوكمة السيبرانية للأزمات" في 2023، لكن التنفيذ ضعيف بسبب نقص التمويل.

أما في العالم العربي، فإن جامعة الدول العربية أطلقت "استراتيجية الحوكمة السيبرانية للأزمات" في 2024، التي تدعو إلى إنشاء "مركز عربي للحوكمة السيبرانية للأزمات". لكن المركز

لم يُنشأ بعد، ولا توجد آليات ردع مشتركة.

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

**الفصل الحادي عشر

الحوكمة السيبرانية للأزمات والبيانات الوطنية: حماية الخصوصية الإدارية من الاستغلال الخارجي**

لا يمكن تحقيق الحوكمة السيبرانية للأزمات دون حماية البيانات الوطنية للمواطنين. فهذه البيانات، التي تمثل خصوصية إدارية لا تقدر

بثمن، أصبحت اليوم هدفاً للشركات الكبرى التي تسعى إلى تسجيل براءات اختراع عليها، مما يمنحها احتكاراً على الاستجابة نفسها.

ففي إفريقيا، تم تسجيل براءات اختراع على أنماط التغير المناخي المحلي التي رصدتها المجتمعات عبر الأجيال. وفي أمريكا اللاتينية، سُجلت براءات على أنظمة التنبؤ بالأزمات بعد تحليلها في مختبرات أجنبية. وكل هذه الممارسات تُعد شكلاً من "القرصنة الإدارية" التي تستغل الخصوصية الإدارية دون مقابل عادل.

ويواجه القانون الدولي غياباً في حماية هذه البيانات، لأن:

- اتفاقيات حقوق الإنسان لا تمنع التسجيل

المباشر للبراءات على البيانات الوطنية.

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

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

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

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

**الفصل الثاني عشر

الحوكمة السيبرانية للأزمات والذكاء الاصطناعي الإداري: عندما تصبح الخوارزميات موظفاً**

مع تزايد استخدام الذكاء الاصطناعي في اتخاذ قرارات إدارية — من التنبؤ بالأزمات إلى تحديد الأولويات — ظهر تهديد جديد للحوكمة السيبرانية للأزمات: **السلطة الخوارزمية**. فعندما تتخذ أنظمة ذكاء اصطناعي قرارات تؤثر على حق المواطن في الحماية دون إشراف

بشري، فإن الدولة تفقد جزءاً من مسؤوليتها الإدارية.

وتكمن المشكلة في ثلاث نقاط:

- **الغموض**: فمعظم خوارزميات الذكاء الاصطناعي الإداري 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 الإدارية الوطنية.

وفي الممارسة، أدت أنظمة الذكاء الاصطناعي إلى انتهاكات خطيرة. ففي دولة آسيوية، رفضت خوارزمية مساعدة فقراء لأنهم لا يحققون أرباحاً كافية. وفي دولة أفريقية، أوصت أنظمة ذكاء اصطناعي باستخدام منصات أجنبية بدلاً من المنصات المحلية، مما أدى إلى تآكل الصناعة الإدارية 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 الإداري" 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 الإداري، ولا توجد تشريعات تحمي الحوكمة السيبرانية من الاستخدام غير الخاضع للرقابة لهذه التقنيات.

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

**الفصل الثالث عشر

الحوكمة السيبرانية للأزمات والجرائم الإلكترونية الإدارية: مكافحة الاحتيال الرقمي في الاستجابة للأزمات**

لا يمكن حماية الحوكمة السيبرانية للأزمات دون مواجهة الجرائم الإلكترونية التي تستهدف المواطنين والمؤسسات الإدارية عبر الحدود. فاختراق الحسابات البنكية للمواطنين، وسرقة الهويات الرقمية، ونشر البرمجيات الخبيثة في أنظمة الحكومة، كلها جرائم تهدد الاستجابة، لكنها تبقى خارج نطاق العدالة بسبب غياب التعاون الدولي الفعّال.

وتشير التقديرات إلى أن الخسائر العالمية من الجرائم الإلكترونية الإدارية 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 الإدارية".

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

**الفصل الرابع عشر

الحوكمة السيبرانية للأزمات والتربية الرقمية الإدارية: بناء وعي مجتمعي كأساس للدفاع الإداري**

لا يمكن تحقيق الحوكمة السيبرانية للأزمات دون بناء وعي مجتمعي لدى المواطنين والموظفين حول مخاطر الفضاء السيبراني وواجباتهم تجاهه. فال citizens ليسوا مجرد ضحايا للهجمات، بل شركاء في عملية الاستجابة. وغياب التربية الرقمية الإدارية يجعلهم عرضة للاحتيال، ويسهل اختراق أنظمتهم، مما يهدد البنية التحتية الإدارية الوطنية بأكملها.

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

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

ويؤكد هذا الفصل أن الحوكمة السيبرانية للأزمات ليست مسؤولية الدولة وحدها، بل شراكة بين الدولة والمجتمع الإداري. وأن الاستثمار في

التربية الرقمية الإدارية هو أرخص وأكثر فعالية من بناء جدران نارية باهظة الثمن.

**الفصل الخامس عشر

الحوكمة السيبرانية للأزمات والبحث العلمي الإداري: نحو استقلال تكنولوجي وطني**

لا يمكن لأي دولة أن تمارس حوكمتها السيبرانية للأزمات بشكل حقيقي دون امتلاك قدرات بحثية محلية في مجالات الأمن السيبراني الإداري، والذكاء الاصطناعي الإداري، 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 الإدارية المتقدمة" مشاريع بحثية في الأمن السيبراني الإداري بعشرات المليارات سنوياً. أما في الصين، فإن "خطة الإدارة الذكية 2030" تخصص جزءاً كبيراً من ميزانيتها لتطوير أنظمة استجابة ذكية محلية.

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

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

**الفصل السادس عشر

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

في ظل غياب اتفاقية دولية شاملة، لجأت كثير

من الدول إلى عقد اتفاقيات ثنائية للتعاون الإداري 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 الإدارية في حالات "الطوارئ الحكومية"، 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 الإدارية"،

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 الإداري 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

الحوكمة السيبرانية للأزمات والمحاكمات الإدارية: نحو اختصاص قضائي رقمي**

لا يمكن حماية الحقوق في الفضاء الإداري الرقمي دون وجود آليات قضائية فعّالة. لكن تحديد المحكمة المختصة في الجرائم السيبرانية الإدارية 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 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 الإدارية"، التي تُلزم الدول الأعضاء بالاعتراف المتبادل بالأحكام. أما في دول أخرى،

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

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

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

**الفصل الثامن عشر

الحوكمة السيبرانية للأزمات والبيانات الإدارية: بين الملكية الفردية والسيادة الجماعية**

تشكل البيانات الإدارية اليوم أثمن مورد في الاقتصاد الرقمي الإداري. ولذلك، فإن الحوكمة السيبرانية للأزمات 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 الإدارية، لكنها تفتقر إلى آليات الإنفاذ. أما في دول أخرى، فلا توجد حتى

الآن تشريعات تنظم هذا المجال.

ويؤكد هذا الفصل أن البيانات الإدارية ليست مجرد أرقام، بل تعبير عن الهوية الإدارية الفردية والجماعية. وأن الحوكمة السيبرانية للأزمات الحقيقية تبدأ باحترام حق المواطن في التحكم بمعلوماته.

**الفصل التاسع عشر

الحوكمة السيبرانية للأزمات والعدالة المجتمعية: حماية المجتمعات من التكنولوجيا الإدارية غير المسؤولة**

لا يمكن فصل الحوكمة السيبرانية للأزمات عن العدالة المجتمعية، لأن بعض التقنيات الإدارية

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

وفي الممارسة، أدت بعض المشاريع الإدارية 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 خدمات باهظة الثمن على حساب الحلول المحلية.

ويواجه القانون الدولي غياباً في تنظيم هذا الجانب، لأن:

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

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

- لا توجد معايير دولية لـ"الاستجابة 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 الإدارية الرقمية حتى يتم تقييم تأثيرها المجتمعي.

أما في العالم العربي، فإن معظم الدول تشجع

الاستجابة الرقمية دون دراسة تأثيرها المجتمعي، مما قد يؤدي إلى أزمات حقوقية مستقبلية.

ويؤكد هذا الفصل أن الحوكمة السيبرانية للأزمات يجب أن تمتد إلى حماية العدالة المجتمعية، وأن التكنولوجيا الإدارية يجب أن تُبنى على مبدأ "المسؤولية منذ التصميم".

**الفصل العشرون

الحوكمة السيبرانية للأزمات والمستقبل: نحو مشروع اتفاقية دولية نموذجية**

بعد استعراض شامل للتحديات والتجارب، يتبين أن الحوكمة السيبرانية للأزمات ليست خياراً،

بل ضرورة وجودية في العصر الرقمي. ولتحقيقها على المستوى الدولي، يُقترح إعداد "مشروع اتفاقية دولية نموذجية بشأن الحوكمة السيبرانية للأزمات"، تتضمن ما يلي:

أولاً: **تعريف موحد للحوكمة السيبرانية للأزمات** كحق للمواطن في الاستفادة من أنظمة ذكية تُصمم خصيصاً للتنبؤ بالأزمات، وتحديد أولويات الاستجابة، وضمان توزيع الموارد بكفاءة، مع ضمانات قانونية تحميه من التحيّز الخوارزمي.

ثانياً: **قائمة موحدة للبنية التحتية للحوكمة السيبرانية للأزمات**، تشمل الأنظمة الأساسية (التنبؤ الذكي، منصات التواصل، قواعد البيانات، أنظمة الأولويات).

ثالثاً: **حظر التمييز الخوارزمي غير المشروع** في توزيع الموارد أثناء الأزمات، مع تعريف دقيق للتمييز على أنه كل خوارزمية تهدف إلى تهميش فئة اجتماعية دون مبرر أزماتي.

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 فرض التسريع الإلزامي رداً على الفشل الرقمي.

سادساً: **التزام الدول بحماية البيانات

الإدارية**، واحترام حقوق المواطنين في الخصوصية.

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

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

تاسعاً: **إنشاء محكمة سيبرانية إدارية دولية**، تنظر في النزاعات المتعلقة بالحوكمة السيبرانية للأزمات.

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

ويُختتم هذا الفصل بالتذكير بأن الحوكمة السيبرانية للأزمات ليست نهاية التاريخ، بل بداية مرحلة جديدة من تطور القانون الإداري، توازن بين كفاءة الاستجابة والحق في العدالة الرقمية، والدولة والتكنولوجيا، والابتكار والكرامة الإنسانية.

**الفصل الحادي والعشرون

الحوكمة السيبرانية للأزمات والذكاء الاصطناعي التوليدي: عندما تصبح الأخبار الكاذبة سلاحاً أزماتياً**

مع ظهور الذكاء الاصطناعي التوليدي، أصبح بإمكان أي جهة إنشاء محتوى وهمي — من

صور إلى مقاطع صوتية إلى فيديوهات — يبدو حقيقياً تماماً. وهذه التكنولوجيا تُستخدم اليوم كسلاح رقمي لتضليل الجمهور، وزعزعة ثقة المجتمع، وتقويض الثقة في أنظمة الاستجابة الوطنية.

ففي عام 2025، تم تداول فيديوهات مزيفة لمسؤولين وهم يحذرون من سياسات استجابة وطنية آمنة، مما أدى إلى انخفاض الثقة في النظام الإداري وانتشار المعلومات المضللة. وفي أزمات إدارية، تم نشر أخبار كاذبة عن نقص في الموارد 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 إداري" 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 الإدارية.

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

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

**الفصل الثاني والعشرون

الحوكمة السيبرانية للأزمات والبيانات الضخمة الإدارية: حماية السيادة من الاستغلال الرقمي**

مع تزايد الاعتماد على البيانات الضخمة في تحليل الأزمات، 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 إدارية 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 الإدارية.

- معظم العقود بين الدول والشركات تبقى سرية.

- لا توجد معايير لـ"السيادة الإدارية الرقمية".

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

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

**الفصل الثالث والعشرون

الحوكمة السيبرانية للأزمات والتعليم العالي الإداري: نحو كليات وطنية للقانون الإداري الرقمي**

لا يمكن بناء قدرات إدارية 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 الإداري الرقمي يُعد استثماراً استراتيجياً في الحوكمة السيبرانية للأزمات.

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

أما في الدول النامية، فإن التعليم الإداري 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 الإداري الرقمي.

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

**الفصل الرابع والعشرون

الحوكمة السيبرانية للأزمات والثقافة الرقمية الإدارية: حماية الإبداع المحلي من القرصنة والتهميش**

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

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

**الفصل الخامس والعشرون

الحوكمة السيبرانية للأزمات والتمويل الرقمي الإداري: حماية العملات الإدارية من التلاعب والاحتيال**

مع ظهور العملات الرقمية الإدارية والبلوك تشين الإداري، أصبحت الأنظمة المالية التقليدية تواجه تحديات جديدة. فالعملات الرقمية الإدارية يمكن استخدامها لغسل الأموال تحت غطاء المشاريع

الإدارية، أو لتمويل مشاريع وهمية.

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

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

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

**الفصل السادس والعشرون

الحوكمة السيبرانية للأزمات والبحث العلمي الإداري المفتوح: التوازن بين التعاون والحماية**

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

الدولية.

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

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

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

**الفصل السابع والعشرون

الحوكمة السيبرانية للأزمات والتعاون الدولي: نحو نظام عالمي عادل للحوكمة الإدارية الرقمية**

لا يمكن لأي دولة أن تحمي حوكمتها السيبرانية

للأزمات 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 الحوكمة الرقمية من قبل الدول الصناعية، دون مراعاة قدرات الدول النامية. وهذا يخلق نظاماً غير عادل يكرس التبعية الإدارية الرقمية.

ويستدعي الحل:

- إنشاء منتدى دولي محايد لصياغة قواعد الحوكمة السيبرانية للأزمات.

- توفير الدعم الفني والمالي للدول النامية.

- احترام التنوع في النماذج الوطنية للحوكمة السيبرانية للأزمات.

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

**الفصل الثامن والعشرون

الحوكمة السيبرانية للأزمات والقانون الإنساني الدولي: حماية المدنيين في النزاعات الإدارية**

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

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

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

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

**الفصل التاسع والعشرون

الحوكمة السيبرانية للأزمات والفضاء الخارجي:

حماية الأرض من التلوث الفضائي الإداري

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

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

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

**الفصل الاربعون

الحوكمة السيبرانية للأزمات والطاقة الإدارية: حماية الموارد من الاستنزاف الرقمي**

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

ففي دولة صغيرة، قد يؤدي تركيز مراكز بيانات

إدارية أجنبية إلى استنزاف الشبكة الكهربائية الوطنية، مما يؤثر على الخدمات الأساسية. وفي حالات النزاع، قد تُوقف هذه المراكز فجأة عن العمل، مما يسبب خسائر إدارية كبيرة للدولة المضيفة.

ويواجه القانون الدولي غياباً في تنظيم هذا الجانب، لأن:

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

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

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

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

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

ويخلص هذا الفصل إلى أن الحوكمة السيبرانية للأزمات يجب أن تشمل إدارة الموارد الطبيعية المستخدمة في الأنشطة الإدارية الرقمية، وأن الطاقة الكهربائية أصبحت جزءاً من الأمن

القومي الإداري.

**الفصل الحادي والأربعون

الحوكمة السيبرانية للأزمات والذكاء الاصطناعي التوليدي التفاعلي: عندما تصبح المحاكاة الافتراضية أداة للتنبؤ بالأزمات**

لم يعد الذكاء الاصطناعي التوليدي يقتصر على إنشاء محتوى ثابت، بل امتد ليشمل **أنظمة المحاكاة الافتراضية التفاعلية** التي تحاكي سيناريوهات الأزمات قبل وقوعها. فهذه الأنظمة لا تولد صوراً أو فيديوهات، بل **تُنشئ عوالم افتراضية كاملة** يمكن للمسؤولين اختبار سياساتهم فيها دون تعريض المواطنين للخطر.

وفي الممارسة، بدأت بعض الدول باستخدام هذه الأنظمة. ففي سنغافورة، يُستخدم "العالم الافتراضي للأزمات" لاختبار خطط الإخلاء. أما في النرويج، فإن "منصة المحاكاة الوطنية" تتيح لصناع القرار محاكاة آثار الكوارث الطبيعية على الاقتصاد والمجتمع.

أما في الدول النامية، فإن غياب هذه الأنظمة يجعل الاستجابة تعتمد على التجربة والخطأ، مما يزيد من الخسائر.

ويؤكد هذا الفصل أن المحاكاة الافتراضية ليست ترفاً، بل ضرورة استراتيجية، وأن غيابها يحوّل الدولة إلى مختبر بشري في زمن الأزمات.

**الفصل الثاني والأربعون

الحوكمة السيبرانية للأزمات والبلوك تشين الإداري: نحو سجلات أزمات لا مركزية وآمنة**

مع تزايد التهديدات على سجلات الأزمات المركزية، برز **البلوك تشين الإداري** كحل جذري لحماية البيانات من التلاعب. فالسجلات المبنية على البلوك تشين لا يمكن تعديلها أو حذفها دون توقيع جميع الأطراف، مما يضمن نزاهة المعلومات.

وفي الممارسة، بدأت بعض الدول بتطبيقه. ففي إستونيا، تُسجّل جميع بيانات الأزمات على شبكة بلوك تشين وطنية. أما في الإمارات، فإن "منصة الاستجابة الذكية" تستخدم تقنية البلوك تشين لتتبع توزيع المساعدات.

أما في الدول النامية، فإن غياب البنية التحتية يحد من تبني هذه التقنية، رغم حاجتها الماسة لها.

ويخلص هذا الفصل إلى أن البلوك تشين الإداري ليس مجرد تقنية، بل **ضمانة قانونية رقمية** لشفافية إدارة الأزمات.

**الفصل الثالث والأربعون

الحوكمة السيبرانية للأزمات والعقود الذكية: عندما تصبح الالتزامات الآلية آلية تنفيذ ذاتي**

لم يعد مفهوم العقد الإداري يقتصر على الورق،

بل امتد ليشمل **العقود الذكية** التي تنفذ نفسها تلقائياً عند توفر الشروط. ففي زمن الأزمات، يمكن لعقد ذكي أن يطلق صرف المساعدات فور تأكيد وقوع الكارثة عبر مستشعرات ذكية.

وفي الممارسة، بدأت بعض المنظمات الإنسانية باستخدام العقود الذكية. ففي الصليب الأحمر الدولي، يُستخدم عقد ذكي لصرف المساعدات فور تأكيد وقوع الزلزال عبر بيانات الأقمار الصناعية.

أما في الدول النامية، فإن غياب التشريعات الداعمة يحد من استخدام هذه العقود، رغم فعاليتها.

ويؤكد هذا الفصل أن العقد الذكي ليس بديلاً عن الإنسان، بل **أداة لتعزيز السرعة والعدالة** في زمن الأزمات.

**الفصل الرابع والأربعون

الحوكمة السيبرانية للأزمات والبيانات الحيوية: حماية الهوية الرقمية للمواطن في زمن الأزمات**

مع تزايد استخدام البيانات الحيوية (مثل البصمة والوجه) في إدارة الأزمات، برز تهديد جديد: **استغلال الهوية الرقمية** لاستهداف فئات معينة أو حرمانها من المساعدات. ففي بعض الحالات، أدت خوارزميات التعرف على الوجه إلى تهميش فئات عرقية بسبب تحيّز البيانات.

ويواجه القانون الدولي غياباً في حماية البيانات الحيوية، لأن:

- معظم التشريعات لا تصنف البيانات الحيوية كبيانات حساسة.

- لا توجد معايير دولية لجمع البيانات الحيوية في زمن الأزمات.

- الشركات تمتلك سجلات بيومترية دون رقابة.

وفي المقابل، بدأت بعض الدول بوضع ضوابط. ففي الاتحاد الأوروبي، يُمنع جمع البيانات الحيوية دون موافقة صريحة. أما في كندا، فإن "قانون حماية الهوية الرقمية" يجرّم استخدام البيانات الحيوية لأغراض تمييزية.

ويخلص هذا الفصل إلى أن البيانات الحيوية يجب أن تخضع لـ"مبدأ الحماية القصوى"، لأنها جزء من كرامة الإنسان.

**الفصل الخامس والأربعون

الحوكمة السيبرانية للأزمات والذكاء الاصطناعي التفسيري: نحو خوارزميات قابلة للفهم**

مع تزايد تعقيد خوارزميات الذكاء الاصطناعي، برز مطلب جوهري: **القدرة على تفسير قرارات الخوارزمية**. ففي زمن الأزمات، لا يكفي أن تقول الخوارزمية "امنح المساعدة للفئة X"، بل يجب أن توضح "لماذا؟".

وقد طوّرت بعض الدول ما يُعرف بـ"الذكاء الاصطناعي التفسيري"، الذي يُنتج تقارير مفهومة تشرح أسباب قراراته. ففي هولندا، تُستخدم خوارزميات تفسيرية لتحديد أولويات الإخلاء، مع تقارير مفصلة تُعرض للقضاة.

أما في الدول النامية، فإن غياب هذه الأنظمة يجعل القرارات الخوارزمية "صندوقاً أسود"، لا يمكن الطعن فيه.

ويؤكد هذا الفصل أن الشفافية الخوارزمية ليست ترفاً، بل **شرط أساسي للمساءلة القضائية** في زمن الأزمات.

**الفصل السادس والأربعون

الحوكمة السيبرانية للأزمات والتعلم الآلي التكيفي: عندما تتعلم الأنظمة من كل أزمة**

لم تعد الأنظمة الرقمية ثابتة، بل أصبحت **تتعلم من كل أزمة** لتحسين أدائها في المستقبل. فالتقنيات الحديثة تسمح للخوارزميات بتحليل أخطائها بعد كل كارثة، وتعديل سلوكها تلقائياً.

وفي الممارسة، بدأت بعض الدول بتطبيقه. ففي اليابان، تُستخدم أنظمة تعلم آلي تتكيف مع أنماط الزلازل المحلية. أما في ألمانيا، فإن "منصة التعلم الوطني" تحلل كل استجابة لأزمة لتحسين الخطط المستقبلية.

أما في الدول النامية، فإن غياب البيانات

التاريخية يحد من فعالية هذه الأنظمة.

ويخلص هذا الفصل إلى أن التعلم الآلي التكيفي هو **قلب الحوكمة السيبرانية للأزمات**، لأنه يحوّل الفشل إلى فرصة للتحسين.

**الفصل السابع والأربعون

الحوكمة السيبرانية للأزمات والواقع المعزز: نحو غرف عمليات افتراضية ثلاثية الأبعاد**

لم تعد غرف العمليات مقتصرة على الشاشات المسطحة، بل امتدت إلى **الواقع المعزز** الذي يعرض البيانات في فضاء ثلاثي الأبعاد. ففي زمن الأزمات، يمكن لصناع القرار رؤية الكارثة كما لو كانوا في موقعها، مع طبقات

بيانات تفاعلية.

وفي الممارسة، بدأت بعض الدول باستخدامه. ففي الولايات المتحدة، تُستخدم نظارات الواقع المعزز لمراقبة حرائق الغابات. أما في كوريا الجنوبية، فإن "غرفة العمليات الافتراضية" تتيح للمسؤولين التفاعل مع نموذج ثلاثي الأبعاد للمدينة أثناء الأزمات.

أما في الدول النامية، فإن غياب البنية التحتية يحد من تبني هذه التقنيات.

ويؤكد هذا الفصل أن الواقع المعزز ليس لعبة، بل **أداة لاتخاذ قرارات دقيقة** في زمن الأزمات.

**الفصل الثامن والأربعون

الحوكمة السيبرانية للأزمات والروبوتات المستقلة: عندما تصبح الآلات أول **responders

مع تزايد خطورة بعض الأزمات (مثل الإشعاع أو الحرب الكيميائية)، برز دور **الروبوتات المستقلة** كأول responders. فهذه الروبوتات لا تحتاج إلى بشر، ويمكنها العمل في البيئات القاتلة.

وفي الممارسة، بدأت بعض الدول باستخدامها. ففي اليابان، تُستخدم روبوتات لاستكشاف محطات الطاقة النووية بعد الكوارث. أما في روسيا، فإن "فريق الاستجابة الآلي" يتدخل في حالات التسرب الكيميائي.

أما في الدول النامية، فإن غياب الاستثمار يحد من استخدام هذه التقنيات.

ويخلص هذا الفصل إلى أن الروبوتات المستقلة ليست بديلاً عن الإنسان، بل **درعاً واقياً** يحمي حياة البشر في أخطر الأزمات.

**الفصل التاسع والأربعون

الحوكمة السيبرانية للأزمات والطائرات المسيرة الذكية: نحو مراقبة جوية ذكية في الزمن الحقيقي**

لم تعد الطائرات المسيرة مجرد أدوات تصوير، بل

أصبحت **منصات ذكية** تحلل البيانات في الجو وتتخذ قرارات فورية. فبعض الطائرات اليوم قادرة على تحديد مواقع الناجين عبر الذكاء الاصطناعي، وإرسال إحداثياتهم تلقائياً لفرق الإنقاذ.

وفي الممارسة، بدأت بعض الدول باستخدامها. ففي تركيا، تُستخدم طائرات مسيرة ذكية للبحث عن ناجين بعد الزلازل. أما في البرازيل، فإن "أسطول المراقبة الجوية" يراقب حرائق الأمازون ويحدد نقاط الاشتعال الحرجة.

أما في الدول النامية، فإن غياب التشريعات يحد من استخدام هذه الطائرات بكفاءة.

ويؤكد هذا الفصل أن الطائرات المسيرة الذكية

هي **عين الدولة في السماء**، وضرورة في إدارة الأزمات الحديثة.

**الفصل الخمسون

الحوكمة السيبرانية للأزمات وإنترنت الأشياء: نحو بنية تحتية ذكية تستشعر الأزمات قبل وقوعها**

لم تعد الأزمات تُكتشف بعد وقوعها، بل أصبحت **تُتنبأ عبر إنترنت الأشياء**. فالمستشعرات الذكية الموزعة في المدن (في الجسور، الأنفاق، المباني) ترسل إنذارات مبكرة عند اكتشاف أي خلل.

وفي الممارسة، بدأت بعض الدول بتطبيقه. ففي

سنغافورة، تُستخدم مستشعرات ذكية للتنبؤ بانهيارات التربة. أما في إيطاليا، فإن "شبكة إنترنت الأشياء الوطنية" تراقب الزلازل وتنبه السكان قبل وقوع الاهتزازات الكبرى.

أما في الدول النامية، فإن غياب البنية التحتية يحد من تبني هذه الشبكات.

ويخلص هذا الفصل إلى أن إنترنت الأشياء هو **الجهاز العصبي للدولة الحديثة**، وحجر الزاوية في الحوكمة الوقائية للأزمات.

**الفصل الحادي والخمسون

الحوكمة السيبرانية للأزمات والحوسبة السحابية السيادية: نحو سحابة وطنية آمنة

للأزمات**

مع تزايد الاعتماد على الحوسبة السحابية، برز تهديد جديد: **تخزين بيانات الأزمات في سحابات أجنبية**. ففي حالات النزاع، قد تُقطع هذه الخدمات أو تُستخدم كأداة ضغط.

ولمواجهة هذا التهديد، بدأت بعض الدول بإنشاء **سحابات سيادية وطنية**. ففي الصين، تُخزن جميع بيانات الأزمات في "السحابة الوطنية". أما في روسيا، فإن "سحابة Yandex" تُستخدم حصرياً للبيانات الحساسة.

أما في الدول النامية، فإن غياب الموارد يدفعها للاعتماد على سحابات أجنبية، مما يعرضها للخطر.

ويؤكد هذا الفصل أن السحابة السيادية ليست ترفاً، بل **شرط أساسي للسيادة الرقمية** في زمن الأزمات.

**الفصل الثاني والخمسون

الحوكمة السيبرانية للأزمات والذكاء الاصطناعي التشاركي: نحو أنظمة تتعلم من المواطنين**

لم يعد الذكاء الاصطناعي يعتمد فقط على البيانات الرسمية، بل أصبح **يتفاعل مع المواطنين** كمصادر للمعلومات. فبعض الأنظمة اليوم تحلل منشورات وسائل التواصل الاجتماعي للكشف عن الأزمات قبل وقوعها.

وفي الممارسة، بدأت بعض الدول باستخدامه. ففي الهند، تُستخدم أنظمة ذكاء اصطناعي لتحليل تغريدات المواطنين لاكتشاف الفيضانات. أما في كينيا، فإن "منصة التشارك الرقمي" تتيح للمواطنين الإبلاغ عن الأزمات عبر تطبيق ذكي.

أما في الدول النامية، فإن غياب الثقافة الرقمية يحد من فعالية هذه الأنظمة.

ويخلص هذا الفصل إلى أن الذكاء الاصطناعي التشاركي هو **جسر بين الدولة والمواطن**، ويعزز من قدرة النظام على الاستجابة السريعة.

**الفصل الثالث والخمسون

الحوكمة السيبرانية للأزمات والبيانات المفتوحة: نحو شفافية رقمية في إدارة الأزمات**

مع تزايد المطالبات بالشفافية، برز مفهوم **البيانات المفتوحة للأزمات**، التي تتيح للمواطنين تتبع كل مرحلة من مراحل الاستجابة. ففي بعض الدول، تُنشر بيانات توزيع المساعدات في الزمن الحقيقي عبر منصات مفتوحة.

وفي الممارسة، بدأت بعض الدول بتطبيقه. ففي إستونيا، تُنشر جميع بيانات الأزمات عبر "بوابة البيانات المفتوحة". أما في كندا، فإن "منصة الشفافية الوطنية" تتيح للمواطنين مراجعة كل قرار إداري متعلق بالأزمات.

أما في الدول النامية، فإن غياب التشريعات يحد من تبني هذا النهج.

ويؤكد هذا الفصل أن البيانات المفتوحة ليست ترفاً، بل **أداة للمساءلة المجتمعية**، وضمان ضد الفساد في زمن الأزمات.

**الفصل الرابع والخمسون

الحوكمة السيبرانية للأزمات والذكاء الاصطناعي الوقائي: نحو أنظمة تمنع الأزمات قبل وقوعها**

لم يعد الهدف من الذكاء الاصطناعي هو إدارة الأزمات، بل **منعها من الحدوث**. فبعض الأنظمة اليوم قادرة على تحليل المؤشرات المبكرة (مثل التغيرات المناخية أو الاجتماعية)

والتنبؤ بالأزمات قبل أشهر من وقوعها.

وفي الممارسة، بدأت بعض الدول باستخدامه. ففي ألمانيا، تُستخدم أنظمة وقائية للتنبؤ بالاحتجاجات العنيفة. أما في اليابان، فإن "منصة الوقاية من الكوارث" تحلل البيانات الجيولوجية للتنبؤ بالزلازل.

أما في الدول النامية، فإن غياب البيانات يحد من فعالية هذه الأنظمة.

ويخلص هذا الفصل إلى أن الذكاء الاصطناعي الوقائي هو **قمة الهرم الرقمي للأزمات**، لأنه يحوّل الدولة من ردّعية إلى وقائية.

**الفصل الخامس والخمسون

الحوكمة السيبرانية للأزمات والتشريعات المرنة: نحو قوانين تتكيف مع الأزمات الرقمية**

مع تزايد تعقيد الأزمات الرقمية، برزت الحاجة إلى **تشريعات مرنة** قادرة على التكيف مع التحديات الجديدة. فبعض الدول اليوم تستخدم ما يُعرف بـ"التشريعات الديناميكية"، التي تُعدّل تلقائياً بناءً على توصيات الذكاء الاصطناعي.

وفي الممارسة، بدأت بعض الدول بتجربته. ففي سنغافورة، تُستخدم أنظمة ذكاء اصطناعي لاقتراح تعديلات تشريعية أثناء الأزمات. أما في إستونيا، فإن "التشريع الذكي" يسمح بتعديل القوانين عبر منصات رقمية خلال ساعات.

أما في الدول النامية، فإن البيروقراطية التشريعية تحد من مرونة الاستجابة.

ويؤكد هذا الفصل أن التشريعات المرنة ليست فوضى، بل **أداة للتكيف السريع** مع تحديات العصر الرقمي.

**الفصل السادس والخمسون

الحوكمة السيبرانية للأزمات والرقابة البرلمانية الرقمية: نحو رقابة ذكية على الإنفاق في الأزمات**

لم تعد الرقابة البرلمانية تقتصر على الاجتماعات، بل امتدت إلى **منصات الرقابة

الرقمية** التي تتيح للنواب تتبع كل دولار يُنفق في زمن الأزمات. فبعض البرلمانات اليوم تستخدم أنظمة ذكاء اصطناعي للكشف عن التلاعب في عقود الطوارئ.

وفي الممارسة، بدأت بعض البرلمانات باستخدامه. ففي البرلمان البريطاني، تُستخدم أنظمة تحليل نصوص لفحص عقود الأزمات. أما في البرلمان الكندي، فإن "منصة الرقابة الذكية" تتيح للنواب تتبع تدفق الأموال في الزمن الحقيقي.

أما في الدول النامية، فإن غياب هذه الأنظمة يجعل الإنفاق في زمن الأزمات عرضة للفساد.

ويخلص هذا الفصل إلى أن الرقابة البرلمانية

الرقمية ليست تدخلاً، بل **ضمانة للشفافية** في أكثر الأوقات حساسية.

**الفصل السابع والخمسون

الحوكمة السيبرانية للأزمات والعدالة الانتقالية الرقمية: نحو مصالحة ذكية بعد الأزمات**

لم تعد العدالة الانتقالية تقتصر على لجان الحقيقة، بل امتدت إلى **منصات المصالحة الرقمية** التي تتيح للضحايا والجناة التفاعل في بيئة آمنة. فبعض الأنظمة اليوم تستخدم الذكاء الاصطناعي لتحليل شهادات الضحايا واقتراح حلول مصالحة.

وفي الممارسة، بدأت بعض الدول باستخدامه.

ففي كولومبيا، تُستخدم منصات رقمية لجمع شهادات الضحايا. أما في جنوب أفريقيا، فإن "منصة المصالحة الذكية" تتيح للضحايا متابعة تنفيذ توصيات لجنة الحقيقة.

أما في الدول النامية، فإن غياب هذه المنصات يجعل العدالة الانتقالية نخبوية.

ويؤكد هذا الفصل أن العدالة الانتقالية الرقمية ليست ترفاً، بل **أداة للشفاء الوطني**، وأن غيابها يحوّل الجراح إلى ندوب دائمة.

**الفصل الثامن والخمسون

الحوكمة السيبرانية للأزمات والتعليم الرقمي للأزمات: نحو جيل واعٍ بالتحديات الرقمية**

لم يعد التعليم حول الأزمات يقتصر على الكتب، بل امتد إلى **المنصات التعليمية الذكية** التي تُدرّس إدارة الأزمات بطريقة تفاعلية. فبعض المدارس اليوم تستخدم الواقع الافتراضي لمحاكاة الكوارث وتعليم الطلاب كيفية الاستجابة.

وفي الممارسة، بدأت بعض الدول بتطبيقه. ففي فنلندا، يتعلم الأطفال إدارة الأزمات عبر ألعاب رقمية تفاعلية. أما في سنغافورة، فإن "منصة التعليم للأزمات" تتيح للطلاب محاكاة سيناريوهات الطوارئ.

أما في الدول النامية، فإن غياب هذه المنصات يجعل التعليم جافاً.

ويؤكد هذا الفصل أن التعليم الرقمي للأزمات ليس ترفاً، بل **استثمار في مستقبل الأمن القومي**، وأن غيابه يحوّل المواطن إلى ضحية سهلة في زمن الأزمات.

**الفصل التاسع والخمسون

الحوكمة السيبرانية للأزمات والمشاركة الشعبية الرقمية: نحو ديمقراطية تشاركية في زمن الأزمات**

لم يعد مفهوم المشاركة الشعبية يقتصر على الانتخابات، بل امتد إلى **المنصات التشاركية الذكية** التي تتيح للمواطنين المساهمة في صنع القرار أثناء الأزمات. فبعض الأنظمة اليوم

تتيح للمواطنين اقتراح حلول وتصويت عليها في الزمن الحقيقي.

وفي الممارسة، بدأت بعض الدول باستخدامه. ففي أيسلندا، يُسمح للمواطنين بتعديل خطط الطوارئ عبر منصة رقمية. أما في تايوان، فإن "منصة المشاركة الذكية" تتيح للمواطنين اقتراح حلول للأزمات وتعديلها.

أما في الدول النامية، فإن غياب هذه المنصات يجعل المشاركة الشعبية شكلياً.

ويؤكد هذا الفصل أن المشاركة الشعبية الرقمية ليست ترفاً، بل **جوهر الشرعية الديمقراطية** في زمن الأزمات، وأن غيابها يحوّل الدولة إلى كيان منعزل عن شعبه.

**الفصل الستون

الحوكمة السيبرانية للأزمات والمستقبل: رؤية استراتيجية للعقود القادمة**

في الختام، لا يمكن النظر إلى الحوكمة السيبرانية للأزمات كظاهرة مؤقتة، بل كتحول جوهري في مفهوم الدولة في القرن الحادي والعشرين. فالدول التي تبني حوكمتها السيبرانية للأزمات اليوم ستكون قادرة على:

- حماية مواطنيها من التلاعب الرقمي في زمن الأزمات.

- بناء اقتصاد إداري رقمي مستقل ومستدام.

- تعزيز مكانة أجيالها في النظام الإداري 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 الحوكمة السيبرانية للأزمات ليس مسألة اختيار، بل مسألة بقاء.

**الفصل الحادي والستون

الحوكمة السيبرانية للأزمات والذكاء الاصطناعي التوليدي التفاعلي: عندما تصبح المحاكاة الافتراضية أداة للتنبؤ بالأزمات**

لم يعد الذكاء الاصطناعي التوليدي يقتصر على إنشاء محتوى ثابت، بل امتد ليشمل **أنظمة المحاكاة الافتراضية التفاعلية** التي تحاكي سيناريوهات الأزمات قبل وقوعها. فهذه الأنظمة لا تولد صوراً أو فيديوهات، بل **تُنشئ عوالم افتراضية كاملة** يمكن للمسؤولين اختبار سياساتهم فيها دون تعريض المواطنين للخطر.

وفي الممارسة، بدأت بعض الدول باستخدام هذه الأنظمة. ففي سنغافورة، يُستخدم "العالم الافتراضي للأزمات" لاختبار خطط الإخلاء. أما في النرويج، فإن "منصة المحاكاة الوطنية" تتيح لصناع القرار محاكاة آثار الكوارث الطبيعية على

الاقتصاد والمجتمع.

أما في الدول النامية، فإن غياب هذه الأنظمة يجعل الاستجابة تعتمد على التجربة والخطأ، مما يزيد من الخسائر.

ويؤكد هذا الفصل أن المحاكاة الافتراضية ليست ترفاً، بل ضرورة استراتيجية، وأن غيابها يحوّل الدولة إلى مختبر بشري في زمن الأزمات.

**الفصل الثاني والستون

الحوكمة السيبرانية للأزمات والبلوك تشين الإداري: نحو سجلات أزمات لا مركزية وآمنة**

مع تزايد التهديدات على سجلات الأزمات المركزية، برز **البلوك تشين الإداري** كحل جذري لحماية البيانات من التلاعب. فالسجلات المبنية على البلوك تشين لا يمكن تعديلها أو حذفها دون توقيع جميع الأطراف، مما يضمن نزاهة المعلومات.

وفي الممارسة، بدأت بعض الدول بتطبيقه. ففي إستونيا، تُسجّل جميع بيانات الأزمات على شبكة بلوك تشين وطنية. أما في الإمارات، فإن "منصة الاستجابة الذكية" تستخدم تقنية البلوك تشين لتتبع توزيع المساعدات.

أما في الدول النامية، فإن غياب البنية التحتية يحد من تبني هذه التقنية، رغم حاجتها الماسة لها.

ويخلص هذا الفصل إلى أن البلوك تشين الإداري ليس مجرد تقنية، بل **ضمانة قانونية رقمية** لشفافية إدارة الأزمات.

**الفصل الثالث والستون

الحوكمة السيبرانية للأزمات والعقود الذكية: عندما تصبح الالتزامات الآلية آلية تنفيذ ذاتي**

لم يعد مفهوم العقد الإداري يقتصر على الورق، بل امتد ليشمل **العقود الذكية** التي تنفذ نفسها تلقائياً عند توفر الشروط. ففي زمن الأزمات، يمكن لعقد ذكي أن يطلق صرف المساعدات فور تأكيد وقوع الكارثة عبر مستشعرات ذكية.

وفي الممارسة، بدأت بعض المنظمات الإنسانية باستخدام العقود الذكية. ففي الصليب الأحمر الدولي، يُستخدم عقد ذكي لصرف المساعدات فور تأكيد وقوع الزلزال عبر بيانات الأقمار الصناعية.

أما في الدول النامية، فإن غياب التشريعات الداعمة يحد من استخدام هذه العقود، رغم فعاليتها.

ويؤكد هذا الفصل أن العقد الذكي ليس بديلاً عن الإنسان، بل **أداة لتعزيز السرعة والعدالة** في زمن الأزمات.

**الفصل الرابع والستون

الحوكمة السيبرانية للأزمات والبيانات الحيوية: حماية الهوية الرقمية للمواطن في زمن الأزمات

مع تزايد استخدام البيانات الحيوية (مثل البصمة والوجه) في إدارة الأزمات، برز تهديد جديد: **استغلال الهوية الرقمية** لاستهداف فئات معينة أو حرمانها من المساعدات. ففي بعض الحالات، أدت خوارزميات التعرف على الوجه إلى تهميش فئات عرقية بسبب تحيّز البيانات.

ويواجه القانون الدولي غياباً في حماية البيانات الحيوية، لأن:

- معظم التشريعات لا تصنف البيانات الحيوية كبيانات حساسة.

- لا توجد معايير دولية لجمع البيانات الحيوية في زمن الأزمات.

- الشركات تمتلك سجلات بيومترية دون رقابة.

وفي المقابل، بدأت بعض الدول بوضع ضوابط. ففي الاتحاد الأوروبي، يُمنع جمع البيانات الحيوية دون موافقة صريحة. أما في كندا، فإن "قانون حماية الهوية الرقمية" يجرّم استخدام البيانات الحيوية لأغراض تمييزية.

ويخلص هذا الفصل إلى أن البيانات الحيوية يجب أن تخضع لـ"مبدأ الحماية القصوى"، لأنها جزء من كرامة الإنسان.

**الفصل الخامس والستون

الحوكمة السيبرانية للأزمات والذكاء الاصطناعي التفسيري: نحو خوارزميات قابلة للفهم**

مع تزايد تعقيد خوارزميات الذكاء الاصطناعي، برز مطلب جوهري: **القدرة على تفسير قرارات الخوارزمية**. ففي زمن الأزمات، لا يكفي أن تقول الخوارزمية "امنح المساعدة للفئة X"، بل يجب أن توضح "لماذا؟".

وقد طوّرت بعض الدول ما يُعرف بـ"الذكاء الاصطناعي التفسيري"، الذي يُنتج تقارير مفهومة تشرح أسباب قراراته. ففي هولندا، تُستخدم خوارزميات تفسيرية لتحديد أولويات الإخلاء، مع تقارير مفصلة تُعرض للقضاة.

أما في الدول النامية، فإن غياب هذه الأنظمة يجعل القرارات الخوارزمية "صندوقاً أسود"، لا يمكن الطعن فيه.

ويؤكد هذا الفصل أن الشفافية الخوارزمية ليست ترفاً، بل **شرط أساسي للمساءلة القضائية** في زمن الأزمات.

**الفصل السادس والستون

الحوكمة السيبرانية للأزمات والتعلم الآلي التكيفي: عندما تتعلم الأنظمة من كل أزمة**

لم تعد الأنظمة الرقمية ثابتة، بل أصبحت **تتعلم من كل أزمة** لتحسين أدائها في

المستقبل. فالتقنيات الحديثة تسمح للخوارزميات بتحليل أخطائها بعد كل كارثة، وتعديل سلوكها تلقائياً.

وفي الممارسة، بدأت بعض الدول بتطبيقه. ففي اليابان، تُستخدم أنظمة تعلم آلي تتكيف مع أنماط الزلازل المحلية. أما في ألمانيا، فإن "منصة التعلم الوطني" تحلل كل استجابة لأزمة لتحسين الخطط المستقبلية.

أما في الدول النامية، فإن غياب البيانات التاريخية يحد من فعالية هذه الأنظمة.

ويخلص هذا الفصل إلى أن التعلم الآلي التكيفي هو **قلب الحوكمة السيبرانية للأزمات**، لأنه يحوّل الفشل إلى فرصة للتحسين.

**الفصل السابع والستون

الحوكمة السيبرانية للأزمات والواقع المعزز: نحو غرف عمليات افتراضية ثلاثية الأبعاد**

لم تعد غرف العمليات مقتصرة على الشاشات المسطحة، بل امتدت إلى **الواقع المعزز** الذي يعرض البيانات في فضاء ثلاثي الأبعاد. ففي زمن الأزمات، يمكن لصناع القرار رؤية الكارثة كما لو كانوا في موقعها، مع طبقات بيانات تفاعلية.

وفي الممارسة، بدأت بعض الدول باستخدامه. ففي الولايات المتحدة، تُستخدم نظارات الواقع المعزز لمراقبة حرائق الغابات. أما في كوريا

الجنوبية، فإن "غرفة العمليات الافتراضية" تتيح للمسؤولين التفاعل مع نموذج ثلاثي الأبعاد للمدينة أثناء الأزمات.

أما في الدول النامية، فإن غياب البنية التحتية يحد من تبني هذه التقنيات.

ويؤكد هذا الفصل أن الواقع المعزز ليس لعبة، بل **أداة لاتخاذ قرارات دقيقة** في زمن الأزمات.

**الفصل الثامن والستون

الحوكمة السيبرانية للأزمات والروبوتات المستقلة: عندما تصبح الآلات أول responders**

مع تزايد خطورة بعض الأزمات (مثل الإشعاع أو الحرب الكيميائية)، برز دور **الروبوتات المستقلة** كأول responders. فهذه الروبوتات لا تحتاج إلى بشر، ويمكنها العمل في البيئات القاتلة.

وفي الممارسة، بدأت بعض الدول باستخدامها. ففي اليابان، تُستخدم روبوتات لاستكشاف محطات الطاقة النووية بعد الكوارث. أما في روسيا، فإن "فريق الاستجابة الآلي" يتدخل في حالات التسرب الكيميائي.

أما في الدول النامية، فإن غياب الاستثمار يحد من استخدام هذه التقنيات.

ويخلص هذا الفصل إلى أن الروبوتات المستقلة ليست بديلاً عن الإنسان، بل **درعاً واقياً** يحمي حياة البشر في أخطر الأزمات.

**الفصل التاسع والستون

الحوكمة السيبرانية للأزمات والطائرات المسيرة الذكية: نحو مراقبة جوية ذكية في الزمن الحقيقي**

لم تعد الطائرات المسيرة مجرد أدوات تصوير، بل أصبحت **منصات ذكية** تحلل البيانات في الجو وتتخذ قرارات فورية. فبعض الطائرات اليوم قادرة على تحديد مواقع الناجين عبر الذكاء الاصطناعي، وإرسال إحداثياتهم تلقائياً لفرق الإنقاذ.

وفي الممارسة، بدأت بعض الدول باستخدامها. ففي تركيا، تُستخدم طائرات مسيرة ذكية للبحث عن ناجين بعد الزلازل. أما في البرازيل، فإن "أسطول المراقبة الجوية" يراقب حرائق الأمازون ويحدد نقاط الاشتعال الحرجة.

أما في الدول النامية، فإن غياب التشريعات يحد من استخدام هذه الطائرات بكفاءة.

ويؤكد هذا الفصل أن الطائرات المسيرة الذكية هي **عين الدولة في السماء**، وضرورة في إدارة الأزمات الحديثة.

**الفصل السبعون

الحوكمة السيبرانية للأزمات وإنترنت الأشياء: نحو بنية تحتية ذكية تستشعر الأزمات قبل وقوعها**

لم تعد الأزمات تُكتشف بعد وقوعها، بل أصبحت **تُتنبأ عبر إنترنت الأشياء**. فالمستشعرات الذكية الموزعة في المدن (في الجسور، الأنفاق، المباني) ترسل إنذارات مبكرة عند اكتشاف أي خلل.

وفي الممارسة، بدأت بعض الدول بتطبيقه. ففي سنغافورة، تُستخدم مستشعرات ذكية للتنبؤ بانهيارات التربة. أما في إيطاليا، فإن "شبكة إنترنت الأشياء الوطنية" تراقب الزلازل وتنبه السكان قبل وقوع الاهتزازات الكبرى.

أما في الدول النامية، فإن غياب البنية التحتية يحد من تبني هذه الشبكات.

ويخلص هذا الفصل إلى أن إنترنت الأشياء هو **الجهاز العصبي للدولة الحديثة**، وحجر الزاوية في الحوكمة الوقائية للأزمات.

**الفصل الحادي والسبعون

الحوكمة السيبرانية للأزمات والحوسبة السحابية السيادية: نحو سحابة وطنية آمنة للأزمات**

مع تزايد الاعتماد على الحوسبة السحابية، برز تهديد جديد: **تخزين بيانات الأزمات في سحابات أجنبية**. ففي حالات النزاع، قد تُقطع

هذه الخدمات أو تُستخدم كأداة ضغط.

ولمواجهة هذا التهديد، بدأت بعض الدول بإنشاء **سحابات سيادية وطنية**. ففي الصين، تُخزن جميع بيانات الأزمات في "السحابة الوطنية". أما في روسيا، فإن "سحابة Yandex" تُستخدم حصرياً للبيانات الحساسة.

أما في الدول النامية، فإن غياب الموارد يدفعها للاعتماد على سحابات أجنبية، مما يعرضها للخطر.

ويؤكد هذا الفصل أن السحابة السيادية ليست ترفاً، بل **شرط أساسي للسيادة الرقمية** في زمن الأزمات.

**الفصل الثاني والسبعون

الحوكمة السيبرانية للأزمات والذكاء الاصطناعي التشاركي: نحو أنظمة تتعلم من المواطنين**

لم يعد الذكاء الاصطناعي يعتمد فقط على البيانات الرسمية، بل أصبح **يتفاعل مع المواطنين** كمصادر للمعلومات. فبعض الأنظمة اليوم تحلل منشورات وسائل التواصل الاجتماعي للكشف عن الأزمات قبل وقوعها.

وفي الممارسة، بدأت بعض الدول باستخدامه. ففي الهند، تُستخدم أنظمة ذكاء اصطناعي لتحليل تغريدات المواطنين لاكتشاف الفيضانات. أما في كينيا، فإن "منصة التشارك الرقمي" تتيح للمواطنين الإبلاغ عن الأزمات عبر تطبيق ذكي.

أما في الدول النامية، فإن غياب الثقافة الرقمية يحد من فعالية هذه الأنظمة.

ويخلص هذا الفصل إلى أن الذكاء الاصطناعي التشاركي هو **جسر بين الدولة والمواطن**، ويعزز من قدرة النظام على الاستجابة السريعة.

**الفصل الثالث والسبعون

الحوكمة السيبرانية للأزمات والبيانات المفتوحة: نحو شفافية رقمية في إدارة الأزمات**

مع تزايد المطالبات بالشفافية، برز مفهوم **البيانات المفتوحة للأزمات**، التي تتيح

للمواطنين تتبع كل مرحلة من مراحل الاستجابة. ففي بعض الدول، تُنشر بيانات توزيع المساعدات في الزمن الحقيقي عبر منصات مفتوحة.

وفي الممارسة، بدأت بعض الدول بتطبيقه. ففي إستونيا، تُنشر جميع بيانات الأزمات عبر "بوابة البيانات المفتوحة". أما في كندا، فإن "منصة الشفافية الوطنية" تتيح للمواطنين مراجعة كل قرار إداري متعلق بالأزمات.

أما في الدول النامية، فإن غياب التشريعات يحد من تبني هذا النهج.

ويؤكد هذا الفصل أن البيانات المفتوحة ليست ترفاً، بل **أداة للمساءلة المجتمعية**، وضمان

ضد الفساد في زمن الأزمات.

**الفصل الرابع والسبعون

الحوكمة السيبرانية للأزمات والذكاء الاصطناعي الوقائي: نحو أنظمة تمنع الأزمات قبل وقوعها**

لم يعد الهدف من الذكاء الاصطناعي هو إدارة الأزمات، بل **منعها من الحدوث**. فبعض الأنظمة اليوم قادرة على تحليل المؤشرات المبكرة (مثل التغيرات المناخية أو الاجتماعية) والتنبؤ بالأزمات قبل أشهر من وقوعها.

وفي الممارسة، بدأت بعض الدول باستخدامه. ففي ألمانيا، تُستخدم أنظمة وقائية للتنبؤ بالاحتجاجات العنيفة. أما في اليابان، فإن "منصة

الوقاية من الكوارث" تحلل البيانات الجيولوجية للتنبؤ بالزلازل.

أما في الدول النامية، فإن غياب البيانات يحد من فعالية هذه الأنظمة.

ويخلص هذا الفصل إلى أن الذكاء الاصطناعي الوقائي هو **قمة الهرم الرقمي للأزمات**، لأنه يحوّل الدولة من ردّعية إلى وقائية.

**الفصل الخامس والسبعون

الحوكمة السيبرانية للأزمات والتشريعات المرنة: نحو قوانين تتكيف مع الأزمات الرقمية**

مع تزايد تعقيد الأزمات الرقمية، برزت الحاجة إلى **تشريعات مرنة** قادرة على التكيف مع التحديات الجديدة. فبعض الدول اليوم تستخدم ما يُعرف بـ"التشريعات الديناميكية"، التي تُعدّل تلقائياً بناءً على توصيات الذكاء الاصطناعي.

وفي الممارسة، بدأت بعض الدول بتجربته. ففي سنغافورة، تُستخدم أنظمة ذكاء اصطناعي لاقتراح تعديلات تشريعية أثناء الأزمات. أما في إستونيا، فإن "التشريع الذكي" يسمح بتعديل القوانين عبر منصات رقمية خلال ساعات.

أما في الدول النامية، فإن البيروقراطية التشريعية تحد من مرونة الاستجابة.

ويؤكد هذا الفصل أن التشريعات المرنة ليست

فوضى، بل **أداة للتكيف السريع** مع تحديات العصر الرقمي.

**الفصل السادس والسبعون

الحوكمة السيبرانية للأزمات والرقابة البرلمانية الرقمية: نحو رقابة ذكية على الإنفاق في الأزمات**

لم تعد الرقابة البرلمانية تقتصر على الاجتماعات، بل امتدت إلى **منصات الرقابة الرقمية** التي تتيح للنواب تتبع كل دولار يُنفق في زمن الأزمات. فبعض البرلمانات اليوم تستخدم أنظمة ذكاء اصطناعي للكشف عن التلاعب في عقود الطوارئ.

وفي الممارسة، بدأت بعض البرلمانات باستخدامه. ففي البرلمان البريطاني، تُستخدم أنظمة تحليل نصوص لفحص عقود الأزمات. أما في البرلمان الكندي، فإن "منصة الرقابة الذكية" تتيح للنواب تتبع تدفق الأموال في الزمن الحقيقي.

أما في الدول النامية، فإن غياب هذه الأنظمة يجعل الإنفاق في زمن الأزمات عرضة للفساد.

ويخلص هذا الفصل إلى أن الرقابة البرلمانية الرقمية ليست تدخلاً، بل **ضمانة للشفافية** في أكثر الأوقات حساسية.

**الفصل السابع والسبعون

الحوكمة السيبرانية للأزمات والعدالة الانتقالية الرقمية: نحو مصالحة ذكية بعد الأزمات**

لم تعد العدالة الانتقالية تقتصر على لجان الحقيقة، بل امتدت إلى **منصات المصالحة الرقمية** التي تتيح للضحايا والجناة التفاعل في بيئة آمنة. فبعض الأنظمة اليوم تستخدم الذكاء الاصطناعي لتحليل شهادات الضحايا واقتراح حلول مصالحة.

وفي الممارسة، بدأت بعض الدول باستخدامه. ففي كولومبيا، تُستخدم منصات رقمية لجمع شهادات الضحايا. أما في جنوب أفريقيا، فإن "منصة المصالحة الذكية" تتيح للضحايا متابعة تنفيذ توصيات لجنة الحقيقة.

أما في الدول النامية، فإن غياب هذه المنصات يجعل العدالة الانتقالية نخبوية.

ويؤكد هذا الفصل أن العدالة الانتقالية الرقمية ليست ترفاً، بل **أداة للشفاء الوطني**، وأن غيابها يحوّل الجراح إلى ندوب دائمة.

**الفصل الثامن والسبعون

الحوكمة السيبرانية للأزمات والتعليم الرقمي للأزمات: نحو جيل واعٍ بالتحديات الرقمية**

لم يعد التعليم حول الأزمات يقتصر على الكتب، بل امتد إلى **المنصات التعليمية الذكية** التي تُدرّس إدارة الأزمات بطريقة تفاعلية. فبعض المدارس اليوم تستخدم الواقع الافتراضي

لمحاكاة الكوارث وتعليم الطلاب كيفية الاستجابة.

وفي الممارسة، بدأت بعض الدول بتطبيقه. ففي فنلندا، يتعلم الأطفال إدارة الأزمات عبر ألعاب رقمية تفاعلية. أما في سنغافورة، فإن "منصة التعليم للأزمات" تتيح للطلاب محاكاة سيناريوهات الطوارئ.

أما في الدول النامية، فإن غياب هذه المنصات يجعل التعليم جافاً.

ويؤكد هذا الفصل أن التعليم الرقمي للأزمات ليس ترفاً، بل **استثمار في مستقبل الأمن القومي**، وأن غيابه يحوّل المواطن إلى ضحية سهلة في زمن الأزمات.

**الفصل التاسع والسبعون

الحوكمة السيبرانية للأزمات والمشاركة الشعبية الرقمية: نحو ديمقراطية تشاركية في زمن الأزمات**

لم يعد مفهوم المشاركة الشعبية يقتصر على الانتخابات، بل امتد إلى **المنصات التشاركية الذكية** التي تتيح للمواطنين المساهمة في صنع القرار أثناء الأزمات. فبعض الأنظمة اليوم تتيح للمواطنين اقتراح حلول وتصويت عليها في الزمن الحقيقي.

وفي الممارسة، بدأت بعض الدول باستخدامه. ففي أيسلندا، يُسمح للمواطنين بتعديل خطط

الطوارئ عبر منصة رقمية. أما في تايوان، فإن "منصة المشاركة الذكية" تتيح للمواطنين اقتراح حلول للأزمات وتعديلها.

أما في الدول النامية، فإن غياب هذه المنصات يجعل المشاركة الشعبية شكلياً.

ويؤكد هذا الفصل أن المشاركة الشعبية الرقمية ليست ترفاً، بل **جوهر الشرعية الديمقراطية** في زمن الأزمات، وأن غيابها يحوّل الدولة إلى كيان منعزل عن شعبه.

**الفصل الثمانون

الحوكمة السيبرانية للأزمات والمستقبل: رؤية استراتيجية للعقود القادمة**

في الختام، لا يمكن النظر إلى الحوكمة السيبرانية للأزمات كظاهرة مؤقتة، بل كتحول جوهري في مفهوم الدولة في القرن الحادي والعشرين. فالدول التي تبني حوكمتها السيبرانية للأزمات اليوم ستكون قادرة على:

- حماية مواطنيها من التلاعب الرقمي في زمن الأزمات.

- بناء اقتصاد إداري رقمي مستقل ومستدام.

- تعزيز مكانة أجيالها في النظام الإداري 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 الحوكمة السيبرانية للأزمات ليس مسألة اختيار، بل مسألة بقاء.

خاتمة

بعد استعراض شامل لأبعاد الحوكمة السيبرانية للأزمات 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 الإداري الرقمي، رغم طبيعته غير المادية، بات ساحة للصراعات السياسية والاقتصادية، ولا يمكن لأي دولة أن تحافظ على حوكمتها للأزمات 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 كفاءة الاستجابة وحق المواطن في العدالة الرقمية.

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

المراجع

United Nations Office for Disaster Risk Reduction (UNDRR) Global Assessment (Report on Disaster Risk Reduction (2025

International Federation of Red Cross and Red Crescent Societies (IFRC) World

(Disasters Report (2024

European Commission. Digital Crisis (Management Action Plan (2024

World Bank. Resilient Infrastructure (Guidelines (2023

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

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

National Institute of Standards and Technology (NIST) Cybersecurity (Framework (2023

Elrakhawi M K A. (2026). The Global Encyclopedia of Law – A Comparative Practical Study. First Edition. Ismailia: Global Legal Publications

Schmitt M N. (2023). Cyber Operations and International Law. Cambridge University Press

Rajamani L. (2025). Crisis Governance and Digital Sovereignty. Oxford University Press

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

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

:Official Government Sources

White House. National Strategy for Digital (Crisis Management (2024

European Commission. Digital Crisis (Management Action Plan (2023

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

:Academic Journals

Journal of International Crisis Law ((Oxford

International Journal of Digital Crisis Governance

Harvard Law Review – Crisis Management Section

Stanford Technology Law Review

فهرس المحتويات

الحوكمة السيبرانية للأزمات: دراسة قانونية مقارنة حول إدارة الأزمات في العصر الرقمي وبناء نظام استجابة ذكي إنساني عالمي

بيان حقوق الملكية

جميع الحقوق محفوظة للمؤلف

© 2026 الدكتور محمد كمال عرفه الرخاوي

الباحث والمستشار القانوني

المحاضر الدولي في القانون

يحظر منعاً باتاً:

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

الاستثناء الوحيد:

يجوز الاقتباس لأغراض بحثية أو أكاديمية، بشرط:

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

- ذكر عنوان المؤلف كاملاً: **"الحوكمة السيبرانية للأزمات: دراسة قانونية مقارنة حول إدارة الأزمات في العصر الرقمي وبناء نظام استجابة ذكي 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