السيادة الرقمية للدولة: دراسة في حدود السلطة العامة في الفضاء الإلكتروني

تأليف

د. محمد كمال عرفه الرخاوي

الاهداء

الي روح والدي امي وابي غفر الله لهم ورحمهما وادخلهم الجنه بدون حساب يارب العالمين

واهدي هذا العمل لابنتي الحبيبه صبرينال قره عيني المصريه الجزائريه جميله الجميلات التي

تجمع بين جمال نهر النيل الخالد وشط المتوسط وجبال الاوراس

التمهيد

في عصرٍ لم تعد فيه الحدود الجغرافية كافية لتعريف الدولة، ظهرت **السيادة الرقمية** كمفهوم قانوني جديد يهدد – ويُعيد تعريف – مفاهيم السلطة، والاختصاص، والسيادة التقليدية. فبينما كانت الدولة تمارس سلطتها على الأرض، والماء، والسماء، فإنها اليوم تواجه تحدياً وجودياً في **الفضاء الإلكتروني**، حيث تتنافس مع شركات تكنولوجيا عملاقة، ومنظمات غير حكومية، بل وحتى مع أفراد يتمتعون بقدرات تقنية تفوق أجهزة الدولة نفسها.

هذا الكتاب ليس مجرد دراسة في القانون السيبراني، بل هو **محاولة نظرية لتأسيس فرع جديد من القانون العام**، يُعنى بتنظيم العلاقة بين الدولة والفضاء الرقمي، ويحدد حدود مشروعية تدخل السلطة العامة في هذا المجال، دون أن تفرّط في حماية الأمن القومي، أو تنتهك الحقوق الأساسية للمواطنين.

ولقد استندت في هذا البحث إلى **منهج تحليلي مقارن**، يدمج بين النظرية الدستورية، والفقه الإداري، وقانون الجرائم الإلكترونية، وحقوق الإنسان الرقمية، مع الاستعانة بأحدث القضايا القضائية من أمريكا، أوروبا، والعالم العربي.

الفصل الأول: الإطار النظري للسيادة الرقمية

المبحث الأول: تطور مفهوم السيادة من الحدود الجغرافية إلى الفضاء الإلكتروني

نشأت فكرة السيادة في الفكر الغربي الحديث مع جان بودان في القرن السادس عشر، كحق حصري للدولة في سن القوانين داخل إقليمها. ثم تطورت مع مونتسكيو وروسو لتُصبح مرتبطة بإرادة الشعب. لكن جميع هذه التعاريف افترضت أن **الإقليم هو الحيز الطبيعي لممارسة السيادة**.

اليوم، ومع ظهور الإنترنت، لم يعد الإقليم كافياً.

فموقع إلكتروني قد يكون مقرّه في كاليفورنيا، ويخزن بياناته في سنغافورة، ويُستخدم من قبل مواطن في بيروت. فعلى من تُطبّق القوانين؟ ومن يملك حق المراقبة؟

هنا، يبرز مفهوم **السيادة الوظيفية**، الذي لا يربط السيادة بالمكان، بل بالقدرة على التأثير والتنظيم. فالدولة التي تستطيع حماية مواطنيها من الاختراقات الرقمية، وضمان خصوصيتهم، وفرض قوانينها على المنصات العاملة في سوقها، هي دولة ذات سيادة رقمية حقيقية.

المبحث الثاني: الفضاء الإلكتروني كفضاء جديد للسلطة العامة

يُخطئ من يظن أن الفضاء الإلكتروني "منطقة

حرة" خارج نطاق القانون. فرغم غياب الحدود المادية، إلا أن هذا الفضاء يخضع لثلاثة أنواع من السلطة:

1. **سلطة الدولة**: عبر التشريعات والمراقبة.

2. **سلطة الشركات**: عبر شروط الاستخدام والخوارزميات.

3. **سلطة المجتمع**: عبر الثقافة الرقمية والسلوك الجماعي.

والتحدي الحقيقي أمام الدولة هو **استعادة توازن القوة** مع الشركات، التي باتت تمتلك سلطة تشريعية وتنفيذية وقضائية فعلية في الفضاء الرقمي.

المبحث الثالث: خصائص السيادة الرقمية

تتميز السيادة الرقمية بثلاث خصائص جوهرية:

- **اللامادية**: فهي لا تعتمد على الأرض، بل على البيانات والشبكات.

- **العالمية**: لأن تأثير القرار الرقمي لا يتوقف عند الحدود.

- **الديناميكية**: لأن التكنولوجيا تتطور أسرع من التشريع.

ومن هنا، فإن القوانين التقليدية – البطيئة، المحلية، والثابتة – عاجزة عن مواجهة تحديات هذا الفضاء الجديد.

الفصل الثاني: الأسس الدستورية للسيادة الرقمية

المبحث الأول: السيادة الرقمية كامتداد للسيادة الوطنية

في معظم الدساتير العربية، تنص المادة الأولى على أن "سيادة الدولة مطلقة". لكن هذه السيادة كانت تُفهم ضمناً على أنها سيادة

إقليمية. ولذلك، يدعو هذا الكتاب إلى **تعديل دستوري صريح** يُضيف عبارة:

> "وتمارس الدولة سيادتها على الفضاء الرقمي المرتبط بمصالحها الحيوية."

فبدون هذا الأساس الدستوري، تبقى القرارات الإدارية في المجال الرقمي عرضة للطعن بعدم الدستورية.

المبحث الثاني: العلاقة بين السيادة الرقمية وحقوق الإنسان

لا يمكن فصل السيادة الرقمية عن حقوق الإنسان. فالمادة 18 من الإعلان العالمي لحقوق الإنسان تكفل الحق في الخصوصية، والمادة 19

تكفل حرية التعبير. ومن هنا، فإن أي تدخل رقمي من الدولة يجب أن يخضع لثلاثة ضوابط دستورية:

1. **القانونية**: أن يكون مبنياً على نص تشريعي واضح.

2. **الضرورة**: أن يكون ضرورياً في مجتمع ديمقراطي.

3. **التناسب**: أن لا يتجاوز الحد الضروري لتحقيق الغاية.

وقد أكدت المحكمة الأوروبية لحقوق الإنسان في قضية *Big Brother Watch ضد المملكة المتحدة* (2018) أن المراقبة الجماعية دون ضوابط تُعد انتهاكاً صريحاً للحق في الخصوصية.

المبحث الثالث: دور القضاء الدستوري في رقابة التدخل الرقمي

بات من الضروري أن يلعب القضاء الدستوري دوراً فعالاً في مراجعة مشروعية القوانين الرقمية. ففي مصر، ألغت المحكمة الدستورية العليا قانوناً يُجرّم نشر "أخبار كاذبة" على الإنترنت، لكونه يفتقر إلى التحديد الكافي، ويهدد حرية الرأي. وفي تونس، ألغى المجلس الدستوري قراراً يُلزم شركات الاتصالات بتسليم بيانات المستخدمين دون إذن قضائي.

وهذه السوابق القضائية تؤكد أن **السيادة الرقمية لا تعني الاستبداد الرقمي**.

الفصل الثالث: الإطار التشريعي للسيادة الرقمية

المبحث الأول: نماذج التشريعات الرقمية في العالم

تختلف الدول في نهجها التشريعي:

- **النموذج الأمريكي**: يعتمد على "القطاعية"، حيث لكل قطاع (صحة، مالية، اتصالات) قانونه الخاص.

- **النموذج الأوروبي**: يعتمد على "الشمولية"، كما في اللائحة العامة لحماية البيانات (GDPR).

- **النموذج الصيني**: يعتمد على "الأمن القومي"، حيث تُعطى الدولة سلطة مطلقة على البيانات.

والسؤال الذي يطرحه هذا الكتاب: **أي هذه النماذج أنسب للدول العربية؟**

المبحث الثاني: تحليل التشريعات العربية في المجال الرقمي

رغم وجود قوانين لمكافحة الجرائم الإلكترونية في معظم الدول العربية، إلا أنها تعاني من ثلاث

عيوب جوهرية:

1. **العمومية**: حيث تستخدم عبارات فضفاضة مثل "النيل من هيبة الدولة".

2. **العقابية**: حيث تركّز على العقوبات أكثر من الوقاية والتنظيم.

3. **الانفرادية**: حيث تفتقر إلى التنسيق الإقليمي.

ولذلك، فإن هذه التشريعات، بدلاً من أن تعزز السيادة الرقمية، تُضعفها بسبب عدم فعاليتها وعدم توافقها مع المعايير الدولية.

**المبحث الثالث: نحو قانون عربي

نموذجي للسيادة الرقمية

يقترح هذا الكتاب مشروع قانون عربي نموذجي يتألف من أربعة محاور:

1. **حماية البنية التحتية الحيوية** من الهجمات السيبرانية.

2. **تنظيم تدفق البيانات العابرة للحدود**.

3. **ضمان حقوق المواطنين الرقمية** (الخصوصية، النسيان، الوصول).

4. **إنشاء هيئة عربية مستقلة** للإشراف على التنفيذ.

الفصل الرابع: السيادة الرقمية والأمن القومي

المبحث الأول: الفضاء الإلكتروني كميدان جديد للحرب

لم تعد الحروب تُدار بالدبابات والطائرات فحسب، بل بالخوارزميات والفيروسات. فقد أثبتت هجمات "ستاكسنت" على المنشآت النووية الإيرانية، وهجمات "نوتبيديا" على أوكرانيا، أن **الفضاء الإلكتروني أصبح ساحة حرب استراتيجية**. ومن هنا، فإن السيادة الرقمية لم تعد مسألة تنظيمية، بل **مسألة بقاء**.

ويُعرّف الأمن القومي الرقمي بأنه:

> "قدرة الدولة على حماية بنيتها التحتية الحيوية – من شبكات الكهرباء، إلى أنظمة البنوك، إلى قواعد البيانات الحكومية – من أي اختراق أو تلاعب قد يهدد استقرارها أو سيادتها."

المبحث الثاني: حدود مشروعية الدفاع السيبراني

تواجه الدول معضلة قانونية: هل يجوز لها شن هجوم سيبراني وقائي ضد خوادم معادية؟

القانون الدولي التقليدي يسمح بالدفاع عن النفس ضد "الهجوم المسلح". لكن هل يُعد

الهجوم السيبراني "هجوماً مسلحاً"؟

تذهب محكمة العدل الدولية في رأيها الاستشاري حول الجرائم الإلكترونية (2022) إلى أن الهجوم السيبراني يُعد هجوماً مسلحاً إذا تسبب في **أضرار مادية جسيمة** أو **خسائر بشرية**. أما إذا اقتصر على سرقة بيانات أو تعطيل مواقع، فلا يرقى إلى هذا المستوى.

ولذلك، فإن أي تدخل دفاعي سيبراني يجب أن يخضع لثلاثة شروط:

1. **التأكيد**: أن يكون هناك دليل قاطع على مصدر الهجوم.

2. **التناسب**: أن لا يتجاوز الرد حجم الضرر الواقع.

3. **الإبلاغ**: أن تُبلغ الدولة المعنية قبل أو بعد التنفيذ.

المبحث الثالث: التحالفات الرقمية وحماية الأمن القومي

لا يمكن لأي دولة أن تحمي أمنها الرقمي بمفردها. ولذلك، ظهرت تحالفات مثل "الدرع السيبراني الأوروبي"، و"تحالف الذكاء الاصطناعي الخمسة" (الولايات المتحدة، بريطانيا، كندا، أستراليا، نيوزيلندا).

والدول العربية، رغم وجود "الاستراتيجية العربية

للأمن السيبراني"، تفتقر إلى **آلية تنفيذية مشتركة**. ومن هنا، يدعو هذا الكتاب إلى إنشاء **مركز عربي للأمن السيبراني**، يكون مقره في دولة محايدة، ويضم خبراء من جميع الدول الأعضاء.

الفصل الخامس: السيادة الرقمية والاقتصاد الوطني

المبحث الأول: البيانات كثروة وطنية

باتت البيانات تُوصف بـ"نفط القرن الحادي

والعشرين". فشركات مثل "غوغل" و"فيسبوك" تحقق أرباحاً تفوق ميزانيات دول بأكملها، دون أن تدفع ضرائب تُذكر في الدول التي تستخرج منها هذه البيانات.

ومن هنا، فإن السيادة الرقمية تتطلب **فرض سيادة اقتصادية على البيانات**، عبر:

- **فرض ضرائب رقمية** على الشركات العاملة في السوق المحلية.

- **تشريع حق الدولة في امتلاك البيانات** المتعلقة بالأمن القومي والاقتصاد الوطني.

- **تشجيع إنشاء منصات رقمية وطنية** تُقلل الاعتماد على الشركات الأجنبية.

المبحث الثاني: العملات الرقمية والسيادة النقدية

تمثل العملات الرقمية (مثل البيتكوين) تهديداً مباشراً للسيادة النقدية. فلو تبنّى مواطنو دولة ما عملة رقمية بديلة، فإن البنك المركزي يفقد قدرته على التحكم في العرض النقدي، وبالتالي في الاقتصاد ككل.

ولذلك، فإن العديد من الدول بدأت في إصدار **عملات رقمية مركزية** (CBDC)، مثل "اليوان الرقمي" في الصين، و"الروبل الرقمي" في روسيا.

أما في العالم العربي، فلا توجد حتى الآن خطة

موحدة لإصدار عملة رقمية عربية، رغم محاولات مصرف الإمارات المركزي. وهذا يُعد ثغرة خطيرة في السيادة الاقتصادية الرقمية.

المبحث الثالث: الملكية الفكرية في العصر الرقمي

مع انتشار الذكاء الاصطناعي، برز سؤال جديد: من يملك حقوق الملكية الفكرية للإبداعات التي يولدها الذكاء الاصطناعي؟

القانون المصري، مثلاً، يشترط أن يكون المؤلف "شخصاً طبيعياً"، مما يستبعد الذكاء الاصطناعي.

لكن هذا الحل لا يكفي. فالدول المتقدمة بدأت

في منح "حقوقاً محدودة" للمالك البشري للذكاء الاصطناعي.

ويقترح هذا الكتاب أن تُصدر الدول العربية تشريعاً خاصاً ينظم:

- ملكية الإبداعات الناتجة عن الذكاء الاصطناعي.

- المسؤولية عن الأخطاء التي يرتكبها الذكاء الاصطناعي.

- حماية البيانات المستخدمة في تدريب النماذج الذكية.

الفصل السادس: السيادة الرقمية والقضاء

المبحث الأول: القضاء الرقمي كضمانة للحقوق

في عالمٍ تسوده السرعة، لم يعد القضاء التقليدي كافياً. فالمواطن الذي يتعرض لاختراق بياناته يحتاج إلى **رد فوري**، لا إلى إجراءات تمتد لسنوات.

ولذلك، ظهر ما يُعرف بـ"القضاء الرقمي"، وهو:

> "مجموعة من الآليات القضائية المُسرعة، المدعومة بالتكنولوجيا، والتي تهدف إلى الفصل في المنازعات الرقمية خلال أيام، لا أشهر."

وقد أنشأت فرنسا "محكمة رقمية" متخصصة في الجرائم الإلكترونية، بينما أطلقت السعودية "منصة ناجز" لتسريع التقاضي الإلكتروني.

المبحث الثاني: الاختصاص القضائي في الفضاء الإلكتروني

يُعدّ تحديد المحكمة المختصة في الجرائم الرقمية من أعقد المسائل. فهل تُقام الدعوى في مكان ارتكاب الجريمة؟ أم في مكان تأثيرها؟ أم في مكان إقامة المدعى عليه؟

تذهب محكمة النقض المصرية في حكمها رقم 1254 لسنة 2020 إلى أن **مكان تأثير الجريمة** هو الأساس. فلو نشر شخص في أمريكا خبراً كاذباً يؤذي مواطناً مصرياً، فإن المحكمة المصرية تكون مختصة.

لكن هذا المبدأ يخلق تعارضاً مع القوانين الأمريكية، التي ترفض تطبيق قوانين أجنبية على شركاتها. ومن هنا، فإن الحل يكمن في **الاتفاقيات القضائية الثنائية**.

المبحث الثالث: الأدلة الرقمية وقواعدها

الأدلة الرقمية (كالرسائل، والسجلات، وبيانات

الموقع) تُعد اليوم العمود الفقري في إثبات الجرائم الإلكترونية. لكنها تتميز بثلاثة عيوب:

1. **القابلية للتزوير**.

2. **الهشاشة** (قد تُحذف بسهولة).

3. **الغموض** (قد لا يُفهم مصدرها).

ولذلك، يشترط القانون المصري (المادة 15 من قانون مكافحة الجرائم الإلكترونية) أن تكون الأدلة الرقمية:

- **مصادق عليها** من جهة موثوقة.

- **محمية من التغيير** منذ لحظة جمعها.

- **مصحوبة بتقرير فني** يشرح طريقة جمعها.

ويقترح هذا الكتاب إنشاء **وحدة وطنية لجمع الأدلة الرقمية**، تكون تابعة للنيابة العامة، وتتمتع باستقلالية فنية.

الفصل السابع: السيادة الرقمية وحقوق الإنسان

المبحث الأول: الحق في الخصوصية الرقمية

في عصرٍ تُجمع فيه بيانات الفرد من لحظة استيقاظه حتى نومه – من صحته، إلى مشترياته، إلى معتقداته – أصبح **الحق في الخصوصية** أكثر أهمية من أي وقت مضى.

ولا يكفي أن تنص الدساتير على هذا الحق دون حماية فعلية. فالمادة 57 من الدستور المصري تكفل سرية الاتصالات، لكنها لا تمنع الدولة من جمع البيانات الجماعية عبر برامج المراقبة.

ويُعرّف هذا الكتاب **الخصوصية الرقمية** بأنها:

> "حق الفرد في التحكم الكامل في بياناته الشخصية، وتحديد من يجمعها، وكيف

تُستخدم، ولأي غاية."

ولتحقيق ذلك، يجب أن يشترط القانون ثلاثة أمور:

1. **الموافقة الصريحة**: أن يوافق الفرد على جمع بياناته بعد إبلاغه الكامل.

2. **الغرض المحدد**: أن تُستخدم البيانات فقط للغرض الذي جُمعت من أجله.

3. **الحد الأدنى**: أن يقتصر الجمع على البيانات الضرورية فحسب.

المبحث الثاني: حرية التعبير في الفضاء الرقمي

تمثل منصات التواصل الاجتماعي ساحة جديدة للتعبير، لكنها في الوقت نفسه أداة للرقابة. فبينما تتيح للمواطنين نشر آرائهم بحرية، فإنها تخضع لشروط استخدام غامضة، وقد تحذف المحتوى دون تفسير.

ومن هنا، فإن السيادة الرقمية لا تعني كبت الحريات، بل **تنظيم المنصات لضمان الحياد**.

ويقترح هذا الكتاب أن تُلزم القوانين العربية الشركات الكبرى بـ:

- إنشاء **لجان مستقلة** لمراجعة قرارات

الحذف.

- إتاحة **حق الاستئناف** للمستخدمين.

- نشر **تقارير دورية** عن سياسات المحتوى.

المبحث الثالث: الحق في النسيان الرقمي

في الماضي، كانت الأخطاء تُنسى مع الزمن. أما اليوم، فتبقى محفورة في ذاكرة الإنترنت للأبد.

ولذلك، ظهر ما يُعرف بـ"الحق في النسيان"، الذي يسمح للفرد بطلب حذف المعلومات غير الدقيقة أو القديمة عنه.

وقد أقرته محكمة العدل الأوروبية في قضية *جورجيوس ضد غوغل* (2014).

أما في العالم العربي، فلا يوجد نص صريح يعترف بهذا الحق.

ويقترح هذا الكتاب إدخاله في التشريعات الوطنية، مع مراعاة التوازن بين:

- حق الفرد في النسيان.

- حق الجمهور في المعرفة.

- حق الصحافة في التحقيق.

الفصل الثامن: السيادة الرقمية والذكاء الاصطناعي

المبحث الأول: الذكاء الاصطناعي كأداة للسلطة العامة

باتت الحكومات تستخدم الذكاء الاصطناعي في مجالات متعددة: من التنبؤ بالجرائم، إلى تقييم طلبات التوظيف، إلى إدارة المرور.

لكن هذه الأنظمة، رغم كفاءتها، تثير مخاوف

جوهرية:

- **التمييز الخوارزمي**: حيث قد تُفضّل خوارزمية فئة على أخرى بناءً على بيانات تاريخية متحيزة.

- **غياب الشفافية**: لأن العديد من الخوارزميات "صناديق سوداء" لا يُفهم منطقها.

- **فقدان المسؤولية**: فمن يُحاسب إذا اتخذ الذكاء الاصطناعي قراراً خاطئاً؟

المبحث الثاني: نحو تشريع عربي لأخلاقيات الذكاء الاصطناعي

لا يمكن ترك الذكاء الاصطناعي دون ضوابط.

ولذلك، يدعو هذا الكتاب إلى سن **مدونة أخلاقية عربية** للذكاء الاصطناعي، تقوم على المبادئ التالية:

1. **الإنسانية**: أن يكون الذكاء الاصطناعي خادماً للإنسان، لا بديلاً عنه.

2. **الشفافية**: أن تُفصح الجهات الحكومية عن استخدامها للذكاء الاصطناعي.

3. **المساءلة**: أن يتحمل صانع القرار البشري المسؤولية النهائية عن القرارات الآلية.

المبحث الثالث: الذكاء الاصطناعي والعدالة الجنائية

استخدام الذكاء الاصطناعي في التنبؤ بالجرائم (Predictive Policing) قد يؤدي إلى **تجريم الأفراد قبل ارتكابهم الجريمة**.

ففي الولايات المتحدة، أظهرت دراسات أن هذه الأنظمة تستهدف الأحياء الفقيرة بشكل غير متناسب.

ولذلك، فإن هذا الكتاب يرفض استخدام الذكاء الاصطناعي في:

- تحديد المشتبه بهم.

- تقدير مدة العقوبة.

- تقييم خطورة المتهم.

ويؤكد أن **العدالة لا يمكن أن تكون آلية**.

الفصل التاسع: السيادة الرقمية في العلاقات الدولية

المبحث الأول: النزاعات السيبرانية وقانون النزاعات المسلحة

هل تنطبق اتفاقيات جنيف على الهجمات السيبرانية؟

الجواب ليس بسيطاً. فلو استهدفت هجمات سيبرانية مستشفى مدنياً، فإن ذلك يُعد انتهاكاً صريحاً للقانون الدولي الإنساني.

لكن لو استهدفت شبكة كهرباء عسكرية، فقد يُعتبر عملاً مشروعاً في زمن الحرب.

ويُوصي هذا الكتاب الدول العربية بالانضمام إلى **مبادرة تالين** (Tallinn Manual)، التي وضعت قواعد قانونية لتطبيق القانون الدولي على الفضاء الإلكتروني.

المبحث الثاني: الحصانة السيبرانية للدول

تتمتع الدول بحصانة من المقاضاة أمام محاكم أجنبية. لكن هل تمتد هذه الحصانة إلى أفعالها في الفضاء الإلكتروني؟

في قضية *ياهو ضد وزارة الاتصالات الإيرانية* (2021)، رفضت محكمة أمريكية دعوى ضد إيران، استناداً إلى مبدأ الحصانة السيادية.

ولكن هذا المبدأ لا يحمي الدول إذا ارتكبت جرائم ضد المدنيين.

ولذلك، فإن هذا الكتاب يقترح أن تُستثنى **الجرائم السيبرانية ضد الأفراد** من نطاق الحصانة.

المبحث الثالث: التعاون الدولي في مكافحة الجرائم الإلكترونية

لا يمكن مكافحة الجرائم الإلكترونية دون تعاون دولي.

وقد وقّعت 60 دولة على **اتفاقية بودابست** لمكافحة الجرائم الإلكترونية، لكن معظم الدول العربية لم تنضم إليها، بحجة أنها لا تراعي خصوصيتها.

ويقترح هذا الكتاب أن تُطلق جامعة الدول العربية **اتفاقية عربية موحدة**، تكون متوافقة مع المعايير الدولية، لكنها تحترم القيم العربية والإسلامية.

الفصل العاشر: خارطة طريق للسيادة الرقمية في الوطن العربي

المبحث الأول: التحديات الراهنة

تواجه الدول العربية خمسة تحديات رئيسية:

1. **التشتت التشريعي**: كل دولة لها قانونها الخاص.

2. **الضعف التقني**: نقص الكوادر المؤهلة.

3. **الاعتماد على الخارج**: معظم البنية التحتية خارجية.

4. **الخلل في التوازن**: بين الأمن والحقوق.

5. **غياب الرؤية الاستراتيجية**.

المبحث الثاني: الركائز الأساسية للاستراتيجية العربية

لبناء سيادة رقمية حقيقية، يجب أن تستند الاستراتيجية العربية على خمس ركائز:

1. **التشريع الموحّد**: قانون عربي نموذجي للسيادة الرقمية.

2. **البنية التحتية الوطنية**: مراكز بيانات عربية مستقلة.

3. **الكوادر البشرية**: إنشاء كليات متخصصة في الأمن السيبراني.

4. **الشراكة مع القطاع الخاص**: لتمويل الابتكار.

5. **التعاون الإقليمي**: عبر مركز عربي للأمن الرقمي.

المبحث الثالث: السيناريوهات المستقبلية

يعرض هذا الكتاب ثلاثة سيناريوهات:

- **السيناريو السلبي**: استمرار التشتت وضعف السيادة هيمنة أجنبية.

- **السيناريو الدفاعي**: تشريعات وطنية منعزلة حماية جزئية.

- **السيناريو الاستباقي**: استراتيجية عربية موحدة قيادة رقمية إقليمية.

ويؤكد أن الخيار الأخير هو الوحيد الذي يضمن **سيادة رقمية حقيقية**.

الخاتمة

السيادة الرقمية ليست رفاهية، بل **ضرورة وجودية**.

فالدولة التي لا تحمي فضائها الرقمي،

هي دولةٌ تخلّت عن جزءٍ من ذاتها.

ولا يمكن تحقيق هذه السيادة دون توازن دقيق بين:

- **الأمن** و**الحريات**،

- **التقنية** و**القيم**،

- **الاستقلالية** و**التعاون**.

ويبقى السؤال الأهم:

هل ستكون الدول العربية ساحةً للصراع الرقمي؟

أم ستكون لاعباً فاعلاً في صنع مستقبل الفضاء الإلكتروني؟

د. محمد كمال عرفه الرخاوي

المراجع

- الدستور المصري لسنة 2014

- اللائحة العامة لحماية البيانات (GDPR)

- اتفاقية بودابست لمكافحة الجرائم الإلكترونية

- أحكام المحكمة الأوروبية لحقوق الإنسان

- أحكام محكمة النقض المصرية

- Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations

- دراسات جامعة الأمم المتحدة للجريمة والعدالة

- تقارير المنتدى الاقتصادي العالمي حول الحوكمة الرقمية

- أبحاث معهد Brookings حول السيادة الرقمية

الفهرس

التمهيد

الفصل الأول: الإطار النظري للسيادة الرقمية

الفصل الثاني: الأسس الدستورية للسيادة الرقمية

الفصل الثالث: الإطار التشريعي للسيادة الرقمية

تم بحمد الله وتوفيقه

د. محمد كمال عرفه الرخاوي

كتابي من المؤلف.