العمارة العالمية للسيادة الرقمية

العنوان: العمارة العالمية للسيادة الرقمية: تحليل مقارن لنماذج الرقابة والتحكم في الإنترنت لعام ٢٠٢٥.

المؤلف *NOX*

ملخص

تستكشف هذه المقالة تطور ممارسات الرقابة والتحكم في الإنترنت في دول رئيسية اعتباراً من عام ٢٠٢٥. يعتمد التحليل على منهج مقارن، يحدد ثلاثة نماذج مهيمنة: السلطوي-السيادي (الصين، روسيا، إيران، كوريا الشمالية)، الليبرالي-التنظيمي (الولايات المتحدة، الاتحاد الأوروبي، إسرائيل)، والهجين (تركيا، مصر، وعدة دول في آسيا، وإفريقيا، وأمريكا اللاتينية). يُجادل بأنه بحلول عام ٢٠٢٥، تحول مفهوم "الإنترنت السيادي" من فكرة نظرية إلى عمارة تقنية قانونية ملموسة تنفذها عدد من الدول. التركيز على الأدوات التكنولوجية (*AI*، *DPI*)، والأطر القانونية، والأهداف الجيوسياسية الكامنة وراء القيود. تختتم المقالة بتعزيز تفتت الإنترنت العالمي ("*Splinternet*") وتشكيل أنظمة رقمية مرنة تحكمها قواعدها الخاصة.

الكلمات المفتاحية: رقابة الإنترنت، السيادة الرقمية، ٢٠٢٥، فحص الحزم العميق (*DPI*)، الذكاء الاصطناعي، التنظيم، حقوق الإنسان، الأمن السيبراني.

المقدمة

بحلول عام ٢٠٢٥، توقف الإنترنت عن كونه فضاء عالمي موحد كما تصور عند إنشائه. مدفوعاً بالتوترات الجيوسياسية، ومخاوف الأمن القومي، والرغبة في السيادة الثقافية، برزت نماذج وطنية وإقليمية مختلفة للتحكم في المجال المعلوماتي الرقمي. تطور مصطلح "الرقابة" ليشمل ليس فقط حجب المحتوى، ولكن أيضاً نظام معقد من الاعتدال الاستباقي، والضغط التشريعي على المنصات، وتلاعب حركة المرور، والمعلومات المضللة المستهدفة.

يهدف هذا المقال إلى إجراء تحليل مقارن لنماذج التحكم في الإنترنت في القوى العالمية الكبرى، وتحديد السمات المشتركة والاختلافات الأساسية بينها، وتقييم تأثيرها على الحقوق المدنية، والاقتصاد الرقمي، والاستقرار الدولي.

١. المنهجية

تقوم هذه الدراسة على تحليل مقارن نوعي. تم اختيار الدول بناءً على تأثيرها على السياسة الرقمية العالمية وتمثيلها للنماذج المختلفة للتحكم. المصادر تشمل:

- القوانين الوطنية (قوانين "الإنترنت السيادي"، حماية البيانات، مكافحة التطرف)؛
- تقارير من المنظمات الدولية (*Freedom House، RSF، Access Now*)؛
- تقارير تقنية من شركات الأمن السيبراني (*Citizen Lab، Palo Alto Networks*)؛
- تصريحات علنية من المسؤولين الحكوميين والجهات التنظيمية.

٢. التحليل المقارن لنماذج التحكم في الإنترنت

٢.١. نموذج السيادة الرقمية السلطوية

الصين:

بحلول عام ٢٠٢٥، تطور الجدار الناري العظيم للصين (*GFW*) إلى نظام شامل لإدارة المجتمع الرقمي يسمى "الائتمان الاجتماعي ٢.٠". تم استكمال الحجب القائم على فحص الحزم العميق (*DPI*) بخوارزميات ذكاء اصطناعي (*AI*) تنبؤية قادرة على تحديد وقمع المناقشات "غير المرغوب فيها" في مراحلها المبكرة. تم استبدال جميع المنصات العالمية الكبرى ببدائل محلية (*WeChat، Douyin، Baidu*)، التي تخضع لسيطرة الدولة الكاملة. أصبح تصدير هذا النموذج - خاصة إلى الدول الأفريقية والآسيوية من خلال مبادرة الحزام والطريق - أداة رئيسية للقوة الناعمة.

روسيا:

اكتمال تنفيذ قانون "الإنترنت السيادي" (٢٠١٩). بحلول عام ٢٠٢٥، أصبح نظام اسم النطاق الوطني (*DNS*) جاهزاً للعمل، مما يمكن من عزل الجزء الروسي من الإنترنت (*Runet*) عن الشبكة العالمية عند الضرورة. يُستخدم فحص الحزم العميق (*DPI*) بنشاط لقمع شبكات *VPN* والمرور المشفر. الأهداف الرئيسية للرقابة هي انتقاد السلطات، العمليات

العسكرية، محتوى المثليين (*LGBTQ+*)، ووسائل الإعلام المستقلة. الأسس القانونية تشمل قوانين "الأخبار المزيفة"، "وكلاء أجانب"، و"التطرف".

إيران:

يجمع نموذج إيران بين التحكم التقني والقمع الشديد. تحافظ البلاد على واحدة من أكثر أنظمة ترشيح المحتوى تقدماً في العالم، قادرة على حجب المراسلات (*Telegram*، *WhatsApp*) ووسائل التواصل الاجتماعي ديناميكياً أثناء الاحتجاجات. بحلول عام ٢٠٢٥، أصبحت هوية المستخدم الإلزامية مطلوبة للوصول إلى *Wi-Fi* وشراء بطاقات *SIM*. خنق عرض النطاق الترددي للإنترنت إلى مستويات منخفضة بشكل خطير يمارس بشكل شائع خلال الاضطرابات.

كوريا الشمالية:

تبقى معياراً للتحكم الكلي. الإنترانت *Kwangmyong* معزولة تماماً عن الإنترنت العالمي. يقتصر الوصول إلى الإنترنت الدولي على النخبة الضيقة. المحتوى مقصور على الدعاية الحكومية، المواد الأيديولوجية، والمعلومات العلمية المحدودة للغاية.

٢.٢. النموذج الليبرالي-التنظيمي (الولايات المتحدة، الاتحاد الأوروبي، إسرائيل)

الولايات المتحدة:

الرقابة الحكومية التقليدية غائبة، لكن نظاماً معقداً من التنظيم الخاص والعام ظهر. تحت الضغط العام والإشراف من قبل *FCC* و *FTC*، شددت المنصات الرئيسية (*Meta*، *X*، *Google*) سياسات الاعتدال فيما يتعلق بخطاب الكراهية، والمعلومات المضللة، والتحريض. يدور نقاش مركزي في عام ٢٠٢٥ حول القسم ٢٣٠، القانون الذي يمنح المنصات حصانة من المسؤولية عن المحتوى الذي ينشئه المستخدمون. الدعوات إلى إلغائه أو تعديله تدفع المنصات إلى الرقابة الاستباقية لتجنب المخاطر القانونية. وهكذا، يتم تفويض الرقابة بشكل فعال إلى الشركات الخاصة.

الاتحاد الأوروبي:

طور الاتحاد الأوروبي أكثر الأطر التنظيمية تقدماً في العالم، والتي تحدد في الواقع المعايير العالمية. الرقابة غير مباشرة، تُفرض من خلال الامتثال الصارم للقوانين:

- *GDPR*: حجب المواقع التي تنتهك متطلبات حماية البيانات؛
- قانون الخدمات الرقمية (*DSA*): ملزمة بإزالة المحتوى غير القانوني (مثل الإرهاب، خطاب الكراهية) فوراً تحت تهديد غرامات ضخمة؛
- قانون الأسواق الرقمية (*DMA*): يستهدف المنصات الاحتكارية.

لا يشارك الاتحاد الأوروبي في الحجب على مستوى الدولة، لكنه يخلق بيئة قانونية يؤدي فيها عدم الامتثال إلى الإقصاء الفعلي من السوق.

إسرائيل:

تقدم إسرائيل حالة فريدة من النموذج الليبرالي-التنظيمي مع تركيز قوي على الأمن القومي. كديمقراطية عالية التقنية، تلتزم إسرائيل عموماً بمبادئ الإنترنت المفتوح. ومع ذلك، وسط الصراع المستمر والتهديدات الأمنية، تطبق الرقابة بشكل انتقائي وعلى أسس قانونية صلبة.

الإطار القانوني: الأداة الرئيسية هي الرقابة العسكرية، الموروثة من عصر تأسيس الدولة. يجب على جميع وسائل الإعلام والمنافذ الإلكترونية تقديم المواد المتعلقة بالأمن للمراجعة المسبقة من قبل مكتب الرقابة العسكرية. بحلول عام ٢٠٢٥، تم تكييف هذا المبدأ للعصر الرقمي.

التكنولوجيا والممارسة: يمكن للسلطات أن تطلب من مقدمي خدمة الإنترنت والمنصات الاجتماعية إزالة المحتوى الذي يعتبر تهديداً للأمن القومي أو تحريضاً على العنف. كثيراً ما يتم الطعن في هذه القرارات في المحكمة العليا، التي تعمل كموازنة حرجة. خلال فترات التصعيد العسكري، ت intensify الرقابة، وتواجه المنصات ضغوطاً متزايدة للامتثال. على عكس الأنظمة السلطوية، تحافظ إسرائيل على مجتمع مدني نابض بالحياة وصحافة حرة تتحدى قرارات الرقابة، مما يجعل العملية أكثر شفافية.

٢.٣. النموذج الهجين (تركيا، مصر، آسيا، إفريقيا، أمريكا اللاتينية)

تركيا:

تحافظ على واحدة من أكبر قوائم حجب المحتوى في العالم بموجب قوانين تحمي مصالح الدولة والنظام العام. تم strengthening القانون رقم ٥٦٥١ في عام ٢٠٢٥، مما يمكن المنظم *BTK* من حجب أي محتوى في غضون أربع ساعات دون أمر قضائي. يضغط القانون

رقم ٧٤١٦ على المنصات لتعيين ممثلين محليين والامتثال للتوجيهات الحكومية، مع استخدام الخنق تدريجياً حتى تعطل الخدمة بالكامل.

مصر:

تستخدم تراخيص الاتصالات كأداة تحكم. حجب شبكات *VPN* والتطبيقات المشفرة (مثل *Signal*) هو ممارسة قياسية. خلال التوترات السياسية، يمكن أن تحدث عمليات إغلاق الإنترنت على مستوى البلاد. تمنح قوانين الجرائم الإلكترونية سلطات واسعة النطاق لحجب المواقع ومراقبة المواطنين.

آسيا (الهند وفيتنام):

تمارس الهند عمليات إغلاق إنترنت إقليمية روتينية تحت ذرائع السلامة العامة. توفر قوانين تكنولوجيا المعلومات (*IT*) الحكومة بسلطات حجب واسعة. تحاكي فيتنام النموذج الصيني، حيث تطلب من شركات التكنولوجيا تخزين بيانات المستخدمين محليًا، ومشاركتها عند الطلب، وإزالة المحتوى في غضون ٢٤ ساعة.

إفريقيا:

تستخدم الحكومات في إثيوبيا وأوغندا وزيمبابوي عمليات إغلاق الإنترنت بشكل متزايد خلال الانتخابات والاحتجاجات. التكنولوجيا والنماذج الصينية للتحكم - التي غالباً ما تكون مجمعة مع بنية *Huawei* و *ZTE* التحتية - تكتسب نفوذاً.

أمريكا اللاتينية:

بحلول عام ٢٠٢٥، تظهر المنطقة اتجاهات مختلطة، تناسب إلى حد كبير النموذج الهجين مع اختلافات كبيرة.

البرازيل:

كأكبر اقتصاد في المنطقة، تحاول البرازيل الموازنة بين حرية التعبير ومكافحة المعلومات المضللة والجرائم الإلكترونية. يظل *Marco Civil da Internet* المستوحى من الاتحاد الأوروبي حجر الزاوية التنظيمي. ومع ذلك، أدت أوامر المحكمة المتزايدة بحجب تطبيقات المراسلة الشهيرة (مثل *WhatsApp* و *Telegram*) لرفضها توفير بيانات المستخدمين أو كبح المعلومات المزيفة إلى إثارة النقاش. غالباً ما تكون الرقابة مستهدفة ومؤقتة لكنها تتزايد في التكرار.

فنزويلا ونيكاراغوا:

تتجه نحو النماذج السلطوية. تستخدم الحكومات أدوات تقنية لحجب مواقع الأخبار المستقلة والمنصات الاجتماعية، خاصة خلال الاضطرابات السياسية. ينسق مركز *Conatec* الفنزويلي (المركز الوطني للتحكم في الفضاء الإلكتروني) الرقابة. تجرم قوانين الجرائم الإلكترونية القاسية انتقاد الحكومة عبر الإنترنت.

كوبا:

قريبة من السيطرة الكاملة للدولة. على الرغم من توسع الوصول إلى الإنترنت بحلول عام ٢٠٢٥، إلا أنه يظل مكلفاً ومنظماً بشدة. تتيح احتكارية الاتصالات الحكومية *ETECSA* ترشيح المحتوى ومراقبة المستخدمين. يتم حجب انتقاد الحكومة والوصول إلى وسائل الإعلام المستقلة بشكل روتيني.

٣. المناقشة والاستنتاجات

بحلول عام ٢٠٢٥، انتقل العالم من إنترنت موحد إلى مجموعة من المجالات الرقمية الوطنية والإقليمية المجزأة - الـ *Splinternet*. تشمل الاتجاهات الرئيسية:

- **التطور التكنولوجي:** أفسح حجب المحتوى البسيط الطريق لأنظمة قائمة على فحص الحزم العميق (*DPI*) والذكاء الاصطناعي (*AI*) قادرة على الاعتدال التنبؤي والقمع الجراحي لأدوات التحايل.
- **التمويه القانوني:** يتم تبرير الرقابة بشكل متزايد من خلال مكافحة التطرف، حماية البيانات (الاتحاد الأوروبي)، أو السيادة والأمن (روسيا، الصين، إسرائيل)، مما يمنحها شرعية متصورة في الساحة الدولية.
- **خصخصة الرقابة:** في الديمقراطيات الليبرالية (الولايات المتحدة، الاتحاد الأوروبي)، انتقل دور الرقيب من الدولة إلى الشركات، التي تضطر إلى اتباء التفويضات التنظيمية تحت تهديد العقوبات. تحتفظ إسرائيل بالرقابة الحكومية، ولكن في سياقات أمنية ضيقة ومع رقابة قضائية.
- **البعد الجيوسياسي:** نموذجان عالميان يتنافسان: النهج التنظيمي للولايات المتحدة وال الاتحاد الأوروبي (القائم على الحقوق ومعايير السوق) مقابل نموذج الصين وروسيا (التحكم الحكومي والعزل). تتبنى الدول الهجينة - خاصة في أمريكا اللاتينية - عناصر من كليهما، اعتماداً على الظروف السياسية.

يكمن الخطر في إنشاء فقاعات معلوماتية دائمة، وصعود السلطوية، وتقليل تبادل المعرفة

عبر الحدود. كما تظهر حالة إسرائيل، فإن الصراع بين الانفتاح والأمن القومي هو التناقض المركزي الذي يشكل مستقبل الإنترنت.

الملحق: فحص الحزم العميق (DPI) واعتراض الشهادات

فحص الحزم العميق (*DPI*) هو تقنية لتحليل حركة المرور تسمح لمقدمي الخدمة أو الجهات الفاعلة الحكومية ليس فقط برؤية مكان اتصالك ولكن أيضاً فحص المحتويات الفعلية لحزم البيانات. هذا يكشف عن سلوك المستخدم - مشاهدة مقاطع الفيديو، استخدام شبكات *VPN*، المراسلة، الوصول إلى *Tor*، إلخ.

في الممارسة العملية، يتيح فحص الحزم العميق (*DPI*):

- حجب أو خنق خدمات محددة؛
- التحايل على إخفاء الهوية لـ *VPN* أو *Tor*؛
- مراقبة السلوك عبر الإنترنت؛
- رقابة جماعية - حتى داخل حركة المرور المشفرة.

يكمن التهديد الأشد في تقويض الثقة في تقنيات الإنترنت الأساسية.

في العديد من البلدان، تحت ذريعة مكافحة الإرهاب، حماية الأطفال، فرض العقوبات، أو دوافع مماثلة، تجبر الحكومات مقدمي خدمة الإنترنت على تنفيذ فحص الحزم العميق (*DPI*) وإدخال سلطات الشهادات الخاصة بها (*CAs*). يمكن لهذه الـ *CAs* إصدار شهادات *HTTPS* مزيفة - لن يلاحظ المستخدمون، لن تحذر المتصفحات، ويمر المرور عبر عقدة خاضعة للتحكم.

يظل الاتصال "آمناً" في المظهر، ولكن يمكن للحكومة أن تقرأ وتسجل وتعدل حركة المرور بشكل قانوني - دون اختراق - من خلال اختطاف بنية الثقة. هذا يعرف باسم **اعتراض الشهادة (*certificate interception*)** ويشكل، إلى جانب فحص الحزم العميق (*DPI*)، نظام اقتحام قانوني.

تنتهك هذه الآليات حيادية الشبكة، والخصوصية، وفكرة الاتصالات الآمنة ذاتها. عندما تحل الدولة محل الثقة - لم تعد تحمي. إنها تتحكم.