الدكتاتورية الرقمية من المراقبة إلى تشكيل السلوك العام

د. عبد المنعم دهمان

مدرب واستشاري تطوير المشاريع - ألمانيا

عضو هيئة تحرير مجلة الاقتصاد الإسلامي العالمي

من التجسّس إلى الهندسة السلوكية

تبدو الرقمنة وعداً بالكفاءة والسرعة وتوسيع الوصول إلى الخدمات. لكن الوجه الآخر يظهر حين تُستخدم الأدوات نفسها لبناء قابلية حكم جديدة: ليس فقط معرفة ما يحدث، بل توقّع ما قد يحدث، ثم التدخل المبكر لتعديل الاحتمالات الاجتماعية والسياسية. هنا تتقاطع التقنية مع أخلاق السلطة: فالتحذير القرآني: **وَلَاتَجَسَّسُوا** (الحجرات: ١٢) لا يقدّم موقفًا وعظيًا فحسب، بل يضع حداً مبدئيًا لفكرة تحويل الرصد إلى قاعدة، والخصوصية إلى استثناء؛ وهو ما يعيننا لفهم لماذا تصبح المراقبة الرقمية – حين تُعمَّم وتُطبّع – مدخلاً لتآكل الاستقلال الفردي والثقة العامة.

وفي الأدبيات المعاصرة، تُظهر **فريدوم هاوس** أن **السلطوية الرقمية** تُروَّج بوصفها طريقة لتمكين الحكومات من التحكم بالمواطنين عبر التكنولوجيا الحديثة، بما يقلب فكرة الإنترنت كأداة تحرر إلى أداة ضبط وإكراه[1].

أولاً– ماذا نعني بالدكتاتورية الرقمية؟

يطرح **أوليفر شلومبرغر** (Oliver Schlumberger) إطاراً تحليليًا لدراسة **الدكتاتورية الرقمية** ينطلق من منطق السلطوية الداخلي لا من سحر الابتكار التقني؛ فالتكنولوجيا لا تُنشئ الاستبداد من العدم، لكنها تعيد تشكيل أدواته ووتيرته ومداه[2]. ويؤكد أن **رقمنة الدكتاتورية** تجعلها متميزة عن أنماط الحكم السلطوي التقليدية لأنها تضيف:

---

[1]. Freedom House. Freedom on the Net 2018- The Rise of Digital Authoritarianism. Freedom House, Washington 2018. P12.

[2]. Schlumberger, Oliver; Edel, Mirjam; Maati, Ahmed; Saglam, Koray. *How Authoritarianism Transforms: A Framework for the Study of Digital Dictatorship.* Government and Opposition (Cambridge University Press), Cambridge 2024. P13.

- كثافة البيانات.
- السرعة الزمنية للتدخل.
- قابلية التنبؤ.
- توسيع نطاق الضبط دون عنفٍ مباشر دائم.

ومن جهة ضبط المفاهيم، يناقش **جيمس بيرسون** (James S. Pearson) مفهوم **السلطوية الرقمية** بوصفه توصيفًا لحالة تستخدم فيها الأنظمة السلطوية التقنيات الرقمية للمراقبة والقمع والتلاعب[1]. وعلى الرغم من تداخل المصطلحات الاستبداد الرقمي مع الديكتاتورية الرقمية (Digital Authoritarianism / Digital Dictatorship)، يمكن الاستفادة منهجيًا من التمييز التالي:

- **السلطوية الرقمية**: طيف واسع من الممارسات الرقمية السلطوية (قد تظهر جزئيًا في سياقات متعددة).
- **الدكتاتورية الرقمية**: حالة أكثر اكتمالاً تتكامل فيها البنية الرقمية مع بنية الحكم، بحيث تصبح الخوارزميات والبيانات جزءاً من عقل النظام التنفيذي.

ثانيًا- من المراقبة إلى تشكيل السلوك العام: آليات التحول

١- المراقبة الشاملة وتحويل المجتمع إلى بيانات قابلة للمعالجة

الخطوة الأولى هي بناء قدرة دائمة على الرصد: كاميرات ذكية، تعرف وجوه، تتبّع أجهزة، اعتراض بيانات شبكية، وربط ذلك بقواعد بيانات الهوية والسجلات. لا يكون الهدف معرفة الفعل فقط، بل بناء ملف احتمالي للفرد والجماعة. تحذّر تقارير حرية الإنترنت من تصاعد أنماط المراقبة وجمع بيانات المستخدمين واستعمال قوانين فضفاضة لتقييد التعبير.

٢- الفرز الخوارزمي والتصنيف:

[1]. Pearson, James S. Defining Digital Authoritarianism. Philosophy & Technology (Springer Nature), Berlin 2024. P11.

حين تُدمَج البيانات، يتحول الفرد إلى درجة أو تصنيف: أهلية خدمة، اشتباه أمني، قابلية ائتمان، أو ترتيب اجتماعي. في هذا المستوى يصبح الضبط أقل حاجة إلى الاعتقال المباشر، لأنه ينتقل إلى **حرمانٍ إداري** أو **تقييد فرص** أو **تأخير معاملات**، وهو ما يسميه بعض الباحثين قمعًا بلا ضجيج، يعتبر هذا التحول إعادة هندسة لآليات السيطرة تحت السلطوية عبر أدوات رقمية تزيد الفاعلية وتخفض الكلفة السياسية للعنف الظاهر.

٣- التنبؤ والتدخل المبكر: سياسة ما قبل الحدث

تُتيح التحليلات التنبؤية الانتقال من ردّ الفعل إلى التدخل المسبق(Pre-emption)، مراقبة أنماط التواصل، تحليل الشبكات، تقدير احتمالات الاحتجاج أو المعارضة، ثم الإجراءات الوقائية (رسائل ردع، توقيفات استباقية، أو تعطيل رقمي موضعي). هذا ما يجعل الزمن السياسي أقصر: بدل انتظار الحدث، يجري تفكيكه قبل تشكّله.

٤- تشكيل السلوك العام: الاقتصاد السياسي للهندسة السلوكية

هنا نبلغ جوهر العنوان **من المراقبة إلى تشكيل السلوك**، يقدّم **هال فاريان (Hal Varian)**-كبير اقتصاديي غوغل-صياغةً تلخص منطق القيمة: "البيانات مثل النفط في جانبٍ واحد: يجب تكريرها لكي تصبح مفيدة... فالبيانات الخام وحدها لا تساوي الكثير[1]".

هذه العبارة تكشف الحلقة الحاكمة:

الخام (سلوك الناس) ← تكرير (نماذج وتنبؤ) ← فائدة (قرار / ربح / سيطرة)

في الدكتاتورية الرقمية، **الفائدة** قد تكون سياسية: تعديل احتمالات الرأي العام، ترجيح سردية، إضعاف تنظيم اجتماعي، أو خلق انضباط ذاتي خوفًا من الرصد.

[1]. Melbourne Business School. Hal Varian from Google: Like oil data must be refined before it can be used. Melbourne Business School, Melbourne – 2018. https://mbs.edu/news/hal-varian-from-google-like-oil-data-must-be-refi?utm_source=chatgpt.com

وتوضح **شوشانا زوبوف** (Shoshana Zuboff) في تحليل **رأسمالية المراقبة** أن التجربة الإنسانية تُنتزع كمادة خام لترجمتها إلى بيانات سلوكية[1] . ورغم أن زوبوف تركز على الشركات، فإن منطقها يشتبك مباشرة مع الدكتاتورية الرقمية عندما تتلاقى مصلحة الدولة السلطوية (الضبط) مع مصلحة اقتصاد المنصات (التنبؤ والتأثير) .

ثالثًا– الاقتصاد السياسي للدكتاتورية الرقمية : لماذا تندمج السلطة مع البيانات ؟

١– البيانات كسلعة. . . وكأداة لاستخراج ريع معلوماتي

في الاقتصاد الرقمي لا تُعد البيانات مجرد مدخل إنتاج، بل مصدر قوة سوقية وسياسية، يبينّ صندوق النقد الدولي أن البيانات الفردية قد تُستخدم استراتيجيًا لاستخراج **ريع** (Rents) من موضوع البيانات نفسه، أي من الشخص الذي تُجمع عنه البيانات[2] .

وعندما تمتلك السلطة (أو تحالف السلطة–المنصة) قدرةً حصرية على الرؤية والتحليل، يتشكل عدم تكافؤ جوهري : المواطن لا يرى كيف يُصنَّف، ولا لماذا رُفضت خدمته، ولا كيف استُخدم أثره الرقمي ضده . هكذا يتحول **الريع المعلوماتي** إلى **ريع سياسي** أيضًا : مكاسب حكم من التحكم اللامرئي .

٢– تحالف الدولة والمنصات : تبادل المنافع

تقارير حرية الإنترنت تلفت إلى تصدير نماذج وأدوات المراقبة وتقنيات تعرف الوجوه وتحليلات البيانات إلى حكومات ذات سجلات حقوقية ضعيفة . هذا يضيء بنية تبادل المنافع :

- الشركات : أسواق، عقود، بيانات، نفوذ .
- السلطة : أدوات ضبط، هندسة خطاب، شرعنة إجراءات باسم الأمن أو مكافحة التضليل .

٣– انهيار الثقة العامة : كلفة غير مرئية على الاقتصاد والمجتمع

---

[1]. Zuboff, Shoshana. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. PublicAffairs, New York – 2019. https://www.hbs.edu/faculty/Pages/item.aspx?num=56791&utm_source=chatgpt.com

[2]. Carrière-Swallow, Yan; Haksar, Vikram; Patnam, Manasa; Schoelermann, Philip. The Economics and Implications of Data: An Integrated Perspective. International Monetary Fund, Washington 2019. P29.

عندما يشعر الأفراد أن المجال العام مراقَب وأن التعبير محفوف بعواقب غير مفهومة (قرار خوارزمي، تصنيف، منع خدمة)، تتراجع الثقة ويزداد التحايل وتضعف المشاركة. هنا يصبح الاستبداد الرقمي ليس خطراً حقوقيًا فقط، بل خطراً على الإنتاجية الاجتماعية: لأن الابتكار يحتاج فضاءً عامًا يسمح بالنقاش والخطأ والتجريب دون خوفٍ بنيوي.

رابعًا- مؤشرات تشخيص الدكتاتورية الرقمية:

يمكن تشخيص الدكتاتورية الرقمية عبر مؤشرات عملية:

١. **الدمج القسري للهوية والسجلات** دون ضمانات مستقلة (رقابة قضائية، شفافية، حق اعتراض).

٢. **الغموض الخوارزمي**: قرارات تؤثر على الحقوق دون تفسير قابل للطعن.

٣. **مركزية البيانات** مع صلاحيات وصول واسعة ومساءلة محدودة.

٤. **تطبيع المراقبة** في الحياة اليومية وربطها بالخدمات الأساسية.

٥. **التحكم بالمحتوى** (حجب/تصفية/قوانين فضفاضة) مع خطاب الأمن/الأخلاق/مكافحة الشائعات.

٦. **استخدام التنبؤ** لسياسات ما قبل الحدث. (Pre-emptive governance)

خامسًا- مسارات الحماية: من "الدكتاتورية الرقمية" إلى "الدولة الرقمية المقيدة بالقانون"

ليس المقصود رفض الرقمنة أو تعطيلها، بل تأطيرها بضمانات دستورية وقانونية وتقنية تمنع انزلاقها إلى بنية مراقبة أو استبداد. وتقدّم التجربة الألمانية هنا مبدأً تأسيسيًا بالغ الأهمية: الحق في تقرير المصير المعلوماتي (Informational Self-Determination / informationelle Selbstbestimmung) الذي كرّسته المحكمة الدستورية الاتحادية الألمانية في حكمها الشهير عام ١٩٨٣ في سياق معالجة البيانات على نطاق واسع[1]. جوهر هذا المبدأ أن كرامة الإنسان لا تُختزل إلى

[1]. Federal Constitutional Court of Germany (Bundesverfassungsgericht). Judgment of 15 December 1983 (Census Act / Informational Self-Determination). Bundesverfassungsgericht, Karlsruhe – 1983. https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/1983/12/rs19831215_1bvr020983en.html?utm_source=chatgpt.com

"ملف بيانات" تتحكم به السلطة بلا حدود؛ بل يبقى الفرد صاحب القرار في حدود ما يُجمع عنه، ولماذا، وكيف يُستخدم، ومع من يُشارك — ولا تُجيز الدولة أي تقييد لهذا الحق إلا وفق مصلحة عامة راجحة وبأساس قانوني واضح وبما يحقق التناسب والضرورة.

وتتجلى ترجمة هذا المبدأ عمليًا في نماذج الصحة الرقمية بألمانيا؛ إذ تقوم بعض ترتيبات تبادل/استخدام بيانات الصحة على حجب الهوية عبر الترميز (pseudonymisation) بدل كشف هوية المواطن، مع بناء آليات واضحة للاعتراض والانسحاب (Opt-out/Widerspruch) وإدارة ذلك رقميًا، بما يضمن أن المشاركة ليست **قدرًا إجباريًا** بل خيارًا محميًا، بهذا المعنى تصبح الرقمنة جزءًا من دولة قانون: حدود الغرض (Purpose limitation)، وتقليل البيانات (Data minimisation)، والشفافية وإشعار المواطن، وسجلات تدقيق لمن اطلع على البيانات، وتشفير وأمن افتراضي (Privacy & Security by design)، ورقابة مستقلة، وهي جميعًا مسارات حماية تنقل الدولة من **سلطة بيانات إلى حوكمة بيانات** تُخضع الرقمي للحق لا العكس.

وتشير منظمة التعاون الاقتصادي والتنمية إلى أن حوكمة البيانات تمكّن الحكومات من إدارة البيانات بأمان وأخلاق وكفاءة، وأن استخدام الذكاء الاصطناعي يزيد الحاجة إلى أطر حوكمة قوية لضمان خدمات شاملة ومستدامة[1]. كما يؤكد البنك الدولي في أدبيات **البنية العامة الرقمية** أن الخصوصية وحماية البيانات قضايا حاسمة لأي نظام رقمي، خصوصًا الأنظمة التي تتعامل مع بيانات شخصية أو حساسة[2].

بناءً عليه، يمكن تلخيص مسارات الحماية في خمس قواعد تشغيلية:

١. **تقليل البيانات** (Data Minimization): جمع ما يلزم فقط، وبزمن احتفاظ محدد.

٢. **فصل السلطات الرقمية**: فصل الجهة المقدِّمة للخدمة عن الجهة الأمنية وعن مخازن البيانات، مع سجل تدقيق.

---

1. OECD. Digital government (policy topic page). OECD, Paris. https://www.oecd.org/en/topics/policy-issues/digital-government.html?utm_source=chatgpt.com

2. World Bank. Digital Public Infrastructure and Development: A World Bank Group Approach (Digital Transformation White Paper, Volume 1). World Bank, Washington 2025. P45.

٣. **حق التفسير والطعن** في القرارات الآلية/الخوارزمية التي تمس الحقوق.

٤. **رقابة قضائية مستقلة** على الوصول للبيانات الحساسة، ومعايير واضحة للتناسب والضرورة.

٥. **بنى ثقة تقنية**: تشفير، إدارة مفاتيح، مصادقة قوية، وسجلات تدقيق، حتى لا تصبح البنية التحتية الرقمية نقطة هيمنة أحادية.

خاتمة

الدكتاتورية الرقمية ليست تكنولوجيا قمع فقط، بل **تحول بنيوي في ممارسة السلطة**: من السيطرة عبر الخوف الظاهر إلى السيطرة عبر **المعرفة غير المتكافئة** و**التعديل السلوكي**، يوضح إطار شلومبرغر أن الدكتاتورية عندما تُرقمن تصبح أكثر سرعةً ودقةً ومرونةً وأقل كلفةً سياسية، بينما يكشف طرح فاريان أن القيمة تُستخرج من تكرير السلوك إلى نماذج تنبؤية، ما يفتح الباب أمام هندسة المجال العام. لذلك فإن معركة مواجهة الدكتاتورية الرقمية ليست ضد الرقمنة، بل ضد تحويلها إلى منظومة ضبط بلا حوكمة ولا حقوق، إن المعيار الفاصل هو:

- هل تبقى الدولة الرقمية مقيدة بالقانون والشفافية وحقوق الإنسان؟
- أم تتحول إلى آلة حكم تسبق المجتمع بخطوة عبر التنبؤ والتوجيه؟

المصادر:

1. Freedom House. Freedom on the Net 2018- The Rise of Digital Authoritarianism. Freedom House, Washington 2018.
2. Schlumberger, Oliver; Edel, Mirjam; Maati, Ahmed; Saglam, Koray. *How Authoritarianism Transforms: A Framework for the Study of Digital Dictatorship.* Government and Opposition (Cambridge University Press), Cambridge 2024
3. Pearson, James S. Defining Digital Authoritarianism. Philosophy & Technology (Springer Nature), Berlin 2024.
4. Melbourne Business School. Hal Varian from Google: Like oil data must be refined before it can be used. Melbourne Business School, Melbourne – 2018. https://mbs.edu/news/hal-varian-from-google-like-oil-data-must-be-refi?utm_source=chatgpt.com
5. Zuboff, Shoshana. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. PublicAffairs, New York – 2019. https://www.hbs.edu/faculty/Pages/item.aspx?num=56791&utm_source=chatgpt.com

6. Carrière-Swallow, Yan; Haksar, Vikram; Patnam, Manasa; Schoelermann, Philip. The Economics and Implications of Data: An Integrated Perspective. International Monetary Fund, Washington 2019.
7. Federal Constitutional Court of Germany (Bundesverfassungsgericht). Judgment of 15 December 1983 (Census Act / Informational Self-Determination). Bundesverfassungsgericht, Karlsruhe – 1983. https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/1983/12/rs19831215_1bvr020983en.html?utm_source=chatgpt.com
8. OECD. Digital government (policy topic page). OECD, Paris. https://www.oecd.org/en/topics/policy-issues/digital-government.html?utm_source=chatgpt.com
9. World Bank. Digital Public Infrastructure and Development: A World Bank Group Approach (Digital Transformation White Paper, Volume 1). World Bank, Washington 2025.