التسلم Received	التعديل Revised	القبول Accepted	الرقم التعريفي DOI
25-07-2022	24-08-2022	27-09-2022	https://doi.org/10.31430/TESO6208

شريف عبد الرحمن سيف النصر | * Sherif Abdul Rahman Seif El-Nasr

جدلية الكشف والحجب: العلاقات الرقمية المتوترة بين الدولة والناشطين في الشرق الأوسط

The Dialectic of Disclosure and Concealment: The Strained Digital Relations between Political Regimes and Activists in the Middle East

ملخص: تهدف هذه الدراسة إلى الانخراط، من خلال مقاربة وصفية وتصنيفية، في الجدل الدائر حول علاقة السلطة بالعالم الافتراضي، وذلك عبر رصد بنية منظومة "المراقبة الرقمية" في بلدان الشرق الأوسط ومكوّناتها، وتتبع أثرها في طموحات التمكين المعلوماتي التي كثيرًا ما راودت الناشطين والحركيين في الفضاء الرقمي. في هذا الصدد، تلقي الدراسة الضوء على أهم تقنيات الرقابة/ المراقبة التي تستخدمها الحكومات، والطرائق التي تُطوِّع من خلالها منظوماتها القانونية خدمة لأغراض التتبع الرقمي، وذلك في محاولة لفهم الكيفية التي أثّرت بها التقانة الرقمية في طبيعة العلاقة بين الأنظمة والناشطين، وتقييم مدى النجاح الذي أحرزته الأنظمة (المُمَكَّنة تقانيًا) في تطويع خصائص الافتراضي لأغراض الرقابة والمراقبة. وتخلص الدراسة إلى أنه على الرغم من أن الفضاء والتقانة الرقميين قد مثّلا لبعض الوقت مساحة وأداة للانعتاق أمام الناشطين، عبر الالتفاف على مظاهر التضييق التي قد تمارسها الأنظمة على المجال العام، فإن الأخيرة قد نجحت بدرجة كبيرة في أن تستوعب المدخلات الجديدة، وأن تمارس الرقابة/ المراقبة على المجال الافتراضي أيضًا. وهو ما يُلقي بظلال من الشك حول مستقبل الدور الذي يمكن أن ينهض به الافتراضي في موازنة إجراءات التتبع الحكومية.

كلمات مفتاحية: الرقابة، المراقبة الرقمية، القرصنة الحكومية، الفضاء/ المجال الافتراضي/ الرقمي، الناشطون الرقميون، صحافيو الإنترنت، الشرق الأوسط.

Abstract: This study aims to engage, through a descriptive approach, with the controversy surrounding the relationship of political regimes to the virtual world. This is done by examining the structure and components of digital monitoring systems in the countries of the Middle East and their impact on activists' aspirations for informational empowerment. In this regard, the study sheds light on the relevant censorship/surveillance techniques used by Middle Eastern governments and the ways in which they adapt their legal systems to serve the purposes of digital monitoring, to understand how information and communications technology (ICT) has impacted the relationship between regimes and activists. The study attempts to assess the extent to which ICT-enabled regimes have succeeded in manipulating the characteristics of the virtual sphere for their censorship and surveillance purposes. The study concludes that although the virtual space and ICT used to represent a space for and instrument of emancipation for activists, by evading the restrictions exercised by regimes on the public sphere, these regimes have succeeded to a large extent in absorbing new inputs and exercising control over the digital sphere as well. This casts doubt on the future role of ICT in counter-balancing government tracking procedures.

Keywords: Censorship, Digital Surveillance, Government Hacking, Digital/Virtual Space, Digital Activists, Internet Journalists, Middle East.

* أستاذ الحوسبة الاجتماعية، كلية الاقتصاد والعلوم السياسية، جامعة القاهرة.
Professor of Social Computing, Faculty of Economics and Political Science, Cairo University.
Email: sherif.seif@gmail.com

مقدمة

تشتهر في أدبيات التصوف ثنائيات تصف تقلّب حال "المريد" بين الحجب المطلق والكشف الكامل، وذلك في إشارة إلى علاقة هذا المريد بمصدر اليقين الذي يرتبط به، والذي يمثل بالنسبة إليه سلطة نهائية ومطلقة، قد يقترب منها ويفنى فيها، وتُكشف له أسرارها، وقد ينأى عنها وتُحجب عنه خصائصها وصفاتها.

يمكن، مع مراعاة اختلاف السياق، أن نستدعي هذه الثنائية إطارًا نظريًا لدراسة واقع السياسية الافتراضية أو عالم السياسة الرقمي، كي تساعدنا في فهم أحد جوانب العلاقة المتوترة بين الأنظمة الرسمية والناشطين السياسيين في منطقة الشرق الأوسط. ووجه الاستدعاء أن هذه العلاقة التي تتم في الوسط الافتراضي الذي قد يشبه في جوانب منه المجال الصوفي في غموضه، تتقلب هي أيضا بين الحجب والكشف في إطار علاقة بين طرف فاعل هو الأنظمة السياسية وطرف منفعل هم الناشطون وصحافيو الإنترنت.

ويُلاحظ أن سياسات الكشف والحجب تمارس في هذا السياق، ضمن طقس رقابي، تسعى من خلاله الأنظمة لأن تسحب معارضيها من عالمهم الافتراضي، إلى حدود العالم المادي، بكل ما يتسم به من قابلية لممارسة التحكم/ النفوذ/ السلطة، على نحو يُجرّد الافتراضي من خصائصه، أو يحتفظ له من بين هذه الخصائص بالقدر المناسب لإخضاعه للمراقبة فحسب. وتثير هذه العلاقة المتوترة من التساؤلات عن طبيعتها وأبعادها، ما تذهب هذه الدراسة إلى أنه يستحق البحث والاستقصاء.

منطلقات الدراسة وإشكاليتها

يتضمن تغلغل الأنظمة السياسية في العالم الافتراضي تطبيقًا عمليًا لثنائية الكشف والحجب، ويتضمن الحضور الكامل في حياة المراقَبين من الناشطين (وغيرهم) أيضًا محاولة جليّة من السلطة لاستباحة كافة المساحات الخاصة للشخص أو الأشخاص المستهدفين، والكشف عن كامل التفاصيل التي تُعبّر عن اهتمامات وأفكار وتفاعلات، الكثير منها قد لا يتعلق بأي درجة بالاعتبارات التي من أجلها تمارس المراقبة أصلًا. وفي مقابل القدرة على الكشف، هناك أيضًا القدرة على الحجب، التي تشير إلى ممارسات الأنظمة لمنع الأفراد من جني ثمار المعلوماتية بأي أسلوب لا يتفق وأغراضها، ومن ذلك حجب الوصول إلى مواقع معيّنة، وحجب نتائج معيّنة من الظهور باستخدام محركات البحث، أو الحجب الكامل للمعلومات عن طريق قطع الاتصال وعزل الأفراد عن الفضاء الرقمي بأكمله.

يطرح ما سبق إشكالية العلاقة بين السلطة والمجال الافتراضي بصفة عامة، فمن الواضح أن السلطة حينما تدخل إلى الافتراضي لا تقبل بأقل من أن تمارس فيه صلاحياتها الكاملة، أو هي بعبارة أخرى تسعى لتجريده من خواصه وتحويله إلى مكان للتحكم والتضييق والمحاصرة، عبر استجلاب خصائص العالم المادي وفرضها عليه، في ما يشبه أن يكون محاولة لتأميم الفضاء الافتراضي، إجهاضًا لطموحات التمكين التي تصوَّر بعضهم أن الحركية السياسية المعاصرة يمكن أن تستفيد منها من خلال استخدام تقانات المعلومات والاتصالات وتوظيفها، وتقييدًا للقدرات التحررية التي كثيرًا ما ربط بعضهم بين التقانات الرقمية وإمكان تحقيقها. هذه الإشكالية هي مما ترى هذه الدراسة أنه يستحق البحث والاستقصاء.

وجهتا نظر حول التمكين الرقمي والحركية السياسية

لا تطمح هذه الدراسة إلى تقييم حدود القدرات التمكينية للتقانة الرقمية والفضاء الافتراضي، أو الأثر الذي أحدثته ثورة المعلومات والاتصالات في "الحركية السياسية"، فالطريقة والمدى التي/ الذي تؤثر بها التقانة الرقمية ووسائل الإعلام الجديدة في العلاقة بين السلطة والمجتمع، لا تزال موضع نقاش كبير[1]. غاية ما ترمي إليه هذه الدراسة هو أن تشتبك، من خلال جهد وصفي وتصنيفي، مع هذا الجدل الذي يمكن أن نُميّز في إطاره بين تيارين أساسيين.

من جهة تذهب بعض الدراسات إلى أن الفضاء الافتراضي[2] يمثل مساحة لممارسة التأثير، لم يتم (أو لا يمكن) الاستحواذ عليها رسميًا. ولعل أوسع ادّعاء يتعلق بالفضاء الافتراضي هو أنه يدفع في اتجاه تحوّل شامل في السلطة من النخب السياسية إلى الأفراد. وفي هذا الصدد، ينظر إلى الفضاء الافتراضي باعتباره مجالًا للتحرر من الاستبداد والقهر والسلطة المركزية عمومًا؛ فعلى خلاف مجتمع الدولة الهرمي، يعتبر الفضاء الافتراضي فضاءً شبكيًا، لا مجال فيه للمركزية والهرمية، بكل ما يتفرع منهما من رقابة وتحكّم وبيروقراطية. فالمجتمعات الافتراضية لا تكاد توجد فيها سلطة نهائية مطلقة، بعبارة أخرى هي مجتمعات لا تعرف ظاهرة "السيادة" بالمعنى الشائع في إطار العلوم السياسية، إنما هي مجتمعات ذاتية الانتظام، من دون الحاجة إلى أي بنى هرمية أو قرارات مركزية تستحضر معنى السلطة[3].

منذ وقت مبكر من عمر الثورة الرقمية، وتحديدًا في منتصف التسعينيات، كان العديد من روّاد المعلوماتية يجادلون بأن الفضاء الافتراضي ينبغي له أن يكون خاليًا من تدخل الأنظمة والحكومات. وفي هذا الصدد اقترح جون بيري بارلو "إعلان استقلال الفضاء الافتراضي" الذي يقضي بألّا تؤدي الحكومات أي دور في تنظيم هذا الفضاء. مؤكدًا أن المجتمع الرقمي سيضع قواعده، ويُدير نزاعاته بمعزل عن القوانين والسلطات القضائية. ومما له أهمية خاصة، وفقًا لهذا الإعلان، ضرورة حماية حرية التعبير والتبادل بين الشخصيات المتفاعلة في هذا الفضاء، مع إخفاء الموقع والهوية المادية لمن يشارك في نشاطاته[4].

وقد تشكلت منظمات، مثل مؤسسة الحدود الإلكترونية Electronic Frontier Foundation، بهدف حماية استخدام الفضاء الافتراضي، موقعًا لتبادل المعرفة والأفكار بحرية. وتسعى هذه المنظمات لتحقيق هذا الهدف، من خلال مجموعة منوعة من الممارسات، بما في ذلك معارضة التشريعات التي يُنظر إليها باعتبارها

---

1 ينظر على سبيل المثال: جمال نون وغسان مراد، **الفعل السياسي الرقمي في العالم العربي ومنظومة القيم والتحولات** (الدوحة: مركز الجزيرة للدراسات، 2019)؛ جوهر الجموسي، **الافتراضي والثورة: مكانة الإنترنت في نشأة مجتمع مدني عربي** (الدوحة/ بيروت: المركز العربي للأبحاث ودراسة السياسات، 2016)؛ كمال عبد اللطيف، **المعرفي، الأيديولوجي، الشبكي: تقاطعات ورهانات** (الدوحة/ بيروت: المركز العربي للأبحاث ودراسة السياسات، 2012)؛ شريف سيف النصر، "السيبرانية: المفهوم، الخصائص، الفرص، الإشكاليات"، **قضايا ونظرات**، العدد 21 (نيسان/ أبريل 2021)، ص 5، 17.

2 على الرغم مما يمكن أن يوجد بينها من اختلافات طفيفة، فإن هذه الدراسة تستخدم تعبيرات مثل الفضاء السيبراني، الفضاء الرقمي، الفضاء الافتراضي، الإنترنت، على نحو مترادف.

3 شريف سيف النصر، "المجتمعات الافتراضية على حافة المواجهات السياسية، ويكيبيديا وأزمات الشرق الأوسط المعلوماتية نموذجًا"، **سياسات عربية**، العدد 44 (أيار/ مايو 2020).

4 John Perry Barlow, "A Declaration of the Independence of Cyberspace," Electronic Frontier Foundation, accessed on 19/10/2022, at: https://bit.ly/3SexWah

تتعارض مع الاستخدام الحر للتقانة، ورفع قضايا أمام المحاكم المختصة للحفاظ على حقوق الأفراد، وتنظيم حملات الدعاية لإعلام الجماهير وإشراكها في مسائل حرية الفضاء الافتراضي والتقانة[5].

على العموم، تذهب وجهة النظر هذه إلى أهمية أن يحتفظ الفضاء الافتراضي باستقلاليته، حيث يمكنه من خلال هذه الاستقلالية أن يمنح المواطنين تأثيرًا أكبر في عملية صنع السياسات، كما يُمكنه أن يتيح للمجتمع المدني الرقمي القيام بدور أفضل، من خلال مراقبة أداء الحكومات وكشف الانحرافات والحيلولة دون التستر عليها؛ الأمر الذي يتوقع أن يفرض على صانعي السياسات الاستجابة بدرجة أكبر للرأي العام الرقمي. ولهذه الاعتبارات وغيرها، يذهب أنصار هذا الرأي إلى القول إن الفضاء الافتراضي والأدوات الرقمية تُبشّر بنوع من "الديمقراطية الرقمية" أكثر نقاءً وفاعلية من الديمقراطية التقليدية[6].

أما وجهة النظر المقابلة، وإن كانت تعترف للفضاء الافتراضي والتقانة الرقمية بنوع من الفاعلية، فإنها تتجنّب المبالغة في الحديث عن قدراتهما التمكينية، نظرًا إلى أنه من خلال هذا الفضاء الافتراضي نفسه، وباستخدام هذه التقانة الرقمية نفسها، يمكن أن تمارس الأنظمة السياسية السيطرة السياسية، أو حتى أن تنخرط في القمع[7]. فمنذ اللحظة الأولى لظهور الفضاء الافتراضي، أظهرت الحكومات اهتمامًا بشأن تنظيمه، وأكدت أهمية أن تبقى الجهات الفاعلة فيه مقيّدة بالقوانين التي تحكم موقعها المادي. وفي هذا الإطار، بدأت الحكومات في تطوير قوانين لتنظيم الاستخدام الرقمي، ومن ذلك تنظيم التجارة الإلكترونية وحقوق الملكية الفكرية الرقمية وحقوق النشر والعلامات التجارية. وتناولت القوانين المُنظّمة للفضاء الافتراضي أيضًا الموضوعات المتعلقة بنشر المواد الإباحية وخطابات الكراهية والتشهير عبر الإنترنت والجرائم الإلكترونية، والموضوعات المتخصصة، مثل أثر التوقيعات الإلكترونية في العقود[8].

من ناحية أخرى، يمثّل أحد مظاهر تدخل الحكومات في الفضاء الافتراضي في ما مارسته هذه من رقابة على المحتوى المعلوماتي، على نحو تضمن في الكثير من الأحيان فرض قيود على الوصول إلى الموارد المعلوماتية، حيث تخشى العديد من الحكومات من الإمكانات التحررية للفضاء الافتراضي؛ لكونه يوفر وسيلة لتجاوز (أو حتى للاستغناء عن) وسائل الإعلام الجماهيرية التي تسيطر عليها الدول عادة. وهكذا، فإنه في التوقيت نفسه التي تولّدت فيها طموحات التحرر من خلال الفضاء الافتراضي، تولّدت مخاوف من نشوء فكرة الأخ الأكبر التقاني e-big brother، فكثيرًا ما جرى تطوير التقانة لخدمة مصالح الأنظمة أو المجموعات القوية، وتقانات المعلومات والاتصالات ليست استثناءً. وعلى عكس الصورة الشائعة بأنها أدوات للتحرير، توفر الهواتف المحمولة وشبكات التواصل الاجتماعي وتقانات الاتصالات والمعلومات، بالفعل لأجهزة الأمن والبيروقراطية، إمكان الوصول إلى كمية هائلة من المعلومات بشأن تحركات الناشطين السياسيين والمواطنين العاديين وآرائهم

5 David J. Gunkel, *Hacking Cyberspace* (Oxford: West View, 2001), p. 14.

6 Erik Ringmar, *A Blogger's Manifesto, Free Speech and Censorship in the Age of the Internet* (London: Anthem Press, 2007), p. 136.

7 Steven Feldstein, *The Rise of Digital Repression: How Technology Is Reshaping Power, Politics, and Resistance* (New York: Oxford University Press, 2021).

8 Barney Warf, *The SAGE Encyclopedia of the Internet* (California: SAGE Publications Inc., 2018), p. xxviii

ونشاطاتهم. على هذا النحو، توفر تقنيات العالم الافتراضي أيضًا وسيلة فعالة جدًا للسيطرة على السلوك المنشق واحتواء المعارضة السياسية[9].

بعبارة أخرى، لا تزال الأنظمة السياسية وفقًا لهذا الرأي صاحبة كلمة عليا، فهي مُطلقة اليد في ممارسة الرقابة والمراقبة والسيطرة على العديد من المنصّات الرقمية، وتملك أيضًا تقييد تدفق (أو حتى التلاعب بـ) المعلومات غير المتوافقة مع أهدافها. وقد أكد تقرير "حرية الإنترنت" 2021، أن المعلومات المضلّلة والدعاية الرقمية التي تمارسها الأنظمة السياسية قد أدّت إلى تسميم المجال العام في العديد من الدول. كما أدّى الجمع الجامح للبيانات الشخصية إلى انتهاك المفاهيم التقليدية للخصوصية. ورصد التقرير زيادة في عدد الدول التي تمارس "الاستبداد الرقمي" من خلال تبنّي النموذج الصيني للرقابة المكثفة والمراقبة الآلية ومحاكاته[10].

تساؤلات الدراسة ونطاقها المكاني

اختبارًا للتصورات السابقة، تسعى هذه الدراسة للوقوف على المدى الذي يمكن أن تبلغه الأنظمة الرسمية في محاولتها فرض خصائص سياساتها الرقابية على العالم الافتراضي. ويتفرّع من هذا عدد من التساؤلات الجزئية، مثل: ما الذي يُميّز الرقابة من المراقبة من القرصنة (الحكومية)؟ وما أبرز مكوّنات كل من هذه الممارسات؟ وما علاقة المراقبة بالقانون؟ وكيف تسكن الأنظمة ممارساتها الرقابية داخل منظوماتها القانونية؟ ولماذا "تتحرر" بعض الحكومات من المنظومة القانونية، على الرغم من قدرتها على تسكين معظم أفعالها الرقابية في داخلها؟ وما مخاطر ممارسة الأنظمة للقرصنة الحكومية؟ وما خصائص الرقابة الرقمية؟

النطاق المكاني للدراسة هو منطقة الشرق الأوسط وشمال أفريقيا (دول العالم العربي، مضافًا إليها كل من تركيا وإيران وإسرائيل)، وهو نطاق تفرضه طبيعة الموضوع، بما ينطوي عليه من تفاعلات بينية، فضلًا عن اشتراك دول هذا النطاق في العديد من الخصائص ذات الصلة؛ الأمر الذي يُبرّر وضعها في بوتقة واحدة. ومما تجدر الإشارة إليه أن منطقة الشرق الأوسط تُعدّ من أكثر المناطق التي تمارس الرقابة على المحتوى الرقمي في العالم. ولا أدلّ على ذلك من أنه بين أربع عشرة دولة شرق أوسطية شملها تقرير Freedom on the Internet لعام 2021، لم تُصنّف أي دولة في المنطقة دولةً "حرة" رقميًا، بينما قُيِّمت ست دول فقط حرةً جزئيًا (العراق، الأردن، لبنان، ليبيا، المغرب، تونس)[11].

وإذا كان التقييم السلبي للحريات الرقمية في المنطقة لم يتغير كثيرًا منذ أن انخرطت دولها في إطار ثورة المعلومات والاتصالات، ابتداء من منتصف تسعينيات القرن الماضي (ولهذا تتكرر الانتقادات التي تُوجَّه إليها من المنظمات العاملة في مجال الدفاع عن حرية التعبير، كونها تمارس ما يطلق عليه "القمع الرقمي"

9 Ibid., p. 134.

10 Adrian Shahbaz & Allie Funk, "Freedom on the Net 2021: The Global Drive to Control Big Tech," Freedom House, 2021, accessed on 19/10/2022, at: https://bit.ly/3eK9QGL; Samantha Bradshaw & Philip N. Howard, "The Global Organization of Social Media Disinformation Campaigns," *Journal of International Affairs*, 29/7/2018, pp. 23-32.

11 "Internet Freedom Scores," Freedom House, accessed on 10/23/2022, at: https://bit.ly/3spT7f7; Ronald Deibert et al. (eds.), *Access Denied: The Practice and Policy of Global Internet Filtering* (Cambridge, MA: MIT Press, 2008), p. 208.

Digital Repression)، فإن النطاق الزمني للدراسة ينهض على أمثلة تتركز بدرجة أكبر على الفترة التي تلت نشوب ثورات الربيع العربي 2011-2021[12].

مفاهيم الدراسة

تُسلّط الدراسة الضوء على مفهومَي الرقابة Censorship والمراقبة Surveillance، حيث تشير الرقابة إلى ما تقوم به الحكومات أو الأجهزة التابعة لها من عمليات يتم بموجبها **حجب** المعلومات أو الآراء أو الأفكار التي تعتبرها مرفوضة أو ضارة أو حساسة أو غير صحيحة سياسيًا أو غير ملائمة، وذلك بطرائق مختلفة، منها ما هو فني، ومنها ما هو قانوني، إما عبر إزالة المواد المستهدفة، وإما عبر تقييد الوصول إليها[13]. أما المراقبة، فتشير إلى تتبع سلوك الأفراد ونشاطاتهم بغرض **الكشف** عمّا يتعلّق بهم من معلومات قد تُستخدَم لممارسة التأثير فيهم لاحقًا. وتختلف المراقبة عن التجسس لكون الأخير بحكم تعريفه سريًا وغير قانوني في العادة، في حين أن معظم أنواع المراقبة علنية ومشروعة (يُقرّها القانون)[14].

وتتعرّض الدراسة أيضًا لمفهوم "القرصنة الحكومية" Government Hacking الذي يشير إلى الممارسات التي تلجأ إليها الحكومات باستخدام أدوات التقانة الرقمية لأغراض التتبع والرصد، ويتضمن ذلك قيام الطرف المهاجم بالوصول عن بُعد وخفية إلى الأجهزة الشخصية وأنظمة المعلومات، ومن ثم إلى جميع البيانات المخزّنة في تلك الأجهزة/ الأنظمة. كما يتضمّن التلاعب بهذه البيانات والمعلومات[15]. ما يميز "القرصنة الحكومية" ويجعل منها ظاهرة مستقلة لا يتعلق إذًا بفعل القرصنة في حد ذاته، إنما بمن يمارسها[16]. فالقرصنة الحكومية هي القرصنة التي يمارسها أشخاص يملكون نوعًا من السلطة الرسمية، أو يجري الاعتراف بسلوكهم وتبنّيه لاحقًا من الحكومات على أنه سلوك موافق لمصالحها (قد يُطلق على النوع الأخير اسم "القرصنة الوطنية" Patriotic Hacking[17]). بهذا المعنى يمكن تعريف القرصنة الحكومية بأنها شكل من أشكال المراقبة الحكومية، غير القانونية، باستخدام التقانات الرقمية. ويتفق العديد من الدراسات على أن

12 تُعرّف هذه الدراسات القمع الرقمي بأنه: "استخدام تقانات المعلومات والاتصالات للمراقبة، أو الإكراه، أو التلاعب بالأفراد، أو الجماعات من أجل ردع نشاطات أو معتقدات محددة تتحدى الدولة"، ينظر:

Feldstein, p. 25; Ronald Deibert et al. (eds.), *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace* (Cambridge, MA: MIT Press, 2010), p. 524.

13 Bernadette H. Schell, *Internet Censorship: A Reference Handbook* (Oxford: ABC-CLIO, 2014) p. 3; Jennifer Earl et al., "The Digital Repression of Social Movements, Protest, and Activism: A Synthetic Review," *Science Advances*, vol. 8, no. 10 (2022).

14 Deibert et al. (eds.), *Access Controlled*, p. 532; Christian Fuchs, *Internet and Surveillance: The Challenges of Web 2.0 and Social Media* (New York: Routledge, 2011), p. 1.

15 Privacy International, "Government Hacking," accessed on 24/10/2022, at: https://bit.ly/3PrgxL1

16 للقرصنة عدد من الدلالات المختلفة بحسب الطرف الذي يمارسها، وبحسب الغرض الذي تُمارَس من أجله. فقد ظهر مفهوم القرصنة في البداية كي يشير إلى المحاولات التي يبذلها بعضهم من أجل فهم تقانة ما بشكل أفضل مما يفهمها به القائمون على هذه التقانة، ولاحقًا أصبح يُقصد بالمفهوم العمليات التي من شأنها أن تدفع التقانة إلى القيام بما يريده المتسلل، بطريقة لم يقصدها المصنع أو المالك أو المستخدم أو لم يتوقعها. ينظر:

Amie Stepanovich, "A Human Rights Response to Government Hacking," Access Now, Sep. 2016, p. 15, accessed on 23/10/2022, at: https://bit.ly/3gAuEB9

17 Forrest B. Hare, "Privateering in Cyberspace: Should Patriotic Hacking Be Promoted as National Policy?" *Asian Security*, vol. 15, no. 2 (2019), pp. 93-102.

عددًا متزايدًا من الأنظمة حول العالم يمارس العديد من مظاهر القرصنة الرقمية. وأنه حتى في الحالات التي تحاول فيها الأنظمة توفيق هذه الممارسات مع الأطر القانونية، فإنها تفعل ذلك على نحو لا يرقى إلى استيفاء الضمانات التي يفرضها القانون الدولي لحقوق الإنسان. ولهذا يُقابَل هذا السلوك بمعارضة العديد من المنظمات الحقوقية التي تعتبر أن "القرصنة الحكومية" وأساليبها وتقنياتها "اجتياحية جدًا"، وتمس بالحق الأساسي في الخصوصية. وتعبّر المنظمات المعنية عن قلقها من أن استخدام تقنيات القرصنة من شأنه أن يعصف بمعايير الخصوصية ويعرّض أمن المعلوماتية للخطر[18].

وإذا كان الناشطون بصفة عامة عرضةً للمراقبة والتضييق، فإن الأمثلة المستخدمة في إطار هذه الدراسة تصدق بدرجة أكبر بحق من يطلق عليهم اسم "الناشطين الرقميين" الذين تشير إليهم بعض المصادر باسم "صحافيي الإنترنت" Internet Journalists، وهم الناشطون، معلومو الهوية، ممن يستخدمون الوسائط الرقمية في إيصال رسائلهم[19]. ويتعرّض هؤلاء للملاحقة القانونية (وللقرصنة غير القانونية أحيانًا)، جراء اتهامات توجّه إليهم، تتعلق عادة بنشر الأخبار الكاذبة ودعم الإرهاب وإساءة استخدام وسائل التواصل الاجتماعي. وفي الكثير من الأحيان تتعلق الممارسات التي يلاحق بسببها كثيرون من هؤلاء الناشطين بانتقادهم رموز الدولة وحكومتها وإجراءاتها الاقتصادية والسياسية. كما يمكن أن يتعرّض هؤلاء الناشطون للتضييق حال نشرهم أخبارًا من شأنها إضعاف الدعم الشعبي للخطابات الرسمية، أو خلخلة الثقة بقدرات أجهزة الدولة على بسط الاستقرار وتحقيق الأمن[20]. وعلى الرغم من محورية دور هؤلاء الناشطين بالنسبة إلى موضوع هذه الدراسة، فإنهم لا يحضرون فيها إلّا على نحو غير مباشر، بوصفهم الطرف المستهدف غالبًا من وراء سياسات الرقابة والمراقبة التي تركز عليها الدراسة بدرجة أكبر.

منهج الدراسة

منهج الدراسة وصفي تصنيفي، يقوم على التمييز بين المفاهيم المستخدمة لوصف طرائق التدخّل الحكومي في المجال العام الرقمي، في محاولة لتعزيز الفهم العام بأساليب التتبع الرقمي للناشطين. وإذا كان الوصف يُمثّل المستوى المنهجي الأدنى من بين مستويات الاستدلال الأخرى، بوصفه "يُخبرنا عن شيء نستطيع اكتشافه

18 Jennifer Stisa Granick, "Challenging Government Hacking: What's at Stake," *ACLU*, 2/11/2022, accessed on 23/10/2022, at: https://bit.ly/3RJHg71; Chen-Yu Li et al., "A Comprehensive Overview of Government Hacking Worldwide," *IEEE Access*, vol. 6 (2018), p. 55053, accessed on 23/10/2022, at: https://bit.ly/3VU7dTt

19 يختلف صحافيو الإنترنت عن القراصنة الرقميين Hacktivists، وهم أولئك الناشطون ذوو الهويات المجهولة الذين تشير إليهم بعض الدراسات باسم المتسللين أو قراصنة المعلومات، ولا تعترف معظم الأنظمة لهم بالحق في ممارسة المعارضة أو الاحتجاج الرقمي، على اعتبار أن ما يقومون به هو أحد أشكال القرصنة غير المقبولة، لكونها تستهدف التأثير في أمن المعلومات وسلامتها، ولهذا تنص معظم تقارير الأمن السيبراني للدول على أن قراصنة المعلومات هم مصدر تهديد، وتضع الاستراتيجيات الأمنية لمحاصرة تأثيرهم. ينظر:

David J. Gunkel, "Introduction to Hacking and Hacktivism," *New Media Society*, vol. 7, no. 5 (2005), pp. 625-646.

20 ترصد المؤسسات المعنية أن عدد من ينتهي به المطاف منهم إلى التوقيف كل عام في جميع أنحاء العالم في ازدياد مستمر. فقد جرى اعتقال 66 صحافيًا عبر الإنترنت في عام 2008، و95 في عام 2009، و116 في عام 2010، وفي عام 2016 ارتفع عدد صحافيي الإنترنت الذين جرى اعتقالهم إلى 157 (من إجمالي 179 صحافيًا معتقلًا)، وفي عام 2021 وصل عدد صحافيي الإنترنت رهن الاعتقال إلى 162، منهم حوالى 90 صحافيًا فقط من منطقة الشرق الأوسط، من إجمالي 293 صحافيًا معتقلًا عبر العالم. ينظر: الأمم المتحدة، مفوّضية الأمم المتحدة السامية لحقوق الإنسان، "المراقبة الرقمية تتعامل مع 'الصحافيين وكأنّهم مجرمون'"، 2022/5/3، شوهد في 2022/10/24، في: https://bit.ly/3cXpddY؛

"294 Journalists Imprisoned," Committee to Protect Journalists (CPJ), 1/12/2021, accessed on 24/10/2022, at: https://bit.ly/3oaPIif

بمجرد النظر إليه"، فإنه ينبغي لنا عدم المسارعة إلى اعتباره مفتقرًا إلى القدرة على تقديم شيء جديد، فالوصف لا يكون دائمًا لظواهر معروفة جيدًا، ففي كثير من الأحيان، تكون الظواهر الاجتماعية متداخلة الأبعاد، ومن ثم يُعدّ النجاح في وصفها على نحو منظم، يجمع التفاصيل المشتتة في نسق واحد، خطوة على الطريق الصحيحة[21]. من ناحية أخرى، يمكن أن يقدم الوصف مدخلًا تصنيفيًا يساعد في تناول الحقائق على نحو تحليلي. من هذه الزاوية، يمكن أن تمثل هذه الدراسة بمقتربها الوصفي نقطة ارتكاز للأبحاث التطبيقية اللاحقة، من خلال توفير ملف تعريفي بأساليب التدخل الرقمي، يساعد في فهم الطريقة التي تتفاعل بها الحركية الرقمية مع المكونات السلطوية.

هذا، وتعتمد الدراسة على مصادر بيانات ثانوية، ممثلة في تقارير المنظمات الدولية المعنية، ذات الموثوقية المعتبرة[22]. وبخاصة تقرير منظمة " فريدم هاوس" Freedom House، تحت عنوان Freedom on the Internet، الذي يُصنّف الحكومات حرة، وحرة جزئيًا، وغير حرة، في ما يتعلق بسياساتها المتعلّقة بالعالم الافتراضي[23]. كما تعتمد الدراسة، وإن بدرجة أقل، على تقارير منظمات أخرى مثل CPJ، Privacy International، Citizen Lab، Access Now، فضلًا عن الكتابات المتخصصة والمعتبرة في هذا المجال.

أولًا: الرقابة

في إطار الرقابة الرقمية، تستخدم الأنظمة تقانة المعلومات والاتصالات لحجب المعلومات عمّن يريدون الوصول إليها؛ إنها إذًا معركة لإفراغ التمكين المعلوماتي من مضمونه، فمن الشائع ألّا تقبل الأنظمة (خاصة السلطوية منها) اكتساب معارضيها زخمًا من خلال توظيفهم التقانات الرقمية. ومن اللافت أنه ضمن الدول العشر الأكثر رقابة على المحتوى المعلوماتي، تأتي دولتان من دول الشرق الأوسط في القائمة (المملكة العربية السعودية وإيران)[24].

لماذا تثير المعلومات قلق الأنظمة؟

ثمة قدرة كامنة للمعلومة على تغيير الواقع، وهذا هو ما يجعل من الوصول إليها عملًا مثيرًا للقلق عند الكثير من الأنظمة. فالوصول إلى المعلومات فعل لا يمكن عكسه، ولا يمكن التراجع عن آثاره. بعبارة أخرى، إن حزم الممكنات الناتجة من استهلاك المعلومات هي حزم غير محددة، ولا يمكن حصرها مسبقًا، لكونها تفتح الباب أمام مجال فاعلية شديد الاتساع إزاء واقع شديد التعقيد، إنها قائمة من احتمالات التحقق العابرة ثنائية هنا والآن[25]. وبناء عليه، فإنه إذا كانت الرقابة التقليدية تحاول منع الأفراد من الوصول إلى شيء ما في مكان وزمان معينين، فإن الرقابة الرقمية، تحاول احتواء الافتراضي الذي تتجاوز إمكانات تحققه ثنائية هنا والآن.

21 إدوارد دو بونو، **التفكير العملي**، ترجمة إيهاب محمد (القاهرة: الهيئة المصرية العامة للكتاب، 1999)، ص 24.

22 ثمة دراسات تقترح تصنيفات مغايرة، مثل دراسة ستيفن فيلدشتاين، التي تميز بين المراقبة، والرقابة، والتلاعب الاجتماعي والمعلومات المضللة، وإغلاق الإنترنت، والاضطهاد المستهدف لمستخدمي الإنترنت. ينظر: Feldstein, p. 25.

23 حول منهجية تصميم هذا التقرير، ينظر:

"Freedom on the Net Research Methodology," Freedom House, accessed on 10/24/2022, at: https://bit.ly/3xgOeb2

24 Committee to Protect Journalists (CPJ), "10 Most Censored Countries," *A special report*, 10/9/2019, accessed on 10/23/2022, at: https://bit.ly/3RBJEMg

25 بيير ليفي، **عالمنا الافتراضي: ما هو، وما علاقته بالواقع؟** ترجمة رياض الكحال (المنامة: هيئة البحرين للثقافة والآثار، 2018).

لهذا الغرض، يلجأ مراقبو (العديد من) الأنظمة إلى الحل المباشر المتمثل في حجب المحتوى الرقمي غير المرغوب فيه؛ أي ممارسة الرقابة على المحتوى الضار من وجهة نظرهم[26]. ويتوقّف نجاح هذا الإجراء، ضمن أشياء أخرى، على قدرة الطرف المراقب على التفكير الاستباقي، فكل ما يمكن أن يفكر فيه المستخدم/ الناشط، يتعيّن استباقه ورصده في إطار قائمة سوداء بالمصطلحات والكلمات والمفردات والعناوين والمواقع، المرشحة للحجب، حيث يجري قطع الطريق أمام من يبحث عنها، أو يحاول الوصول إلى مواقع يمكن أن تشتمل عليها.

تقانيًا، يجري تنفيذ سياسات الرقابة بأكثر من طريقة، أشهرها وأكثرها استخدامًا هي طريقة الفلترة أو التصفية Filtering، وتهدف هذه الطريقة إلى منع الناشطين (وسائر المستخدمين العاديين في حقيقة الأمر) من الوصول إلى المواقع التي تعرض وجهات نظر مغايرة لوجهة النظر الرسمية. وكما تحظر الأنظمة الـمواقع المعارضة، فإنها تحجب كذلك المواقع التي تدعم المتمردين، أو التي تعرض مضمونًا تُصنّفه متطرفًا أو إرهابيًا أو يمثل تهديدًا، من وجهة نظرها، للأمن القومي[27].

على سبيل المثال، تحجب الحكومة الإيرانية المواقع التي ترتبط بمجموعات عرقية، مثل الأكراد وعرب إقليم خوزستان (الأهواز). وتحركت الحكومة أيضًا لحجب المواقع التي تبثّ أخبارًا من منافستها الإقليمية، السعودية. ولمواجهة هذا العمل، حجبت المملكة بدورها المواقع المرتبطة بإيران كافة[28]. وسواء كان المستهدف موقعًا أم مؤثرًا أو موضوعًا، فإنه يجري إعداد قوائم (يجري تحديثها باستمرار) بالمواقع المستهدفة بالحظر، يُخطر بها مزودو خدمات الإنترنت ISP الذين يستخدمون طرائق مختلفة للتصفية، نشير إلى أشهرها في ما يلي[29].

أ. تصفية الحزم

من أشهر الطرائق المستخدمة في التصفية طريقة فلترة الحِزم Packet Filtering. فعندما تُرسل البيانات عبر الإنترنت، يجري تجميعها في وحدات صغيرة تسمى الحزم، تحتوي على محتويات الرسالة، إضافة إلى معلومات عن المرسل والمستقبل. تقوم طريقة تصفية الحزم على فحص محتويات هذه الحزم، وقطع الاتصال الذي يحتوي على كلمات بحث مثيرة للجدل. وقد يتلقى المستخدمون واحدة من "رسائل الخطأ" Error Messages، التي لا تشير صراحة إلى أنهم يخضعون للرقابة[30]. وفي الآونة الأخيرة، بدأ عدد من دول المنطقة (إيران، الإمارات العربية المتحدة، سورية، لبنان على سبيل المثال) في تطوير تقنية تصفية الحزم، عبر ما يطلق عليه "الفحص العميق للحزم" Deep Packet Inspection التي تعطي مقدمي الخدمة القدرة على معرفة الكثير عن سلوك المستخدمين، مثل تحديد موقعهم الجغرافي، تمهيدًا لتتبعهم ومراقبتهم[31].

26 William R. Marczak et al., "When Governments Hack Opponents: A Look at Actors and Technology," 23rd USENIX Security Symposium, San Diego, CA 20–22/8/2014, p. 511.

27 Nick Rahimi & Bidyut Gupta, "A Study of the Landscape of Internet Censorship and Anti-Censorship in Middle East," *EPiC Series in Computing*, vol. 69 (2020), p. 62; Deibert et al. (eds.), *Access Denied*, p. 9.

28 Helmi Noman, "Internet Censorship and the Intraregional Geopolitical Conflicts in the Middle East and North Africa, " Berkman Klein Center Research Publication, no. 1 (2019), at: https://bit.ly/3TXNEsx; Rahimi & Gupta, p. 62.

29 Deibert et al. (eds.), *Access Denied*, p. 210.

30 Ibid., pp. 59, 60.

31 Christian Christensen, "Iran: Networked Dissent," *Le Monde Diplomatique*, 1/7/2009, accessed on 23/10/2022, at: https://bit.ly/3RCJVyr; "Freedom on the Net 2020 (Lebanon)," accessed on 23/10/2022, at: https://bit.ly/3TWCnbL; "Freedom on the Net 2019 (UAE)," accessed on 23/10/2022, at: https://bit.ly/3qpvaDA.

ب. حجب العناوين

تختلف طريقة حجب العناوين Internet Protocol (IP) Address Blocking عن سابقتها في أنها تمنع الاتصال على أساس المكان الذي ستذهب إليه الحزم أو تأتي منه - أي عنوانها، وليس على أساس محتوياتها، كما هي الحال في طريقة تصفية الحزم. وهنا يقوم مراقبو الحكومات بوضع "قوائم سوداء" بعناوين معينة لا يراد للأفراد الوصول إليها. وعندما يحاول المستخدم الوصول إلى عنوان مصنف باعتباره أحد هذه المواقع المحظورة، يقوم "مزود خدمة الإنترنت" بإسقاط الاتصال. وإذا كان العنوان المستهدف بالحظر مستضافًا على خادم استضافة مشترك، يجري حظر جميع المواقع الموجودة على الخادم نفسه. وبصفة عامة، تُعتبر الرقابة القائمة على حجب عنوان الإنترنت من طرائق الرقابة الضعيفة نسبيًا، حيث يُمكن أن تغير المواقع/ الخدمات التي تتعرَّض للحجب، عبر هذه الطريقة، عنوانَ بروتوكول الإنترنت بسهولة، كما يُبطل انتشار خدمات شبكات توصيل المحتوى Content Delivery Network فاعلية هذا النوع من الحجب بدرجة كبيرة. كما أن اضطرار الحكومات إلى حظر خوادم كاملة لمنع الوصول إلى حساب ناشط أو صحافي أو مؤثر هو أمر له تكلفته الكبيرة.

ج. حجب المواقع

تلجأ العديد من الأنظمة إلى استخدام تقنية حجب المواقع Blocking Websites التي ترى أنها تشكل تهديدًا لها. وتُمثّل هذه التقنية طريقة رقابة أكثر دقة، لكنها أكثر تكلفة في الوقت نفسه. ويجري تنفيذها من خلال آلية تصفية عناوين المواقع URL التي تفحص مكوّنات العنوان، بحثًا عن الكلمات المستهدفة. فإذا تضمن العنوان مصطلحات محظورة، يجري حظر الاتصال به[32]. من ذلك، ما قامت به الحكومة التركية في عام 2017 عندما حظرت الوصول إلى موقع **ويكيبيديا** بحجة حماية النظام العام وتعزيزه، كما تحركت السلطات أيضًا لحظر استخدام منصّات التواصل الاجتماعي، مثل "واتساب" WhatsApp و"إنستغرام" Instagram و"فيسبوك" Facebook و"تويتر" Twitter في أعقاب محاولة الانقلاب في عام 2015. وابتداء من عام 2017 صار من حق الأجهزة المعنية في إسرائيل استصدار أوامر قضائية بحجب المواقع التي يُكتشف أنها تنشر محتوى "مسيئًا"[33]. وتُعدّ سورية حاليًا من بين أكثر بيئات الإنترنت رقابة على المواقع، وهو وضع تفاقم بسبب العقوبات الدولية التي فرضت عليها، والتي دفعت بعض المواقع الأجنبية إلى تقييد خدماتها هناك[34]. وفي بعض الأحيان يحظر مزوّدو الخدمة عددًا من المواقع المحايدة سياسيًا (مثل مواقع الترجمة عبر الإنترنت)، خوفًا من استخدامها لتجاوز أنظمة التصفية. كما قد يجري حظر عدد من مواقع التواصل الاجتماعي ومواقع مشاركة الصور والفيديو بسبب احتمالية وجود محتوى مرفوض فيها.

د. رقابة البوابات

يحدث في الكثير من الحالات أن تستخدم الحكومات نفوذها لإجبار الشركات المالكة لمحركات البحث الكبرى على حجب نتائج معيّنة، فيما يعرف بالرقابة على البوابات Portal Censorship، ويقصد بهذه الطريقة

32 Deibert et al. (eds.), *Access Denied*, pp. 37, 43, 210; James Lynch, "Iron Net: Digital Repression in the Middle East and North Africa," European Council on Foreign Relations, 29/6/2022, accessed on 24/10/2022, at: https://bit.ly/3vmwrOT

33 Freedom House, "Freedom on the Net 2022 (Israel)," 3/11/2022, accessed on 24/10/2022, at: https://bit.ly/3qwkfrG

34 Lynch, p. 5.

ممارسة الرقابة على المواقع التي تحتوي في داخلها على محركات بحث Search Engines، وذلك عبر إزالة نتائج معيّنة مما تعرضه؛ ما يجعل النتائج المستهدفة غير مرئية للأشخاص الذين قد لا يعرفون طريقة أخرى للوصول إليها، الأمر الذي يكون له تأثير ممارسة الحجب نفسه[35].

في بعض الأحيان، قد يجري الحجب بتقدير من المسؤولين عن محركات البحث أنفسهم[36]. لكن الغالب أن تجري ممارسة هذا النوع من الرقابة رضوخًا لضغوط الحكومات وتجنّبًا لقرارات أسوأ تتعلق بحظر البوابات بالكامل. وتحاول الشركات الكبرى تطوير قواعد لتحقيق معيار الشفافية في ما يتعلق بالطلبات التي تتلقاها من الحكومات المختلفة لحجب النتائج. تنشر شركة غوغل، على سبيل المثال، تقريرًا مفصلًا عن الدول التي تتقدم بطلبات لحجب المواقع، والمواقع التي يُراد استبعادها من النتائج، والأسباب التي تسوقها الحكومات لتقديم هذه الطلبات، وخلال عام 2021، جاءت تركيا وإسرائيل في مقدمة دول الإقليم التي تقدمت بطلبات حجب لنتائج بحث محركات غوغل لأسباب مختلفة[37].

هـ. قطع الإنترنت

تغامر بعض الأنظمة أحيانًا باتخاذ قرار الانسحاب الكامل من الفضاء الافتراضي، وتقطع الاتصال عن الجميع. تقانيًا، تمثل هذه الطريقة الشكل الأسهل لممارسة الرقابة، لكن على مستوى تقييم الآثار يُعدّ هذا حلًا باهظ التكلفة. وتبرر الحكومات قرار الإغلاق Internet Shutdown بقولها إنه يهدف إلى المحافظة على الأمن العام ومنع انتشار الشائعات، لكن، يكون غرض مثل هذه القرارات، في الأغلب، التضييق على فعاليات معارضة يجري تنظيمها رقميًا. وخلال عام 2021، قطعت دولتان في الإقليم الإنترنت (إيران والسودان)[38]، وبالعودة بالنطاق الزمني إلى فترة نشوب ثورات الربيع العربي، تنضم إلى القائمة العديد من دول المنطقة الأخرى (تركيا، اليمن، مصر، سورية، العراق، الجزائر)[39].

و. إبطاء الاتصال

في إجراء أقل وطأة من الإغلاق الكامل، تلجأ بعض الحكومات إلى إبطاء الاتصال بصفة ملحوظة. وهكذا، بينما تركز تقنيات التدخل الأخرى على حظر الوصول إلى المحتوى أو منعه، يمكن أن تلجأ الحكومات إلى

35 Deibert et al. (eds.), *Access Denied*, p. 37.

36 على سبيل المثال، يقوم المسؤولون عن موقع غوغل في نسختيه الألمانية والفرنسية (Google.de وGoogle.fr) بإزالة قوائم النازيين الجدد والقوائم الأخرى بما يتوافق مع القانونين الألماني والفرنسي.

37 "Government Requests to Remove Content," *Google Transparency Report*, accessed on 23/10/2022, at: https://bit.ly/3PITIlH; Jason Cohen, "These Countries Ask Google to Remove the Most Content," *PC*, 7/1/2022, accessed on 24/9/2022, at: https://bit.ly/3KNg985

38 لا يتضمن هذا الحصر الدول التي قطعت الإنترنت لأسباب تتعلق بالامتحانات العامة، التي تضم كلًا من الجزائر، وسورية، والأردن، والسودان أيضًا. ينظر:

Marianne Díaz Hernández et al., "Internet Shutdowns in 2021: The Return of Digital Authoritarianism," Access Now, 28/4/2022, accessed on 23/10/2022, at: https://bit.ly/3ARGE7M

39 "انقطاع الإنترنت: لماذا تقرر حكومات تعطيل الشبكة العنكبوتية"، **بي بي سي عربي**، 2020/2/25، شوهد في 2022/10/23، في: https://bbc.in/3v6CFSF؛ ينظر أيضًا:

Waseem Abdulali Alsahafi, "The Socio-Political Implications of Social Media Participation and Activism among Young Adults in Saudi Arabia," PhD Thesis, Nottingham Trent University, September 2019, p. 21; Hanna Duggal, "2020 Mapping Internet Shutdowns around the World," *Aljazeera*, 3/3/2021, accessed on 23/10/2022, at: https://bit.ly/3RAdNeI

استراتيجية لا تمنع تمامًا الوصول إلى وجهة أو خدمة معيّنة، لكن بدلًا من ذلك تُقلّل من كفاءة الاتصال بالشبكة ذات الصلة. فالخبرة السيئة، الناتجة من زيارة موقع متدهور الأداء، يمكن أن تدفع المستخدمين إلى أن يختاروا استخدام مواقع أو خدمة أو طريقة اتصال مختلفة، أو حتى ألّا ينخرطوا في الاتصال على الإطلاق إذا لم تكن هناك بدائل. ويوظف العديد من حكومات المنطقة (إيران والسودان) هذا الأسلوب، خصوصًا في الحالات التي يحاول فيها الأفراد الوصول إلى مواقع مشفّرة، وذلك لدفعهم بطريقة غير مباشرة إلى الوصول إلى مواقع بديلة غير مشفّرة يمكن رقابة ما يجرى خلالها من تفاعلات[40].

ز. امتلاك البنية التحتية

تمتلك الكثير من دول المنطقة صلاحيات واسعة إزاء شركات التقانة ومزوّدي خدمات الإنترنت ISPs، حيث تقع هذه تحت الولاية القانونية أو التشغيلية للحكومات المعنيّة. وهنا يمكن أن تفرض الحكومات (ضمن إجراءات أخرى) استخدام آليات التصفية على مزوّدي خدمة الإنترنت، كي يساهموا في إجراءات الرقابة الحكومية على الأفراد.

على الرغم من أنه يمكن تصوّر أن هذه الصلاحيات كفيلة بتحقيق الرقابة المطلوبة، فإنه غالبًا ما تجد الأنظمة أنه من المفيد أن تكون هي المتحكّم في البنية التحتية للمعلومات. ويراوح هذا التحكم بين ملكية البوابات الرئيسة للإنترنت، أي ملكية شبكة الاتصالات السلكية واللاسلكية الرئيسة Internet Backbones، وامتلاك الشركات المسؤولة عن تزويد الأفراد بالخدمات المعلوماتية. فعن طريق امتلاك البوابات، تتمكّن الحكومات من تعقّب حركة المرور غير المرغوب فيها من داخل الدولة إلى خارجها وتصفيتها، والعكس، وعن طريق تأسيس شركات الخدمات الرقمية الحكومية، تتمكّن من رقابة المحتوى الذي ينتقل بين المستخدمين داخل الدولة الواحدة[41].

وقد استفادت العديد من الحكومات في الشرق الأوسط من ملكيتها شبكات الاتصالات السلكية واللاسلكية في حظر الاتصالات غير المرغوب فيها وغيرها من أشكال التبادل المعلوماتي، وكذا في استهداف مستخدمي الشبكات الافتراضية الخاصة VPN، وتطبيقات VoIP المشفّرة المصممة لمنع مراقبة المكالمات. وتشمل الأمثلة كلًا من السعودية، والأردن، والإمارات التي رفعت قيود الاستخدام على إجراء المكالمات عبر كل من واتساب و"سكايب" Skype للزوار الدوليين إلى معرض Expo 2020، قبل أن تستأنف حظر إجراء المكالمات المشفّرة عبر هذين التطبيقين لاحقًا[42].

---

40 Steven Feldstein, "Government Internet Shutdowns Are Changing. How Should Citizens and Democracies Respond?" *Working Paper,* Carnegie Endowment for International Peace, 31/3/2022, p. 10, accessed on 3/11/2022, at: https://bit.ly/3gzuY34; United Nations, "Internet Shutdowns: UN Report Details 'Dramatic' Impact on People's Lives and Human Rights," 23/6/2022, accessed on 3/11/2022, at: https://bit.ly/3IS3ujm

41 Deibert et al. (eds.), *Access Denied*, p. 12.

42 Lynch, p. 5; Freedom House, "Freedom on the Net 2021 (Saudi Arabia)," accessed on 3/11/2022, at: https://bit.ly/3qwDilY; Freedom House, "Freedom on the Internet Report (UAE 2021)," accessed on 3/11/2022, at: https://bit.ly/3qwnDTq

ثانيًا: المراقبة

يحدث، عندما تحجب الحكومات المواقع، أن يلجأ مستخدمو الإنترنت إلى أساليب التفافية تُمكّنهم من الوصول إلى ما جرى حجبه، لكن بعض الأنظمة تناور بدورها من خلال رفع الرقابة وممارسة المراقبة بدلًا منها[43]. فعندما يرفع الحظر عن المواقع، يمكن أن تُستخدَم طعمًا، حيث يجري تتبع المستخدمين الذين عادة ما يتخلّون عن الطرائق الاحترازية (التي تؤدي عادة إلى إبطاء اتصالهم بالإنترنت)، وتكون تكلفة ذلك أن كل ما يفعلونه يصبح قابلًا للتتبع. ونعرض في ما يلي لأهم أشكال المراقبة الحكومية.

1. استخدام البرمجيات الخبيثة

من خلال هذه التقنية، يجري إرسال وتثبيت برمجيات خبيثة Malware/ Spyware في الأجهزة المستهدفة عن بُعد، للحصول على معلومات يجري نقلها (أو تخزينها) إلى/ على أجهزة غير معلومة. تتحكم البرمجيات الخبيثة في أنظمة تشغيل الأجهزة المستهدفة، ما يمنح المتسللين قوة كبيرة، يمكن عن طريقها اختراق الأنظمة الصوتية والبصرية، والاستفادة من تقنيات تحديد المواقع سرًا. كما يُمكنها التقاط لقطات مستمرة لشاشة الجهاز المخترق، ورؤية أي مدخلات أو مخرجات من هذا الجهاز، بما في ذلك تفاصيل تسجيل الدخول وكلمات المرور وسجلات تصفح الإنترنت والمستندات والاتصالات التي قام بها المستخدم. وقد أدّت برامج التجسس دورًا حاسمًا في "احتواء" العديد من الحركات الاجتماعية في الكثير من دول الشرق الأوسط[44]. ويشتهر في هذا السياق قيام الحكومة الإماراتية باستخدام برمجية كارما في إطار مشروع رافن RAVEN لمراقبة المعارضين السياسيين، والمشروع الذي دشّنه النظام السوري في الفترة 2007-2012 لبناء منظومة مراقبة للاتصالات القومية في سورية[45].

2. استغلال الثغرات

قد تكتشف الحكومات (من خلال خبرائها التقانيين) ثغرات أمنية في التقانات الشائعة، تكون غير معلومة لمستخدمي هذه التقانات ولا حتى للشركات المطوّرة لها، ثم تستخدمها في أغراض استقصائية أو أغراض "أخرى". يشار إلى هذا النوع من الثغرات باسم "زيرو داي" Zero-day. وإلى هذه الطريقة في المراقبة باسم استغلال الثغرات Stockpiling[46].

---

43 تجدر الإشارة إلى حقيقة قيام عدد من الدول بالالتفاف على الطرائق الالتفافية للناشطين من خلال العديد من الطرائق، أبرزها تقييد الوصول إلى مواقع الـ "VPN"، نفسها، ومن بين عشر دول عبر العالم تلجأ إلى هذا الإجراء، توجد خمس دول شرق أوسطية (تركيا، العراق، إيران، الإمارات، عُمان). ينظر:

"Which Countries Block VPNs, and Why?" *VPN*, accessed on 24/10/2022, at: https://bit.ly/3TQXOtQ

44 Marc Lynch, "Digital Activism and Authoritarian Adaptation in the Middle East," *Pomeps Studies*, no. 43 (August 2021), p. 5, accessed on 3/11/2022, at: https://bit.ly/3xFzliT

45 "Building Syria's Surveillance State: A Privacy International Investigation," Ifex, 10/1/2017, accessed on 23/10/2022, at: https://bit.ly/3qkJBZq

46 "Government Hacking and Surveillance: 10 Necessary Safeguards," Privacy International, accessed on 23/10/2022, at: https://bit.ly/3SoMsMB; "Government Hacking and Subversion of Digital Security," Electronic Frontier Foundation, accessed on 23/10/2022, at: https://bit.ly/3B3LMaI

من أشهر البرمجيات التي توظِّف هذا النوع من الثغرات برنامج "بيغاسوس" Pegasus حيث كُشف النقاب في عام 2018 عن أن حكومات شرق أوسطية (السعودية، الإمارات، البحرين، عُمان) تستخدمه لمراقبة معارضيها[47]. ويعمل هذا البرنامج من خلال إرسال "رابط تصيُّد" إلى الشخص المستهدف، يجري بوساطة الضغط عليه اختراق حماية هاتفه وتحميل البرنامج عليه[48]. وحالما يقع تحميله، فإنه يبدأ بالاتصال بمركز التحكم، لاستقبال أوامر المتسلل وتنفيذها، ثم يرسل البرنامج البيانات والملفات والرسائل الخاصة بالشخص المستهدف، فضلًا عن مكالماته الصوتية المباشرة. كما يمكن للمتسلل أن يشغل كاميرا الهاتف والميكروفون لالتقاط أي نشاط في المحيط الذي يوجد فيه الهاتف وتسجيله[49].

3. الأبواب الخلفية

يستخدم معظم الأجهزة الرقمية اليوم أنظمة للتشفير Encryption، تمنع أي شخص، بخلاف صاحب الجهاز، من استخدامه، من خلال تقديمه ما يسمح بالتحقق من هويته؛ كلمة مرور أو بصمة إصبع أو من خلال تقنية التعرف إلى الوجه. تساعد هذه الأنظمة في حماية البيانات الشخصية. فحتى إذا وقع الجهاز الرقمي في يد شخص ما، فإنه لن يتمكّن من الوصول إلى المعلومات الموجودة في داخله إلّا إذا عرف رمز المرور الخاص بصاحب الجهاز الأصلي. وفي إطار أنظمة التشفير الشائعة، عادة ما يجري إغلاق الجهاز كليًّا، أو جعله غير قابل للاستخدام لفترة، إذا حاول شخص ما تجاوز إجراء التحقق من الشخصية عدة مرات بصورة خاطئة[50].

يمثل الباب الخلفي أو Backdoor طريقة مدمجة في نظم التشغيل للتحايل على هذا النوع من التشفير، حيث يسمح بصفة أساسية للمُصنّع بالوصول إلى البيانات الموجودة على أي جهاز يقوم بصنعه (في حال مثلًا نسي المستخدم كلمة المرور التي اختارها بنفسه). وهناك طرائق كثيرة يمكن من خلالها تطوير أبواب خلفية لأنظمة التشفير؛ إذ يمكن أن تأتي على شكل جزء مخفي من نظام تشغيل الجهاز نفسه، أو برمجية خارجية يمكن استخدامها مفتاحًا للوصول إلى الجهاز، أو كودٍ معيّن يخلق ثغرة في البرنامج للتحكم فيه[51].

---

47 "Pegasus Affair: Who Was Wiretapped in the Middle East?" Warsaw Institute, 30/8/2021, accessed on 23/10/2022, at: https://bit.ly/3AUnVIM; Bill Marczak & John Scott-Railton, "The Million Dollar Dissident: NSO Group's iPhone Zero-days Used Against a UAE Human Rights Defender," *The Citizen Lab*, 24/8/2016, accessed on 23/10/2022, at: https://bit.ly/2rRi8ke; Bill Marczak et al., "Journalists Hacked with Suspected NSO Group iMessage 'Zero-Click' Exploit," *The Citizen Lab*, 20/12/2020, accessed on 23/10/2022, at: https://bit.ly/3L2h04V

48 في الإصدارات الحديثة، جرى التخلّي عن هذا الشرط، وأصبح الاصطياد عن طريق تقانة الـ Zero-click Attacks التي لا تتطلب الضغط على أي رابط. ينظر:

"What is Zero-click Malware, and How do Zero-click Attacks Work?" *Kaspersky*, accessed on 23/10/2022, at: https://bit.ly/3KVpmey; Marczak et al.

49 طورت الولايات المتحدة الأميركية منظومة The Vulnerability Equities Process, VEP التي توازن من خلالها بين الاعتبارات المختلفة حول الكشف عن نقاط ضعف البرامج، أو الاستمرار في استغلالها لأغراض إنفاذ القانون أو لأغراض استخباراتية. بطبيعة الحال يؤدي الإفصاح عن الثغرات إلى تمكين الشركات المعنية من تصحيحها وحماية الأمن المعلوماتي لمستخدمي منتجاتها، وبالعكس، فإن عدم الكشف عن هذه الثغرات يبقي هذه الشركات ومستخدميها تحت رحمة الإدارات الأميركية. وهو الأمر الذي تعارضه الشركات الأميركية بقوة. ينظر:

Bill Chappell, "WannaCry Ransomware: Microsoft Calls Out NSA for 'Stockpiling' Vulnerabilities," *National Public Radio*, 15/5/2017, accessed on 23/10/2022, at: https://n.pr/3v6Bzqa

50 "Government Hacking and Subversion of Digital Security."

51 Chris Wysopal, Chris Eng & Tyler Shields, "Static Detection of Application Backdoors," *Datenschutz und Datensicherheit-DuD*, vol. 34, no. 3 (2010), pp. 149-155.

في هذا السياق، تعمد بعض الحكومات إلى محاولة فك الشيفرات المستخدمة في تأمين بيانات الأفراد وأجهزتهم، سواء من خلال سن تشريعات تعطيها هذا الحق، أم عبر إجبار الشركات المصنعة هذه التقانات على الرضوخ والسماح لها بالولوج إلى أنظمة أجهزتها المشفرة. وتجادل الحكومات التي تريد تجاوز أنظمة التشفير بأن البيانات المراد الوصول إليها تستخدم من وكالات إنفاذ القانون، نظرًا إلى أن الكثير من التحقيقات قد تعطل في الماضي؛ لأن سلطات إنفاذ القانون لم تتمكن من فتح الأجهزة المشفرة للمشتبه بهم[52].

على الرغم من أن تجاوز أنظمة التشفير قد يكون بالفعل أمرًا ضروريًا لإجراءات التحقيق، عبر الاطلاع على المعلومات الشخصية للمشتبه بهم، فإنه من المفهوم أيضًا أنه قد يجري استخدام طريقة "الأبواب الخلفية" لأغراض تتعلق بمراقبة المعارضين والناشطين السياسيين، والوصول إلى بياناتهم الشخصية، وانتهاك خصوصيتهم[53].

4. تقنية المستنقع

من الأشكال الشهيرة للمراقبة الحكومية ما يعرف باسم تقنية المستنقع Watering Hole، وهذا الاسم مستوحى من فكرة "تسميم" مصدر مياه رئيس على نحو يتسبب بعد ذلك بإصابة أي شخص يشرب منه. كما أنه يستحضر أيضًا صورة وجود مفترس متربص بالقرب من مصدر مياه في انتظار الفريسة التي لا بد من أن تتوقف عنده. ووجه الشبه أن هذه الطريقة تتضمن قيام طرف (رسمي أو غير رسمي) بالسيطرة على موقع ما (قد يكون هو نفسه موقعًا رسميًا)، ويبدأ من خلاله بنشر برمجيات ضارّة على الأجهزة التي تزور هذا الموقع. ويمكن تثبيت هذه البرمجيات بمجرد نقر المستخدم على رابط بعينه داخل هذا الموقع، أو حتى بمجرد وصوله إلى الموقع من دون الضغط على أي روابط، فيما يعرف بأسلوب النقرة الصفرية Zero-click. وهنا تبدأ هذه البرمجيات بالتحكم في المحتويات المعلوماتية، قبل أن ترسلها إلى المصدر (المتسلّل)[54].

تشير الدراسات إلى أنه على الرغم من أن هجمات مستنقع المياه قد تبدو عشوائية، فإنه عادة ما يكون لدى الطرف المراقِب (الأجهزة الرسمية في حالتنا) القدرة على استهداف ضحاياه بدقة كبيرة، مثلًا، بحسب نوع الجهاز أو عبر استهداف مستخدمي متصفّحات بعينها، أما الطريقة الأهم في هذا الصدد، فهي عن طريق تحديد البلد الذي يأتي منه عنوان الإنترنت IP الخاص بالطرف المستهدف. وتؤكدESET (إحدى شركات أمن الإنترنت) أنها تكتشف هجمات عدة، تتم بهذه الطريقة في كل عام، كما تكتشف مجموعة تحليل المخاطر TAG التابعة لشركة غوغل Google هجومًا واحدًا على الأقل شهريًا[55]. وقد أظهرت النتائج التي توصلت

52 Julia Carrie Wong, "US, UK and Australia Urge Facebook to Create Backdoor Access to Encrypted Messages," *The Guardian*, 4/10/2019, accessed on 23/10/2022, at: https://bit.ly/2Oho4z5; "Governments Want Encryption Backdoors: New Report Examines the Legal and Policy Implications," Access Now, 14/2/2018, accessed on 23/10/2022, at: https://bit.ly/2FlKARa

53 Tim Jordan, *CyberPower: The Culture and Politics of Cyberspace and the Internet* (London: Routledge, 1999), p. 134.

54 Jelle Van Haaster et al., *Cyber Guerilla* (London: Elsevier, 2016), pp. 57, 58.

55 "Hacker Lexicon: What Is a Watering Hole Attack?" *WIRED*, 28/11/2021, accessed on 23/10/2022, at: https://bit.ly/3RPpEGU

إليها ESET أن المواقع الرقمية التي جرى اختراقها بهذه الطريقة في عام 2021 قد ضمّت مواقع حكومية في كل من السعودية واليمن وإيران وسورية[56].

5. طرائق أخرى للمراقبة الرقمية

على خلاف المراقبة التقليدية، تفتح المراقبة الرقمية المجال أمام احتمالات متجددة، فهي لا تكتفي بإنتاج فعل المراقبة، إنما تُنتج أهدافًا جديدة، وتضيف إلى المراقبة معانيَ جديدة؛ ذلك أنها على خلاف المراقبة التقليدية، ما عادت مجرد عملية تتبع جامدة، إنما تقترح بدائل ربما لم تكن في ذهن من قام بتوظيف هذا النوع من المراقبة في الأصل. بعبارة أخرى تشهد المراقبة الحالية تغيّرًا في قواعد الفعالية، ومعايير التقويم والمنفعة[57].

بناء عليه، يمكن القول إن المراقبة الرقمية لم تؤدِّ إلى تسريع ما كان يمكن القيام به على نحو أبطأ فحسب، لكنها أصبحت أداةً لتنويع الهدف والتفكير في احتمالات جديدة، من ذلك ما يعرف بالمراقبة التنبؤية Predictive Policing، القائمة على أساس استخدام البيانات التاريخية الضخمة لصوغ الاستراتيجيات المستقبلية[58]، وهناك أيضًا المراقبة باستخدام كاميرات الـ CCTV والمراقبة باستخدام الطائرات المسيّرة، وغيرها من الأساليب[59].

من ناحية أخرى، ما عادت المراقبة الرقمية تقتصر على مراقبة المواقع، أو التنصت على الاتصالات، إنما أصبحت أداة للتعرّف إلى ملامح الوجوه والانفعالات وقراءة الأفكار والتعرف إلى الأصول العرقية للأشخاص[60]. وينشط العديد من دول الخليج في توظيف تقانة التعرف إلى الوجوه، وتجمع في هذا الصدد الكميات الهائلة من البيانات والمعلومات البيومترية، مستفيدة من التعاون مع شركات مهمة في هذا المجال مثل NTechLab، المملوكة جزئيًا للحكومة الروسية، التي تدّعي أن منتجاتها يمكنها التعرّف إلى عواطف الأفراد ومشاعرهم[61]. كما تتعاون الإمارات مع شركة "سينس تايم" SenseTime، الصينية التي سبق لها أن طوّرت نظامًا للتعرف إلى وجوه المنتمين إلى قومية الإيغور، وقد ترجم هذا التعاون بقيام الشركة الأخيرة بإنشاء مركز للبحث والتطوير في مدينة أبوظبي. وبشكل عام، فإن ثمة توافقًا ملحوظًا بين مصالح شركات التقانة التي تجمع البيانات الشخصية كجزء من نموذج أعمال يُطلق عليه أحيانًا اسم "رأسمالية المراقبة"، ومصالح الأنظمة التي

56 "ESET Research Discovers Watering Hole Attacks on Websites in the Middle East with Links to Candiru Spyware," *Eset*, 22/11/2021, accessed on 24/10/2022, at: https://bit.ly/3CT7jBW

57 ليفي، ص 103.

58 تشهد هذه الطريقة انتشارًا في العديد من الدول، على الرغم مما تُظهره الدراسات من أن خوارزمياتها تميل إلى التمييز ضد المجتمعات المهمّشة أو المستبعدة بالفعل. ينظر:

Albert Meijer & Martijn Wessels, "Predictive Policing: Review of Benefits and Drawbacks," *International Journal of Public Administration*, vol. 42, no. 12 (2019), pp. 1031-1039.

59 James Lynch, "Iron Net"; Cathy O'Neil, *Weapons of Math Destruction, How Big Data Increases Inequality and Threatens Democracy* (New York: Crown Publishers, 2016); Rashida Richardson, Jason M. Schultz & Kate Crawford, "Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice," *The New York University Law Review*, vol. 94, no. 15 (2019), pp. 193-223.

60 Ana Swanson & Paul Mozur, "U.S. Blacklists 28 Chinese Entities Over Abuses in Xinjiang," *The New York Times*, 7/10/ 2019, accessed on 23/10/2022, at: https://nyti.ms/31Zvpre

61 Chris Burt, "Qatar Equips 15,000 Cameras with Facial Recognition for Soccer World Cup 2022," *Biometrics Updates*, 18/8/2022, accessed on 23/10/2022, at: https://bit.ly/3RTBxL5

تجمع البيانات الشخصية لأغراض الرقابة الاجتماعية[62]. شجّع هذا التوافق الموضوعي العديد من الشركات الأخرى على تقديم خدماتها لأنظمة المنطقة، نعرض في ما يلي أشهرها.

أ. شركة غاما الدولية

من أشهر الشركات العالمية المتخصصة في برمجيات المراقبة، التي ذاع صيتها بسبب تسويقها برنامج "فين فيشر" FinFisher، المعروف أيضًا باسم "فين سباي" FinSpy، وهو برنامج مراقبة يجري تثبيته على الأجهزة المستهدفة، من خلال استغلال الثغرات الأمنية في إجراءات تحديث البرامج، وعبر مرفقات رسائل البريد الإلكتروني أيضًا، وعيوب الأمان في البرامج الشائعة. كما يمكن تثبيت البرنامج، المصمم لتجنب الاكتشاف عن طريق برامج مكافحة الفيروسات، في الهواتف المحمولة للعلامات التجارية الكبرى كافة[63]. وتروّج شركة "غاما إنترناشيونال" Gamma International الأنكلو-ألمانية لمنتجاتها على مستوى الحكومات، وتتيح التدريب على استخدام برمجياتها التي توفرها من خلال العديد من اللغات، ومنها اللغة العربية بطبيعة الحال، لكون السوق العربية (الإمارات، لبنان) مستهلكًا شرهًا لهذا النوع من البرمجيات[64].

ب. هاكينغ تيم

من جانبها تقدم شركة "هاكينغ تيم" Hacking Team - والتي تحولت الآن إلى اسم "ميمنتو لابز" Memento Labs الإيطالية - برمجياتها المعدّة لأغراض المراقبة إلى الحكومات وهيئات إنفاذ القانون في الدول الديمقراطية والسلطوية على حد سواء. وقد اشتهرت بمنظومة RCS (ثم بعد استحواذ شركة "إن ذي سايبر" In TheCyber عليها، اشتهرت بمنظومة "كرايت" KRAIT التي يمكنها السيطرة على الهواتف العاملة بنظام "أندرويد" Android)[65].

في عام 2015، أظهرت وثائق مُسرّبة من الشركة قيام العديد من الحكومات الشرق أوسطية بشراء أنظمتها. وقد كشفت منظمة Citizen Lab الكندية غير الحكومية أن العديد من حكومات المنطقة قد استفادت من منتجات الشركة لتتبع نشاطات خصومها السياسيين من صحافيي الإنترنت وناشطي حقوق الإنسان وغيرهم[66]. وفي العام التالي، منعت الحكومة الإيطالية الشركة من تصدير منتجاتها خارج الاتحاد الأوروبي، بعد ظهور أدلة على استخدامها على نحو ارتبط بانتهاكات لحقوق الإنسان. لكن بفعل (ما بدا أنه) نوع من التحايل، استمرت الشركة بتسويق منتجاتها في دول المنطقة. وقد تعرّضت الشركة لانتقادات واسعة بسبب

62 Lynch, "Iron Net"; Alina Polyakova & Chris Meserole, "Exporting Digital Authoritarianism: The Russian and Chinese Models," *Policy Brief, Democracy and Disorder Series* (Washington, DC: Brookings, 2019), pp. 1-22.

63 Jennifer Valentino-Devries, "Surveillance Company Says It Sent Fake iTunes, Flash Updates," *The Wall Street Journal*, 21/11/2011.

64 Marczak et al., p. 511; Freedom House, "Freedom on the Net 2021 (Lebanon)"; Freedom House, "Freedom on Net 2021 (UAE)".

65 Lynch, "Iron Net."

66 Patrick Howell O'Neill, "The Fall and Rise of a Spyware Empire," *MIT Technology Review*, 29 November 2019, accessed on 24/10/2022, at: https://bit.ly/3ojRbmc; Bill Marczak, "Mapping Hacking Team's 'Untraceable' Spyware," *The Citizen Lab*, 17/1/2014, accessed on 24/10/2022, accessed on 24/10/2022, at: https://bit.ly/3qvNDys

تقديمها هذه القدرات لحكومات وأنظمة لديها سجلات حقوقية معيبة، على الرغم من أن ميثاق الشركة ينص على أن لها الحق في إيقاف برامجها إذا جرى استخدامها بطريقة غير أخلاقية[67].

ج. مجموعة NSO

شركة مجموعة "إن إس أو" NSO Group هي الشركة المالكة لبرنامج التجسس الشهير بيغاسوس. تدّعي هذه الشركة أنها تزوّد ببرمجياتها الحكومات المستهدفة بالهجمات الإرهابية فحسب لمساعدتها في مكافحة الإرهاب. وتعمل الشركة تحت الولاية القانونية للحكومة الإسرائيلية، التي تصنف برنامج بيغاسوس سلاحًا، حيث يجب على الشركة الحصول على موافقتها قبل تصديره إلى أي حكومة أجنبية[68]. ووفقًا للعديد من التقارير، فقد جرى استخدام برامج مجموعة "إن إس أو" لاستهداف ناشطي حقوق الإنسان وصحافيي الإنترنت في دول مختلفة، كما جرى استخدامها للتجسس الحكومي ضد دول معادية لإسرائيل، وكذا في أعمال للمراقبة قامت بها الشرطة الإسرائيلية إزاء مواطنين "من عرب الداخل". كما يُرجّح أنه كان لهذه التقنية دورٌ في عملية اغتيال المعارض السعودي جمال خاشقجي[69].

بخلاف مجموعة "إن إس أو"، تتعاون العديد من الشركات الإسرائيلية مع أنظمة المنطقة وتقدم لها خدماتها، بموافقة الحكومة الإسرائيلية. ومن ذلك شركة "كانديرو" Candiru الناشطة في مجال إنتاج برامج القرصنة[70]، وكذا شركة "سيليبرايت" Cellebrite (المملوكة لشركة "صن كوربوريشن" Sun Corporation)، والتي قدّمت في عام 2020 خدماتها لإحدى الدول العربية (السعودية) لمساعدتها في مراقبة المعارضين السياسيين. كما تنشط في هذا الإطار العديد من الكيانات الأمنية الرسمية، ولا سيما وحدة النخبة 8200 التابعة لجيش الدفاع الإسرائيلي، التي يشار إليها أحيانًا باسم "وكالة الأمن القومي الإسرائيلية". وقد ارتبطت هذه الوحدة بمراقبة الناشطين الفلسطينيين من خلال "جمع معلومات مسيئة في خصوصهم"[71].

وتختبر العديد من الشركات الإسرائيلية، العاملة في مجال الأمن السيبراني والمتعاونة مع الجيش الإسرائيلي، تقنياتها، عبر عمليات تُجرى على الفلسطينيين. على سبيل المثال، قامت شركة "أني فيجن" AnyVision (التي تسمى الآن "أوستو" Oosto) باختبار منظومتها (الخاصة بالتعرف إلى الوجوه) على مواطني الضفة الغربية قبل أن تقوم الشركة بتسويق منتجاتها للمراقبة وبيعها على أنها "مختبرة ميدانيًا". يذكر أن شركة أني فيجن تستفيد بطريقة غير مباشرة من دعم عدد من الأنظمة العربية التي تستثمر في مجال تقنيات تطوير الذكاء الصناعي لأغراض المراقبة. وبشكل عام فقد أدّت تقنيات "الأمن السيبراني" دورًا محوريًا في تعميق الروابط الاستراتيجية بين إسرائيل والعديد من جيرانها العرب، وهي العملية التي بلغت ذروتها بتوقيع إسرائيل الاتفاقيات الإبراهيمية مع عدد من الأطراف الإقليمية (الإمارات، البحرين) في عام 2020[72].

67 Ibid.

68 بلغت قيمة صادرات الأمن السيبراني الإسرائيلية 11 مليار دولار، أي ما يعادل تقريبًا صادراتها من الأسلحة. ينظر: Lynch "Iron Net".

69 Miles Kenyon, "A UAE Agency put Pegasus Spyware on Phone of Jamal Khashoggi's Wife Months before his Murder, New Forensics Show," *The Citizen Lab*, 21/12/2021, accessed on 24/10/2022, at: https://bit.ly/3L3TK6o

70 Bill Marczak et al., "Hooking Candiru: Another Mercenary Spyware Vendor Comes into Focus," *The Citizen Lab*, 15/7/2021, accessed on 24/10/2022, at: https://bit.ly/3DdmmZa

71 Lynch, "Iron Net."

72 Richard Silverstein, "Israel Is Hacking the Phones of Palestinian NGOs," *Jacobin*, 13/11/2021, accessed on 24/10/2022, at: https://bit.ly/3xhvkRr

بخلاف الشركات السابقة، تتعاون أنظمة المنطقة مع عدد من شركات الأمن السيبراني الأخرى (مثل DarkMatter, Nexa Technologies, Sandvine, Ercom (Thales), Suneris, Dassault Système, Blue Coat Systems, Narus)، كما تلجأ إلى توظيف خبراء سابقين في وكالات الأمن القومي الغربية، للمساعدة في تطوير قدراتها الخاصة في مجال المراقبة الرقمية. ويشتهر في هذا الصدد نموذج منصة "كارما" Karma التي تسمح باختراق منظومات أجهزة الهواتف الخلوية، وبرمجية "بروكسي إس جي" ProxySG التي تتيح استخدام تقنية الفحص العميق للحزم لتحديد الموقع الجغرافي للمستخدمين واختراق معظم تطبيقات التواصل الاجتماعي، وبرمجتا "كورتكس" Cortex و"فورتكس" Vortex اللتان تُتيحان اعتراض المكالمات والرسائل النصّية ومراقبة حركة الإنترنت أو تحديد الموقع الجغرافي لهدف ما[73].

6. المراقبة والقانون

لا تُمارَس نشاطات التتبع الرقمي عادة من دون غطاء قانوني، ولهذا عندما تمارس حكومة ما "المراقبة"، فإن الاحتمال الأقرب أنها تفعل ذلك بطريقة تُقرّها قوانينها الداخلية، يدخل في ذلك قيامها بأعمال المراقبة بغرض جمع الأدلّة في التحقيقات الجنائية أو الاستخبارية. ففي كثير من الحالات، تقوم الحكومات باختراق الأجهزة الرقمية جزءًا من التحقيقات الجنائية المشروعة، وبخاصة في الحالات التي يقوم فيها المشتبه بهم باستخدام برامج إخفاء الهوية. وهنا، ولتحديد من يقف وراء جريمة ما، قد تلجأ الأجهزة الرسمية إلى تثبيت برمجيات خفية، أو استخدام "تقنية استقصاء الشبكة" NIT للبحث عن معلومات على الجهاز الرقمي للهدف، قبل أن تقوم بإرسالها إلى الأجهزة المعنية. ومع الكشف عن موقع المشتبه به (وربما هويته)، يمكن أن يركز التحقيق على هذا الهدف والمضيّ قدمًا بالطريقة المعتادة[74].

من ناحية أخرى، عادة ما تفضي إجراءات المراقبة إلى نوع من التدابير القانونية في حق متداولي المحتويات المحظورة. والأمر نفسه في ما يتعلق بمراقبة مواقع التواصل الاجتماعي، حيث تقوم الأنظمة بمتابعة ما يقوم الأفراد عمومًا، والناشطون والمؤثرون خصوصًا، بنشره، ويجري هنا أيضًا ملاحقة الأفراد المُدانين. ولهذا الغرض، تبنّت العديد من الدول تعديلات تشريعية، أضفت بموجبها الصفة القانونية على ممارسات المراقبة الرقمية التي تقوم بها أجهزتها الأمنية.

وقد حدثت الطفرة الحقيقية في هذا الصدد بعد صدمة "الربيع العربي"، حيث سنّت/ عدّلت معظم حكومات المنطقة قوانين لفرض قيود على المحتوى الرقمي، وعلى القدرة على الوصول إليه، تضاهي القيود المطبّقة على المحتوى الصحافي والإعلامي. وقد شملت هذه القوانين، قوانين الصحافة والنشر، قوانين الطوارئ، قوانين مكافحة الإرهاب، القوانين الخاصة بالإنترنت، شروط مزوّدي خدمات الإنترنت وأحكامهم، وقوانين الاتصالات[75].

73 Lynch, "Digital Activism and Authoritarian Adaptation in the Middle East."

74 Ahmed Shaheed, "Binary Threat: How Governments' Cyber Laws and Practice Undermine Human Rights in the MENA Region," *Project on Middle East Political Science (POMEPS)*, accessed on 24/10/2022, at: https://bit.ly/3RB4pIt

75 Deibert et al. (eds.), *Access Controlled*, p. 526.

كما أُدخلت العديد من التعديلات القانونية على قوانين هي أصلًا استثنائية بطبيعتها، مثل التعديلات التي أُعلن عن أن الهدف من ورائها هو مواجهة انتشار وباء فيروس كورونا المستجد (كوفيد-19)، وهو الظرف الذي قابلته الكثير من حكومات المنطقة بتعديلات/ قوانين تجرّم النشر (ومن ضمنه النشر الرقمي) تعليقًا أو تعقيبًا على الأداء الحكومي، على اعتبار أن انتقاد الأداء الحكومي في تلك الأزمة يمثل نوعًا من التهديد للسلم والأمن الاجتماعيين[76] (بشكل عام، قدمت جائحة كوفيد-19 للحكومات في جميع أنحاء الإقليم سببًا مقنعًا لجمع مكثف للبيانات الشخصية الخاصة بالأفراد)[77].

بموجب هذه التشريعات والتعديلات، أصبح من الوارد أن يعتبر نشر التعليقات جريمة يعاقب عليها القانون، وذلك إذا اعتبرت الحكومات أنها تمثل تهديدًا لمصالح الدولة أو لأمنها العام. كما جرى (في الكثير من الأحيان) الخلط بين النقد السياسي وتهمة نشر "الأخبار الكاذبة" وغيرها من أشكال المعلومات المُضلِّلة، ما سمح للكثير من الحكومات بتوصيف ما تمارسه من "ملاحقات قانونية" على أنه نوع من الدفاع عن الأمن الداخلي والسلام الاجتماعي. وقد جرى اعتقال العديد من الناشطين الرقميين وصحافيي الإنترنت ومستخدمي شبكات التواصل الاجتماعي العاديين في العديد من دول المنطقة بموجب هذه القواعد الجديدة[78].

أثارت هذه الإجراءات تساؤلات مكثفة حول الحدود المسموحة للنشاطين الصحافي والإعلامي (الرقميين)، وحول حرية التعبير عمومًا في المجال الافتراضي، خصوصًا في ضوء تعدد الجهات الحكومية التي بادرت إلى اتخاذ إجراءات عقابية ضد صحافيي الإنترنت، فضلًا عن الإجراءات الأمنية والإدارية التي اتُّخذت ضد كل من يستخدم أدوات العالم الافتراضي في التعبير عن وجهات نظر مخالفة لوجهة النظر الرسمية، أو منتقدة لأداء الحكومات[79].

وقد ساعد غموض مفهوم "الأمن السيبراني" وعدم وجود توافق دولي على ما يشكّل تهديدًا أمنيًا في المجال الافتراضي، الأنظمة في إضفاء المشروعية على مختلف الاستراتيجيات المستخدمة في مجال السياسية الرقمية[80]. وفي هذا السياق جرى، في العديد من الدول، استحداث وحدات للرصد والمتابعة، تتولّى تحريك دعاوى قضائية ضد مستخدمي ومستخدمات مواقع التواصل الاجتماعي، بناء على مراقبة مواقعهم، وصفحاتهم على نحو قانوني ورسمي، بدعوى حماية الأمن القومي والأمن الاجتماعي والقيم الأسرية[81]. كما أصبحت أجهزة النيابة العامة في العديد من دول المنطقة حاضرة في معظم المنابر الافتراضية، لمتابعة ما يُنشر فيها من "أكاذيب وأخبار غير حقيقية" تستهدف "أمن الوطن وسلامته"، واتخاذ الإجراءات القانونية اللازمة حيال أصحاب

76 "تجفيف منابع الحرية"، مؤسسة حرية الفكر والتعبير، 2022/2/22، شوهد في 2022/10/24، في: https://bit.ly/3B3MFjn؛ وينظر أيضًا:
Zeina Hobaika et al., *The MENA Region and COVID-19: Impact, Implications and Prospects* (Oxon: Routledge, 2022); Binoy Kampmark, "The Pandemic Surveillance State: An Enduring Legacy of COVID-19," *Journal of Global Faultlines*, vol. 7, no. 1 (2020), pp. 59-70.

77 Lynch, "Iron Net," p. 13.

78 "أبرز أنماط الانتهاكات في ملفات حرية التعبير"، مؤسسة حرية الفكر والتعبير، 2022/1/22، شوهد في 2022/10/24، في: https://bit.ly/3MWlMBY

79 "تجفيف منابع الحرية".

80 Lynch, "Iron Net."

81 "التحول الرقمي في النيابة العامة، مدخل للمراقبة الجماعية على الإنترنت"، مؤسسة حرية الفكر والتعبير، 2021/8/8، شوهد في 2022/10/24، في: https://bit.ly/3B1P6mD؛ "المراقبة الجماعية، ممارسة ممنهجة في مؤسسات الدولة"، مؤسسة حرية الفكر والتعبير، 2022/5/26، شوهد في 2022/10/24، في: https://bit.ly/3oniKuW

هذه المنشورات. وتلجأ هذه الوحدات إلى مراقبة حسابات المتّهمين على مواقع التواصل الاجتماعي، إلى جانب انتدابها خبراء من إدارات مكافحة جرائم الحوسبة وشبكات المعلومات لحصر الصفحات والحسابات محل الاتهام، تمهيدًا لاتخاذ الإجراءات القانونية ضدّها، بحسب ما تنص عليه قوانين مكافحة جرائم تقنية المعلومات[82].

على العموم، لقد أصبحت الملاحقات الأمنية شائعة؛ ما أثّر في جميع أنواع مستخدمي الإعلام الرقمي ووسائل التواصل الاجتماعي، وساهم في حصار المجال الافتراضي، وأضفى عليه الكثير من خصائص المجال العام التقليدي. وهو الأمر الذي قابلته العديد من المنظمات الدولية بالنقد الحاد، وبخاصة لكون قرارات إنشاء وحدات الرصد التي تنهض بهذه الملاحقات يتعارض، وفقًا لها، مع عدد من التشريعات والمبادئ القانونية العامة، فضلًا عن غياب الشفافية في الكثير من أساليب مباشرة هذه الوحدات لأعمالها[83].

ثالثًا: المراقبة غير القانونية (القرصنة الحكومية)

على الرغم من أن الحكومات تكاد لا تجد أي عائق في تحويل ممارساتها غير المشروعة إلى ممارسات مشروعة، فإنه يمكن رصد حالات تُمارَس من خلالها المراقبة بطرائق لا يُقرّها القانون. فمع وجود رقابة "غير كافية" من النظم القضائية، يمكن أن تحدث المراقبة بطرائق منوعة، وعلى نحو لا يبدو أنه ينتهك القوانين الداخلية، كأن تجري عملية تسلل معلوماتي موسعة ضمن إجراءات الضبط والإحضار. كما أنه من الممكن أن ترفض الأطراف الرسمية مشاركة تفاصيل طرائق التسلل التي تستخدمها مع المدّعى عليهم في أثناء المحاكمة. وعمومًا، لا يمكن التأكد على نحو حاسم من أن المراقبة - حتى وهي تُمارَس وفق القوانين الداخلية - تتوافق مع القوانين والمواثيق الدولية. وذلك لكونها تحمل معنى تدخليًا شديد التماس مع حقوق الأفراد في الخصوصية المعلوماتية[84].

1. لماذا قد تلجأ الحكومات إلى القرصنة غير القانونية؟

تلجأ الحكومات بصفة متزايدة إلى المراقبة غير القانونية (القرصنة)، في الوقت الذي يمكنها أن تسلك مسالك قانونية للحصول على ما تريده من معلومات، لكون "المراقبة" غير القانونية تسهّل عليها إجراءات التتبع والرصد بدرجة كبيرة. على سبيل المثال، البيانات المتعلقة بالأفراد، التي تحاول الحكومات الوصول إليها، عادة ما تكون بحوزة شركات خاصة، هذه الشركات قد تقع ضمن الولاية القانونية/ القضائية لدول أجنبية. يتطلّب هذا من الحكومات أن تحصل على تعاون طرف ثالث، شركات أو حكومات أجنبية أو حتى كلتيهما، للوصول إلى هذه البيانات. لكن هذه العملية عادة ما تستغرق وقتًا طويلًا (يطلق عليها فترة الإظلام Going Dark)، ربما تكون البيانات بعدها غير مُجدِية، كما قد يتبيّن أن الشركة أو الحكومة الأجنبية غير راغبة، أو غير قادرة على إتاحة الوصول إلى البيانات المطلوبة[85].

82 التحول الرقمي في النيابة العامة، مرجع سابق.

83 المرجع نفسه.

84 "Government Hacking and Surveillance: 10 Necessary Safeguards," p. 10.

85 Ibid., p. 7; Chen-Yu Li et al., p. 55054.

لهذا، تمثّل القرصنة (من وجهة نظر بعض الأنظمة) حلًا أكثر ملاءمة وتوفيرًا للوقت من العمليات القانونية التي تشمل تدخّل أطراف متعددة، وتكون نتائجها غير محسومة في الوقت ذاته. وبناء عليه تعمل الحكومات المعنية على تطوير وشراء قدرات لاختراق منتجات وخدمات تلك الشركات ما قد يسمح لها بجمع البيانات التي لا يجري تسليمها طواعية، أو لتجاوز أنظمة التشفير وميزات الأمان الأخرى لدى الأفراد أنفسهم.

2. من المراقبة إلى القرصنة

لا تحظى الهجمات الرقمية (غير القانونية) التي تشنّها الأنظمة باهتمام بحثي كافٍ حتى الآن، إما لكونها ما زالت تُصنّف (على نطاق واسع) أحدَ أشكال المراقبة الحكومية التقليدية، وإما لأنها حال الاعتراف بكونها ظاهرة جديدة يصعب تتبعها والكشف عنها. وهو الأمر الذي يستدعي القيام بالمزيد من الأبحاث الوصفية التي ترصد هذه الظاهرة، وترصد آثارها، حتى يتوافر الأساس النظري الضروري لفهمها.

هذا، ويمكن الزعم أن ممارسة "القرصنة الحكومية" لا تقتصر على أنظمة بعينها، فقد كشفت تسريبات إدوارد سنودن أن الولايات المتحدة، وغيرها، من الأنظمة "الديمقراطية" تمارس القرصنة إزاء الأفراد والمنظمات والدول، المعادية وغير المعادية[86]. وتتطوّع الشركات الخاصة لممارسة هذا الدور ومساعدة الحكومات في مراقبة الأفراد والتعدّي على خصوصياتهم الرقمية، وقد أدلى مؤسس فيسبوك ورئيسها التنفيذي مارك زوكربيرغ بشهادته في الكونغرس حول دور شركته في فضيحة كامبريدج أناليتيكا Cambridge Analytica، حيث جرى الكشف عن أن فيسبوك قد كشف بيانات نحو 87 مليون مستخدم بغرض الاستغلال السياسي[87].

لكن يمكن الزعم أيضًا أن الأنظمة السلطوية، تتمتع على الأقل من الناحية النظرية بحافز أقوى لتوظيف الإمكانات الرقمية لأغراض القرصنة، مقارنة بالديمقراطيات[88]. فنظرًا إلى أن الأنظمة بشكل عام تؤثر في القوانين التي تشكل هيكل الاتصالات، وتُحدّد من ثم مجال تأثير الرقمنة في المجتمع. فإنه يمكن أن نتصوّر أن في مقدور الأنظمة السلطوية، ذات القدرة الأكبر على توجيه المنظومة العدلية في اتجاه مصالحها، أن تُحكِم من قبضتها على منظومة الاتصالات والمعلومات، على نحو يضمن لها قدرات وصلاحيات أكبر للقيام بالمراقبة. كما يضمن لها أن تتجنّب المساءلة حال مارست هذه الرقابة خارج منظومتها القانونية.

3. خطورة القرصنة الحكومية

عندما تنخرط الحكومات في هذا النوع من السلوك، فإنها تخلق أخطارًا كبيرة على المستويات كافة. فعلى المستوى الشخصي، يمكن أن يؤدي تقويض ثقة الأفراد بالقطاع المعلوماتي إلى تقويض أنظمة الاقتصاد الرقمي والحوكمة الرقمية. ويحمل هذا النوع من القرصنة تهديدات لحقوق الأفراد الأساسية في الخصوصية والأمن المعلوماتي

86 Jacob Appelbaum et al., "The Digital Arms Race: NSA Preps America for Future Battle," *Der Spiegel Online*, 17/1/2015, accessed on 24/10/2022, at: https://bit.ly/3QwYAu8

87 "Freedom on the Net 2018, The Rise of Digital Authoritarianism," Freedom House, accessed on 24/10/2022, at: https://bit.ly/3FelHYB

88 Chun-Chih Chang & Thung-Hong Lin, "Autocracy Login: Internet Censorship and Civil Society in the Digital Age," *Democratization*, vol. 27, no. 5 (2020), pp. 874-895; Feldstein, *The Rise of Digital Repression*, p. 5.

والحركية السياسية. إضافة إلى الأضرار التي تلحق الاستقرار المالي للكيانات الخاصة، فالقرصنة الحكومية كفيلة بتقويض أمن الأجهزة والشبكات والبنية التحتية المستهدفة، وربما حتى الفضاء الافتراضي برمته[89].

رابعًا: الرقابة الذاتية

في الحالات التي لا تملك فيها الأنظمة (السلطوية غالبًا) الكفاءة الفنية الكافية لاستغلال التقانة على نحو يدعم قدراتها الرقابية الفعلية، أو حين لا تستطيع التحكم في انتشار المعلومات تقنيًا على نحو فعال، فإنها تستفيد مما يطلق عليه نموذج الرقابة الذاتية[90]، أو "البانوبتيكون" Panopticon[91]، وجوهره استغلال "الخوف من الرقابة" طريقةً للتحكم في نشاطات المعارضين والناشطين والمؤثرين.

هذا، ويمكن رصد حرص كثير من الأنظمة على نشر "معلومة" قيامها بمراقبة المواقع (والمؤثرين والنشاطات) على نطاق واسع، حتى لو لم تكن المراقبة الفعلية بدرجة الشمول التي توحي بها هذه "المعلومة"، ومن دون توظيف تدابير تقانية فعالة لمنع الوصول إلى المواقع المشمولة بالتحذير أو حجبها، وذلك لنجاح هذه الدعاية في حد ذاتها في إثناء كثيرين عن محاولتهم الوصول إلى المحتوى المحظور.

يترتب على "نجاح" هذا النوع من الرقابة الذاتية self-censorship أن يكون الأفراد في ظل الأنظمة السلطوية (الأكثر تطبيقًا له عادة) أقل استفادة من الإمكانات والوسائل المعلوماتية. وذلك لكونهم يتوقعون أن حكوماتهم لن تقبل بحرّية تعبير واسعة، عبر الوسائل الرقمية، ويتوقعون من ثم أن يكونوا دومًا مستهدفين بعمليات مراقبة وتتبع وربما توقيف. من هنا فإن "انعدام الثقة" و"عدم اليقين" بشأن ما تسمح الأنظمة بممارسته، وما (يمكنها أن) تقوم بمراقبته، يمنع مستخدمي التقنيات الرقمية من استخدامها بكامل طاقتها.

بشكل عام، يؤدي اعتقاد أن الفضاء الافتراضي يخضع للمراقبة الحكومية إلى الخوف من محاولة الوصول إلى المعلومات أو نشرها عبره، كما أنه عندما يدرك المواطنون أنهم يخضعون لمراقبة واسعة، يؤدي ذلك بهم إلى قبول الوضع الراهن، على نحو يُحدّ من أي جهود محتملة منهم لتخيّل حقائق اجتماعية وسياسية بديلة[92].

خاتمة واستخلاصات

تخلص هذه الدراسة إلى أنه إذا كانت مراقبة المعارضين والناشطين السياسيين تقع ضمن تقاليد الممارسة السياسية للأنظمة عمومًا، بحجة حماية الأمن القومي، أو النظام العام، أو الصحة العامة، أو الآداب العامة، فإن التقانة الرقمية قد أمدّت هذه الأنظمة بقدرات جديدة وفتحت لها آفاقًا تستطيع من خلالها أن تضيّق

89 Stepanovich, p. 15

90 Deibert et al. (eds.), *Access Denied*, p. 71.

91 سجن البانوبتيكون هو نوع من أبنية السجون، ابتكره المفكر الإنكليزي جيرمي بينثام، وهو عبارة عن: "زنازين ذات شبابيك واسعة على شكل حلقة دائرية، يتوسطها برج مراقبة". تكون هذه الزنازين متاحة لمراقبة الحارس القابع في البرج، لكن لا يمكن للسجناء معرفة ما إذا كان الحارس يراقبهم في اللحظة نفسها. يقوم السجناء باستبطان هذه النظرة المحدقة الخارجية، من الحارس في البرج، إلى نظرة محدقة داخلية، ويتحولون من مجرد مراقَبين إلى مراقبين لأنفسهم. وهكذا، حتى لو نزل الحارس عن البرج وزالت العين المحدقة الخارجية، فإن هذه العين المحدقة الداخلية ستبقى تراقبهم وسترافقهم، حتى لو خرجوا من سجن البانوبتيكون. ينظر: تيموثي ميتشل، **استعمار مصر**، ترجمة بشير السباعي وأحمد حسان (القاهرة: مدارات للأبحاث والنشر، 2013)، ص 8.

92 Deibert et al. (eds.), *Access Denied*, p. 36.

الخناق بدرجة أكبر على المعارضين، وأن تتتبع نشاطاتهم، وتُحيط بخططهم الحالية والمستقبلية، وأن تجعل سعيهم للوصول إلى السلطة أو قدرتهم على التأثير في الجماهير أصعب، وفي بعض الأحيان أمرًا متعذرًا.

وقد كشف العرض السابق عن مدى الفاعلية الذي بلغته محاولات الأنظمة لقلب خصائص المجال الافتراضي. ويمكن تلخيص الدور الذي قامت به سياسات المراقبة الرقمية في هذا الصدد في النقاط التالية[93]:

- **الاشتباه العام:** كما لاحظنا، لا تُحيل سياسات المراقبة إلى أشخاص بذواتهم، ولا تستهدف مشتبهين بهم بأعينهم، لكنها تجعل الجميع تحت مقصلة التتبع؛ إذ تُحيل إلى عدد غير محدود من حالات أو محاولات الوصول إلى معلومة ما أو خبر ما. إنها بهذا المعنى مجردة وعامة، منفصلة عن الذوات، رشيدة، تتّسق مع خصائص الدولة الحديثة، من حيث هي جهاز بيروقراطي موضوعي.
- **افتراض عدم الرشادة:** تنهض المراقبة الرقمية على أساس افتراض عام بعدم رشادة مستخدمي الفضاء الافتراضي، وهذا هو أساس مشروعيتها، فعدم الرشادة يعطي مبررًا كافيًا لوجود سلطة أبوية رشيدة تحدد للأفراد ما يناسبهم وما لا يناسبهم، ليس على مستوى المحتوى الأخلاقي فحسب، إنما أيضًا على المستوى السياسي والثقافي والاجتماعي، وموقع السلطة الرشيدة إزاء المجتمع غير الرشيد، هو بدوره ما يُبرّر قيام الأولى باستباحة خصوصيات الثاني، وممارسة الوصاية عليه، والضرب بأمن معلوماته الشخصية عرض الحائط.
- **الكلمة دليل إدانة:** وفقًا لتقنيات المراقبة الرقمية، يبدأ الاشتباه بمجرد قيام الفرد بالبحث عن كلمة أو موقع أو عنوان، حتى لو لم يكن لهذا الفرد تاريخ يبرر إخضاعه للمراقبة/ الرقابة. فمن يبحث عن معلومة يجري تصنيفه، وإدانته، بغض النظر عن سلوكه السابق أو حقيقة اهتماماته، والعقوبة هنا توقع بصفة مباشرة، إما من خلال المنع والحجب، حيث يحظر عليه الوصول إلى ما يراد الوصول إليه، أو من خلال المراقبة والتتبع.
- **قلب تأثير التقانة:** تستخدم الرقابة الرقمية قوة المعلومات، ضد من يريدون التحرر من خلالها، بهذه الطريقة، فإن التمكين المعلوماتي يجري نفيه أو استغلاله، وفي كلتا الحالتين، فإن التقانة بدلًا من أن تكون أداة للتمكين، تتحوّل إلى مساحة لاختراق الخصوصية ووسيلة للإدانة. من ناحية أخرى، فإن إجراءات التتبع الرقمي تمنع الفرد من أن يفصح على نحوٍ مباشر عمّا في عقله، وتضطره إلى التورية، أو إلى اللجوء إلى الطرائق الالتفافية، لتتحوّل التقانة إلى قيد ضمن قيود أخرى، وتفقد قدرًا معتبرًا من خصائصها.
- **المعلومة أداة للشك:** بحسب نظرية الاتصال الرياضية، تعتبر المعلومة حدثًا يؤدي إلى تراجع الشك في موضوع بعينه. لكن قد يؤدي استخدام معيّن للمعلومات إلى زيادة ارتياب المرء، بمعنى أنه قد يحصل على المعلومة، لكنه لن يصبح أقل شكًا، وذلك إذا ما جُعل الوصول إلى المعلومة نفسه فعلًا مريبًا، يزيد من شك الفرد وقلقه. وهذا ما تصنعه المراقبة، فحينما يقتنع الأفراد بأنهم تحت المراقبة طوال الوقت، يضفي هذا قدرًا كبيرًا من الارتياب على محاولتهم الوصول إلى المعلومة، كما يفقدهم قدرًا كبيرًا من الحماسة، ومن الرغبة في الاستفادة منها لتغيير أوضاع معيّنة.

93 استفادت الدراسة في هذا المبحث، على نحو خاص، من العمل المهم لبيير ليفي، **عالمنا الافتراضي**.

- **ذاكرة المراقبة**: يمكن ملاحظة أن الأجيال الأحدث من المراقبة تملك ذاكرتها الخاصة، وأنها تصنّف الأشخاص بناء على ما تحتفظ به في ذاكرتها من معلومات في خصوصهم. بعبارة أخرى صار في إمكان التقانة أن تصنّف الأشخاص بناء على ما تتوقع أنه يجول في خواطرهم حين يفكرون، حتى لو لم يُفصحوا عن أفكارهم تلك من خلال عبارات صريحة ومفردات محددة يمكن استيعابها في إطار قوائم سوداء. من التداعيات السيئة المرتبطة بهذا الأمر أن ذاكرة التقانة لا يمكن الإفلات منها، كما لا يمكن بسهولة تغييرها، حتى لو تغيّر الأشخاص المستهدفون بهذه المراقبة.
- **تجدد المراقبة**: تفتح المراقبة الرقمية، على خلاف المراقبة التقليدية، المجال أمام احتمالات جديدة تمامًا، فهي لا تكتفي بإنتاج فعل المراقبة، لكنها تنتج أهدافًا جديدة، وتضيف إليها معانيَ جديدة؛ ذلك أنها على التفصيل السابق لم تعد مجرد عملية تتبع جامدة، إنما تقترح بدائل ربما لم تكن في ذهن من قام بتوظيف هذا النوع من المراقبة في الأصل. بعبارة أخرى لم تعد التقانة أداة تسريع لما كان يمكن القيام به على نحو أبطأ، لكنها أصبحت أداة لتنويع الهدف والتفكير في احتمالات جديدة، فالمراقبة الآن لم تعد تستهدف خط سير المشتبه، وما نطق أو ما قام به فحسب، إنما أصبحت أداة للتعرف إلى ملامح الوجوه والانفعالات وقراءة الأفكار. بعبارة أخرى تشهد المراقبة الحالية تغيرًا في قواعد الفعالية ومعايير التقويم والمنفعة.
- **تنويعات المراقبة**: نظرًا إلى تعدد أشكال الرقابة والمراقبة الرقمية، فإنه يمكن دائمًا توقع إمكان الدمج في ما بينها، للحصول على توليفات جديدة، على نحو ينتج أشكالًا أكثر تنوّعًا، ويُضفي عليها قدرًا أكبر من الفاعلية، يُضفي هذا تعقيدًا أكبر على عملية المراقبة، ويجعل الفكاك منها أصعب. وتستفيد الحكومات من هذه الخاصية بدرجة كبيرة، فهي غالبًا ما توظف حزمًا من تقانات الرقابة والمراقبة، وتستخدمها مدمجة، وفق تصورها لماهية التهديد الذي تستشعره من توظيف المعارضة للمنصّات الرقمية.

تعكس الأدوار السابقة مفارقة واضحة، ففي مقابل أحلام التحرر من خلال المعلومات، التي كثيرًا ما راودت الناشطين من مستخدمي الفضاء الافتراضي، صاغت الكثير من الأنظمة سياساتها الرقمية كيما تكون إما أدوات للحجب والمنع وعرقلة الوصول إلى المعلومات، أو أدوات للكشف وانتهاك الخصوصيات الرقمية، باستخدام تقانات المعلومات.

بعبارة أخرى إذا كان الفضاء والتقانة الرقميان قد مثّلا لبعض الوقت مجالًا للانعتاق أمام الناشطين، عبر الالتفاف على مظاهر التضييق التي تمارسها الأنظمة على المجال العام، فإن سياسات المراقبة الرقمية قد نجحت إلى حدٍّ بعيد في سحب الافتراضي مرة أخرى إلى دائرة التحكم. وقد جرى بوضوح القيام بهذا من خلال أدوات العالم الافتراضي نفسها، وهذه تبدو نقطة الضعف الأساسية في الافتراضي.

المراجع Reference

العربية

"أبرز أنماط الانتهاكات في ملفات حرية التعبير". مؤسسة حرية الفكر والتعبير. 2022/1/22. في: https://bit.ly/3MWlMBY

الأمم المتحدة، مفوّضية الأمم المتحدة السامية لحقوق الإنسان. "المراقبة الرقمية تتعامل مع 'الصحافيين وكأنّهم مجرمون'". 2022/5/3. في: https://bit.ly/3cXpddY

"تجفيف منابع الحرية". مؤسسة حرية الفكر والتعبير. 2022/2/22. في: https://bit.ly/3B3MFjn

"التحول الرقمي في النيابة العامة، مدخل للمراقبة الجماعية على الإنترنت". مؤسسة حرية الفكر والتعبير. 2021/8/8. في: https://bit.ly/3B1P6mD

الجموسي، جوهر. **الافتراضي والثورة: مكانة الإنترنت في نشأة مجتمع مدني عربي.** الدوحة/ بيروت: المركز العربي للأبحاث ودراسة السياسات، 2016.

دو بونو، إدوارد. **التفكير العملي.** ترجمة إيهاب محمد. القاهرة: الهيئة المصرية العامة للكتاب، 1999.

سيف النصر، شريف. "المجتمعات الافتراضية على حافة المواجهات السياسية، ويكيبيديا وأزمات الشرق الأوسط المعلوماتية نموذجًا". **سياسات عربية.** العدد 44 (أيار/ مايو 2020).

_____. "السيبرانية: المفهوم، الخصائص، الفرص، الإشكاليات". **قضايا ونظرات.** العدد 21 (نيسان/ أبريل 2021).

عبد اللطيف، كمال. **المعرفي، الأيديولوجي، الشبكي: تقاطعات ورهانات.** الدوحة/ بيروت: المركز العربي للأبحاث ودراسة السياسات، 2012.

ليفي، بيير. **عالمنا الافتراضي: ما هو، وما علاقته بالواقع؟** ترجمة رياض الكحال. مراجعة منصور فرح ومحمد المومني. المنامة: هيئة البحرين للثقافة والآثار، 2018.

"المراقبة الجماعية، ممارسة ممنهجة في مؤسسات الدولة". مؤسسة حرية الفكر والتعبير. 2022/5/26. في: https://bit.ly/3oniKuW

ميتشل، تيموثي. **استعمار مصر.** ترجمة بشير السباعي وأحمد حسان. القاهرة: مدارات للأبحاث والنشر، 2013.

نون، جمال وغسان مراد. **الفعل السياسي الرقمي في العالم العربي ومنظومة القيم والتحولات.** الدوحة: مركز الجزيرة للدراسات، 2019.

الأجنبية

Alsahafi, Waseem Abdulali. "The Socio-Political Implications of Social Media Participation and Activism among Young Adults in Saudi Arabia." PhD Thesis. Nottingham Trent University, September 2019.

Barlow, John Perry. "A Declaration of the Independence of Cyberspace." Electronic Frontier Foundation. at: https://bit.ly/3SexWah

Bradshaw, Samantha & Philip N. Howard. "The Global Organization of Social Media Disinformation Campaigns." *Journal of International Affairs*. 29/7/2018.

"Building Syria's Surveillance State: A Privacy International Investigation." Ifex. 10/1/2017. at: https://bit.ly/3qkJBZq

Chang, Chun-Chih & Thung-Hong Lin. "Autocracy Login: Internet Censorship and Civil Society in the Digital Age." *Democratization*. vol. 27, no. 5 (2020).

Cohen, Jason. "These Countries Ask Google to Remove the Most Content." *PC*. 7/1/2022. at: https://bit.ly/3KNg985

Committee to Protect Journalists (CPJ). "10 Most Censored Countries." *A special report*. 10/9/2019. at: https://bit.ly/3RBJEMg

Deibert, Ronald et al. (eds.). *Access Denied: The Practice and Policy of Global Internet Filtering*. Cambridge, MA: MIT Press, 2008.

_____. *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*. Cambridge, MA: MIT Press, 2010.

Earl, Jennifer et al. "The Digital Repression of Social Movements, Protest, and Activism: A Synthetic Review." *Science Advances*. vol. 8, no. 10 (2022).

"ESET Research Discovers Watering Hole Attacks on Websites in the Middle East with Links to Candiru Spyware." *Eset*. 22/11/2021. at: https://bit.ly/3CT7jBW

Feldstein, Steven. *The Rise of Digital Repression: How Technology Is Reshaping Power, Politics, and Resistance*. New York: Oxford University Press, 2021.

_____. "Government Internet Shutdowns Are Changing. How Should Citizens and Democracies Respond?" *Working Paper*. Carnegie Endowment for International Peace. 31/3/2022. at: https://bit.ly/3gzuY34

"Internet Freedom Scores." Freedom House. at: https://bit.ly/3spT7f7

Freedom House. "Freedom on the Net 2020 (Lebanon)." at: https://bit.ly/3TWCnbL

_____. "Freedom on the Net 2019 (UAE)." at: https://bit.ly/3qpvaDA

_____. "Freedom on the Net 2022 (Israel)." at: https://bit.ly/3qwkfrG

_____. "Freedom on the Net 2021 (Saudi Arabia)." at: https://bit.ly/3qwDilY

_____. "Freedom on the Net 2018, The Rise of Digital Authoritarianism." at: https://bit.ly/3FelHYB

_____. "Freedom on the Net Research Methodology." at: https://bit.ly/3xgOeb2

Fuchs, Christian. *Internet and Surveillance: The Challenges of Web 2.0 and Social Media*. New York: Routledge, 2011.

"Government Hacking and Subversion of Digital Security." Electronic Frontier Foundation. at: https://bit.ly/3B3LMaI

"Government Hacking and Surveillance: 10 Necessary Safeguards." Privacy International. at: https://bit.ly/3SoMsMB

"Government Requests to Remove Content." *Google Transparency Report*. at: https://bit.ly/3PITIlH

"Governments Want Encryption Backdoors: New Report Examines the Legal and Policy Implications." Access Now. 14/2/2018. at: https://bit.ly/2FlKARa

Granick, Jennifer Stisa. "Challenging Government Hacking: What's at Stake." *ACLU*. 2/11/2022. at: https://bit.ly/3RJHg71

Gunkel, David J. *Hacking Cyberspace*. Oxford: West View, 2001.

_____. "Introduction to Hacking and Hacktivism." *New Media Society*. vol. 7, no. 5 (2005).

"Hacker Lexicon: What Is a Watering Hole Attack?" *WIRED*. 28/11/2021. at: https://bit.ly/3RPpEGU

Hare, Forrest B. "Privateering in Cyberspace: Should Patriotic Hacking Be Promoted as National Policy?" *Asian Security*. vol. 15, no. 2 (2019).

Hernández, Marianne Díaz et al. "Internet Shutdowns in 2021: The Return of Digital Authoritarianism." Access Now. 28/4/ 2022. at: https://bit.ly/3ARGE7M

Hobaika, Zeina et al. *The MENA Region and COVID-19: Impact, Implications and Prospects*. Oxon: Routledge, 2022.

Jordan, Tim. *CyberPower: The Culture and Politics of Cyberspace and the Internet*. London: Routledge, 1999.

Kampmark, Binoy. "The Pandemic Surveillance State: An Enduring Legacy of COVID-19." *Journal of Global Faultlines*. vol. 7, no. 1 (2020).

Kenyon, Miles. "A UAE Agency Put Pegasus Spyware on Phone of Jamal Khashoggi's Wife Months before His Murder, New Forensics Show." *The Citizen Lab*. 21/12/2021. at: https://bit.ly/3L3TK6o

Li, Chen-Yu et al. "A Comprehensive Overview of Government Hacking Worldwide." *IEEE Access*. vol. 6 (2018). at: https://bit.ly/3VU7dTt

Lynch, James. "Iron Net: Digital Repression in the Middle East and North Africa." European Council on Foreign Relations. 29/6/2022. at: https://bit.ly/3vmwrOT

Lynch, Marc. "Digital Activism and Authoritarian Adaptation in the Middle East." *Pomeps Studies*. no. 43 (August 2021). at: https://bit.ly/3xFzliT

Marczak, Bill. "Mapping Hacking Team's 'Untraceable' Spyware." *The Citizen Lab*. 17/1/2014. at: https://bit.ly/3qvNDys

Marczak, Bill & John Scott-Railton. "The million dollar dissident: NSO group's iPhone zero-days used against a UAE human rights defender." *The Citizen Lab*. 24/8/2016. at: https://bit.ly/2rRi8ke

Marczak, Bill et al. "Journalists Hacked with Suspected NSO Group iMessage 'Zero-Click' Exploit." *The Citizen Lab*. 20/12/2020. at: https://bit.ly/3L2h04V

_____. "Hooking Candiru: Another Mercenary Spyware Vendor Comes into Focus." *The Citizen Lab*. 15/7/2021. at: https://bit.ly/3DdmmZa

Marczak, William R. et al. "When governments hack opponents: A look at actors and technology." 23rd USENIX Security Symposium. San Diego, CA 20-22/8/2014 .

Meijer, Albert & Martijn Wessels. "Predictive Policing: Review of Benefits and Drawbacks." *International Journal of Public Administration*. vol. 42, no. 12 (2019).

Noman, Helmi. "Internet Censorship and the Intraregional Geopolitical Conflicts in the Middle East and North Africa." Berkman Klein Center Research Publication. no. 1 (2019). at: https://bit.ly/3TXNEsx

O'Neil, Cathy. *Weapons of Math destruction, how big data increases inequality and threatens Democracy*. New York: Crown Publishers, 2016.

O'Neill, Patrick Howell. "The Fall and Rise of a Spyware Empire." *MIT Technology Review*. 29/11/2019. at: https://bit.ly/3ojRbmc

"Pegasus Affair: Who Was Wiretapped in the Middle East?" Warsaw Institute. 30/8/2021. at: https://bit.ly/3AUnVIM

Polyakova, Alina & Chris Meserole. "Exporting digital authoritarianism: The Russian and Chinese models." *Policy Brief*. Democracy and Disorder Series. Washington, DC: Brookings, 2019.

Privacy International. "Government Hacking." at: https://bit.ly/3PrgxL1

Rahimi, Nick & Bidyut Gupta. "A Study of the Landscape of Internet Censorship and Anti-Censorship in Middle East." *EPiC Series in Computing*. vol. 69 (2020).

Richardson, Rashida, Jason M. Schultz & Kate Crawfords. "Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice." *The New York University Law Review*. vol. 94, no. 15 (2019).

Ringmar, Erik. *A Blogger's Manifesto, Free Speech and Censorship in the Age of the Internet*. London: Anthem Press, 2007.

Schell, Bernadette H. *Internet Censorship: A Reference Handbook*. Oxford: ABC-CLIO, 2014.

Shahbaz, Adrian & Allie Funk. "Freedom on the Net 2021: The Global Drive to Control Big Tech." Freedom House, 2021. at: https://bit.ly/3eK9QGL

Shaheed, Ahmed. "Binary Threat: How Governments' Cyber Laws and Practice Undermine Human Rights in the MENA Region." *Project on Middle East Political Science (POMEPS)*. at: https://bit.ly/3RB4pIt

Silverstein, Richard. "Israel Is Hacking the Phones of Palestinian NGOs." *Jacobin*. 13/11/2021. at: https://bit.ly/3xhvkRr

Stepanovich, Amie. "A human Rights Response to Government Hacking." Access Now (Sep. 2016). at: https://bit.ly/3gAuEB9

Van Haaster, Jelle et al. *Cyber Guerilla*. London: Elsevier, 2016.

Warf, Barney. *The SAGE Encyclopedia of the Internet*. California: SAGE Publications Inc., 2018.

"What is Zero-click Malware, and how do Zero-click Attacks Work?" *Kaspersky*. at: https://bit.ly/3KVpmey

"Which Countries Block VPNs, and Why?" *VPN*. at: https://bit.ly/3TQXOtQ

Wysopal, Chris, Chris Eng & Tyler Shields. "Static Detection Of Application Backdoors." *Datenschutz und Datensicherheit-DuD*. vol. 34, no. 3 (2010).