Editorial Board | هيئة التحرير

التحولات التكنولوجية المتسارعة والمراقبة الشاملة
قراءة نقدية في كتاب: إمبراطورية المراقبة

Accelerated Technological Transformations and Comprehensive Surveillance
Critical Reading of: *L'empire de la surveillance*

الرقم التعريفي DOI
https://doi.org/10.31430/SZJE4797

Ignacio Ramonet

L'empire de la surveillance, Suivi de deux entretiens avec Julian Assange et Noam Chomsky, Collection Folio Actuel, Postface inédite (Paris: Gallimard, 2024), 189 p.

كثُر الحديث في الآونة الأخيرة عن فكرة مجتمع المراقبة، بصيغة فكرةٍ مجردة، أو تهديدٍ غامض في أفلام وقصص خيالية للواقع المرير (Dystopia)، أو في نظريات المؤامرة الرائجة. غير أنّ كتاب إغناسيو رامونيه **إمبراطورية المراقبة** يأتي ليوضح بجلاءٍ أن فكرة مجتمع المراقبة ليست ديستوبيا افتراضية أو خيالية، بل هي حقيقة ملموسة على نحوٍ متزايد في عصر الثورة الرقمية.

مؤلّف الكتاب، إغناسيو رامونيه، صحافي وأكاديمي معروف على المستوى الدولي، كان مديرًا للمجلة الشهرية **لوموند ديبلوماتيك** (*Le Monde diplomatique*) على مدى 17 عامًا. وهو يستنكر في هذا الكتاب الانتشار المتزايد للمراقبة الجماعية، بدعمٍ من السياسات الحكومية، وبتواطؤٍ من الشركات، وبفضل التقدم التكنولوجي الفائق. والأطروحة المركزية للكتاب مخيفة مفادها أن العالم يتشكل على نحو متزايد من خلال المراقبة الجماعية السرية، وهي الظاهرة التي تحوّل الدول الديمقراطية وغير الديمقراطية على حدٍ سواء إلى كيانات "أورويلية"[1]. ويرسم صورةً مقلقة لعالم المراقبة الشاملة الذي بدأ يتشكل على مدى العقود القليلة الماضية، ويرجع ذلك جزئيًا إلى التقدم في التكنولوجيا الرقمية. ويؤكد رامونيه أن هذا القسم الأكبر من الدينامية السلبية لا يتأتّى من الدكتاتوريات، كما تصوّر ذلك بعض الأعمال الروائية أو الواقعية[2]، بل من دولة ديمقراطية قديمة: الولايات المتحدة الأميركية، والتي ستكون عنصرًا ثابتًا في هذا الكتاب، الواضح والموجز، والموثّق جيدًا بعددٍ من الدراسات والتقارير، إضافة إلى بعض الأعمال الخيالية.

ويتضمن كتاب **إمبراطورية المراقبة** أيضًا في ملاحقه مقابلتين تسلّطان الضوء على الأبعاد السياسية والأخلاقية لهذه الظاهرة، الأولى مع جوليان أسانج، الذي يناقش تجربته في العمل في شرطة "غوغل" (Google) وفي تسريبات "ويكيليكس" (WikiLeaks)، والثانية مع نعوم تشومسكي، الذي يتخذ موقفًا نقديًا إزاء السياسة الخارجية الأميركية.

أولًا: مضامين الكتاب

يعتبر رامونيه أن النزوع إلى فرض السيطرة الشاملة تعود أصوله إلى الحرب الباردة. ولذلك نجده يخصص فصلًا كاملًا للبرامج المختلفة التي نفذتها الاستخبارات الأميركية، في الولايات المتحدة الأميركية، وفي أماكن أخرى عديدة في العالم. وذريعة ذلك كانت دومًا إمكانية المراقبة الشاملة للحفاظ على الأمن، مع الحفاظ على الخصوصية وحقوق المواطنين. غير أن ما بدأ نشاطًا وطنيًا دفاعيًا انتهى به الأمر إلى الامتداد إلى المجال المدني وخلق "حرب الجيل الرابع"، استنادًا إلى ذريعة مكافحة الإرهاب. وقد أدّت هجمات 11

1 نسبةً إلى جورج أورويل وروايته الشهيرة **1984** التي نُشرت في عام 1949، التي أبرز فيها عواقب الاستبداد والمراقبة الجماعية والتنظيم القمعي للناس وللسلوكيات داخل المجتمع، وصوَّر عالمًا مستقبليًا تكون فيه الحريات محدودة، ويتمّ فيه التلاعب بالحقيقة، ومراقبة المواطنين عن كثب من قبل نظام تمثّله شخصية أسطورية تسمى "الأخ الأكبر" (Big Brother). ينظر:
George Orwell, *Nineteen Eighty-Four* (London: Secker & Warburg, 1949).

2 كما هو الحال مثلًا على مستوى الأعمال الخيالية في رواية **1984**، أو على مستوى الواقع في النموذج الصيني الراهن.

سبتمبر دورًا رئيسًا في هذا التطور، ومن ثمّ يحلل المؤلف التفاصيل الدقيقة لـ "قانون باتريوت"[3] ونظائره المختلفة.

يقدم رامونيه في هذا الكتاب، الصادر سنة 2024[4]، عالمًا شهد تحولاً كبيرًا بفعل الثورة الرقمية؛ إذ انتقلت مراقبة المواطنين من مجرد تدخل جسدي بسيط إلى حضور رقمي غير محسوس وغير محدّد في الزمان أو في المكان. واستنادًا إلى تسريبات "كاشفي الفساد" (Whistleblowing) مثل إدوارد سنودن (Edward Snowden)، يقوم رامونيه بتشريح آليات المراقبة المعاصرة، والتي تراوح بين جمع البيانات من طرف شركات التكنولوجيا العملاقة، والبرامج الحكومية المصممة لاستغلال المعلومات الشخصية على نطاق واسع، مثل الماسحات الضوئية الحيوية (Biometric Scanners)، وصور الأقمار الصناعية، ومعالجة البيانات الخوارزمية، التي تحوّل النشاط البشري إلى بصمات رقمية يمكن تحليلها أو بيعها أو تحويلها إلى أسلحة. ويشير رامونيه، مستشهدًا بتسريبات سنودن، إلى أنّ المشكلة لا تكمن في استخدام هذه الوسائل في مراقبة الإرهابيين المشتبه بهم على سبيل المثال، بل في المراقبة الجماعية والعشوائية لشعوبٍ بأكملها.

ويسلّط الكتاب الضوء على التواطؤ الطوعي للشركات في نظام المراقبة هذا، لا سيما منها الشركات العملاقة غوغل وآبل وفيسبوك. ويؤكدّ جوليان أسانج، في المقابلة التي يجري تضمينها في الملحق الأول للكتاب، أن علاقات شركة غوغل بالحكومة الأميركية ليست مجرد علاقات تجارية أو مؤسسية، بل تمتدّ إلى أجندة جيوسياسية مشتركة. ويضع نعوم تشومسكي، في مقابلته التي يجري تضمينها في الملحق الثاني للكتاب، هذه الظاهرة في سياقها التاريخي، مؤكدًا أن الحكومات سعت منذ فترة طويلة إلى السيطرة على تدفق المعلومات، ولكنها أضحت اليوم تمتلك الوسائل اللازمة للقيام بذلك؛ وهو ما يجعل هذه الطموحات فعالة على نحو خطير.

ويربط رامونيه المراقبة بالاتجاهات المجتمعية الأوسع نطاقًا، مثل تحويل البيانات الشخصية إلى سلعة، وتآكل الخصوصية بوصفها قيمة. ويحذر من مستقبل لا تتنبأ فيه الخوارزميات المعتمدة على البيانات بالسلوك البشري فحسب، بل إنها تتحكّم فيه أيضًا؛ ما يؤدي إلى تقويض استقلالية الفرد. وهذا احتمال

---

3 "قانون باتريوت" (Patriot Act) هو قانون استثنائي لمكافحة الإرهاب، صوّت عليه الكونغرس الأميركي ووقعه جورج بوش الابن في 26 تشرين الأول/ أكتوبر 2001، نتيجة مباشرة لهجمات 11 سبتمبر. وقد كان لهذا القانون تأثير كبير في الولايات المتحدة، من خلال تعزيزه صلاحيات الجيش الأميركي والوكالات الحكومية الأميركية المختلفة (مكتب التحقيقات الفدرالي، ووكالة المخابرات المركزية، ووكالة الأمن القومي)، وترخيصه عمليًا لأجهزة الأمن للوصول إلى البيانات الحاسوبية التي يحتفظ بها الأفراد والشركات، من دون الحصول على إذن مسبق ومن دون إعلام المستخدمين. ينظر في ذلك:

David Cole & James X. Dempsey, *Terrorism and the Constitution: Sacrificing Civil Liberties in the Name of National Security*, 2nd ed. (New York: W. W. Norton & Co., 2002).

4 ظهرت النسخة الأولى من هذا الكتاب في عام 2015، في أعقاب الكشف الذي قدمه إدوارد سنودن في عام 2013، و"كاشفو فساد" آخرون، مثل جوليان أسانج (Julian Assange)، وبرادلي مانينغ (Bradley Manning)، الذين أظهروا أنّ وكالة الأمن القومي وأجهزة الاستخبارات الأميركية الأخرى قد تولّت تتبّع جميع المعلومات المتداولة على شبكة الإنترنت وشبكات التواصل الاجتماعي وتحليلها، في كثير من الأحيان بطرائق غير قانونية.

مخيف لمجتمع المراقبة لأنه يعمل على تطبيع أفول الخصوصية المؤسسة للمواطنة، ومن ثمّ يقوض أسس الديمقراطية.

إضافة إلى ذلك، يقدم الكتاب أمثلةً مثيرة للقلق بشأن كيفية إعادة استخدام التكنولوجيات، التي كان من المفترض في الأصل أن تحمي المواطنين، للسيطرة عليهم، ومن أبرزها "إنترنت الأشياء" (Internet of Things, IoT). فمن أجهزة الاتصال الشخصية، إلى برمجيات التتبّع المضمنة في الأجهزة والأدوات المنزلية، إلى أنظمة المراقبة البيومترية في المطارات، يرسم رامونيه صورةً قاتمة يصبح فيها إخفاء الهوية أمرًا مستحيلاً. وهو يشير إلى أن إنترنت الأشياء سيضمن قريبًا أن تصبح حتى أكثر الأماكن خصوصية مراقبةً باستمرار. وهذا تذكير صارخ بأن نطاق المراقبة لا يقتصر على الجهات الحكومية، بل يشمل أيضًا منظومة متنامية من الشركات الخاصة.

ويربط موضوع المراقبة الشاملة بإطاره التاريخي والفلسفي الأوسع. فبالاعتماد على مفهوم ميشيل فوكو للمراقبة والسيطرة والعقاب[5]، يوضح رامونيه كيفية عمل آليات المراقبة الحديثة على توسيع هذا النموذج من السيطرة إلى أبعاد لا يمكن تصورها. فعلى عكس القيود المادية لنموذج جيريمي بنثام الأصلي[6]، تخلق المراقبة الرقمية قوة غير مرئية، ولكنها موجودة في كل مكان، تعمل على تشكيل السلوك من خلال إمكانية مراقبتها.

ثانيًا: تزايد المراقبة الشاملة في ظل التطورات التكنولوجية المتسارعة

من النقاط المحورية في الكتاب أنه أبرز تطور المراقبة في العقود الأخيرة من الملاحظة الجسدية للأفراد إلى شبكة واسعة مترابطة من الأنظمة التكنولوجية التي تراقب حياة المليارات من البشر وتسجلها وتحللها. ويستند هذا التحول إلى التقدم السريع في مجال الذكاء الاصطناعي، والتعرف على الوجه،

5 يصف نموذج ميشيل فوكو للمراقبة، كما يعبر عنه في استعارته "البانوبتيكون" (Panopticon) من جيريمي بنثام، نظامًا للسلطة يستبطن فيه الأفراد آثار المراقبة؛ ما يؤدي إلى الانضباط الذاتي والسيطرة. وتعمل المراقبة آلية لإنتاج المعرفة عن الأفراد؛ ما يسمح للسلطة بالعمل على توحيد السلوكيات وتعزيز المعايير المجتمعية. ويتجاوز منظور فوكو الفضاءات المادية؛ إذ يسلط الضوء على كيفية استخدام المؤسسات الحديثة، مثل السجون والمدارس والمستشفيات، للملاحظة والتصنيف لممارسة السيطرة. وفي السياقات المعاصرة. ويساعد هذا الإطار في تفسير الطبيعة الشاملة للمراقبة الرقمية؛ إذ يجري توزيع السلطة على نحو لامركزي، وتتم ممارستها من خلال جمع البيانات والمراقبة الخوارزمية، وتشكيل السلوكيات على المستويين الفردي والمجتمعي. ينظر:

Michel Foucault, *Surveiller et punir: Naissance de la prison* (Paris: Gallimard, 1975).

6 يتجسد مفهوم جيريمي بنثام للمراقبة في تصميمه سجن "البانوبتيكون"، وهو سجن دائري فيه برج مراقبة مركزي يسمح للحراس بمراقبة جميع السجناء من دون علمهم بموعد مراقبتهم. ويخلق هذا الشك تأثيرًا نفسيًا لدى السجناء؛ إذ يشجعهم على تنظيم سلوكهم وكأنهم لا يزالون تحت المراقبة؛ ما يقلل من الحاجة إلى التدخل المباشر. وقد تصوّر بنثام البانوبتيكون باعتباره نظامًا فعالاً للسيطرة يمكن تطبيقه على مؤسسات أخرى، مثل المدارس، والمصانع، والمستشفيات؛ إذ يمكن أن تكون المراقبة، من منظور منفعي، وسيلةً للانضباط والإصلاح والإنتاجية. ينظر:

Jeremy Bentham, *The Panopticon Writings*, Miran Bozovic (ed.) (London: Verso, [1791] 1995).

والخوارزميات، ووسائل التواصل الاجتماعي، وغيرها من التقنيات. وتعتمد المراقبة اليوم على التقارب بين التقنيات المتطورة التي تجمع كميات هائلة من البيانات وتعالجها. ومن بين أبرز هذه الأدوات نجد الذكاء الاصطناعي والتعلم الآلي. إذ يمكن خوارزميات الذكاء الاصطناعي غربلة مجموعات كبيرة من البيانات لتحديد نماذج السلوك، والتنبؤ بها، وحتى استنتاج النيّات. وتستخدم الحكومات والشركات هذه القدرات لمراقبة الأفراد والتنبؤ بسلوكهم. ويمكن خوارزميات التعلم الآلي تحديد الأنشطة المشبوهة، وتتبع الأفراد، وحتى التنبؤ بالسلوك المستقبلي بناءً على البيانات التاريخية. ورغم أن هذه القدرات غالبًا ما يتم الترويج لها باعتبارها تقدمًا أمنيًا، فإنها تشكّل أيضًا مخاطرَ كبيرة على الخصوصية والحريات المدنية. فعلى سبيل المثال، جرى تنفيذ أنظمة "الشرطة التنبئية" (Predictive Policing)، التي تعتمد على بيانات الجريمة التاريخية لتوقّع النشاط الإجرامي[7].

وتُعدّ تقنية التعرف على الوجه أداة أساسية أخرى في ترسانة المراقبة. وتُعرف أنظمة مثل برنامج "سكاي نت" (Skynet) الصيني بالقدرة على تحديد هوية الأفراد وتتبّعهم في الزمن الحقيقي عبر المناطق الحضرية الكبيرة[8]. وفي حين حظيت هذه التكنولوجيا بالإشادة بدورها في تحسين السلامة العامة، فقد جرى استخدامها أيضًا سلاحًا ضد المعارضين السياسيين والأقليات العرقية. وتوثّق تقارير من منظمات مثل منظمة العفو الدولية استخدام تقنية التعرف على الوجه في منطقة شينجيانغ الصينية؛ إذ إنها تؤدي دورًا محوريًا في مراقبة المسلمين الأويغور وقمعهم[9]. ويسلط هذا المثال الضوء على الطبيعة المزدوجة الاستخدام لتقنيات المراقبة، التي يمكن أن تخدم أغراضًا مفيدة وقمعية على حد سواء اعتمادًا على نشرها. ويوضح التعرف على الوجه الذي يعمل بالذكاء الاصطناعي أنّ التكنولوجيا يمكنها أن تعمل على تعزيز الأمن وإضعافه في الوقت نفسه. وفي البلدان الديمقراطية، يجري في الغالب تقديم تقنية التعرف على الوجه بوصفها أداة لتحديد المجرمين وضمان السلامة العامة. ومع ذلك، فإن التكنولوجيا معرّضة للأخطاء، خاصة عندما يتعلق الأمر بتحديد هوية أفراد ينتمون إلى أقليات مجتمعية[10]. ويمكن أن تؤدي هذه الأخطاء إلى عواقب مدمرة، تراوح بين الاعتقالات غير القانونية وتآكل ثقة الجمهور بإنفاذ القانون.

ويزيد إنترنت الأشياء من تعقيد مشهد المراقبة؛ إذ تجمع الأجهزة اليومية، من منظمات الحرارة الذكية إلى أجهزة تتبع النشاط القابلة للارتداء، البيانات حول عادات المستخدمين وتفضيلاتهم، وحتى المؤشرات الصحية. وغالبًا ما تنقل هذه الأجهزة البيانات إلى خوادم سحابية، حيث يمكن تحليلها أو بيعها أو

---

7 مع ذلك، تعمل هذه الخوارزميات غالبًا على إدامة التحيزات النظامية، وتستهدف المجتمعات المهمشة على نحو غير متناسب. ينظر: Cathy O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy* (New York: Crown Publishers, 2016).

8 Rogier Creemers, "China's Social Credit System: An Evolving Practice of Control." *SSRN Electronic Journal* (May 2018).

9 Amnesty International, *Like We Were Enemies in a War: China's Mass Internment, Torture and Persecution of Muslims in Xinjiang* (London: Amnesty International, 2021).

10 Hannah Fry, *Hello World: How to be Human in the Age of the Machine* (London: Transworld Publishers, 2018).

مشاركتها مع أطراف ثالثة. ويحذّر رامونيه في هذا الصدد من التسلل الصامت للمراقبة إلى الأماكن الخاصة، والذي تسهّله أجهزة إنترنت الأشياء. ذلك أن هذا النظام البيئي المترابط من الأجهزة يعمل على طمس الخطوط الفاصلة بين المجالَين العام والخاص، ما يجعل المراقبة حضورًا دائمًا في الحياة الحديثة.

ومن جهةٍ أخرى، أصبحت شبكات التواصل الاجتماعي مثل فيسبوك وإنستغرام وتويتر (سابقًا) تشكّل أدوات لا غنى عنها للتواصل والتعبير الشخصي؛ ولكنها تشكّل أيضًا جزءًا لا يتجزأ من جهاز المراقبة الشاملة. وتجمع هذه المنصات كميات هائلة من البيانات الشخصية، بما في ذلك الموقع، وسجلّ التصفح، والاتصالات الاجتماعية، التي يمكن استخدامها لإنشاء ملفات تعريف مفصلة للمستخدمين. وفي كثير من الأحيان، يتم استثمار هذه البيانات من خلال الإعلانات المستهدفة، ولكنها متاحة أيضًا للحكومات وأجهزة إنفاذ القانون. وترى شوشانا زوبوف في هذا الصدد أنّ وسائل التواصل الاجتماعي تجسّد تسليع البيانات الشخصية[11]، وتصف استغلال شركات مثل فيسبوك ما تسميه "الفائض السلوكي" (Behavioral Surplus) للتنبؤ بسلوك المستخدم والتأثير فيه، وتحويل الناس فعليًا إلى سلع[12]. علاوةً على ذلك، تورطت هذه المنصات في برامج المراقبة التي ترعاها الدولة. فعلى سبيل المثال، كشفت "فضيحة بيانات كامبريدج أناليتيكا" (Cambridge Analytica Data Scandal) عن كيفية جمع بيانات مستخدمي فيسبوك واستخدامها للتلاعب بالنتائج السياسية؛ ما أثار تساؤلات عدة بشأن المسؤوليات الأخلاقية لشركات التكنولوجيا[13].

ومن ثمّ، فإن انتشار تقنيات المراقبة له آثار عميقة في الحوكمة وحقوق الإنسان وديناميكيات السلطة العالمية. ففي الأنظمة الاستبدادية، تُستخدم هذه الأدوات في أغلب الأحيان لقمع المعارضة والحفاظ على السيطرة؛ فـ "نظام الائتمان الاجتماعي" في الصين، على سبيل المثال، يعتمد على الذكاء الاصطناعي والتعرف على الوجه وبيانات وسائل التواصل الاجتماعي لمراقبة المواطنين وتقييمهم بناءً على سلوكهم؛ ومن يحصلون على درجات منخفضة يواجهون قيودًا على الحركة والتعليم والتوظيف؛ ما يخلق نظامًا من الإكراه الرقمي[14]. بيد أنّ أنظمة المراقبة الشاملة هذه تمتدّ إلى مختلف أنحاء العالم، الديمقراطية منها وغير الديمقراطية. فقد سلّطت تسريبات كاشفي الفساد، مثل إدوارد سنودن، الضوء على برامج مثل "بريسم" (PRISM) لوكالة الأمن القومي الأميركية (NSA)، التي تجمع البيانات من شركات

11 Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (New York: PublicAffairs, 2019).

12 Ibid.

13 Margaret Hu, "Cambridge Analytica's Black Box," *Big Data & Society,* vol. 7, no. 2 (2020), pp. 1-6.

14 Genia Kostka, "China's Social Credit Systems and Public Opinion: Explaining High Levels of Approval," *New Media & Society*, vol. 21, no. 7 (2019), pp. 1565-1593.

التكنولوجيا الكبرى لمراقبة الاتصالات العالمية[15]. وفي حين يؤكد مؤيدو هذه البرامج أنها ضرورية لحفظ الأمن والسلم الاجتماعي ومكافحة الإرهاب، فإن منتقديها يعتبرون أنها تقود إلى تآكل الحريات المدنية، وتؤسس لسابقة خطيرة لإساءة استخدام الحكومات للسلطة.

ثالثًا: المراقبة الشاملة في السياقات العربية

من أبرز الجوانب الغائبة عن كتاب رامونيه نجد الفحص التفصيلي لكيفية نشر تقنيات المراقبة في العالم العربي، وخاصة في أعقاب الربيع العربي؛ إذ إن استخدام الأنظمة الاستبدادية العربية للمراقبة الرقمية يوضح كيفية تمكّن هذه الأدوات من قمع المعارضة وتعزيز السلطة. وتكشف ذلك العديد من التقارير، فقد جرى استخدام برامج التجسس مثل "بيغاسوس" (Pegasus) لمراقبة الناشطين والصحافيين وشخصيات المعارضة في جميع أنحاء المنطقة[16].

ويقدّم العالم العربي مثالاً واضحًا على نحو خاص لكيفية استخدام تقنيات المراقبة أسلحةً. ففي أعقاب انتفاضات الربيع العربي، استثمرت الحكومات في المنطقة إلى حد بعيد في المراقبة الرقمية لدرء قيام احتجاجات مماثلة في المستقبل. وفي العديد من الدول العربية، تتم مراقبة منصات التواصل الاجتماعي بحثًا عن أي علامات معارضة، أو حتى موقفٍ نقدي من النظام، ويتكرر استهداف الناشطين باستخدام برامج التجسس. ويسلط استخدامُ أدوات تجسس، مثل برنامج بيغاسوس لاختراق هواتف الصحافيين والمدافعين عن حقوق الإنسان، الضوءَ على تواطؤ الشركات الخاصة في القمع الذي ترعاه الدولة.

تُظهر بذلك تجربة العالم العربي أنّ التكنولوجيا يمكن أن تؤدي دورًا مزدوجًا؛ فهي يمكن أن تسهل الحركات الشعبية وتعبئة السكان، ولكنها أيضًا تزود الأنظمة بوسائل غير مسبوقة للسيطرة. ومن ثمّ، يتبيّن أنّ تأكيد رامونيه على أنّ تكنولوجيات المراقبة هي ذروة أسلحة الاستبداد صحيح على نحوٍ خاص في السياق العربي. وعلى نحو مماثل، يعكس استخدام أدوات القرصنة المتطورة، التي غالبًا ما تطورها وتستوردها شركات أجنبية، التواطؤ العالمي في القمع الذي ترعاه الدولة. ومن ثم، فإن المنطقة العربية تشكّل مثالاً لكيفية تناسب تكنولوجيات المراقبة بإساءة استخدام السلطة على نحو غير منضبط.

15 Juhi Tariq, "The NSA's PRISM Program and the New EU Privacy Regulation: Why U.S. Companies with a Presence in the EU Could Be in Trouble," *American University Business Law Review*, vol. 3, no. 2 (2014), pp. 385-418.

16 Bill Marczak et al., "The Great iPwn: Journalists Hacked with Suspected NSO Group iMessage 'Zero-Click' Exploit," *Citizen Lab*, University of Toronto, 20/12/2020, accessed on 5/2/2025, at: https://acr.ps/1L9zQlC

رابعًا: قراءة نقدية في الكتاب

على الرغم من أن كتاب **إمبراطورية المراقبة** نجح في تسليط الضوء على نطاق المراقبة الجماعية وخطورتها، ونسج حجاجًا متماسكًا وأدلةً تاريخية وسياسية وتكنولوجية متعددة لتعزيز هذا الطرح، فإنه لا يخلو مع ذلك من بعض الثغرات، فالنطاق الطموح للكتاب يأتي في بعض الأحيان على حساب العمق التحليلي. فعلى سبيل المثال، يفتقر الكتاب إلى استكشاف دقيق للأطر القانونية التي تمكّن ممارسات المراقبة في مناطق مختلفة أو تحدّ منها[17].

وتتمثّل ثغرة أخرى في أنّ الكتاب أحيانًا ينحو إلى الخلط بين المراقبة والسيطرة. ففي حين نجد رامونيه يسلط الضوء على نحوٍ مكثّف على مخاطر جمع البيانات الجماعية، فإنه يقلل من شأن إمكانات المقاومة المدنية. وفي هذا الصدد، يشير عدد من الدراسات إلى أنه يمكن استغلال التكنولوجيا أيضًا لمكافحة المراقبة والنشاط السياسي[18]. وهذا المنظور غائب إلى حد بعيد عن تحليل رامونيه؛ ما يترك للقارئ شعورًا بالحتمية يقترب من الهزيمة.

علاوةً على ذلك، وعلى الرغم من أن رامونيه يعرض المعضلات الأخلاقية التي تفرضها المراقبة، فإن الحلول المقدمة تفتقر إلى التحديد. فهي تدعو إلى زيادة الوعي العام والإصلاح القانوني، ولكنها لا تقدم سوى القليل من الاستراتيجيات الملموسة لتحقيق هذه الأهداف. فعلى سبيل المثال، كيف يمكن المؤسسات الديمقراطية أن تنظم بفاعلية الشركات المتعددة الجنسيات التي تتجاوز أنشطتها الحدود الوطنية؟

وإدراج المقابلات مع جوليان أسانج ونعوم تشومسكي يعزّز طرح الكتاب، غير أنه يحدّ في الآن ذاته من نطاقه. فعلى الرغم من أهمية طروحات أسانج وتشومسكي المعروفة جيدًا، يفتقر الكتاب إلى تنوع الأصوات الذي كان من الممكن أن يثري المناقشة. فعلى سبيل المثال، كان من شأن تضمين وجهات نظر من مناطق عديدة من العالم، لا سيما الجنوب الكبير، حيث تتقاطع المراقبة الشاملة مع ديناميكيات ما بعد الاستعمار، أن يوسع النطاق التحليلي للكتاب. وملاحظة تشومسكي بأن المراقبة الجماعية هي امتداد طبيعي للإمبريالية في العصر الرقمي هي ملاحظة عميقة، ولكنها تترك أسئلة من دون إجابة بشأن كيفية تأثير تقنيات المراقبة على نحو غير متناسب في المجتمعات المهمشة.

يُضاف إلى ذلك أن استكشاف رامونيه لمستقبل المراقبة مقنع ولكنه غير مكتمل. ويعترف الكتاب بدور الذكاء الاصطناعي والتعلم الآلي في تحسين قدرات المراقبة، لكنه لا يقدّم تحليلاً أعمق لذلك. فمع تطور خوارزميات الذكاء الاصطناعي، أصبحت تُستخدم على نحو متزايد ليس فقط لتحليل البيانات، بل أيضًا للتنبؤ بالسلوك والتأثير فيه. وهذا له آثار عميقة في الديمقراطية والحكم، كما يتضح من دور التحيز الخوارزمي في إنفاذ القانون وأنظمة العدالة. وفي هذا الصدد، كان في إمكان رامونيه أن يستلهم

17 Zuboff.

18 Evgeny Morozov, *The Net Delusion: The Dark Side of Internet Freedom* (New York: PublicAffairs, 2011).

أفكاره من بعض الأعمال التي تبحث في كيفية مساهمة الخوارزميات الغامضة في إدامة عدم المساواة والتحيزات[19]. وكان من الممكن أن يستفيد الكتاب أيضًا من مناقشة أكثر تفصيلاً للتحديات الأخلاقية التي تفرضها التقنيات الناشئة، مثل التعرف على الوجه، ومقاطع الفيديو المزيفة، التي تعمل على طمس الخط الفاصل بين الواقع والتلاعب به[20].

وكان من الممكن استكشاف رامونيه لمفهوم "الشرطة التنبئية" في سياق تأثيرها في المجتمعات المهمشة أن يقود إلى تعميق انتقاده للمراقبة المدعومة بالذكاء الاصطناعي. فعلى سبيل المثال، تظهر دراسات الحالة من الولايات المتحدة كيفية استهداف هذه التقنيات الأقليات على نحو غير متناسب؛ ما يؤدي إلى تعزيز التفاوتات المؤسسية. وعلى الرغم من التطرق إليها على نحو هامشي، فقد كانت هذه الأسئلة تستحق أن يجري تناولها بمزيد من التفصيل في عمل يسعى لمعالجة الآثار العالمية للمراقبة الشاملة.

خامسًا: على سبيل الختم

كتاب **إمبراطورية المراقبة** مهمّ ويأتي في وقته المناسب؛ إذ إنه يسلّط الضوء على إحدى القضايا الرئيسة في عصرنا. فسردية رامونيه النابضة بالحياة، واستخدامه الوفير للأمثلة الملموسة، يجعلان الكتاب في متناول الجميع ومقنعًا بشأن تأثيرات التطور السريع لتقنيات المراقبة ودورها في تحويل العالم على نحوٍ عميق ومثير للقلق. ففي حين تتيح هذه الأدوات التكنولوجية والرقمية مزايا كبرى، من تحسين السلامة العامة إلى تبسيط الخدمات، فإنها تمثّل أيضًا مخاطر جدية على الخصوصية والحريات المدنية والحكم الديمقراطي.

يظل الكتاب، على الرغم من بعض أوجه محدوديته، موردًا أساسيًا لأي شخص يسعى لفهم التفاعل بين المراقبة والتكنولوجيا والسلطة، في الحاضر وفي المستقبل. ففي عالمٍ أصبحت فيه الحدود بين المجالين العام والخاص غير واضحة على نحوٍ متزايد، فإن تحذير رامونيه واضحٌ: الدفاع عن الخصوصية هو دفاع عن الديمقراطية. ومن خلال عرض مخاطر المراقبة غير المقيدة، يتحدّانا لتخيّل مستقبل تخدم فيه التكنولوجيا الإنسانية بدلاً من السيطرة عليها. ومع سعي المجتمعات إلى التعامل مع آثار هذه التقنيات، فإن التحدي يتمثل في إيجاد التوازن بين استغلال إمكاناتها وحماية الحقوق الأساسية. ولا يتطلب هذا فقط أطرًا قانونية وأخلاقية قوية، بل يتطلب أيضًا التزامًا جماعيًا بالشفافية والمساءلة ومقاومة إساءة استخدام السلطة. وفي نهاية المطاف، فإن مستقبل المراقبة الشاملة سوف يتشكل من خلال الاختيارات التي نتخذها اليوم، وهي الاختيارات التي سوف تحدد إن كانت التكنولوجيا تعمل أداةً للتحرير أو وسيلةً للسيطرة.

---

19 ومنها مثلاً: O'Neil; Fry.

20 Meredith Whittaker, Kate Crawford & Sarah Myers West, "Artificial Intelligence and Ethics: Risks, Opportunities, and Governance of Facial Recognition and Deepfake Technologies," *Journal of Technology and Society*, vol. 35, no. 2 (2021), pp. 45-68.

المراجع

Amnesty International. *Like We Were Enemies in a War: China's Mass Internment, Torture and Persecution of Muslims in Xinjiang*. London: Amnesty International, 2021.

Bentham, Jeremy. *The Panopticon Writings*. Miran Bozovic (ed.). London: Verso. [1791] 1995.

Cole, David & James X. Dempsey. *Terrorism and the Constitution: Sacrificing Civil Liberties in the Name of National Security*. 2nd ed. New York: W. W. Norton & Co., 2002.

Creemers, Rogier. "China's Social Credit System: An Evolving Practice of Control." *SSRN Electronic Journal* (May 2018).

Foucault, Michel. *Surveiller et punir: Naissance de la prison*. Paris: Gallimard, 1975.

Fry, Hannah. *Hello World: How to be Human in the Age of the Machine*. London: Transworld Publishers, 2018.

Hu, Margaret. "Cambridge Analytica's Black Box." *Big Data & Society*. vol. 7. no. 2, 2020.

Kostka, Genia. "China's Social Credit Systems and Public Opinion: Explaining High Levels of Approval." *New Media & Society*. vol. 21. no. 7 (2019).

Marczak, Bill et al. "The Great iPwn: Journalists Hacked with Suspected NSO Group iMessage 'Zero-Click' Exploit." *Citizen Lab*. University of Toronto. 20/12/2020. at: https://acr.ps/1L9zQlC

Morozov, Evgeny. *The Net Delusion: The Dark Side of Internet Freedom*. New York: PublicAffairs. 2011.

O'Neil, Cathy. *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. New York: Crown Publishers, 2016.

Orwell, George. *Nineteen Eighty-Four*. London. Secker & Warburg, 1949.

Tariq, Juhi. "The NSA's PRISM Program and the New EU Privacy Regulation: Why U.S. Companies with a Presence in the EU Could Be in Trouble." *American University Business Law Review*. vol. 3, no. 2 (2014).

Whittaker, Meredith, Kate Crawford & Sarah Myers West. "Artificial Intelligence and Ethics: Risks, Opportunities, and Governance of Facial Recognition and Deepfake Technologies." *Journal of Technology and Society*. vol. 35, no. 2 (2021).

Zuboff, Shoshana. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: PublicAffairs, 2019.