

سوريا.. فرص وتحديات (ملف خاص)



سوريا الجديدة والتحولات الإستراتيجية في الشرق الأوسط

من الحرب على غزة
إلى التغيير في سوريا

دليل للمقاومة في عصر
الذكاء الاصطناعي

إفريقيا في المنظور
الصيني للعالم



للدراسات الاستراتيجية
دورية محكمة تصدر عن مركز الجزيرة للدراسات
السنة السابعة - العدد 26 - مايو/أيار 2025

رئيس التحرير
د. محمد المختار الخليل

نائب رئيس التحرير
أ.د. لقاء مكي

مدير التحرير
محمد عبد العاطي

هيئة التحرير
د. عز الدين عبد المولى
العنود أحمد آل ثاني
د. فاطمة الصمادي
د. محمد الراجي
د. سيدي أحمد ولد الأمير
د. شفيق شقير
د. عبدالله العمادي
الحواس تقيّة
د. الحاج محمد الناسك
يارا النجار

المراجع اللغوي
إسلام عبد التواب



مركز الجزيرة للدراسات
ALJAZEERA CENTRE FOR STUDIES

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

آراء الباحثين والكتاب لا تعبر بالضرورة عن اتجاهات تنبناها المجلة
أو مركز الجزيرة للدراسات

ترتيب الدراسات يخضع لاعتبارات فنية فقط

جميع الحقوق محفوظة

مركز الجزيرة للدراسات
ALJAZEERA CENTRE FOR STUDIES



الدوحة - قطر

هاتف: 40158384 (+974)

فاكس: 44831346 (+974) - البريد الإلكتروني: E-mail: lubab@aljazeera.net

ISSN 2617-8753

تصميم الغلاف: قطاع الإبداع الفني بشبكة الجزيرة الإعلامية

الطباعة : مطابع قطر الوطنية - الدوحة - قطر - هاتف : 8452 4444 974+

عبيد الخوارزميات: دليل للمقاومة في عصر الذكاء الاصطناعي

Book Review: Esclavos del algoritmo: Manual de resistencia en la era de la inteligencia artificial by Laura Garcia de Rivera

عبد الرفيع زعنون – Abderrafie Zaanoun *

ملخص:

يستهدف الكتاب رصد تجليات الرقابة الخوارزمية وتداعياتها؛ حيث سعت الباحثة والصحفية الإسبانية، لورا غارسيا دي ريفيرا، إلى تحليل تأثير تطبيقات الذكاء الاصطناعي على مختلف المجالات السياسية والاقتصادية والاجتماعية والثقافية. تخلص الكاتبة إلى أن الشركات الكبرى للتكنولوجيا الضخمة جعلت حرية الناس أكثر تقييداً، وفق تقنيات رقمية تجعلهم مُسيَّرين في قرارات التصويت والاستهلاك واتخاذ الرأي، وفي إعادة ترتيب علاقاتهم مع الأفراد والمجتمعات والسوق والدولة. في ضوء ذلك تُقدِّم الكاتبة دليلاً إرشادياً لمقاومة تسلط المعالجات الخوارزمية وتلمس طريق التخلص من أسر "العبودية الرقمية"، انطلاقاً من خبرتها كمتخصصة في مجال الأمن السيبراني ومن توصيات كبار الخبراء والمختصين في هندسة المعلومات والأخلاقيات الرقمية، من خلال اقتراح حزمة من المداخل التشريعية والتقنية والمنهجية من أجل التصدي للنزعة الهيمنية لأوليغارشية الذكاء الاصطناعي التي تقتات من السطو المستمر على بيانات مستعملي المنصات والشبكات الإلكترونية.

الكلمات المفتاحية: الذكاء الاصطناعي، استعمار البيانات، العبودية الرقمية، الرقابة الخوارزمية، المقاومة.

Abstract

The book aims to trace the manifestations and implications of algorithmic surveillance. Spanish researcher and journalist Laura García de Rivera analyses the impact of artificial intelligence applications across political,

* د. عبد الرفيع زعنون، باحث مشارك بالمعهد المغربي لتحليل السياسات، أستاذ زائر بالكلية متعددة التخصصات بالعرائش/ جامعة عبد الملك السعدي بالمغرب.

Dr. Abderrafie Zaanoun, Research Associate at the Moroccan Institute for Policy Analysis, and Visiting Professor at the Polydisciplinary Faculty in Larache, Morocco.

economic, social and cultural spheres. She concludes that major Big Tech companies have increasingly restricted people's freedom through digital technologies that guide their choices in voting, consumption and opinion-making, and in reshaping their relationships with individuals, communities, the market and the state. In light of this, the author offers a practical guide to resisting the dominance of algorithmic processes and finding a path toward liberation from the shackles of "digital slavery". Drawing on her expertise in cybersecurity and the recommendations of leading experts in information engineering and digital ethics, de Rivera proposes a set of legislative, technical and methodological approaches to confront the hegemonic drive of the AI oligarchy – an oligarchy that thrives on the ongoing exploitation of users' data across platforms and digital networks.

Keywords: artificial intelligence, data colonisation, digital slavery, algorithmic censorship, resistance.

عنوان الكتاب

عبيد الخوارزميات: دليل للمقاومة في عصر الذكاء الاصطناعي

Esclavos del algoritmo: Manual de resistencia en la era de la inteligencia artificial

المؤلفة: لورا غارسيا دي ريفيرا (Laura G. De Rivera)

قراءة: عبد الرفيع زعنون

دار النشر: جدل (DEBATE)

تاريخ النشر: يناير/كانون الثاني 2025

اللغة: الإسبانية

الطبعة: الأولى

عدد الصفحات: 393

يندرج كتاب "عبيد الخوارزميات: دليل للمقاومة في عصر الذكاء الاصطناعي (1) ضمن أدبيات دراسة استعمار البيانات (2)، التي تسعى جاهدة لكشف أبرز مظاهر "سرقة" المعطيات الخاصة بمستعملي المنصات والشبكات من طرف شركات التكنولوجيا الضخمة (3) "Big Tech". ويُعد الكتاب حصيلة ثلاثين سنة من البحث في الثقافة الرقمية عملت خلالها الكاتبة لورا غارسيا دي ريفيرا على رصد سياقات تطور "التكنولوجيا التخريبية" (Disruptive Technology)، كما يُعد تنويجاً لسلسلة من الدراسات والتحقيقات الاستقصائية أصدرتها الباحثة لفائدة عدة مؤسسات بإسبانيا والمكسيك، على غرار "الثقافة السيبرانية" و"الجانب الدموي للانتقال الأخضر" و"تور: قمة جبل الجليد غير المرئية للإنترنت"، وغيرها من الأعمال التي نالت بموجبها عدة جوائز دولية كجائزة الأمن المعلوماتي بسلوفاكيا في 2018، وجائزة بيت العلوم في 2020، وجائزة "المجلس الأعلى للأبحاث العلمية بإسبانيا (CSIC) في سنة 2022.

يتألف الكتاب من أربعة فصول تحليلية ونقدية، تناقش موضوعات عديدة من أهمها جشع البيانات، والمراقبة الجماعية، والتلاعب بمعطيات البشر، والديجيتال المكيافيلي، والذكاء الاصطناعي المتحيز، والاستعمار الرقمي، والإغراق الأخلاقي (dumping moral)، والعبودية الرقمية الجديدة. بالإضافة إلى الفصول ذات النّفس النقدي، يشتمل الكتاب على فصلين استشرافيين حول سبل جعل التكنولوجيا الرقمية في خدمة البشرية، باقتراح مجموعة من المداخل من أجل التصدي للرقابة الخوارزمية ولتحصين الخصوصية الرقمية المستباحة من قبل شبكات التواصل ومنصات الذكاء الاصطناعي.

تنطلق الكاتبة في تحليلها من الاستفهام الاستنكاري التالي: هل سترك حياتك في أيدي خوارزمية؟ وهو سؤال مركزي يستبطن العديد من الأسئلة الفرعية: هل أصبحنا فعلاً عبيداً للخوارزميات التي تتحكم في قراراتنا اليومية؟ وكيف يمكن أن تؤثر هذه التقنيات على مفاهيم الحرية والخصوصية والسيادة والديمقراطية؟ وهل قدر البشرية الاستكانة والخضوع أم ثمة منافذ لاستعادة السيطرة على التكنولوجيا؟ في محاولتها للإجابة عن هذه الإشكالات، اعتمدت لورا دي ريفيرا بشكل أساسي على أدوات المقارنة للترجيح بين تأثيرات المعالجات الخوارزمية على مناحي الحياة السياسية والاقتصادية والاجتماعية، مع توظيف مكثف لتقنية المقابلة؛ حيث أجرت سلسلة

من اللقاءات مع عدد كبير من المختصين في ميادين القانون والهندسة المعلوماتية وأخلاقيات الذكاء الاصطناعي، ومع مسؤولين سابقين بوكالات حكومية وبالشركات الكبرى للتواصل الشبكي.

تُقر الكاتبة منذ البداية بالقيمة المضافة لأدوات الذكاء الاصطناعي، خاصة فيما يتعلق بتحليل البيانات الضخمة واستثمارها في تلبية حقوق حيوية، كالصحة عبر تحسين دقة التشخيص الطبي، وتطوير الأدوية والاكتشاف المبكر لبعض الأمراض في ضوء قواعد معطيات ضخمة لمعالجة صور الأشعة وتقارير التحاليل الطبية، والتعليم من خلال تيسير الوصول إلى المعرفة وتنمية آليات التعلم الذاتي. إضافة إلى العائد الاقتصادي؛ حيث تفيد المعالجة الخوارزمية في خفض التكاليف وتعزيز الإنتاجية والتنافسية، والعائد الأمني؛ حيث تساعد أنظمة المراقبة الذكية في مكافحة الجرائم الإلكترونية ورصد التهديدات الإرهابية. فضلاً عن ذلك، فهي تسهم في تحسين تفاعل البشر مع التكنولوجيا أمام التطور المذهل لتقنيات التفاعل مع الأجهزة المعلوماتية، كالتعرف على الصور والأوامر الصوتية وأدوات المساعدة الرقمية.

غير أن كل مكسب من هذه المكاسب يحمل في طياته تأثيرات لا حصر لها يتجاوز ضررها مجرد انتهاك الحياة الخاصة إلى التحكم في القرار السياسي والسيادة الاقتصادية للدول، ليس فقط لأسباب "بيداغوجية" تعود لسوء استخدام المنصات، بل لأصول منهجية مرتبطة بهندستها المعلوماتية التي صُممت في الأصل وفق تركيبة "انتقائية" تجعلها تعكس تحيزات صانعيها، ولكون خوارزميات الذكاء الاصطناعي غير قادرة على تمثيل الأخلاقيات المهنية، بل إن فكرة بناء ذكاء اصطناعي أخلاقي تتعارض في الأصل مع رهانات مطوّريه، وما إنشاء الشركات لأقسام أخلاقيات الذكاء الاصطناعي سوى "مكياف" لإخفاء وجهها البشع على حدّ تعبير رودولفو هابر (Rodolfo Haber)، مدير مركز الأتمتة والروبوتات في جامعة البوليتكنيك في مدريد (CAR). وكل من يقاوم هذه النزعة فمصيره الإقصاء كما حصل مع تيمنيت جيبرو (Timnit Gebru)، خبيرة أخلاقيات الذكاء الاصطناعي بشركة غوغل، التي كشفت عن التحيز الفادح في خوارزميات التعرف على الوجه؛ حيث وجدت أن هذه الأنظمة تعترّيتها معدلات خطأ أعلى عند التعرف على أصحاب البشرة الداكنة (4).

بمعزل عن الحمولة الرمزية لعبارة "عبيد الخوارزميات" ثمة مؤشرات عديدة على تكريس عبودية جديدة ذات صبغة رقمية، في ظل وجود مئات الآلاف من الأشخاص

الذين يقومون بعمل غير مرئي وغير مدفوع الأجر في الزوايا المحرومة من الكوكب لجعل الذكاء الاصطناعي يبدو أكثر عبقرية، والذين يشكلون العبيد الجدد لمافيا الاتجار بالمواد النادرة التي تدخل في تصنيع الأجهزة الإلكترونية، كاستخدام عصابات الاتجار في هذه المعادن لعشرات الآلاف من الأطفال كعبيد في مناجم الكولتان (Coltan) والكوبالت (Cobalt) في عدة دول إفريقية، مثل رواندا والكونغو الديمقراطية، بدون أية ضمانات لحمايتهم من مخاطر الألغام والإشعاعات السامة. إضافة إلى استغلال الآلاف من الأشخاص في البلدان الفقيرة للقيام بأعمال قدرة لصالح شركات معالجة البيانات الضخمة مقابل أجور زهيدة، كمشاهدة المحتوى غير اللائق بتركيز شديد لساعات طويلة من أجل تصنيفه. ناهيك عن دفع المستخدمين إلى العمل بشكل مجاني لصالحها من خلال استخراج بياناتهم بدون إذنهم وإعادة استخدامها وبيعها لأطراف ثالثة.

بهذا الصدد، تشير الباحثة إلى أن التفاصيل الشخصية تشكل في حد ذاتها منابع لا تنضب يجني من ورائها عمالقة التكنولوجيا أرباحاً خيالية، وقد حاول بعض الخبراء تقديم تقديرات حسابية لقياس قيمة "الداتا المنهوبة"، والتي تبلغ في الحد الأدنى 240 دولاراً سنوياً للفرد، مع وجود بعض المتغيرات بحسب حالة كل شخص وقانون العرض والطلب، وهكذا فبيانات شاب أبيض أغلى من بيانات امرأة من أصل إسباني في الخمسينات من عمرها. أما بخصوص طبيعة المعلومات المُسلعة، فتُعتبر "الداتا الديمغرافية" هي الأرخص مقابل بيانات أخرى عالية القيمة خاصة ذات الطابع الطبي والمالي (5). وتكمن أهمية "سوق البيانات" في استعمالاتها المتعددة التي تتجاوز المراقبة الأمنية إلى التسويق والتحكم في الأذواق والاختيارات السياسية والاقتصادية للناس.

على المستوى الأمني، أصبحت أنظمة المراقبة الجماعية بمنزلة أسلحة فتاكة بيد بعض الأنظمة السياسية للتحكم في مصير الأشخاص، ففي الولايات المتحدة الأمريكية، درجت المؤسسات الأمنية (6) على توظيف الحلول الرقمية للشركات الكبرى، على غرار برنامج المراقبة الجماعية لشركة كليرفيو (Clearview AI) الذي يُمكن من التعرف على أي شخص انطلاقاً من مقارنة صورته بقاعدة بيانات تشتمل على ملياري صورة مأخوذة من شبكات التواصل الاجتماعي، بدون أخذ أية موافقة مسبقة أو اتخاذ أية احتياطات لتفادي التعسف في معالجتها، فوفقاً لدراسة أجراها مركز

الخصوصية والتكنولوجيا في كلية الحقوق بجامعة جورج تاون (CPT)، أسهمت المراقبة الذكية بدائرة إنفاذ الهجرة والجمارك الأميركية (ICE) في المس بحقوق المهاجرين؛ حيث أدت نتائج المعالجة الخوارزمية لبعض بؤر الهجرة إلى ترحيل آلاف المهاجرين بشكل سري وبدون أية ضمانات قانونية وخارج رقابة القضاء؛ الأمر الذي لم يُمكن من تفادي التحيزات على أساس اللون والجنس والثقافة ومن تدارك الأخطاء المادية التي شابت معالجة المعطيات.

أما في الصين، فإن أكثر من 600 مليون كاميرا تقوم بعملية الرصد الحي لحركة المواطنين في الشوارع والمواصلات والمرافق العامة ومراكز التسوق والمباني السكنية، ولا تكتفي المراقبة بالفيديو على التسجيل بل هي متصلة ببرنامج للذكاء الاصطناعي يربط كل وجه برقم الهوية الرقمية (Digital ID) لكل شخص، مع توفره على عدة تعليمات ضبطية حول ما يجب التركيز عليه ومن تجب متابعته، وهي متصلة بنظام (الائتمان الاجتماعي) الذي يمنح (رصيداً) قيمياً لكل مواطن على أساس سلوكه الخاضع للمراقبة.

ولا تقتصر قائمة المشتبهين المعنيين بالمراقبة المشددة على المجرمين والمدمنين والمرضى العقليين بل أيضاً أولئك الذين يقدمون شكاوى أو ادعاءات إلى الإدارات العامة، وكل من ينشر تدوينات قد تحتل نقداً للسلطات، وما قد ينجم عن ذلك من إضرار بحقوق ومصالح الأفراد، بحيث تؤدي خسارة النقط من "السجل الرقمي للمواطن" إلى تقليص مستحقات الائتمان الاجتماعي، والرفع من قيمة تذاكر النقل والضرائب، فضلاً عن تعقيد شروط الحصول على الوظائف أو الترقية أو القروض. لكن أنظمة تقييم سمعة المواطنين (Social Credit System) لا تقتصر على الديكتاتوريات المعلنة (7)، بل أصبحت ممارسات ضمنية بالعديد من الديمقراطيات الغربية، فمساطر الحصول على التأمينات وتقنيات احتساب الأقساط والشروط البنكية المتعلقة بقيمة القروض والفوائد وآجال وضمانات السداد، تتم صياغتها استناداً على خوارزميات تعالج السلوك الاقتصادي للشخص وحالته الوظيفية والاجتماعية والصحية وتاريخ ديونه.

بهذا المعنى، تقر لورا دي ريفيرا بكون الخوارزميات في طريقها لتجاوز إرادة الإنسان، من خلال تحكمها فيما يجب أن يشاهده ويشتره، وبتوجيهها لطريقة تفكيره على نحو

قد يجعله سجينًا للتكنولوجيا الرقمية وغير قادر على التقرير في مصيره، وعلى التأثير الإيجابي في أسرته ومجتمعه. في هذا السياق، تستعمل الكاتبة استعارة دالة لوصف تحولات المراقبة بين الفضاء السيبراني والعالم المادي: الخوارزميات تعرفك أفضل من والدتك. صحيح أنه لا جدال في السطوة التي تمارسها شركات التكنولوجيا الكبرى وما تمثله من تهديد للحرية الإنسانية، لكن أحكام الكاتبة قد تحتل بعض المبالغة بسبب انطلاقها من مسلمة تعتبر المستخدمين مجرد ضحايا للخوارزميات وفاقدين للإرادة أمامها، دون الإشارة إلى دورهم النشط في محاولة الانفكاك من أسرها، بالرغم من تواتر حالات عديدة للهجمات المعارضة (Adversarial Attacks) لإبراز قصور المعالجات الخوارزمية، كتلاعب باحثين بجامعة هارفارد بصور الأشعة السينية المعالجة بالذكاء الاصطناعي لإثارة الانتباه إلى الأخطاء الطبية للخوارزميات في التشخيص الطبي ككشف أمراض غير موجودة وإخفاء أمراض فعلية، وبتجارب فريق بحثي عمل على وضع ملصقات صغيرة على الطريق تسببت في انحراف سيارات تسلا ذاتية القيادة عن مسارها؛ حيث قرأ النظام الملصقات على أنها علامة طريق خاطئة (8).

ارتباطًا بمجالات الضبط والمراقبة، تشير لورا دي ريفيرا إلى دور الذكاء الاصطناعي في تطوير تطبيقات الإنترنت القضائي (Judicial Internet)، ففي الصين، أصبح العديد من المحاكم الصينية يُصدر منذ 2017 أحكام الإدانة دون تدخل القضاة البشريين، وفي ولايتي أركنساس وأيداهو، أثبتت دراسة مشتركة أشرفت عليها جامعة نيويورك أن استخدام الخوارزميات في نظام التقاضي قد أثر سلبًا على حقوق وحريات المواطنين، ويسبب مخاطر تجريم الأبرياء فقد حظرت مدن أخرى بالولايات المتحدة استخدام تقنيات الذكاء الاصطناعي في معالجة القضايا الجنائية، مثل بوسطن وبورتلاند وسان فرانسيسكو. كما أبرزت تقارير تقييم أثر النظام المعلوماتي لمراقبة السجون الأمريكية (COMPAS) تحيزه على أساس اللون؛ حيث يُصنّف البيض بشكل منهجي على أنهم أقل خطورة من الأميركيين الأفارقة، وجرّاء ذلك، تقل فرص حصول السجناء السود على الإفراج المشروط. وفي كاتالونيا، طوّرت جامعة برشلونة نموذجًا رياضيًا مشابهًا (RisCanvi) لحساب الأخطار المستقبلية للسجناء ولمساعدة القضاة في تحديد ما إذا كان شخص ما يستحق الإفراج المشروط أم لا، وما ينجم عن ذلك من تحيزات يصعب تداركها.

أما على المستوى السياسي، فقد تنامى تأثير شركات تحليل البيانات الضخمة في فبركة المشهد السياسي، كشركة كمبردج أناليتيكا (Cambridge Analytica) التي وظفت الذكاء الاصطناعي في توجيه نوايا التصويت عبر آليات الدعاية الحاسوبية (9) (Computational Propaganda)، كحجب الأفكار غير المرغوبة واستهداف الناخبين برسائل مُخصَّصة لتعزيز دعمهم، وخلق انطباع مصطنع بالزخم الشعبي لتوجهات معينة؛ حيث ساعدت بعض الشخصيات والأحزاب السياسية في تجميع وتحليل المعلومات الخاصة لإقناع الناخبين بطريقة مُخصَّصة وموجهة، كما حصل في نييجيريا سنة 2015، وفي الولايات المتحدة بدعم وصول ترامب إلى الرئاسة، وفي بريطانيا بالتأثير على نتائج استفتاء الخروج من الاتحاد الأوروبي في 2016. وبالرغم من إغلاق الشركة إثر الفضائح التي تسببت فيها، فإن هذا لا يحجب استمرار تكتيكات غسل العقل الجمعي بالذكاء الاصطناعي لأغراض سياسية؛ حيث كشف تقرير صادر عن برنامج الديمقراطية والتكنولوجيا التابع لمعهد أكسفورد للإنترنت (OII) عن حملات تضليل وتلاعب بالرأي العام على نطاق واسع في 81 دولة حول العالم. ولم يعد من الضروري أن تكون دولة استبدادية تُخصَّص جزءاً من الميزانية العامة للسيطرة على الخطاب السياسي وإسكات الأصوات المعارضة، بل الأمر أصبح يشمل حتى الدول الديمقراطية بما فيها أعضاء من الاتحاد الأوروبي، بالرغم من تأكيدات مجلس أوروبا حول ضرورة حماية الاستقلال المعرفي للمواطنين من مختلف أشكال "الإقناع الخوارزمي".

سياسياً أيضاً، تعتبر لورا غارسيا دي ريفيرا أن خوارزميات الذكاء الاصطناعي قد أصبحت أدوات أثيرة للتأثير في الرأي العام الدولي. للاستدلال على هذا المآل، تستشهد الكاتبة الإسبانية بالبروباغندا التي صاحبت الحرب الإسرائيلية الأخيرة على قطاع غزة؛ حيث نشر رئيس الوزراء الإسرائيلي، بنيامين نتنياهو، صورة مفبركة لأطفال رضع ادعى أنهم قُتلوا بوحشية في هجوم 7 أكتوبر/تشرين الأول 2023؛ وذلك من أجل التعبئة الداخلية للحرب وقلب الحقائق في أذهان الجمهور الغربي، كما اعتمد لاحقاً على صور "مُفبركة" بواسطة الذكاء الاصطناعي التوليدي بنسبة ضحايا مدنيين إلى هجوم حماس قبل أن تكشف بعض الوكالات أن الإصابات ناجمة عن القصف الإسرائيلي.

أكثر من ذلك، فقد وظفت إسرائيل في حربها الأخيرة على غزة أحدث تقنيات الذكاء الاصطناعي؛ حيث استعانت بكبريات شركات التكنولوجيا في تصميم نظام "حبسورا" (Habsora) الذي ساعد على تحديد ما لا يقل عن 37 ألف هدف بغزة، وما نجم عن ذلك من تدمير للبنى التحتية وتصفية الآلاف من الناس بتوجيه من الخوارزميات القتالة (10). وتكمن خطورة هذا التطور في محاولة خلق حالة من التطبيع مع التأثيرات المدمرة للذكاء الاصطناعي، والتعامل معها كمجرد أعراض جانبية، وهكذا فمن المستساغ تصفية 20 مدنيًا في سبيل القضاء على عسكري واحد، ومن المقبول أن تتسبب الطائرات الموجهة بالذكاء الاصطناعي في تدمير المستشفيات إذا كانت الغاية هي اجتثاث منابع "الإرهاب". ولتكتمل الصورة توظف شبكات التواصل الاجتماعي "خوارزميات الحجب" لإخفاء الحقيقة وتجميل الوجه البشع لحرب الإبادة. وبهذا المعنى، تقوم التكنولوجيا الرقمية بدور حربي مزدوج؛ تارة بأدوات ناعمة لخلق سرديات مضللة، وتارات أخرى بتطوير أسلحة فتاكة مدفوعة بعلم البيانات يجري تجريب العديد منها بغزة (11).

كما تمارس خوارزميات الذكاء الاصطناعي تأثيرًا هيكليًا على تصميم السياسات العامة والإستراتيجيات الجيوسياسية، من حيث طبيعة البيانات المعتمدة وكيفية معالجتها، على نحو قد يؤثر على مصالح وحقوق الملايين من الناس على حدّ تعبير ديبايان غوش (Dipayan Ghosh)، الباحث بجامعة هارفارد ومستشار التكنولوجيا في البيت الأبيض خلال إدارة أوباما والخبير السابق في الخصوصية والسياسة العامة في فيسبوك. وفضلاً عن ذلك، فهي تضر بشكل جسيم بالمجال العام، بتبخيس النقاش الديمقراطي؛ حيث تؤدي خوارزميات تصفية المحتوى (CFA) إلى تكريس العزلة وشحذ المواقف المتطرفة من خلال زيادة التواصل عبر الإنترنت مع الأشخاص الذين يتشاركون نفس وجهات النظر مما يجعل معتقداتهم أكثر راديكالية. وجزءاً من ذلك، يتفاقم الفصل الأيديولوجي بدل إنشاء "أغورا" رقمية (Ágora Digital) لإذكاء التفكير النقدي والمناقشة البناءة. وهو خطر طالما حذر منه العديد من الباحثين منذ سنوات، في ضوء تواتر ارتدادات "فقاعات الفلتر" على الديمقراطية والمجال العام، على اعتبار أن التخصيص المسبق للمحتوى الرقمي يعزل الأفراد داخل رؤى سياسية محددة (12). في هذا السياق، ما تفتأ الشبكات الاجتماعية تخلق المزيد من الحيل لتكريس عبودية المستهلكين للإنترنت، كخوارزميات التوصية لإطالة مدة اتصال

المستعمل بالشبكة لتحقيق عوائد أكبر، فكل نقرة ومشاهدة واشتراك وتعليق وإعادة توجيه هي نقطة بيانات (13)، وتقنيات التصميم الإدماجي، كعرض المحتوى على الشاشة بدون طلب أو التشغيل التلقائي الافتراضي والسحب للتحديث، وتقديم محتويات ونشرات أخبار مُخصَّصة ونشرات أخبار لكل مستعمل تبعاً لتفضيلات تقرر ما يجب أن نراه ونعرفه، وآليات تعقب الأثر، حيث يحتوي أي جهاز على نظام لتحديد المواقع (GPS) يسمح لأطراف ثالثة بالتعرف على جميع الأماكن التي يزورها مستعمل الجهاز، أو التي ينوي زيارتها، فمثلاً من خلال تحليل تاريخ الشخص في تطبيق خرائط غوغل (Google Maps) يمكن التنبؤ بالمكان الذي سيكون فيه في العامين المقبلين.

بهذا الخصوص، تطرح لورا دي ريفيرا مسؤولية المستخدمين الذين تحول الكثير منهم إلى "بيغاوات عشوائية" (Stochastic Parrots) تقبل بشكل "روبوتيكي" كل شروط تثبيت التطبيقات وملفات تعريف الارتباط (Cookies) وتضغط على مربعات إثبات كون المستعمل ليس بروبوت بدون أي اهتمام بالمخاطر المحتملة عن "نقرات بسيطة" تحمل في طياتها قبولاً ببيع البيانات الخاصة والاشتغال مجاناً لفائدة أوليغارشيا رقمية تتألف من خمس شركات كبرى (GAFAM) (14). وتكمن الخطورة في مؤسسة هذا التوجه وشموله للفاعلين على نحو أصبح فيه تعليم الأطفال بيد الشركات الرقمية التي أصبحت تتحكم في البنية التحتية التعليمية الرقمية، عبر خدمات سحابية توظفها في تخزين وتجميع الملاحظات والوظائف والتمارين والدرجات والملفات وقوائم الطلاب ومخرجات الاجتماعات وبيانات وقنوات الاتصال، ففي أميركا نصف المدارس مرتبطة بالأدوات الإنتاجية السحابية لشركة غوغل (Google Workspace). وفي إسبانيا عقدت معظم مناطق الحكم الذاتي اتفاقيات تكرر التبعية طويلة الأجل مع الحزمة التعليمية لشركة مايكروسوفت (Microsoft 365 Education)، وهو تحول ينطوي، بحسب الكاتبة، على تهديدات جدية للخصوصية الرقمية للأطفال. ناهيك عن الضرر الذهني فالخدمات السحابية تجعل الأجيال الجديدة ترى في الإنترنت نوعاً من الذاكرة الخارجية المشتركة.

في محاولتها لاقتراح مسارات التصدي، ترى الباحثة أن المقاومة يجب أن تبدأ بتصحيح عدة أوهام تجعل المستخدم صيداً سهلاً للافتراس التكنولوجي، وعلى رأسها وَهْمُ التفوق على الذكاء البشري، على غرار المعالجين النفسانيين الرقميين المجهزين بالذكاء الاصطناعي الذين يراود لهم أن يحلوا محل أخلاقيات ومهنية

ودفع علم النفس البشري، بدعوى أنها أكثر ذكاء وخصوصية، بالرغم من كون كل المؤشرات توحى بأنها تحتل مخاطر جمة على الحياة الخاصة للأفراد، فضلاً عن ضعف كفاءتها في سبر أغوار النفس الإنسانية. بل حتى في المجال المعرفي لا تزال تطبيقات الذكاء الاصطناعي مخترقة بعيوب عديدة تجعل إجاباتها غير دقيقة وأحياناً كارثية، فضلاً عن كونها تقتصر على تقديم ردود نمطية؛ وهكذا تقول الكاتبة إنه يمكن للخوارزمية أن تتفوق في امتحان القبول في كلية الحقوق بجامعة هارفارد، ولكن ليس بقلم في يدها. كما أنها تظل عاجزة عن مسايرة الذكاء الطبيعي في عوالم التخيل والحكمة والمهارات الاجتماعية، حيث يتساءل ساخرًا نيك بوستروم (Nick Bostrom)، مدير معهد مستقبل الإنسانية (FHI) بجامعة أكسفورد: إذا كان الذكاء الاصطناعي الفائق قادراً على توليد صورة أزهار فهل في استطاعته مساعدتي على شم رائحتها؟ وإذا كان في استطاعته توليد أغنية تناسب حالة طفل يبكي فهل بإمكانه تهدئته عبر ملامسته؟

تكمّن المعضلة، حسب لورا غارسيا دي ريفيرا، في الاعتقاد السائد بأن المعالجة الحاسوبية لا يمكن أن تخطئ، فعموم البشر يميلون إلى إعطاء مصداقية شبه مطلقة للبرامج المعلوماتية كما لو كانت بطبيعتها الرياضية أكثر موضوعية وعقلانية، مع انطباع وثوقي يعتبر الذكاء الاصطناعي أذكى من البشر في كل الأحوال. وهذا الاعتقاد هو المشكلة الحقيقية، خصوصاً في ظل إشكالات عديدة تبرز عجز الخوارزميات في معالجة بعض المعطيات، وما ينجم عن ذلك من انتهاكات جسيمة لحقوق الإنسان. في هذا السياق، تقدم الباحثة حالات دالة من العالم الإسلامي، كاعتقال الشرطة الإسرائيلية لعامل بناء فلسطيني، في سنة 2017، إثر نشره لصورة على صفحته على فيسبوك مصحوبة بكلمة "يصبحهم" - "yusbihuhum"، حيث ترجمتها الشبكة تلقائياً إلى "هاجمهم" باللغتين، العبرية والإنجليزية. وفي حالات كثيرة لا تستطيع أنظمة الترجمة الآلية التعبير عن الاستعارات والصور البلاغية المضمّنة في عدة تعابير لغوية على نحو يؤثر سلبياً على حقوق الأفراد في التعبير والتنقل، كما في قصة امرأة أفغانية فرّت من أفغانستان ورفضت الولايات المتحدة طلبها للجوء بدعوى وجود تناقضات في شهادتها حينما ادعت أنها غادرت بلدها بمفردها؛ حيث أخطأ برنامج الترجمة الفورية القائم على الذكاء الاصطناعي في ترجمة الضمير أنا باللغة البشتونية إلى نحن باللغة الإنجليزية (15).

من بين الأوهام الأخرى، تشير الكاتبة إلى وجود تمثيلات خاطئة بكون من يجب أن يخشى من تسريب بياناته هم الأشخاص المشهورون أو السياسيون والصحفيون، والحال أن الخصوصية لا تتمثل في وجود أمور تستحق الإخفاء بل في وجود أشياء تتوجب حمايتها؛ حيث تنقل الكاتبة تشبيهاً دالاً على لسان إدوارد سنودن (Edward Snowden): عدم القلق بشأن الخصوصية لأنه ليس لديك ما تخفيه يشبه عدم الدفاع عن حرية التعبير لأنه ليس لديك ما تقوله (16)، مشيرة إلى تصاعد التحذيرات من المخاطر الرهيبة للذكاء الاصطناعي على خصوصية الناس؛ حيث وجّه أكثر من ألفي باحث وفاعل في المجال التكنولوجي رسالة إعلامية مفتوحة بهذا الخصوص، من ضمنهم ستيف وزنيك (Steve Wozniak)، المؤسس المشارك لشركة آبل، وجان تالين (Jaan Tallinn)، المؤسس المشارك لشركة سكايب، والعقيد ديفيد راسل (David Russell)، المدير السابق لقسم معالجة المعلومات بوكالة البحث والتطوير العسكرية التابعة لوزارة الدفاع الأميركية (DARPA)، الذي اختصر نصائحه في رسالة تحذيرية: لا تقل أبداً في أي رسالة إلكترونية ما لا ترغب في رؤيته منشوراً باسمك على الصفحة الأولى لجريدة نيويورك تايمز.

انطلاقاً من هذا التأسيس، تدعو لورا دي ريفيرا مستعملي الإنترنت إلى التشبث بحريتهم عند تجولهم بين دروب المنصات الإلكترونية للفرار من مصيدة الديكتاتوريات الرقمية، كما تنبههم إلى ضرورة التوقف عن التعامل كمستهلكين سلبين لكل ما تريد خوارزميات البيانات الضخمة بيعه لهم. وبدل ذلك، يتعين عليهم الإصرار على المقاومة ونبد القابلية للخضوع لسطوة الرقابة الخوارزمية التي تحدد ما يمكنك وما لا يمكنك رؤيته في عالم الإنترنت، على حدّ تعبير لوتشيانو فلوريدي (Luciano Floridi)، مدير مختبر الأخلاقيات الرقمية بمعهد أكسفورد للإنترنت. في ضوء ذلك، ترى الباحثة أن الأوان لم يفت بعد لوقف المد الزاحف لعمالقة التكنولوجيا الرقمية، بشرط اجترار استجابات متكافئة والبعد عن الحلول المثالية التي يصعب تطبيقها، خاصة من قبل الأجيال الصاعدة، لأنها تخدم غرض المنصات، فهي غير عملية ولا تساعد على التحكم فيها، كوضع حدّ زمني للأطفال وهو إجراء يستحيل مقابله مع المراهقين كأن تقول لطفلك: يمكنك التدخين، ولكن فقط من الساعة الخامسة إلى السادسة بعد الظهر (17).

لإسناد المقاومة الجماعية لسطوة الإقطاع التكنولوجي يتعين الاهتمام بالمدخل التشريعي، بإقرار مرجعيات تلزم مصنّعي ومسوّقي تقنيات الذكاء الاصطناعي بمسؤوليتهم القانونية عن كل فشل أو انتهاك للحقوق الدستورية وكل إضرار بمصالح المستعملين. حيث أشادت الكاتبة بقرار الاتحاد الأوروبي في 2015 باشتراط موافقة وكالات حماية البيانات الوطنية على كل إرسال للبيانات من الولايات المتحدة (18)، وبإصدار عدة مرجعيات توجيهية كمدونة قواعد السلوك العالمية للشركات البحثية العادلة (TRUST) التي حددت الأخطار القانونية والتشغيلية والأمنية المحدقة بالبيانات مع التوصية بالتدابير الحمائية اللازمة (19). كما نوّهت لورا دي ريفيرا ببعض التشريعات الأوروبية المهمة، كقانون الخدمات الرقمية (DSA) لسنة 2022 الذي استهدف التأسيس لبيئة آمنة عبر الإنترنت، بإلزام المنصات الرقمية بإزالة المحتوى غير القانوني وضمان شفافية الإعلانات وحماية حقوق المستخدمين (20)، وقانون الذكاء الاصطناعي (AIA) الذي أقره مجلس الاتحاد الأوروبي في سنة 2024، والذي نص على حظر بعض تطبيقات الخوارزميات التنبؤية، كأنظمة الشرطة القائمة على الملفات الشخصية أو الموقع أو السلوك الإجرامي السابق للأفراد ووضعهم الاجتماعي والاقتصادي، مع سَنّ عدة ضمانات لتأمين البيانات والتقليل من تأثيرات أنظمة الذكاء الاصطناعي على الديمقراطية وسيادة القانون والحريات (21).

غير أن التشريعات مهما بلغت جودتها فهي تبقى مرتبهة بتوفير شروط تطبيق للقواعد القانونية، وهو أمر ممكن فقط إذا كان المواطنون يعرفون حقوقهم ويحرصون على الدفاع عنها. بالرغم من تأكيد الكاتبة على تحميل الشركات الكبرى كامل المسؤولية عن التلاعب بالبيانات، فإن مسؤولية المستخدمين تظل قائمة، من خلال مقاومتهم لميكانيزمات الأنظمة الرقمية التي تحكم حياتهم اليومية، بالتوقف عن ابتلاع التوصيات الجاهزة للشبكات الرقمية بعيون مغلقة بالرغم من إمكانية إيجاد حلول أبسط وأرخص وأكثر فاعلية لحل مشكلة معينة. وقد حاولت الكاتبة تلخيص نصائحها بخصوص إذكاء الحس النقدي عبر عدة أسئلة استنكارية: لماذا يجب أن أتبع تعليمات خرائط غوغل حرفيًا عندما يخبرني حدسي أن هذه ليست أفضل طريقة للوصول إلى وجهتي؟ وهل من الضروري أن تباع حريتك مقابل راحتك حيث تحاول الشركات الضخمة تغذية مشاعر الكسل والاعتمادية لتستمر في نهب بياناتك لتعظيم

أرباحها؟ ولماذا نقبل بشكل افتراضي أي منتج تكنولوجي بالرغم من وجود بدائل قد تكون أكثر أمناً؟ ولماذا تترأى لنا باستمرار إعلانات تتطابق مع ما نفكر فيه أو نشعر به؟

للانفكاك، من فخ الخوارزميات، يتعين تقليل الاعتماد على التوصيات الآلية، باستخدام البحث اليدوي بدل الركون للمحتوى الموصى به، وبالاتماد على مصادر متعددة للمعلومات والأخبار بدل الاكتفاء باقتراحات الشبكات الرقمية، وتجنب مشاركة معلومات حساسة يمكن استخدامها لتوجيه الإعلانات أو التلاعب بالمحتوى كمشاركة الموقع الجغرافي في كل منشور، مع الحرص على التحقق من صحة الأخبار المثيرة بالبحث عنها في وكالات الأنباء الرسمية، وتشجيع الصحافة المستقلة التي تقدم الأخبار والمعلومات من مصادر موثوقة غير خاضعة لخوارزميات الإعلانات على شاكلة الغارديان (The Guardian)، والشبكات الاجتماعية المفتوحة المصدر التي لا تعتمد على نماذج إعلانية مدفوعة بالبيانات، كاستخدام ماستودون (Mastodon) بدلاً من تويتر، وسيغنال (Signal) كبديل آمن للواتساب. إضافة إلى التعود على آليات احترازية للحد من ولوج الشبكات الاجتماعية كاستخدام مؤقتات رقمية لتحديد وقت استخدام "تطبيقات إدمانية" مثل تيك توك وإنستغرام.

ارتباطاً بالجانب التقني، تطرح الكاتبة حزمة من البرامج الأكثر حماية للبيانات، كنظام التشغيل لينكس (Linux)، وبرنامج جيتسي للتناظر المرئي (Jitsi Meet) الذي لا يفرض التسجيل وتقديم أية بيانات شخصية لاستعماله، إضافة إلى اقتراح بدائل معلوماتية كمحركات البحث المفتوحة المصدر التي تحترم خصوصيات المتصفح ولا تقدم نتائج متحيزة مثل داك داك جو (DuckDuckGo)، وسيركس (Searx)، ومتصفحات أكثر أمناً مثل "تور" (The Onion Router)، وكذا استخدام أدوات مقاومة التتبع بثبيت إضافات المتصفح التي تكبح التتبع الإعلاني مثل أدبلوك (AdBlock) وبريفسي بادجر (Privacy Badger). إضافة إلى تفعيل الخيارات المتاحة لرفض التلاعب الرقمي كتعطيل الإعلانات المستهدفة في إعدادات الحساب، مع الحث على الاشتراك في بعض الخدمات المدفوعة كالتراسل عبر البريد الإلكتروني المشفر مثل بروتون ميل (ProtonMail)، وبرنامج حماية الهوية أثناء تصفح الإنترنت واستخدام الشبكات الخاصة الافتراضية (VPN). وكذا أدوات مراقبة البيانات والملفات الشخصية التي تجمعها المواقع على غرار أداة "طلب بياناتي" (My Data Request).

بالرغم من دعوة الكاتبة إلى التكتل لمواجهة المد الخوارزمي الزاحف، عبر إحالاتها المتكررة على رواد فكرة المقاومة المدنية، كفروم (22)، وثورو (23)، فإن طرحها ظل ملتبسًا بخصوص فكرة العصيان المدني الإلكتروني (24) (ECD)، فالتدابير الجزئية التي اقترحتها لم تبرز بما فيه الكفاية كليات ممارسة هذا النمط من العصيان، خاصة في ظل تعدد تطبيقاته على المستوى الدولي، فإلى جانب التيارات "التخريبية التي تستهدف مواقع الحكومات والشركات المفترسة للخصوصية الرقمية على هجمات مجموعة أنونيموس (Anonymous)، ظهرت تعبيرات معرفية للعصيان المدني الإلكتروني تركز على التقاسم المجاني للمعارف والتقنيات الرقمية مثل حركة الوصول المفتوح (25) (Open Access Movement). نشير كذلك إلى أهمية التمييز بين المقاومة الدفاعية (defensive resistance) القائمة على التكنولوجيا والمقاومة المنتجة (productive resistance) المستندة على المعرفة: تعتمد الأولى على أدوات معلوماتية لتحديد المراقبة الخوارزمية كتطبيقات المراسلة المشفرة وأنظمة التشغيل، وأنظمة تشغيل لتحسين أمن البيانات كنظام كيوبز أو أس (Qubes) وبرمجيات "تشويش البيانات" بحجب مشاعر المستخدم وحذف ملفات تعريف الشبكات الاجتماعية. أما ديناميكيات المقاومة المنتجة فتتوجه بالأساس نحو محو "أمية البيانات" كمبادرة مقاهي الخصوصية (Cryptopartys)، وأدوات التوجيه الإلكتروني لحماية الحقوق الرقمية للمستخدمين، وحملات المناصرة والتقاضي الاستراتيجي للتأثير على حوكمة البيانات، كحملة استعد وجهك في 2020 للمطالبة بحظر تقنية التعرف على الوجه في الأماكن العامة (26).

بشكل عام، يقدم الكتاب تشخيصًا مهمًا لسياقات تشكّل الإقطاع التكنولوجي ومظاهر تغوله، مع تفكيك الآليات المستعملة في انتهاك الخصوصية وتكريس الإدمان والاعتمادية، ورصد تداعيات ذلك على مختلف المستويات؛ حيث تعتبر الذكاء الاصطناعي ليس مجرد أدوات تقنية للاستعمالات العابرة، بل هي آليات لإعادة تشكيل المجتمعات وتغيير طرق العيش والتدبير. كما يُقدّم الكتاب دليلًا عمليًا من أجل مقاومة متبصرة ومبتكرة انطلاقًا من أدوات متنوعة يمكن أن تسهم في التخفيف من وطأة المعالجة الخوارزمية على إرادة الإنسان وحرية في عصر "استعمار البيانات"، الذي أصبحت مخاطره تتجاوز الحقوق الأساسية للأفراد إلى تهديد السيادة السياسية والاقتصادية للدول، وهو ما يفرض بلورة استجابات جماعية

متكافئة من أجل الوقوف في وجه الأوليغارشيا الرقمية في سعيها لمراكمة ثروات خيالية باستغلال مناجم "الداتا الشخصية" على غرار الاستعمار التقليدي الذي كان ينهب الثروات المادية والرمزية للشعوب المغلوبة على أمرها.

المراجع

(1) Laura G. De Rivera, Esclavos del algoritmo: Manual de resistencia en la era de la inteligencia artificial, (Madrid: DEBATE, 2025).

(2) يشير المفهوم إلى إمبريالية جديدة تستعمل من خلالها شركات التكنولوجيا الضخمة البيانات الرقمية للمستخدمين في تعظيم أرباحها، على غرار الإمبريالية التقليدية التي كانت تنهب الموارد الطبيعية للشعوب. للتوسع، يرجى مطالعة كتاب "الإقطاع التكنولوجي" للمفكر الاقتصادي ووزير المالية اليوناني الأسبق، يانيس فاروفاكيس:

Varoufakis, Yanis, Technofeudalism: What Killed Capitalism (London: Penguin Books, 2023).

(3) Mejias, Ulises A., and Nick Couldry. Data Grab: The New Colonialism of Big Tech and How to Fight Back. New York: W. W. Norton & Company, 2023, P.47-48.

(4) Matzner, Tobias. Algorithms: Technology, Culture, Politics (New York: Routledge, 2024), p.112.

(5) Laura G. De Rivera, p.80.

(6) يتعلق الأمر بشكل أساسي بوكالة الأمن القومي، ومكتب التحقيقات الفيدرالي، ووكالة المخابرات المركزية، ودائرة إنفاذ الهجرة والجمارك.

(7) Laura G. De Rivera, p.83.

(8) Brundage, Miles, Shahar Avin, Jack Clark, Helen Toner, Peter Eckersley, et al. Attacking Artificial Intelligence: AI's Security Vulnerability and What Policymakers Can Do About It. Center for a New American Security, 2018, p.18.

(9) كامبريدج أناليتيكا: شركة لتحليل البيانات السياسية تأسست ببريطانيا منذ سنة 2013، تخصصت في توظيف البيانات الضخمة وتكنولوجيا المعلومات لاستهداف الناخبين بحملات مخصصة، أعلنت إفلاسها في سنة 2018 بعد سلسلة من التحقيقات القضائية والغرامات إثر إثبات تورطها بالتلاعب ببيانات المستخدمين وتضليل الرأي العام.

(10) McKernan, Bethan, and Harry Davies. "‘The Machine Did It Coldly’: Israel Used AI to Identify 37,000 Hamas Targets". The Guardian, April 3, 2024. (Visited on 23 February 2025): <https://bit.ly/3DIR70l>

(11) Gerrit De Vynck. "Google rushed to sell AI tools to Israel’s military after Hamas attack". The Washington Post, January 21, 2025. (Visited on 23 February 2025) <https://bit.ly/4h1ezxY>

(12) Frederik J. Zuiderveen Borgesius et al., "Should We Worry About Filter Bubbles?" Internet Policy Review 5, no. 1 (March 2016), p.6. (Visited on 19 February 2025) <https://doi.org/10.14763/2016.1.401>.

(13) Laura G. De Rivera, p.197.

(14) GAFAM هو اختصار لأكبر خمس شركات كبرى في مجال التكنولوجيا الرقمية: جوجل (ألفابت)، آبل، فيسبوك (ميتا)، أمازون، ومايكروسوفت.

(15) Laura G. De Rivera, p.213.

(16) Snowden, Edward. Permanent Record (Barcelona: Planeta, 2019), p.3.

(17) Laura G. De Rivera, p.224.

(18) أفضت تحقيقات أوروبية بشأن ممارسات شركات التكنولوجيا الأميركية إلى وضع قيود عديدة لحماية بيانات المستعلمين؛ حيث قضت محكمة العدل الأوروبية، في 2015، ببطان اتفاقية "الملاذ الآمن للبيانات" بين الولايات المتحدة الأميركية والمفوضية الأوروبية، لتحل محله اتفاقية "درع الخصوصية الأوروبية الأميركية"، التي تعهدت بموجبها الولايات المتحدة بإحداث هيئة للتعامل مع شكاوى مواطني الاتحاد الأوروبي بشأن الأميركيين الذين يتجسسون على البيانات الخاصة بهم. للتوسع: محمود سعيد موسى، المكان كله مراقب: ماذا يخسر الأوروبيون مقابل الأمان؟ شبكة منشور، 15 نوفمبر/ تشرين الثاني 2017، (تاريخ الدخول: 09 فبراير/ شباط 2025)،

<https://bit.ly/3WW5aAm>

(19) TRUST. The TRUST Code - A Global Code of Conduct for Equitable Research Partnerships. 2018. (Visited on 15 February 2025) <https://doi.org/10.48508/GCC/2018.05>.

(20) Règlement (2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques). (Visited on 15 February 2025) <http://data.europa.eu/eli/reg/2022/2065/oj>.

(21) Karen Silverman and Brinson Elliott, eds. Artificial Intelligence Law: European Union. Edition 1. Law Business Research, 2024, p. 12-13.

(22) إريك فروم (Erich Fromm): فيلسوف وعالم نفس اجتماعي ألماني-أميركي (1900-1980)، عُرف بكتابه "الهروب من الحرية" (1940) الذي أكد فيه على أن الحرية الحقيقية تتطلب الوعي الذاتي والمسؤولية الفردية.

(23) هنري ديفيد ثورو (Henry David Thoreau): كاتب وفيلسوف أميركي عاش في القرن التاسع عشر (1817-1862)، يُعد من أوائل المفكرين الذين نظّروا لفكرة العصيان المدني (Civil Disobedience)، من خلال مقال نشره في سنة 1849، دعا فيه إلى مقاومة القوانين الجائرة بوسائل غير عنيفة، كرفض دفع الضرائب وعدم الامتثال للقوانين التعسفية.

(24) شكل حديث من أشكال العصيان المدني يستخدم الأدوات الرقمية في مواجهة الأنظمة السياسية والاقتصادية مثل الهجمات الإلكترونية، وتسريب البيانات الحكومية، والتضليل الرقمي، وتجاوز الرقابة لمعارضة الأنظمة القمعية أو السياسات غير العادلة.

(25) Delmas, Candice. "Is Hacktivism the New Civil Disobedience?" Social Theory and Practice, vol. 43, no. 4 (2017), p. 79.

(26) Milan, Stefania. "Resistance in the Data-Driven Society" Internet Policy Review 13.4 (2024). <https://doi.org/10.14763/2024.4.1811> (Visited on 17 February 2025).

من إصدارات المركز



للباب

للدراستات الاستراتيجية
دورية محكمة تصدر عن مركز الجزيرة للدراسات

العنوان

وادي السيل، الدوحة، قطر
صندوق البريد: 23123

للتواصل

lubab@aljazeera.net
هاتف: +974 40158384
فاكس: +974 44831346

سعر النسخة: 15 ريالاً أو 4 دولارات