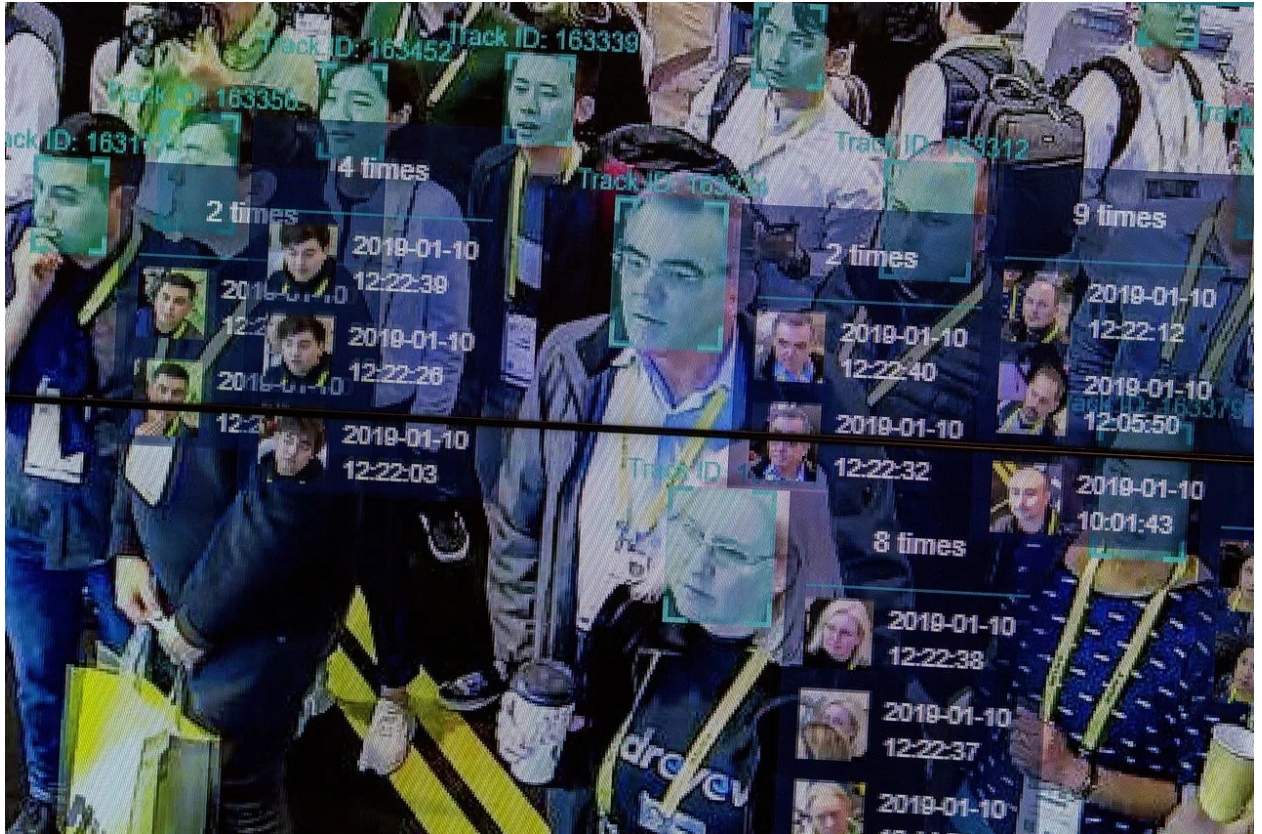


تقنية التعرف على الوجه.. عصر المراقبة الكاملة ونهاية الخصوصية

كتبه مرتضى الشاذلي | 14 أغسطس 2019



في عام 1995، عندما كتب نيكولاس نغروبونتي [كتابه](#) "Being Digital"، وهو أكثر أعماله المؤثرة في الحياة التي تحركها التكنولوجيا، كانت تقنية التعرف على الوجه حينها لا تزال حلمًا، لكنه شعر أن هذه التقنية كانت مقدرًا لها أن تصبح حقيقة واقعية.

“وجهك هو جهاز العرض الخاص بك، وينبغي أن يكون جهاز الكمبيوتر الخاص بك قادرًا على قراءته، الأمر الذي يتطلب التعرف على وجهك وتعبيراته الفريدة”، [كتب](#) نغروبونتي هذه الكلمات، وزاد عليها بقوله إن “التحدي التقني المتمثل في التعرف على الوجوه وتعبيراتها هو تحد هائل، ومع ذلك، تعد عملية تنفيذه قابلة للتحقيق بدرجة كبيرة في بعض السياقات”.

بعد سنوات قليلة من هذه الكلمات، أصبحت تقنية التعرف على الوجوه سلاحًا سريعًا للسلطات في أنشطة المراقبة، وكانت ضمن أحدث الجهود التي بذلتها النخبة السياسية والشركات العالمية الكبرى لجعل محيطنا أكثر قمعًا قدر الإمكان قبل احتراق الكوكب في كارثة مناخية، مما يثير مخاوف جدية بين المواطنين حول الخصوصية والقضايا الأخرى.

التعرف على الوجه.. أحدث سلاح للسلطات

أحد ركائز صناعة المراقبة هي تقنية التعرف على الوجه، التي أثارت القلق في الآونة الأخيرة، خاصةً مع ظهور **عناوين** على شاكلة أن "مكتب التحقيقات الفيدرالي لديه حق الوصول إلى أكثر من 640 مليون صورة" من خلال قاعدة بيانات التعرف على الوجه واستخدام نظارات شمسية ذكية يمكن أن تجعل المراقبة العامة سرية وفي كل مكان.

بالطبع، نحن الآن نعرف الكثير عن حالات الاستخدام الأخرى للتعرف على الوجه، ففي السنوات الأخيرة، تم **تقديم** ميزة التعرف على الوجه في المطارات حول الولايات المتحدة كوسيلة لتأكيد هويات المسافرين، كما تم استخدامه منتصف العام الماضي لتحديد هوية الرجل الذي **قتل** 5 أشخاص في أحد مكاتب الصحف في ولاية ماريلاند، وبعدها بشهر، **أُستُخدم** تحديد شخصين يشتبه في تسممهما العميل الروسي المزدوج سيرجي سكريبال وابنته يوليا في المملكة المتحدة.

هناك المزيد والمزيد من الحالات التي تحاول فيها الحكومات والشركات تطبيق هذه التكنولوجيا على الدوائر التلفزيونية المغلقة وأجهزة تسجيل الفيديو المحمولة

كما **تعمل** شركات التقنية على إنشاء برنامج للتعرف على الوجه يمكنه، من بين أشياء أخرى، مساعدة المكفوف على معرفة من في الصورة، أو حتى من في الغرفة معه، بالإضافة إلى ذلك، **تأمل** شركات بطاقات الائتمان أن يكون التعرف على الوجه هو الخطوة التالية في مصادقة الدفع.

أصبحنا على دراية بميزات التعرف على الوجوه في هواتفنا المحمولة. لكن في المقابل، رأينا كيف يمكن إساءة استخدام تقنية التعرف على الوجه، فهناك المزيد والمزيد من الحالات التي تحاول فيها الحكومات والشركات تطبيق هذه التكنولوجيا على الدوائر التلفزيونية المغلقة وأجهزة تسجيل الفيديو المحمولة.

على سبيل المثال، في أماكن مثل قاعة المغادرة الحدودية في مطار هونغ كونغ الدولي، والكاзиноهات في منطقة ماكاو الصينية، والمدارس في بر الصين الرئيسي، وأماكن الحفلات الموسيقية، وعقارات الإسكان العامة، وحتى عند معابر الطرق، يتم فحص الوجوه بهدوء، حيث يزداد استخدام هذه التقنية يزداد في كل مكان.

وفي حين أن التعرف على الوجوه أصبح بسرعة أحدث سلاح للسلطات في مختلف البلدان، إلا أن المشكلات التي تسببت فيها هذه التقنية أثارت الكثير من الجدل. من المؤكد أن إدارات تطبيق القانون قد وجدت أن تقنية التعرف التلقائي على الوجوه مفيدة، مما يسهل تحديد المشتبه بهم من خلال المقارنة مع قاعدة بيانات تحمل وجوههم، ويعزز الكفاءة في تطبيق القانون.

لكن الدراسات التي أجريت في الولايات المتحدة وأوروبا أشارت إلى أن هذه التقنيات غير موثوق بها.

على سبيل المثال، في العام الماضي، [استخدمت](#) شرطة العاصمة لندن تقنية التعرف على الوجوه عدة مرات في إحدى المحاكمات لفحص وجوه المشاة، ومقارنة تلك السجلات بالأرشفات الخاصة بالمرجمن المطلوبين، من أجل تحديد المشتبه بهم في عمليات البحث.

وجهك يكشف هويتك

فيما يتعلق [بأسلوب المراقبة](#) الأحدث، عرضت الشرطة الصينية في فبراير/شباط 2018 إضافة جديدة إلى مجموعة أدوات مراقبة الحشود، حيث [عمدت](#) مع بدء مئات الملايين من الصينيين في السفر لعطلة رأس السنة القمرية الجديدة إلى الاستعانة بنظارات رياضية مجهزة بأجهزة التعرف على الوجه لاستخدامها في التحقق من ركاب القطارات والطائرات، للقبض على الأفراد الهاربين من العدالة أو من يستخدمون هويات وهمية.

على الرغم من أن هذه التقنية مفيدة على الأرجح في القبض على المجرمين، إلا أنها قد تسهل على السلطات تعقب المنشقين السياسيين وتحديد الأقليات العرقية

وذكرت صحيفة [The Wall Street Journal](#) الأمريكية أن شركة "LLVision" للتكنولوجيا ومقرها بكين، هي المطورة لهذه النظارات الذكية، إذ تنتج الشركة الصينية كاميرات فيديو يمكن ارتداؤها، ورغم بيع نظارات الفيديو لأي شخص، إلا أنها تفحص مشتري نظارة التعرف على الوجه الخاصة بها، كما لا تبيعها للمستهلكين العاديين.

الصين هي بالفعل رائدة عالمية في نشر أحدث تقنيات المراقبة القائمة على الذكاء الاصطناعي، ويمكن لأجهزة التليفون المحمولة توسيع نطاق هذه المراقبة، مما يسمح للسلطات بالبحث في الأماكن التي لا يتم فيها مسح الكاميرات الثابتة، والاستجابة بسرعة أكبر.

وبحسب الشركة الصينية، فإن الاختبارات كشفت أن النظارة الذكية قادرة على التحقق من الأفراد من قاعدة بيانات مكونة من 10 آلاف شخص، ويمكن أن تفعل ذلك خلال لحظات، فقاعدة البيانات المستخدمة لمقارنة الصور موجودة في جهاز محمول باليد بدلا من سحابة، إلا أن دقة النظارة قد تنخفض بعض الشيء في الاستخدام العملي، بسبب "الضوضاء البيئية".

ليس هذا فحسب، وفق ما ذكرته صحيفة ["New York Times"](#)، تقوم الكاميرات في بعض المدن الصينية "بفحص محطات القطار بحثاً عن أكثر الأشخاص المطلوبين للعدالة، وتُظهر الشاشات التي تظهر بحجم لوحة الإعلانات وجوه المتجولين في الشوارع وقائمة بأسماء الأشخاص الذين لا يدفعون ديونهم"، كما [يتم استخدام](#) التعرف على الوجه في منطقة شينجيانغ للمساعدة في اضطهاد أعضاء الأقلية المسلمة في الإيغور، حيث تقوم الدولة بجمع بياناتهم بما في ذلك مسح الوجه لتتبعهم ومعرفة خريطة علاقاتهم مع الأصدقاء والعائلة.



شرطية ترتدي نسخة من النظارات الشمسية للجهاز في محطة للسكك الحديدية في مدينة تشنغتشو بوسط الصين

على الرغم من أن هذه التقنية مفيدة على الأرجح في القبض على المجرمين، إلا أنها قد تسهل على السلطات تعقب المنشقين السياسيين وتحديد الأقليات العرقية، وبحسب وليم ني، الباحث الصيني في منظمة العفو الدولية، فإن القدرة على إعطاء ضباط الشرطة الأفراد تقنية التعرف على الوجه في النظارات الشمسية يمكن أن تجعل حالة المراقبة في الصين في كل مكان في كل مكان.

في المقابل، هناك الكثير من المشجعين لاستخدام هذه التقنية، ففي يونيو/حزيران، نشرت صحيفة [The New York Times](https://www.nytimes.com) الأمريكية مقالة افتتاحية بعنوان "كيف يجعلك التعرف على الوجه أكثر أماناً"، ونقلت عن مفوض شرطة نيويورك جيمس أونيل قوله: "إذا تم استخدامه بشكل صحيح، فإن البرنامج يحدد بفعالية المشتبه في ارتكابهم جرائم دون انتهاك الحقوق"، ولكن كيف يمكن جعل أي شخص أكثر أماناً بسبب شيء غير دقيق بشكل مخيف؟

أداة واحدة تكفي لانتهاك حقوق الإنسان

في العام الماضي، على سبيل المثال، [أجرى](https://www.nytimes.com) الاتحاد الأمريكي للحريات المدنية (ACLU) اختباراً لأداة التعرف على الوجه الخاصة بشركة أمازون، والتي يطلق عليها Rekognition، والتي قارنت بين صور جميع أعضاء الكونغرس الأمريكي وقاعدة بيانات مجانية ومفتوحة.

وفقاً للأداة المستخدمة، كانت النتائج: 28 من أعضاء الكونغرس الأمريكي تم تحديدهم كمجرمين

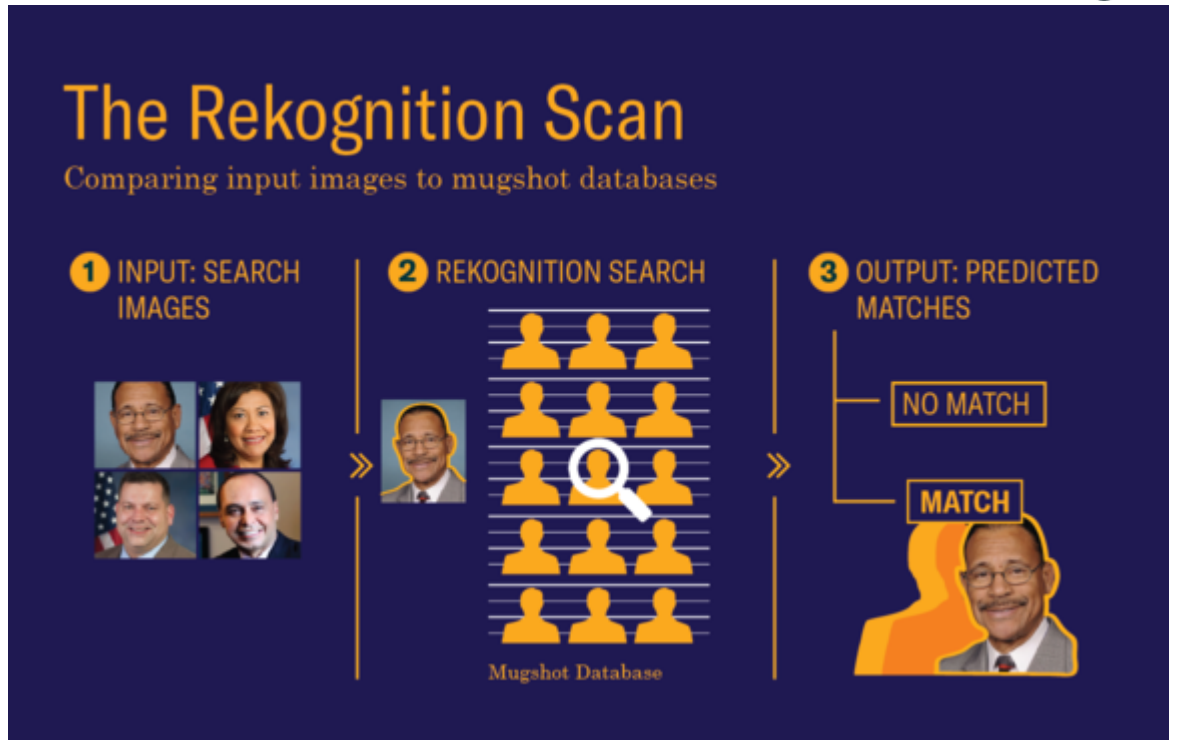
تم اعتقالهم مسبقاً، وكانت الأخطاء في التطابق بين الشخصيات الحقيقية وقاعدة البيانات تتعلق بشكل غير متناسب بأشخاص من نفس اللون، من بينهم على سبيل المثال أيقونة الحقوق المدنية النائب جون لويس. توضح هذه النتائج لماذا يجب على الكونغرس الانضمام إلى الاتحاد الأمريكي للحريات المدنية في الدعوة إلى وقف استخدام تقنية مراقبة الوجه.

براد سميث، الرئيس والمدير القانوني لشركة مايكروسوفت: “تخيل قاعدة بيانات لكل من حضر مسيرة سياسية تشكل جوهر حرية التعبير”

كما توضح العواقب السلبية غير المقصودة والعميقة التي قد تواجهها المراقبة بالنسبة للسود والمهاجرين غير الشرعيين والمتظاهرين، حيث **أظهرت** الأبحاث الأكاديمية بالفعل أن التعرف على الوجوه أقل دقة للوجه ذي البشرة الداكنة والنساء، وتؤكد النتائج هذا الشاغل بوجود ما يقرب من 40% من متطابقات Rekognition الخاطئة في الاختبار لأشخاص ملونين، على الرغم من أنهم يشكلون 20% فقط من الكونغرس.

تحديد الهوية – سواء كانت دقيقة أم لا – يمكن أن يكلف الناس حريتهم أو حتى حياتهم، فإذا كان تطبيق القانون يستخدم أداة مثل Amazon Rekognition، فليس من الصعب تخيل حصول ضابط شرطة على “تطابق” يشير إلى أن الشخص مطلوب القبض عليه في قضية سابقة تتعلق بحيازة أسلحة، أو قد يستدعي تطبيق القانون اقتحام منزل أي شخص واستجوابه أو تفتيش منزله بناءً على هوية مزورة.

يتعرض الأشخاص الملونون بالفعل للأذى غير المتناسب من ممارسات الشرطة، ومن السهل أن نرى كيف يمكن أن تؤدي أداة واحدة إلى تفاقم ذلك، على سبيل المثال، **وقعت** مؤخرًا حادثة في سان فرانسيسكو تقدم مثالاً مقلماً لهذا الخطر، حيث أوقفت الشرطة سيارة، وقيدت سيدة سوداء عجوز، وأجبرتها على الركوع تحت تهديد السلاح، كل ذلك لأن قارئ لوحة الأرقام الأوتوماتيكي حدد سيارتها كمرعبة مسروقة.



تم التعرف على النائب سانفورد بيشوب بشكل خاطئ من قبل أداة Amazon Rekognition كشخص تم اعتقاله بسبب جريمة

مع تصاعد ردود الفعل من الجمهور، أصبحت سان فرانسيسكو، في يونيو/حزيران من هذا العام، أول مدينة في الولايات المتحدة تقوم بحظر استخدام الحكومة تقنية التعرف على الوجه من قبل الشرطة والوكالات الأخرى. ومن المقرر أن تحذو حذوها مدن أخرى. على سبيل المثال، في أوكلاند، هناك خطط لإدخال تشريع مماثل.

بينما في نيويورك، توصل الناس إلى مقترحات لمنع الملاك من تطبيق هذه التكنولوجيا لمراقبة المستأجرين، وفي مايو/أيار من هذا العام، أصدرت كاليفورنيا قوانين لمنع أي شخص من استخدام أجهزة تسجيل الفيديو المحمولة مع تقنية التعرف على الوجه، لكن لا تزال هناك حاجة إلى مزيد من الجهد لوضع حد لفيلم الرعب العلمي أمام أعيننا.

تهديد القانون وليس إنفاذه

توسع استخدام تقنية التعرف على الوجه في الآونة الأخيرة، ومن المتوقع أن تصل قيمة السوق العالمية لكاميرات وبرامج التعرف على الوجه إلى 7.8 مليارات دولار بحلول 2022 وفق توقعات مؤسسة [Markets and Markets](#) لأبحاث السوق. من المتوقع أيضًا أن تكون الحاجة المتزايدة للمراقبة في الأماكن العامة أحد العوامل الرئيسية التي تدفع نمو سوق تقنيات التعرف على الوجه.

تترجع دولة الإمارات على رأس الدول الرائدة في تبني التقنيات الجديدة، ولا يعتبر استخدام برامج التعرف على الوجه استثناءً في ذلك

تخيل الآن المضاعفات التي قد تنشأ عندما تكون مثل هذه التكنولوجيا المضطربة في أيدي مسؤولي إنفاذ القانون في بلدك، والذين أثبتوا بالفعل استعدادهم لإطلاق النار على المتظاهرين دون سبب، أو تصفية المعارضين لهم بحجة "الحرب على الإرهاب". تخيل أيضًا حكومة تتعقبك في كل مكان كنت تسير فيه خلال الشهر الماضي دون إذنك أو معرفتك.

في هذا الشأن **كتب** براد سميث، الرئيس والمدير القانوني لشركة مايكروسوفت، في دعوة عامة لتنظيم تكنولوجيا التعرف على الوجه: "تخيل قاعدة بيانات لكل من حضر مسيرة سياسية تشكل جوهر حرية التعبير، أو لا تتخيل ذلك، فقط ابحث عن الصين، حيث **أتاحت** تقنية التعرف على الوجه جميع أنواع الفرص لإلغاء حقوق الإنسان وقمع المعارضة.

في هذه الحالة، يجب النظر إلى الجغرافيا السياسية بنفس القدر من الأهمية، أي البلدان التي أصبحت المزود الرئيسي والمستهلكين للتكنولوجيا، وفي هذا السياق، يمكن النظر إلى **مطالبات** إحدى الولايات القضائية المتعلقة بالاحتياجات الأمنية على أنها تجسس من جانب الحكومة أو الشركات في دولة أخرى.

في المملكة المتحدة، **تجري** الشرطة تجارب بملايين الجنيهات على تقنية التعرف على الوجه في المناطق العامة في جنوب ويلز وليسترشير والعاصمة لندن، ولا تمانع في إجراء بعض التحقيقات المزعجة التي تكشف عن أن أكثر من 90% من التطابقات التلقائية للتعرف على الوجه غير صحيحة. مع ذلك، لا توجد حاليًا أي قوانين أو سياسات حكومية لتنظيم استخدامها. يتم حاليًا **استخدام** الشرطة للتعرف على الوجه في المحاكم.



Credit: MONOPOLY911 / Shutterstock

وفي الولايات المتحدة، واحد من كل اثنين من المواطنين الأمريكيين موجود في قاعدة بيانات للتعرف على الوجه، بدعوة إنفاذ القانون، وفي كثير من الأحيان، أدّى استخدام هذه التقنية إلى نتائج مضللة، نتجت عن القوالب النمطية العنصرية والجنسانية، وتعرضت لهجمات من جماعات حقوق الإنسان.

عربيًا، تبرع دولة الإمارات على رأس الدول الرائدة في تتبي التقنيات الجديدة، ولا يعتبر استخدام برامج التعرف على الوجه استثناءً في ذلك، وبشكل عام تعتمد الإمارات على تقنيات الذكاء الاصطناعي لمراقبة وحماية الحدود. يوجد في مطار دبي الدولي حوالي 80 كاميرا للتعرف على الوجه لتأكيد هوية المسافرين خلال 10 ثوانٍ، ثم يقوم النظام بمسحهم للدخول إلى البلاد أو تنبيه موظفي الأمن، ويتعلق بذلك خطة لأتمتة مكاتب الهجرة بالكامل بحلول 2020، باستخدام تقنيات الذكاء الاصطناعي والتعرف على الوجه لتأكيد هوية المسموح لهم بدخول البلاد.

في النهاية، يعتقد الخبراء أنه فات أوان إعادة وضع بيانات الوجه في صندوق، أو تقييد حركتها عبر الحدود الجغرافية. في الواقع، فإن التعرف على الوجه ليس سوى الخطوة الأولى من نظام "المراقبة البيومترية" الذي يتعدى مواطني الدولة إلى الأجانب الذين يعبرون الحدود.

رابط المقال : <https://www.noonpost.com/28926/>