التحالف الإسلامي العسكري لمحاربة الإرهاب
ISLAMIC MILITARY COUNTER TERRORISM COALITION
الإدارة العامة للتخطيط والتنسيق

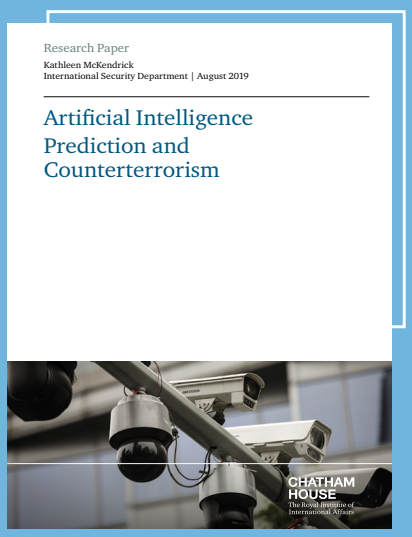
9

تقارير خاصة
يناير 2020

حول

الذكاء الاصطناعي ومحاربة الإرهاب

الحدود والفرص والمخاطر


Research Paper
Kathleen McKendrick
International Security Department | August 2019

Artificial Intelligence Prediction and Counterterrorism

CHATHAM HOUSE
The Royal Institute of International Affairs

التحالف الإسلامي العسكري لمحاربة الإرهاب
ISLAMIC MILITARY COUNTER TERRORISM COALITION

9

تقارير خاصة

يناير 2020

حول

الذكاء الاصطناعي ومحاربة الإرهاب
الحدود والفرص والمخاطر

يـدل **مصطلح الذكاء الاصطناعي** Artificial intelligence (AI) على قدرة الآلات والحواسيب الرقميَّة على القيام بمهامَّ محددةٍ تشبه ما تقوم بها الكائنات الحية الذكية؛ كالقدرة على التفكير والتخطيط، والتعلُّم والإبداع، والتكيُّف والتفاعل، وتحسين الإجراءات، واستخلاص المعارف، والتنبُّؤ من البيانات الرَّقْمية الكبيرة والمتنوعة، وغيرها من العمليات الأُخرى التي تتطلب عمليات ذهنية دقيقة.

ويذكر خبراء محاربة الإرهاب أن هناك طريقتين لمنع الهجَمات الإرهابية، الأولى حماية البنية التحتية والأفراد وتطبيق الضوابط الأمنية. والأخرى حرمان الإرهابيين من القدرة على شنِّ هجَمات، وذلك بالقبض عليهم قبل تنفيذ مخططاتهم، ومكافحة التطرف وتجنيد الإرهابيين.

ويناقش التقرير الذي أعدته الباحثة كاثلين ماكيندريك بعنوان (الذكاء الاصطناعي ومحاربة الإرهاب) والصادر عن معهد تشاثام هاوس في أغسطس 2019م، العلاقة المتعددة الأبعاد بين الإرهاب والذكاء الاصطناعي، وحدودها والفرص الممكنة والمخاطر المحتملة.

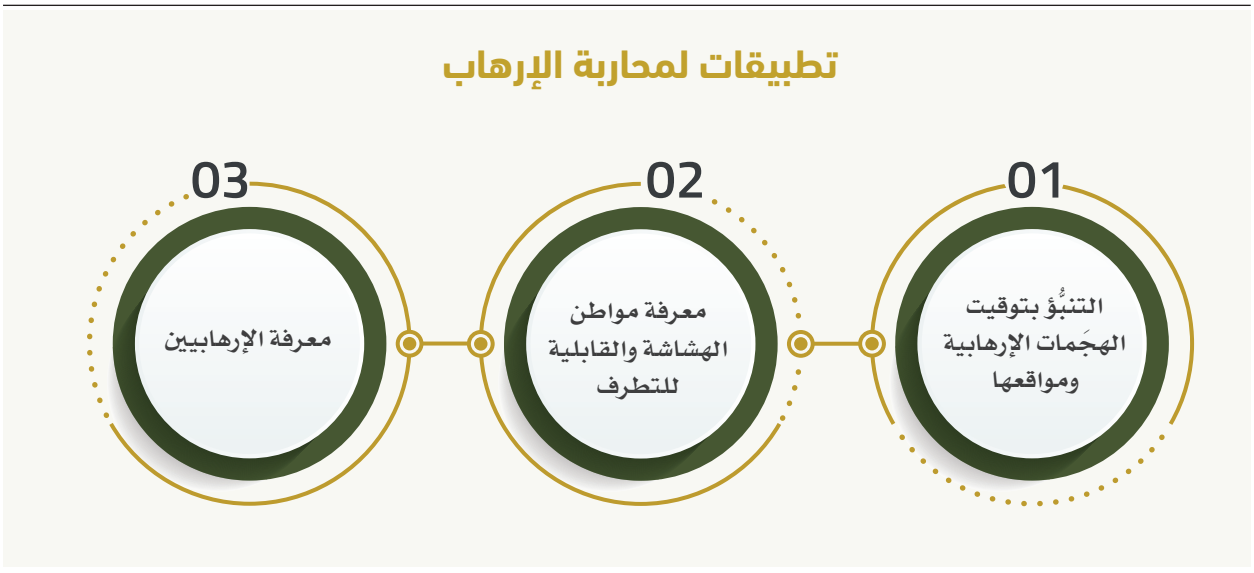
قد يتبادر إلى الذهن تساؤلٌ منطقي عن العَلاقة بين الذكاء الاصطناعي ومحاربة الإرهاب، والإجابة تبدأ بكلمة واحدة هي (التنبُّؤ) الذي يُعَدُّ أحدَ أهم استخدامات الذكاء الاصطناعي، فهو يسهم في منع الهجَمات الإرهابية بتوفير الحماية المادية للبنية التحتية، وتحسين تخصيص الموارد للمواقع التي يُحتمل أن تكون أهدافًا للإرهابيين، ويساعد على منع الإرهابيين من شنِّ هجَمات، بالقبض عليهم قبل تنفيذها، ويساعد أيضًا على مكافحة تجنيد الإرهابيين، ومعرفة الأفراد الأكثر عُرضةً للتطرف أو للتجنيد من قِبَل التنظيمات الإرهابية.

قد يؤدي استخدام الذكاء الاصطناعي في محاربة الإرهاب إلى تنبُّؤات دقيقة تحدُّ من الإجراءات غير الضرورية التي تطبق على أعداد كبيرة من السكان، وتخفف التحيُّز البشري في صنع القرار.

وتهدف محاربة الإرهاب الناجعة إلى توفير الأمن لغالبية المواطنين مع الحدِّ الأدنى من التعدي على الحقوق والحريات. ويسمح التنبُّؤ بتطبيق التدابير الوقائية لتقليل الأضرار على السكان، وقد ينصبُّ على الأعمال العنيفة التي ينوي الإرهابيون تنفيذها أو على الأفراد المعرَّضين للتطرف، وبذلك يكون التنبُّؤ الذي يوفره الذكاء الاصطناعي وسيلةً لتحسين تخصيص الموارد في محاربة الإرهاب، وتوفير الجهود والموارد المهدرة في هذا المجال.

وقد يؤدي استخدام الذكاء الاصطناعي في محاربة الإرهاب إلى تنبُّؤات دقيقة تحدُّ من الإجراءات غير الضرورية التي تطبق على أعداد كبيرة من السكان، وتخفف التحيُّز البشري في صنع القرار، وذلك بتوجيه الانتباه بدقة إلى المناطق أو الأفراد الأكثر عُرضةً للتهديدات، وتقليل عدد المواطنين الذين يخضعون لمزيد من المراقبة. وفي المقابل فإن عدم وجود ضمانات كافية لاستخدام الذكاء الاصطناعي، والسجلَّات الضخمة من البيانات التي يعتمد عليها، لا يؤدي إلى سوء استخدامها لفرض السيطرة على المواطنين وحسب، ولكن يؤدي أيضًا إلى التعدي المفرط على حقوقٍ أخرى مثل الخصوصية وحرية التعبير.

إنَّ نهج استخدام تقنيات التنبُّؤ الدقيقة للذكاء الاصطناعي في محاربة الإرهاب يمكن أن يخضعَ لأهداف متضاربة، ولكن ذلك لا يمنع من النظر في الاحتمالات والتكاليف لمثل هذا النهج، وفي سُبل تنظيم هذا المجال الوليد.



أصبحت قدرات الذكاء الاصطناعي التنبُّئية أمرًا معترفًا به في محاربة الإرهاب، ولكن تطبيقه لا يزال على نطاق ضيِّق، فأجهزة الأمن والاستخبارات تستخدم تحليل البيانات آليًا في تقييم مخاطر المسافرين جوًّا، وكشف الروابط بين التنظيمات الإرهابية وأعضائها. وتستخدمها الشرطة أيضًا في تحليل شبكات العصابات الإجرامية، وتستخدم بعض شركات التقنية التدابير التنبُّئية المتطورة لرصد النشاط الإرهابي على مِنصَّات التواصل الاجتماعي، وتعطيلها، ويُستخدم الذكاء الاصطناعي في قطاع الخِدَمات المالية للإبلاغ عن أي نشاط مشبوه.

عدم وجود ضمانات كافية لاستخدام الذكاء الاصطناعي، والسجلَّات الضخمة من البيانات التي يعتمد عليها، لا يؤدي إلى سوء استخدامها لفرض السيطرة على المواطنين وحسب، ولكن يؤدي أيضًا إلى التعدي المفرط على حقوقٍ أخرى مثل الخصوصية وحرية التعبير.

ونذكر بعض الأمثلة لقدرة الذكاء الاصطناعي على محاربة الإرهاب عبر التنبُّؤ:

1- التنبُّؤ بتوقيت الهجَمات الإرهابية ومواقعها

يمكن استخدام الذكاء الاصطناعي للتنبُّؤ بعمليات الإرهاب استنادًا إلى بيانات تعريف الاتصالات، ومعلومات المعاملات المالية، وأنماط السفر، ونشاط تصفح الشَّابِكة (الإنترنت). وقد طُوِّرت نماذجُ تتنبَّأ بمواقع الهجَمات الإرهابية وتوقيتها. ففي عام 2015 على سبيل المثال، ادَّعت شركة ناشئة تعمل في مجال التقنيات أن نموذجها التنبُّئي كان قادرًا على التنبُّؤ بالهجمات الانتحارية بدقة تبلغ 72%. كذلك اعتمدت بعض النماذج الأخرى على بيانات المصادر المفتوحة للأفراد الذين يستخدمون الوسائط الاجتماعية والتطبيقات على هواتفهم المحمولة، ومنها نظام تعرُّف الأحداث الاستباقي الذي يدمج نتائج مختلِف النماذج التنبُّئية المنفصلة للتنبُّؤ بأحداث محددة. ولا يعني المزيد من البيانات تحسين جودة التنبُّؤ بالضرورة، بل يجب التحقُّق من صحَّتها.

2- معرفة مواطن الهشاشة والقابلية للتطرُّف

طوَّرت بعض شركات التقنية أدواتٍ لتقييم قابلية التعرض للأفكار والعقائد المتطرفة العنيفة. وكانت أعلنت إحدى الشركات مشروعًا باسم (إعادة التوجيه) يستهدف مستخدمي مواقع (الفيديو) الذين قد يكونون عُرضةً للدعاية الإرهابية؛ إذ يُعيد المشروع توجيههم إلى مقاطع (الفيديو) التي تتبنَّى روايةً موثوقة ومضادة لرواية التنظيمات الإرهابية.

3- معرفة الإرهابيين

تبيِّن بعض المعلومات المسرَّبة عن برنامجٍ لوكالة الأمن القومي الأمريكية (SKYNET) أنه استُخدمت خُوارزميَّة معتمِدة على الذكاء الاصطناعي لتحليل البيانات الوصفية لنحو 55 مليون مستخدم للهاتف المحمول بباكستان عام 2007، وكانت النتيجة أن زُهاء 15 ألف فرد يحتمل أن يصيروا إرهابيين من إجمالي عدد السكان البالغ 200 مليون آنذاك. وعلى أن النموذج المستخدم لم يكن فاعلًا في حدِّ ذاته، قد أوضح القيمة التنبُّئية للبيانات عند تحديد روابطَ وثيقة مع الإرهاب.

هذه الأمثلة لحالات استخدام قدرات الذكاء الاصطناعي التنبُّئية في محاربة الإرهاب لا تزال في نطاق الاحتمالات، ولا يُتوقَّع من الذكاء الاصطناعي تقديمُ أجوبة فورية وشاملة ودقيقة للأسئلة المعقدة. ولكن تظل القدرة على تطوير أدوات الذكاء الاصطناعي لهذا الغرض تقع على عاتق أولئك الذين لديهم قدرةٌ على الوصول إلى البيانات أو حمايتها. ومع تحسين أداء الذكاء الاصطناعي، سيكون هناك مجال أكبر لاستخلاص تنبُّؤات دقيقة عن الإرهاب في المستقبل وزيادة استخدامها في محاربته.

التحديات

هناك نوعان من التحديات المتعلقة باستخدام الذكاء الاصطناعي في محاربة الإرهاب، أولهما يتعلق بحقوق الإنسان، وثانيهما يرتبط بالآثار العملية لهذه الممارسة.

أولًا) التحديات المرتبطة بحقوق الإنسان:

1- غياب معاييرَ راسخة لاستخدام تقنية الذكاء الاصطناعي

ليس هناك موقف دَولي موحد بشأن حدود استخدام الذكاء الاصطناعي، وهذا يضع حقوق المواطنين وحرياتهم على المحَكِّ، فتزداد الحاجة إلى ضمانات كافية لاستخدام الذكاء الاصطناعي من قِبَل الحكومات والأجهزة الأمنية، ومراجعة التدابير الموضوعة لحماية الخصوصية والحريات الأساسية للمواطنين.

> **كانت القدرة على التنبؤ بالتورط الإرهابي مستحيلةً في السابق، لكنها لم تعُد كذلك في الوقت الحالي. ويمكننا تحسين دقة النماذج التنبئية المبنية على مصدر واحد للبيانات بدمج النتائج مع الخُلاصات الأخرى.**

وقد أصدرت الجمعية العامة للأمم المتحدة قرارها رقم 68/167، في ديسمبر 2014 بشأن الحق في الخصوصية في العصر الرَّقمي الذي يُلقي على عاتق الدول مسؤوليةَ ضمان امتثال أنشطتها للقانون الدَّولي. وفي ديسمبر 2016 أصدرت المحكمة الأوربية حكمًا ضد بريطانيا لإخفاقها في تلبية الحقوق الأساسية التي يكفلها الاتحاد الأوربي في ممارسات الاحتفاظ بالبيانات.

2- عشوائية جمع البيانات

تعتمد كثير من الممارسات المرتبطة باستخدام التقنية التنبُّئية للذكاء الاصطناعي في محاربة الإرهاب على تطبيقها على جميع السكان، وهذا يجعل الأمر عشوائيًا، فضلًا عن انتهاكه خصوصيات العامَّة. وتميل الأطُر التشريعية ومبادئ الحوكمة المتعلقة باستخدام البيانات إلى العناية بصلاحيات الوصول إلى البيانات، وتتجاهل غالبًا تنظيم كيفية استخدام تلك البيانات أو حمايتها من سوء الاستخدام.

3- وظيفة القِطاع الخاصِّ المتنامي وضعف التنظيم

تتوزع مسؤولية الاستخدامات التنبُّئية للذكاء الاصطناعي في محاربة الإرهاب على مجموعة واسعة من الجهات الفاعلة، ومنها شركات التقنية التي حوَّل بعضُها المعلوماتِ المتعلقةَ بالجمهور إلى سلعةٍ يمكن أن تبيعَها إلى من يدفع! وقد تتمكَّن أجهزة إنفاذ القانون من الحصول عليها بطريقة قانونية، وهذا يعني أن التزامات الشركات الخاصَّة بحماية خصوصية العميل قد تكون موضعَ شك.

4- عدم الشَّفافية

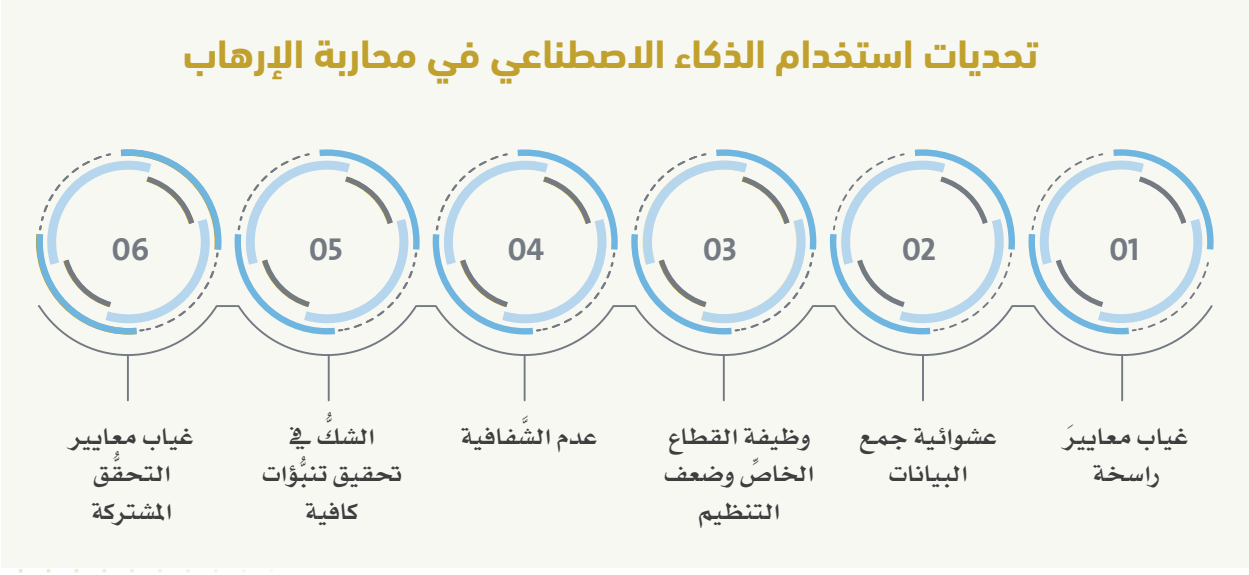
تخضع طرق استخدام الذكاء الاصطناعي في محاربة الإرهاب إلى تعتيم كبير، يصعُب معه الحصول على ضمانات قانونية للشَّفافية في محاربة الإرهاب.

ثانيًا) التحديات العملية:

1- ضعف القدرة على تحقيق تنبُّؤات كافية

للظاهرة الإرهابية صنوفٌ شتَّى ومساراتٌ مختلفة، وهذا يعني استحالةَ إعداد قائمة نهائية لمؤشِّرات التورط في الإرهاب أو الاستبعاد منه. وإن العدد الصغير للإرهابيين من عموم السكان يجعل الوصول إلى خصائصَ واسعةٍ للإرهابيين على أساس التنميط لا قيمةَ تنبُّئية له. فانخفاض معدل وقوع الإرهاب، وميل الوسائل الإرهابية إلى التطور السريع، يجعلان من الصعب بناء نماذج تنبُّئية جيدة.

ومع ذلك أظهرت البحوث أنه قد يكون من الممكن استخدام الذكاء الاصطناعي لتحليل الاتصالات والخصائص المميزة، كدرجة التطرف، أو النية العدوانية، وهذا يعني أن القدرة على التنبُّؤ بالتورط الإرهابي لم تعُد مستحيلة في الوقت



الحالي. ويمكننا تحسين دقة النماذج التنبُّئية المبنية على مصدر واحد للبيانات بدمج النتائج مع الخُلاصات الأخرى، لكن تقييد إمكانية الوصول إلى البيانات قد يحدُّ من (كفاءة) الذكاء الاصطناعي في تحقيق تلك المهام.

2- غياب معايير التحقُّق المشتركة

على الرغم من أهمية الوصول إلى البيانات إلا أن ذلك وحده لا يضمن النجاحَ في بناء نماذج تنبُّئية دقيقة. ويُعَدُّ التحقق من صحة النماذج واختبارها ضروريًّا لقياس الدقة التنبُّئية وتقييم مناسبة استخدامها. وبالنظر إلى مجموعة واسعة من الجهات الفاعلة المعنية، باتت المعايير المشتركة ذات أهمية كبيرة. وإن استيعاب وكالات الاستخبارات، وجهات إنفاذ القانون، والقطاع الخاص، التقنياتِ المستخدمةَ في الذكاء الاصطناعي يعني أن إقبال الجهات الفاعلة على استخدام الذكاء الاصطناعي لمكافحة الإرهاب وتطويره في ازدياد. واهتمَّت مجموعة من البحوث الحديثة بمدى قابلية الذكاء الاصطناعي للانحياز، وأكدت أن النتائج التنبُّئية للذكاء الاصطناعي قد تكون موضوعية علميًّا أكثر من التقييمات البشرية التي تتأثر بالانحياز الثقافي.

فرص ومخاطر

نتجت التحدياتِ المذكورةَ آنفًا عن التطوير غير المنتظم للذكاء الاصطناعي بوصفه وسيلةً للتنبُّؤ بالإرهاب. فهل يمكن استخدام القدرة التنبُّئية للذكاء الاصطناعي بطريقة شرعية كونها أداةً من أدوات الدولة للكشف عن الإرهاب؟ هذا يعني إعطاء الوكالات الحكومية صلاحيةَ وصول أوسع إلى البيانات العامَّة، مع تنظيم أوضح لكيفية استخدام تلك البيانات. وهذا النهج يتطلَّب جمعَ بيانات المواطنين وتحليلها، وهو أمر لا يلقى قبولًا في كثير من البلدان.

أولًا) الفُرَص:

1- تقليل الانتهاك وزيادة الفاعلية

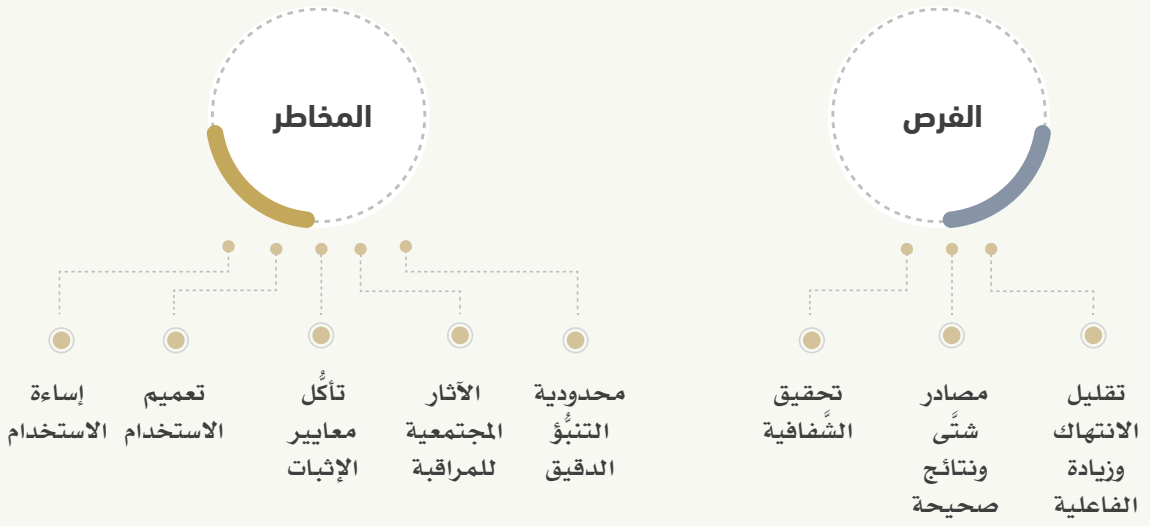
يشوب عملية التحليل الآليِّ للبيانات غير قليل من الانتهاكات، ولكنها مع ذلك تُسهم في تقليل انتهاك الخصوصية للمواطنين مقارنةً بالتحليل البشري. وقد يكون من الضروري عند استخدام نموذج تنبُّئي لأتمتة تحليل بيانات الجمهور اشتراطُ إثبات الفاعلية، أي توفير عَلاقة سببية بهدف محدد، مع عدم وجود خيارات بديلة، وإثبات أن الفوائد تفوق التكاليف المتعلقة بانتهاك الحقوق.

> **أكدت مجموعة من البحوث الحديثة أن النتائج التنبئية للذكاء الاصطناعي قد تكون موضوعية علميًا أكثر من التقييمات البشرية التي تتأثر بالانحياز الثقافي.**

2- مصادر شتَّى ونتائج صحيحة

يمكن العمل بوساطة الذكاء الاصطناعي على تطوير مصادرَ منفصلةٍ لجمع المعلومات والتحقق من صحة النتائج، بدلًا من المركزية المعتمِدة على نظام واحد يشمل جميع الأفراد، سواء كانوا إرهابيين أو معرَّضين للتطرف. ومع أن التحقق من الصحة

فرص استخدام الذكاء الاصطناعي ومخاطره في محاربة الإرهاب



ضروري، لا يزال مجالًا في طَور الارتقاء، ويمنح استخدامَ الطرق الآلية الفرصةَ لتقييم أداء النماذج وقياس جَدواها.

ولا شك أن معاملة الأشخاص المعرَّضين لخطر التطرف والإرهابيين الحقيقيين داخل النظام نفسه يسبب اضطرابًا يحول دون الحفاظ على تمييز حقيقي بينهم إلا عبر أنظمة تنبُّئية تستند إلى تحليل البيانات التي أُنشئت وحُفظت رَقْميًّا، وهي بيانات محايدة وموثوقة وفاعلة، يمكن استخدامها لتوجيه التدخلات المبكرة غير القسرية، كالتدخلات التي تستهدف منعَ الشباب من الانجذاب إلى فكر متطرف عنيف.

ازدياد توافر البيانات قد يؤدي إلى تأكُّل المعايير الحالية المرتبطة بإثبات التهم، فالإمكانات التي توفرها القدرة على جمع البيانات واستخدامها في التنبُّؤ ستؤدي إلى اهتمام أكبر بالعمليات الوقائية والاستباقية، والمعاقبة قبل حدوث الجريمة.

3- تحقيق الشَّفافية

توفر المعايير الكمِّية مقياسًا للشَّفافية التقنية، ويمكن أن يؤديَ تبادل المعايير الكمِّية إلى زيادة الثقة وتهيئة الظروف لتبادل المعلومات على نحو أفضل بين الجهات الفاعلة والوكالات الدَّولية. ومن المهم أيضًا تعزيز شفافية الإطار القانوني المحيط بالتحليل التنبُّئي لتحسين أداء النماذج، وتحقيق فهم واضح ومتسق لماهية التحليل وسببه.

إن مركزية مسؤولية الإشراف على هذا التحليل والعمل مع الجهات الحكومية يُحسِّن القدرة على تحقيق فهم واضح للتحليل، وإتاحة هذه المعلومات من شأنها تحسين الرقابة، ومعالجة المظالم المرتبطة بالتمييز. على سبيل المثال: طُوِّرت إجراءاتُ التوقيف في المطارات وفقَ نموذج يدمج أنماط السفر المشبوهة، والدوافع غير العادية، والعلامات الفسيولوجية لعدم الارتياح، وقد أدى هذا إلى انخفاض العدد الإجمالي للأشخاص الخاضعين لعمليات البحث بنسبة 50%، وإن معرفة المسافرين بهذه الحقيقة ستقلِّل مخاوفهم من إمكان أن تكون هذه الإجراءات قائمة على الانحياز العنصري أو العِرقي. ويمكن أن تؤدِّيَ مشاركة المعايير الكمِّية إلى تهيئة أفضل الظروف لتبادل المعلومات بين الجهات الفاعلة والوكالات الدَّولية. على سبيل المثال: قد يكون مزوِّدو خِدَمات الاتصالات أكثرَ استعدادًا لتلبية طلبات الوصول لما لديهم من بيانات إذا تيقَّنوا أن معايير هذه الطلبات عالية، وأنها ترتبط بهدف مشروع وتحقق نتائجَ جيدة.

ثانيًا) المخاطر:

1- محدودية التنبُّؤ الدقيق

التنبُّؤ بالهجَمات الإرهابية والتعرض للتطرف باستخدام الأساليب الحسابية وحدَها قد يثبت أنه غير دقيق؛ لذا يجب اقتراح الطرق وتجريبها وتقييمها أولًا، بل الاستغناء عنها إذا لم تحقق قيمة تنبُّئية كافية. وهناك كثير من الأمثلة على استخدام الذكاء الاصطناعي بنجاح في المجال الصناعي بتحسين قدرات التنبُّؤ باستخدام التعلم الآلي والتكيُّف الديناميكي، ومن ذلك التكيُّف مع التغييرات في البيانات داخل النظام، وفرض معايير التحقق من الصحة قبل الاستخدام، والتحديث التدريجي. وتوفر تلك الإجراءات الشرطَ السابق للاستخدام المنسق للذكاء الاصطناعي في محاربة الإرهاب، مع الأخذ في الحسبان أن نتائج أي نظام تنبُّئي توفر إمكانيةً فقط وليس دليلًا.

2- الآثار المجتمعية للمراقبة

قد ما يقلِّل التحليل الآليُّ للبيانات من اقتحام الخصوصية على المستوى الفردي، لكنه يرفع احتمال أن يشعر الجميع أنهم مراقبون في جميع الأوقات. وقد درس عدد من الأكاديميين الطريقة التي يمكن أن تتسبب بها المراقبة الرَّقْمية الواسعة النطاق في نشر الخوف من التعامل مع القضايا أو الأنشطة السياسية، أو إبداء رأي مخالف، أو انتقاد الأفكار، أو الاختلاف مع المعايير السائدة. وكانت هذه المسألة مصدرَ قلق جماعات المجتمع المدني، ولا سيَّما بعد ما كشفه إدوارد جوزيف سنودن المبرمج المتعاقد مع وكالة المخابرات المركزية الأمريكية عام 2013 من تفاصيل برنامج التجسُّس بريسم (PRISM) الذي أماط اللثامَ عن حجم برامج المراقبة الوطنية في أمريكا. وتوفر التجربة التاريخية لسلوك المواطنين في ظل الأنظمة الاستبدادية أدلة مقنعة على نتائج تقشعرُّ لها الأبدان للمراقبة الجماعية. وفي المقابل هناك من يرى أن استمرار المعارضة السياسية، وحرية التعبير، وزيادة تبادل المعلومات الطوعية عبر وسائل التواصل الاجتماعي، تقدم دليلًا على المبالغة في الآثار السلبية على تلك المراقبة.

3- تأكُّل معايير الإثبات

هناك تحذيرات من أن ازدياد توافر البيانات قد يؤدي إلى تأكُّل المعايير الحالية المرتبطة بإثبات التهم، فالإمكانات التي توفرها القدرة على جمع البيانات واستخدامها في التنبُّؤ ستؤدي إلى اهتمام أكبر بالعمليات الوقائية والاستباقية، أكثر مما كان في السابق. وهذه التقنيات التنبُّئية الجديدة ستُمكِّن السلطات أن تعاقبَ المتهمين قبل حدوث الجريمة! وهنا يظهر شبح (ما قبل الجريمة) الذي لا يمكن تجنُّبه إلا بالاعتراف بأن أي نموذج تنبُّئي يُعَدُّ احتمالًا وليس دليلًا، وأن التدخل وفق هذه النماذج يجب أن يستند في النهاية إلى قرار بشري يتخذه شخصٌ خبير بحدود هذه النماذج وقدراتها.

4- تعميم استخدام الذكاء الاصطناعي في الجرائم

يمكن رصد سوابق استُخدمت فيها أنظمة الذكاء الاصطناعي المُعَدَّة لمكافحة الإرهاب في مكافحة الجرائم الأخرى، وهو ما فعلته شرطة مدينة نيويورك عندما قامت بدمج 3000 آلة تصوير تلفازية مغلقة بأجهزة استشعار أخرى. والحقيقة أن توفر مجموعة كبيرة من البيانات عن الجمهور يُعَدُّ كنزًا لا يقدَّر بثمن للمَعنيين بالتحقيق مع المجرمين أو المهتمين بالتدخلات الاجتماعية.

استخدام قدرات الذكاء الاصطناعي لأغراض تنبئية في محاربة الإرهاب ليس أمرًا جيدًا ولا سيئًا في حد ذاته، بل يتوقف على الطريقة التي تُستخدم بها هذه القدرات.

5- إساءة استخدام الذكاء الاصطناعي

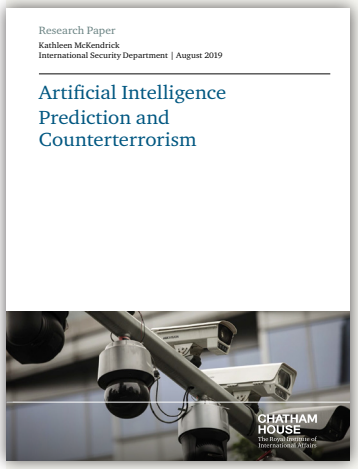
حتى في ظل تنظيم استخدام الذكاء الاصطناعي في محاربة الإرهاب وفرض القيود على ذلك الاستخدام، يظل تفسير مُخرَجاته تفسيرًا شخصيًّا، وهو ما يثير المخاوف من أن مصطلح (إرهابي) قد يُستخدَم ليناسب الأغراض السياسية. فالسماح بجمع البيانات العامَّة وتحليلها يحمل معه خطرًا كامنًا يتمثل في إساءة استخدامها. وتتضاءل جدوى القيود والرقابة المفروضة على استخدام الذكاء الاصطناعي في تحليل البيانات بسبب عدم وجود فهم عامٍّ لحجم البيانات التي أُنشئت وطريقة استخدامها.

يمكننا تأكيد أن استخدام قدرات الذكاء الاصطناعي لأغراض تنبُّئية في محاربة الإرهاب ليس أمرًا جيِّدًا ولا سيِّئًا في حد ذاته، بل يتوقف على الطريقة التي تُستخدَم بها هذه القدرات. ولا يشير التنظيم الحالي لاستخدام الذكاء الاصطناعي في محاربة الإرهاب إلى رُجحان أيٍّ من الجانبين، سواء تعلق الأمر بإساءة الاستخدام، أو بتحقيق الاستخدام الأكثر فائدةً لهذه التقنيات من حيث (كفاءة) التشغيل والالتزام بمبادئ حقوق الإنسان.

ويتطلب الأمر تضافرَ المزيد من الجهود لاستخدام الذكاء الاصطناعي بنجاعة في عمليات محاربة الإرهاب، واحترام حقوق الإنسان في آن، عندئذٍ تصل تقنيات الذكاء الاصطناعي للتنبُّؤ بالإرهاب إلى مرحلة النضج، ويكون الوصول إلى البيانات في ظل تدابير وقائية صارمة.

وينبغي إعادة النظر في الافتراضات الحالية، كافتراض أن الوصول إلى البيانات على نطاق أوسع أمر ضارٌّ دائمًا بحقوق الإنسان، وأن مركزية التحليل سيِّئة بطبيعتها، فإن تطوير القدرات التنبُّئية يمكن أن يكون مسوِّغًا صالحًا للوصول إلى البيانات العامَّة واستخدامها على نطاق أوسع، شرط التحقق من صحة نماذج التنبُّؤ بدقة قبل استخدامها، واتخاذ التدابير التقنية لمنع إساءة الاستخدام، وضمان أن استمرار الوصول إلى أيِّ بيانات لأغراض محاربة الإرهاب يتوقف على القدرة على استخلاص قيمة تنبُّئية كافية من تلك البيانات المحددة، أي تحقيق هدفٍ مشروع لهذا الوصول.

المؤلفة



كاثلين ماكيندريك، ضابط بالجيش البريطاني، خدمت في العراق وأفغانستان، وقدمت دوراتٍ تدريبيةً في التثقيف ومكافحة الإرهاب في مركز التميُّز للدفاع ضد الإرهاب (COE-DAT) التابع لحِلف شمال الأطلسي (الناتو) في أنقرة بتركيا. عملت في عامي 2017 و2018 زميلًا باحثًا في إدارة الأمن الدَّولي بالمعهد الملَكيِّ للشؤون الدَّولية (تشاثام هاوس).

حصلت على شهادة (البكالوريوس) في هندسة النظُم الجوية من جامعة كرانفيلد، وشهادة (الماجستير) في العَلاقات الدَّولية من كلية لندن للاقتصاد والعلوم السياسية.

تشمل مجالات اهتماماتها البحثية: الدفاع والأمن، وتطبيق الذكاء الاصطناعي في العمليات العسكرية.

التحالف الإسلامي العسكري لمحاربة الإرهاب
ISLAMIC MILITARY COUNTER TERRORISM COALITION

التحالف الإسلامي العسكري لمحاربة الإرهاب
ISLAMIC MILITARY COUNTER TERRORISM COALITION
الإدارة العامة للتخطيط والتنسيق