باستخدام تقنيات الرصد والتحليل والتنبؤ

توظيف الذكاء الاصطناعي للحدِّ من التطرف والإرهاب

د.عمران عوان

خبير محاربة الإرهاب وأستاذ علم الجريمة في جامعة برمنجهام، المملكة المتحدة

تتَّسم تقنيةُ الذكاء الاصطناعي بقدرتها على التطور الفائق والتأثير العميق في العديد من جوانب حياتنا اليومية، وتتمتَّع بكمٍّ هائل من المميزات التي تُوجد صيغًا تنافسية بين الكثير من الجهات وفقًا لغايات توظيفها أو استغلالها، إذ يُمكن أن يستغلها الإرهابيون لتحقيق أهدافهم ومآربهم الإجرامية الخاصة، وكذلك تستخدمها أجهزة الأمن وإنفاذ القانون مثل الشرطة؛ للتنبؤ بالهجمات الإرهابية المستقبلية، وإحباطها قبل وقوعها.

وغدت اليوم شركاتٌ عدة تستخدم الذكاء الاصطناعي؛ مثل: مايكروسوفت، وغوغل، وياهو، وأمازون، والبنوك، ومؤسسات بطاقات الائتمان، في إعداد أنظمة الأمان الخاصة بها. كما يمكن استخدامه لتحسين الأداء وعملية صنع القرار في كثير من الهيئات، إذ تُسهم التقنيات التنبؤية للذكاء الاصطناعي في محاربة التهديدات الإرهابية؛ حيث يمكن استخدامها لتحديد الأنماط، والرصد، واستخدام التنبؤات لوضع الإستراتيجيات المضادَّة بفاعلية تامة.

لقد أوجد الذكاء الاصطناعي نموذجًا افتراضيًّا ليتفاعل فيه الأفراد عبر وسائل اتصالات حديثة ومختلفة. وأسهم هذا التقارب في تصاعد حدة التهديدات الأمنية يومًا بعد يوم، وهو ما يؤكِّد ضرورة البحث عن صيغٍ وحلول ذكية لفهم القضايا المجتمعية الصعبة والشائكة. وقد يُعد الذكاء الاصطناعي وسيلة مساعدة لكشف متون التواصل اللغوي بين هؤلاء الأفراد.

فمن منظور أمني، يمكن استخدام تلك التقنيات الحديثة لاعتراض الاتصالات الإرهابية بتسجيلها وتحليلها ووضعها في إطارها المناسب، فيما يُعرف بتطبيقات "التعرف على الكلام". ومع أن شركة "نوانس للاتصالات" جمعت الملايين من عينات "الكلام" التي يمكن استخدامها بسرعة في تلك التطبيقات، فإنها تواجه تحدي القدرة على نسخ هذه الرسائل والاتصالات بدقة باستخدام الذكاء الاصطناعي. ومع ذلك، هناك إيجابيات عدة، منها تحديد الكلمات المفردة أو العبارات في تطبيقات أوامر الكلمات.

وبما أن الإرهابيين سيحاولون الاستفادة من هذه التقنيات أيضًا، فإن الذكاء الاصطناعي يُمثِّل أحدَ المخاطر الكبرى التي تُهدِّد سلامة المجتمع وأمنه على مرِّ التاريخ. حيث كشفت دراسةٌ

حديثة أن بعض التنظيمات الإرهابية وجدت في التقنيات الحديثة وأدوات الذكاء الاصطناعي ضالَّتها، سواء بالتواصل الآمن والسريع بين أعضائها، أو بينهم وبين المجنَّدين المحتملين، أو بالتخفي والهروب من التتبُّع الأمني، أو باستقطاب الأتباع وتجنيدهم والحصول على الأسلحة، أو بتسهيل عملياتهم الإجرامية بالاعتماد على التقنية، سواء بصورة رقمية أو على أرض الواقع.

التهديدات الإرهابية

أصبحت ركيزة التهديدات الإرهابية الناشئة عبر الذكاء الاصطناعي تتغير بوتيرة أسرع، يقول الباحث شيلدون ورايت في كتابه الشرطة والتقنية: «إن الأمن السيبراني أصبح قضية أمن قومي» تقتضي المعالجة. ويشمل ذلك كيفية إدخال الذكاء الاصطناعي واستخدامه في مكافحة التهديدات الإرهابية.

إن التقنيات الحديثة بأنواعها المختلفة لها دورٌ كبير في محاربة التنظيمات الإرهابية وكشف عناصرها، وفي الوقت نفسه يجب حماية الخصوصية وحقوق الإنسان التي تقتضي المعالجة أيضًا، فالملاحقات لا يجب أن تكون خبط عشواء بين كلِّ الناس، فقد تكون التقنية سيفًا ذا حدَّين.

ولا يمكن القول إن أيَّ نظام أمني منيعٌ بصورة تامَّة ضدَّ الهجمات الإلكترونية السيبرانية، ولا سيما عندما تتمكن إحدى التنظيمات الإرهابية من تثبيت برمجيات خبيثة للتحكُّم عن بُعد في أجهزة الحواسيب المخترَقة؛ لربطها فيما بعد في إنشاء شبكات بين الحواسيب الموبوءة. كما تعمل التنظيمات الإرهابية أيضًا على تجنيد الأفراد المستعدين لتنفيذ كلِّ الفظائع من أجل قضيتهم الإجرامية، ويُنفَّذ ذلك بأنماط وإجراءات مختلفة، مستغلين بذلك التقنيات التي وفَّرها الذكاء الاصطناعي لتضخيم تأثير دعايتهم، والبحث عن الأشخاص الضعفاء لاستقطابهم وتجنيدهم ليصبحوا متطرفين.

إن استخدام التحليل الأكثر دقَّة للمعلومات باستخدام تقنيات الذكاء الاصطناعي عبر الإنترنت يجب أن يُوظَّف بكفاءةٍ مُحكمة من الجهات المعنية؛ لدمج مختلف أنواع البيانات المتاحة، بدءًا من الدردشات عبر الإنترنت أو مواقع الشبكات، إلى سجلات الشرطة للإرهابيين المشتبه بهم وقواعد البيانات البيومترية (هي أنظمة تعمل على التعرف أو التأكد من شخصية الأفراد بطريقة آلية). ومن المهم جدّا أن تتمكَّن السلطات المختلفة من التعاون من أجل منع الإرهابيين الذين يستخدمون تقنيات الذكاء الاصطناعي والقبض عليهم. ويلزم تعزيز التعاون الدولي والقوانين الدولية من أجل مواجهة شبكة عالمية من الإرهابيين.

ومن الضروري تعزيز التقنيات المخصصة لتنسيق ردود الفعل المحلية والعالمية الاستباقية. وتُعدُّ إقامةُ شراكات بين القطاعين العام والخاص أحدَ النماذج المحتملة لاستخدام الذكاء الاصطناعي لمواجهة التهديدات الإرهابية؛ حيث ستدفع المنظمات الخاصة مقابل مراقبة الإنترنت وتحليل البيانات «الأولية»، بينما سيدفع الجمهور مقابل اعتقال الإرهابيين الذين يستخدمون خدماتهم الحالية، ومحاكمتهم.

المحاربة والوقاية

يوجد الكثير من التكتيكات الاستباقية التي يمكن استخدامها لمحاربة الإرهاب باستخدام تطبيقات الذكاء الاصطناعي في عمليات مموهة للقبض على الإرهابيين؛ حيث يشكِّل الإرهابيون تهديدًا حقيقيًّا بسبب تطورهم المتزايد في استخدام الإنترنت والتقنيات الحديثة كما يتضح ذلك من أساليب عملهم.

وتوفِّر أدوات "إدارة المعرفة" الحديثة للمنظمات المعنية آلياتٍ متعددة وعملية لمحاربة المخاطر الإرهابية المحتملة والمتزايدة باستخدام تقنيات الذكاء الاصطناعي؛ حيث لا يمكن التصدِّي للإرهاب عن طريق تلك التقنيات الحديثة بفاعلية إلا عبر فهم أوسع لدورة البيانات والأساليب المستخدمة للحصول على المعلومات وتوزيعها، مع الحفاظ على التواصل مع المجتمعات على جميع المستويات. كما يجب أن تتعاون السلطات المعنية فيما بينها لتفعيلٍ أمثلَ لأنظمة إدارة المعرفة وتعزيز الشراكات البينية؛ بغرض تبادل المعلومات اللوجيستية الداعمة، ويجب أن يُؤخذ في الحسبان أنه إذا تعلَّق الأمر بمحاربة الإرهاب بواسطة تطبيقات الذكاء الاصطناعي فإن تعزيز عملية صنع القرار الأمني الجماعي من شأنه أن يقوِّضَ الجماعات الإرهابية ويحدَّ من خطورتها عبر الخطوات التعاونية الاستباقية.

وتُعدُّ الشرطةُ الأوروبية، ووكالةُ تطبيق القانون الأوروبية (اليوروبول)، والشرطةُ الدولية، أمثلةً بارزةً لتبادل المعلومات الاستخباراتية عن طريق الذكاء الاصطناعي، حيث تتماثل الهياكل التنظيمية للأجهزة الأمنية المختصة بمحاربة الإرهابيين، وهو ما يشير إلى أهمية وجود أنظمة مترابطة لجمع البيانات، وتحليل المعلومات، واستخدام تقنية الذكاء الاصطناعي بكفاءة.

ومن غير المرجَّح أن تنجح التحقيقات التي تحتاج إلى إجراءات رسمية طويلة. لذلك، فقد تمكَّنت أجهزة شرطية أوروبية من وضع إستراتيجيات جديدة لمحاربة التهديدات الإرهابية، تعتمد على تقنيات الذكاء الاصطناعي، وذلك بفضل تقنية المعلومات. ويشمل ذلك العمل الشرطي المجتمعي، والعمل الشرطي الذي لا يعرف التهاون، والعمل الشرطي الموجه بالاستخبارات، والعمل الشرطي الموجه نحو حلِّ المشكلات.

وقد ضخَّ كثيرٌ من الحكومات استثماراتٍ كبيرةً في البنية التحتية لتقنية المعلومات والاتصالات؛ إدراكًا منها للتهديد الذي يشكِّله الإرهاب الرقمي، ففي الوقت الحالي، هناك حاجة إلى نهج أكثر شمولية لوضع قوانين وبروتوكولات وإستراتيجيات للتعامل مع ما استجد من تطور هائل في مجال التقنية، في إطار مواجهة التحديات المرتبطة بالذكاء الاصطناعي والإرهاب، إضافةً إلى تعريفات متَّفق عليها؛ لتحلَّ محل اللغة الغامضة المستخدمة في الاتفاقيات الأوروبية الحالية.

وعند معالجة مسألتي الذكاء الاصطناعي والإرهاب، سيعاد تأكيد فكرة التفاعل مع المجتمعات على الصعيد المحلي لتوفير المعلومات والبيانات من أجل تطبيقها على مستويات متعددة. ويركز هذا النهج على المواطن، ويركز أيضًا على استخدام إدارة المعرفة والعمل الشرطي الاستخباراتي بأقصى إمكاناتها بحيث تُلبِّي متطلَّبات المجتمع في محاربة الإرهاب.

التعاون المشترك

إن تطوير تقنيات المعلومات والاتصالات والذكاء الاصطناعي يزيد أهمية التعاون المشترك بين العديد من الأجهزة لتوظيف هذه التقنيات من أجل الحدِّ من خطر الإرهاب؛ حيث يلزم إعداد برامج فاعلة لمحاربة الإرهاب، والبدء في تبادل المعلومات -المعلومات الصحيحة والمعلومات الآنية- بين أجهزة الأمن وإنفاذ القانون والهيئات العسكرية عبر برامج الذكاء الاصطناعي. وينبغي معالجة الأسباب الأساسية لهذه القضية عبر إستراتيجيات استباقية لمحاربة الإرهاب، لذا فإن تعزيز التعاون الأمني والتماسك المجتمعي ضروري لفاعلية الإستراتيجيات المضادة في ثني الإرهابيين عن ارتكاب الجرائم. كما تشكِّل الاتصالات بين الهيئات ضرورة ملحَّة بوجه عام حتى تعمل أجهزة الأمن معًا بتناسق وفاعلية داخل الحدود الوطنية أو خارجها.

إن الشبكات الافتراضية التي تعمل بالذكاء الاصطناعي لديها القدرة على تعزيز التفاعل الاجتماعي، وبناء العلاقات، وتقديم أنظمة الدعم للتحول إلى مجتمع برأس مال اجتماعي. ولكن من أجل فهم الذكاء الاصطناعي المرتبط بالإرهاب، ينبغي على الحكومات وضع إستراتيجيات عملية لمواجهة الخطر الداهم، مع ضرورة اتخاذ إجراءات منسقة وشاملة ومرنة وسريعة تعالج الاستجابات الوقائية على جميع المستويات، من المستوى المحلي إلى الصعيد العالمي؛ حيث إن هناك نماذج شرطية وتحليلية قائمة قد تكون مفيدة عند تطبيقها ضمن أطر معترف بها ومعتمدة يمكنها مواجهة التنظيمات الإرهابية المستخدمة للذكاء الاصطناعي.

ولا شك أنه يمكن استخدام الذكاء الاصطناعي في الجمع بين القدرة والرغبة في تبادل البيانات والمعرفة بين العديد من الأجهزة التي تحتاج إلى العمل في شراكة أمنية بنّاءة وفاعلة للقضاء

على الإرهاب وللوصول إلى الإرهابيين والقبض عليهم، لذلك يحدد مستوى الحاجة إلى مزيدٍ من التعاون الدولي والتشريعات لمكافحة هذا الإجرام. ولا سيَّما مع اشتداد تهديدات العصابات الإجرامية، والإرهابيين، والمخترقين، والحكومات المعادية التي ترغب في شنّ هجمات ضدَّ البنية التحتية الحيوية وأنظمة الإنترنت في ظل «العولمة» وعصر أنظمة الشبكات، فضلًا عن أن تهديدات الإرهاب المتبني لتقنية الذكاء الاصطناعي قد يؤدِّي إلى إقصاء بعض المجتمعات وتفاقم التحيز المتصور.

ختامًا

يفتح الذكاء الاصطناعي المجال أمام الجماعات الإرهابية، ويمكِّنها من تنفيذ مخططاتها الشيطانية، ومع تزايد انتشار تطبيقات الذكاء الاصطناعي والتطور غير المسبوق للتقنيات المبتكرة، فمن المرجَّح أن تبحث تلك الجماعات عن طرق لتوظيف التقنيات الجديدة واستغلالها في مخططاتها الإرهابية. لذا من الضروري التعامل مع هذه الظاهرة عبر أساليب العمل الشرطي الحديثة، والمساعدة في مواجهة التهديدات الإرهابية، واستخدام التقنيات الحديثة المتاحة لإحباط التهديدات الجديدة.

وكما يقول الباحث ليون في كتابه دراسات المراقبة: «إن مسائل المخاطر والثقة والأمن والفرص أمور محورية». ولذا فمن المهم الاستفادة من التقنيات الجديدة لنتقدم بخطوة على الإرهابيين، كما ينبغي أن يكون هناك اتفاق عالمي على البيانات التي تُجمع عبر الذكاء الاصطناعي، ومتى ينبغي مشاركتها، ومع مَن، ليس فقط لمحاربة الإرهاب، ولكن لحماية حرياتنا وهوياتنا الشخصية.