ISNN : 1112-8518 EISSN : 6200-2600

دور الذكاء الاصطناعي في التنبؤ بمكافحة الإرهاب

د. عادل عبد السميع عوض
رئيس قسم الفلسفة
كلية الآداب جامعة المنصورة

تمهيد

يشهد العالم اليوم تصاعدًا في ظاهرة الإرهاب، مما يهدد الأمن والاستقرار في مختلف الدول. ولذلك، تبحث الجهات الأمنية عن أدوات ووسائل جديدة لمكافحة هذه الظاهرة الخطيرة.

وفي هذا السياق، يُعدّ الذكاء الاصطناعي أداة واعدة يمكن أن يؤدي دورًا مهماً في التنبؤ بمكافحة الإرهاب. حيث يمكن للذكاء الاصطناعي تحليل كميات هائلة من البيانات للتعرف على الأنماط والسلوكيات التي قد تشير إلى احتمال وقوع هجمات إرهابية.

يؤدي الذكاء الاصطناعي دورًا مهماً في التنبؤ بمكافحة الإرهاب خلال تطبيقاته المتنوعة، ونذكر منها:

1. تحليل البيانات الضخمة:

تحليل كميات هائلة من البيانات من مختلف المصادر مثل:

وسائل التواصل الاجتماعي، المعاملات المالية، سجلات السفر، بيانات الاتصالات ، تحديد الأنماط والسلوكيات المشبوهة التي قد تشير إلى نشاط إرهابي محتمل.

2. التنبؤ بالهجمات الإرهابية:

استخدام خوارزميات التعلم الآلي للتنبؤ بمكان وتوقيت الهجمات الإرهابية المحتملة. تحديد الأشخاص الأكثر عرضة للتطرف والتجنيد من قبل الجماعات الإرهابية.

3. رصد ومراقبة النشاط الإرهابي:

استخدام تقنيات مثل التعرف على الوجه وتحليل الصور لتحديد الأشخاص المشتبه بهم. مراقبة الإنترنت ومواقع التواصل الاجتماعي للبحث عن محتوى متطرف.

4. تعزيز فعالية التحقيقات:

تحليل البيانات المتعلقة بالهجمات الإرهابية لتحديد هوية الجناة. ربط المعلومات من مختلف المصادر لتكوين صورة كاملة عن الشبكات الإرهابية. لا تزال تقنيات الذكاء الاصطناعي في طور النمو، وهناك حاجة إلى مزيد من البحوث لتطويرها بشكل أفضل.

ISNN : 1112-8518 EISSN : 6200-2600

أهمية الموضوع

يتم افتراض أن استخدام الذكاء الاصطناعي التنبؤي في مكافحة الإرهاب له تأثير سلبي على حقوق الإنسان، ويولد آفات من عقوبات «ما قبل الجريمة» ودول المراقبة. ومع ذلك، فإن استخدام القدرات الجديدة المنظمة بشكل جيد قد يعزز قدرة الدول على حماية حقوق المواطنين في الحياة، مع تحسين الالتزام بالمبادئ المصممة لحماية حقوق الإنسان الأخرى، مثل الشفافية والتناسب والحرية من التمييز غير العادل. ويمكن أن يسهم الإطار التنظيمي نفسه أيضًا في حماية ضد سوء استخدام تقنيات ذات الصلة.

تركز معظم الدول على منع الهجمات الإرهابية بدلاً من التعامل معها. وعلى هذا النحو، فإن التنبؤ يعد مركزيًا بالفعل في مكافحة الإرهاب الفاعلة. يتيح الذكاء الاصطناعي تحليل مزيد من حجم البيانات وقد يلاحظ أنماطًا في تلك البيانات التي ستكون، لأسباب تتعلق بالحجم والبعد، خارج قدرة التفسير البشري. التأثير الذي ينجم عن ذلك هو أن الأساليب التقليدية للتحقيق التي تبدأ من المشتبه بهم المعروفين قد يتم استكمالها بطرق تحليل النشاط لمجموعة واسعة من السكان بأكملهم لكشف التهديدات المجهولة مسبقًا[1].

أحدث التطورات في الذكاء الاصطناعي قد زادت من قدرة إجراء المراقبة دون قيود متعلقة بالموارد. على سبيل المثال، قد يمكن لتكنولوجيا التعرف على الوجوه أن تمكِّن الأتمتة الكاملة للمراقبة باستخدام كاميرات المراقبة في الأماكن العامة في المستقبل القريب.

الطريقة الحالية التي يتم استخدام بها قدرات الذكاء الاصطناعي التنبؤي تطرح عدد من المشاكل المترابطة من منظوري حقوق الإنسان والجانب العملي. حيث إنه حيثما توجد قيود وتنظيمات، فإنها قد تقوض فاعلية النهج المعتمد على الذكاء الاصطناعي، مع عدم ضمان حقوق الإنسان بما يكفي.

انتهاك الخصوصية المرتبط بالتحليل التلقائي لبعض أنواع البيانات العامة ليس خاطئًا في المبدأ، ولكن يجب أن يتم إجراء التحليل في إطار قانوني وموضوع سياسات قوية تفرض قيوداً معقولة على التدخلات بناءً على نتائجه[2].

في المستقبل، قد يتحسن الوصول الأوسع إلى جوانب أقل تدخلًا من البيانات العامة، والتنظيم المباشر لكيفية استخدام تلك البيانات - بما في ذلك الإشراف على أنشطة القطاع الخاص - وفرض إجراءات تقنية وكذلك ضوابط تنظيمية قد تحسن كفاءة التشغيل والامتثال لتشريعات حقوق الإنسان. من المهم أن تتم هذه التدابير بطريقة حساسة تجاه التأثير على حقوق أخرى مثل حرية التعبير وحرية الانضمام والتجمع.

([1])McKendrick, K. (2019). Artificial intelligence prediction and counterterrorism. London: The Royal Institute of International Affairs-Chatham House, 9.
([2]) Ibid.p2.

ISNN : 1112-8518 EISSN : 6200-2600

تسعى السياسات المضادة للإرهاب إلى التوازن بين حفظ أمن السكان واحترام الخصوصية الفردية والحريات مثل حرية التعبير والانضمام والدين. يمكن أن تشكل التطورات التكنولوجية الجديدة تحديًا لتنفيذ هذه السياسات خلال إجبار السلطات على إعادة النظر في كيفية تنفيذ إجراءات مكافحة الإرهاب. الذكاء الاصطناعي واحد من هذه التكنولوجيات[1].

نشير إلي أنه كيف يمكن للذكاء الاصطناعي أن يسهم نظريًا في عمليات مكافحة الإرهاب، فضلاً عن بعض المجالات التي يتم فيها استخدامه بالفعل. نقدم بعض المشاكل المتعلقة باستخدام الذكاء الاصطناعي الحالي لهذه الأغراض، وتدرس كل من القيود العملية والآثار على حقوق الإنسان. كما ينظر المستند إلى الفرص والمخاطر التي تشكلها زيادة استخدام الذكاء الاصطناعي كجزء من نشاط مكافحة الإرهاب من قبل الحكومات. يؤكد أن استخدام الذكاء الاصطناعي في مكافحة الإرهاب ليس خاطئًا بشكل جوهري، ويوجه بعض الشروط الضرورية لاستخدامه المشروع كجزء من نهج تنبؤي لمكافحة الإرهاب من قبل الدول الديمقراطية الليبرالية[2].

تتمحور استخدامات الذكاء الاصطناعي في مكافحة الإرهاب حول إنشاء توقعات دقيقة تساعد في توجيه الموارد لمكافحة الإرهاب بشكل أكثر فاعلية. يمكن أن يقلل الذكاء الاصطناعي التنبؤي أيضًا من التدخل غير الضروري في الغالبية من السكان ومن التحيز البشري في عمليات اتخاذ القرار. في هذه الفترة التي يصبح فيها من الأسهل جمع وتخزين وتحليل بيانات مفصلة عن أنشطة وروابط الأفراد على نطاق واسع، قد تكون الأساليب التنبؤية أكثر أهمية حيث يمكن أن توجه بدقة الاهتمام إلى المناطق أو الأفراد الذين من المرجح أن يشكلوا تهديدات، وتقليل عدد المواطنين الذين يخضعون لمراقبة متطفلة أكثر[3].

هناك مخاطر معروفة مرتبطة بالذكاء الاصطناعي. يمكن أن تظهر خوارزميات تحيط بها تحيزات أصلية أو مكتسبة، وقد تكون ضعيفة في بيئات تصادمية، وتقتصر بشكل أساسي على البيانات التي يمكن الوصول إليها. يمكن أيضًا أن يتعرض الإشراف العام، الذي يكون بالفعل محدودًا بسبب اعتبارات الأمان، للخطر بفعل تضمين أنظمة تحليل تلقائي تكون غامضة بطبيعتها للبشر. يمكن أن يؤدي عدم وجود ضمانات كافية بشأن استخدام الذكاء الاصطناعي وبشأن المخزون الواسع من البيانات التي يعتمد عليها، ليس فقط إلى سوء استخدامه من قبل الدول الاستبدادية من أجل فرض سيطرة تامة على مواطنيها، ولكن أيضًا لانتهاك مفرط لحقوق مثل الخصوصية وحرية التعبير أو الانضمام في الدول الديمقراطية.

(1)Ibid.p3.
(2)Ibid.p3.
(3)Ibid.p3.

ISNN : 1112-8518 EISSN : 6200-2600

الفكرة المتمثلة في استخدام تقنيات تنبؤ دقيقة يدعمها الذكاء الاصطناعي لأغراض مكافحة الإرهاب هي فكرة تخمينية وقابلة للتحقق. فمن المفيد أن نأخذ في الاعتبار مسبقًا إمكانيات وتكاليف هذا النهج، وكيف يمكن تنظيم هذا المجال الناشئ[1].

2 .التنبؤ في مكافحة الإرهاب وتقنيات الذكاء الاصطناعي ذات الصلة

هذا الجزء يصف دور التنبؤ في مكافحة الإرهاب، ويقدم كيفية استخدام بعض أنواع الذكاء الاصطناعي لأغراض التنبؤ. يقدم تعريفًا للذكاء الاصطناعي ويميزه عن تحليلات "البيانات الضخمة" عمومًا. ويؤكد أن التنبؤ الجيد ضروري لتنفيذ استراتيجية مكافحة الإرهاب التي تكون فاعلة في منع الإرهاب من دون انتهاك غير لازم لحقوق المواطنين. كما يشير إلى أن الذكاء الاصطناعي التنبؤي من المرجح أن يكون مفيدًا في الإسهام في ذلك.

تسعى الهجمات الإرهابية في الديمقراطيات الليبرالية إلى تقويض الدعم العام للحكومات التي يستهدفونها. إن مهاجمة الأهداف المدنية بشكل لا يمكن التنبؤ به تعكس وهمًا ببيئة آمنة تكفلها الدولة الوطنية. حتى إذا تم إدارة ما بعد الهجوم بشكل فاعل، فمن الأفضل دائمًا منع وقوع هجوم من هذا القبيل تمامًا. لذلك، تكون الوقاية غالبًا محورًا أساسيًا لاستراتيجيات مكافحة الإرهاب[2].

هناك وسيلتان لمنع الهجمات الإرهابية. الأولى هي الردع: خلال حماية البنى التحتية، وتطبيق فحوصات الأمان، ووعد بالعقاب. والثانية هي منع القدرة على تنفيذ الهجمات: خلال القبض على الإرهابيين قبل تنفيذ مخططاتهم، ومكافحة تجنيد وتطرف الإرهابيين المستقبليين، وفرض قيود على تحرك وحرية الأفراد.

تشترك عديد من هذه الأساليب في خصائص مشتركة. على وجه التحديد، فإنها تفرض متطلبات على الموارد القليلة وتنتهك إلى حد ما حقوق الأشخاص الذين يتم تطبيقها عليهم. يعد انتهاك الحقوق الزائد أو التعسفي خيانة لمبادئ الديمقراطية الليبرالية، وبذلك يفوز الإرهابيون. لذلك، يمكن توصيف مكافحة الإرهاب الفاعلة بناءً على المعايير العملية والمبدئية على حد سواء على أنها مشكلة تهدف إلى التحسين التي تسعى إلى توفير الأمان لمعظم المواطنين مع الحد الأدنى من انتهاك الحقوق والحريات. للوصول إلى هذه النقطة المثلى، يمكن أن تستفيد الوقاية الفاعلة من الإرهاب من طرق تحسين توقع الهجمات أو السلوكيات المرتبطة بها[3].

تتشكل رؤية المدرسة الليبرالية للتكنولوجيا في إطار مقولاتها التي تؤكد تنامي دور الفواعل غير الدولية، والاعتماد المتبادل والتعاون الدولي ودور المؤسسة الدولية والحوكمة العالمية، والاتفاقات الدولية واتساع الأجندة الأمنية، عن

(1)Ibid.p4.
(2)Ibid.p5.
(3)Ibid.p5.

ISNN : 1112-8518 EISSN : 6200-2600

المفهوم الضيق الذي تتبناه المدرسة الواقعية عن الأمن. انطلاقاً من هذا المنظور التفاؤلي للعلاقات الدولية. يؤكد الليبراليون دور التكنولوجيا في التقدم المجتمعي والاقتصادي والسياسي والبشري بشكل عام .

في هذا الإطار تم تفسير ظهور الانترنت وانتشاره بوصفه قوة تحريرية تساعد في تمكين الحركات الاجتماعية، وتعبر عن نوع من أنواع التحول الديمقراطي، وتوفر منصات للتواصل والحراك السياسي نتجاوز تلك الخاصة بالنخب السياسية والاقتصادية، إذ تناول جوزيف ناي انتشار الوصول إلى الانترنت في جميع أنحاء العالم بحسبانه شكلا من أشكال التحول الديمقراطي. كما تناولت عدة دراسات دور وسائل التواصل الاجتماعي في الثورات العربية عام ٢٠١١[1].

كما أكد روبرت كوهين وجوزيف ناي وعديد من الدراسات داخل المنظور الليبرالي علي دور التطور التكنولوجي، خاصة تكنولوجيا المعلومات، واستحداث تقنيات حديثة، مثل الذكاء الاصطناعي بحسبانها إحدى آليات العولمة الاقتصادية، وإنشاء وفاعلية المؤسسات الدولية الجديدة والفواعل غير الدولية، وزيادة الاعتماد المتبادل[2] .

في حين أن نهاية الحرب الباردة شكلت صدمة بالنسبة إلى الواقعيين على اختلاف مشاربهم الفكرية وحتى أولئك الذين كانوا منخرطين في الدراسات الأمنية الدولية، كان العكس صحيحاً بالنسبة إلى الليبراليين من جميع الأطياف، وخاصة أولئك الذين كانوا يهتمون بدراسة الاقتصاد السياسي الدولي توصفا فالجمع بين القطبية الأحادية والعولمة، ، بوصفها السمتين الرئيستين . آفاقاً كبيرة أمام الليبراليين. لقد كانت لفترة ما بعد الحرب الباردة مباشرة، فتح القوة العظمى الليبرالية الوحيدة في وضع قوي لإبراز وحماية القيم الليبرالية الأساسية مثل الديموقراطية واقتصاد السوق وحقوق الإنسان. وقد جلبت العولمة في ظل القوة العظمى الليبرالية أفكار السلام الديموقراطي والعلاقات والمؤسسات الغربي، وأثارت الآمال بشأن إمكانية السعي وراء حقوق الإنسان على نحو أكثر فاعلية ما الدولية متعددة الأطراف إلى الواجهة، وعرضت طريقة لإدخال الصين الصاعدة على الصور أكثر المالية ما فاعلية كان عليه الحال خلال فقرة الحرب الباردة. لقد كان لهذه اللحظة الليبرالية تأثير قوي في العلاقات الدولية خلال التسعينيات، ولكن هذا الوضع شهد بعد ذلك توتراً على نحو متزايد[3].

يتيح التنبؤ استخدام تقدير في تطبيق التدابير الوقائية، مما يقلل من تأثيرها على السكان ككل. يمكن أن يكون للتنبؤ الفاعل، على سبيل المثال، التأثير بحيث يتم مواجهة الإرهابيين العنيفين فقط بالقوة القاهرة أو القيود، في حين يتم توجيه تدابير المصالحة تجاه الأفراد المعرضين للتطرف. في حالة الردع خلال الحماية الجسدية، يمكن أن يكون التنبؤ فاعلًا كوسيلة لتحسين تخصيص الموارد للمواقع التي من المرجح أن تكون أهدافًا[4].

([1]) نسيبة أشرف، الذكاء الاصطناعي والعلاقات الدولية، مجلة السياسة الدولية،العدد231،المجلد58، القاهرة،2023، ص8.
([2]) المرجع نفسه،ص8.
([3]) أميثان أشاريا،باري بوزان،ص351.
([4])Mckendrick,k. P5

ISNN : 1112-8518 EISSN : 6200-2600

وفقًا لمجلس الهندسة والعلوم الفيزيائية والبحوث :

تهدف تقنيات الذكاء الاصطناعي إلى إعادة إنتاج أو تجاوز القدرات (في الأنظمة الحسابية) التي تتطلب «ذكاء» إذا أداها البشر. وتشمل هذه المجالات ما يلي: التعلم والتكيف ؛ والفهم الحسي والتفاعل ؛ والاستدلال والتخطيط ؛ والاستفادة المثلى من الإجراءات والبارامترات ؛ والاستقلال الذاتي ؛ والإبداع ؛ واستخلاص المعارف والتنبؤات من البيانات الرقمية الكبيرة والمتنوعة.

لغرض إجراء التنبؤات، فإن نوع الذكاء الاصطناعي الذي يتيح استخراج المعرفة والتنبؤات من البيانات الرقمية المتنوعة الكبيرة هو الأكثر صلة. يرتبط هذا بمجال تحليلات «البيانات الضخمة»، ولكنه يختلف عنها. تشير «البيانات الضخمة» إلى مجموعات البيانات التي يتجاوز حجمها قدرة أدوات برامج قواعد البيانات النموذجية على التقاط وإدارة وتخزين وتحليل. يحدد التوصيف الشائع «البيانات الضخمة» من حيث ما يسمى بـ «أربعة مقابل»: السرعة والصدق والتنوع والحجم. والجدير بالذكر أن توصيفات «البيانات الضخمة» تقنية، بناءً على طبيعة البيانات[1] .

نركز على الذكاء الاصطناعي، وليس فقط تحليلات «البيانات الضخمة». طرق الاهتمام المتداخلة هي بشكل أساسي تلك التي تستخدم التعلم الآلي لبناء نماذج بناءً على البيانات، ثم إجراء استنتاجات من تلك النماذج. هذه الأساليب - نوع الذكاء الاصطناعي المشار إليه أعلاه - هي في بعض النواحي منطقة اهتمام أضيق من «البيانات الضخمة»، والتي يمكن أن تشمل أيضًا استخدام مجموعات بيانات كبيرة للبحث والتحليل من قبل المشغلين البشريين الذين يقومون بهيكلة استفسارات محددة. من نواحٍ أخرى، وتحديداً تكييف منهجيات «البيانات الضخمة» التقليدية مع مجموعات البيانات الأصغر، فهي أوسع، وليست بالضرورة حصرية للبيانات التي تتميز بها البيانات الأربعة مقابل[2] .

إحدى الطرق الجيدة للكف عن الطبيعة الجوهرية للبيانات هي محاولة فهم ما يعنيه محو أو تدمير، أو فقدان البيانات، تخيل صفحة كتاب كتب بلغة لا تعرفها، وهب أن البيانات كانت في صورة رسوم تخطيطية. يشير النمط الاعتيادي إلى الالتزام بنوع ما من البنية اللغوية. فرغم أننا نمتلك جميع البيانات إلا أننا لا نعرف معناها. ومن ثم لا تتوافر لدينا معلومات لنمح نصف الرسوم التخطيطية. ربما يقال إننا قسمنا البيانات أيضاً خلال عملية المحو تلك، وإذا استمرينا في إجراء هذه العملية إلى أن يتبقى لنا التمثيل أو ربما كانت متماثلة معها. لنقم الآن لنمحو هذا الرسم التخطيطي الأخير . صار لدينا الآن صفحة بيضاء، بيضاء، وإن كانت ليست دون بيانات تماما، إذ لا يزال وجود

(1) Ibid.p.6
(2) Ibid.p6.

ISNN : 1112-8518 EISSN : 6200-2600

الصفحة البيضاء يمثل معطيات طالما كان ، ثمة فرق بين الصفحة البيضاء والصفحة التي كتب شيء ما عليها أو قد يكتب شيء ما عليها[1].

ترتبط البيانات المحللة ونوع التحليلات ارتباطا وثيقا إلى حد ما ؛ وهذا غالبًا ما يسبب ارتباكًا بين تحليلات الذكاء الاصطناعي وتحليلات «البيانات الضخمة». الخوارزميات التي تدعم النماذج التنبؤية مبرمجة ذاتيًا بناءً على التعرض للبيانات. في كثير من الحالات، سيكون من المستحيل تحليل البيانات دون مثل هذا النهج، بقدر ما سيكون من المستحيل بناء النماذج دون البيانات. تحتاج «البيانات الضخمة» إلى الذكاء الاصطناعي لتفسيرها: غالبًا ما يحتاج الذكاء الاصطناعي إلى «بيانات ضخمة» لبناء وتحسين نفسه.

تعني التطورات في مجالات أخرى من الذكاء الاصطناعي أن تحسين دقة التنبؤات قد يصبح ذا أهمية متزايدة، سواء أكان من أجل مكافحة الإرهاب بشكل فاعل أم أو لوقف تآكل الخصوصية. كما لاحظ المقرر الخاص للأمم المتحدة المعني بالخصوصية في عام 2014: «أدى انخفاض تكاليف التكنولوجيا وتخزين البيانات إلى القضاء على المثبطات المالية أو العملية لإجراء المراقبة»[2].

أدت التطورات في الذكاء الاصطناعي إلى تضخيم القدرة على إجراء المراقبة دون تقييد الموارد. قد تتيح تقنية التعرف على الوجه، على سبيل المثال، التشغيل الآلي الكامل للمراقبة باستخدام الدوائر التلفزيونية المغلقة في الأماكن العامة في المستقبل القريب. يمكن استخدام التحليل النصي القائم على الذكاء الاصطناعي «لفهم» محتوى الرسائل الخاصة دون الحاجة إلى اهتمام محلل بشري[3].

من حيث المبدأ، ينبغي أن يظل مستوى التبرير اللازم للإذن بأنشطة المراقبة كما هو، بصرف النظر عن الإمكانات العملية أو الإمكانيات التقنية. على الرغم من ذلك، من الخطأ عدم الاعتراف بأن إمكانية توسيع المراقبة قد تؤدي إلى سحب لا يقاوم للقيام بذلك. إن حل القيود العملية المفروضة على إجراء المراقبة يعني أن مسألة كيفية توجيه المراقبة إلى الأشخاص ذوي الأهمية الاستخباراتية المشروعة، بدلا من تطبيقها بشكل عشوائي، قد تصبح ذات صلة متزايدة. لذلك، في المستقبل القريب، يمكن أن يكون وضع تنبؤات جيدة حول من أو ما يجب مراقبته أمرًا أساسيًا للحد من إساءة استخدام وسائل المراقبة التقنية بالجملة[4].

الإرهاب نفسه لا يمكن التنبؤ به حسب التصميم. يعتمد التحريض على الإرهاب على فكرة أن هجومًا سيتم من قبل شخص مجهول في مكان وزمان يفترض أنهما عشوائيان. على الرغم من ذلك، يتم ضمان استراتيجية فاعلة لمكافحة

([1]) لوتشانو فلوريدي: المعلومات ،ترجمة محمد سعد طنطاوي، مؤسسة هنداوي،القاهرة،2014،ص28.

([2]) McKendrick,K.p5.

([3]) Ibid.p6.

([4])Ibid.p6.

ISNN : 1112-8518 EISSN : 6200-2600

الإرهاب خلال إمكانية التنبؤ. السؤال ليس ما إذا كان هناك مكان للتنبؤ في مكافحة الإرهاب، ولكن ما إذا كان النهج المحدد لاستخدام الذكاء الاصطناعي وكيف يمكن أن يجعل التنبؤ أفضل[1].

3. التطبيقات العملية للذكاء الاصطناعي في مكافحة الإرهاب

يصف هذا الجزء الكيفية التي تم بها بالفعل الاعتراف بإسهامات الذكاء الاصطناعي التنبؤي في مكافحة الإرهاب واستخدامها إلى حد محدود. وهو يقدم بعض النهج والجهات الفاعلة المعنية.

تستخدم التحليلات الآلية للبيانات لدعم أنشطة دوائر الاستخبارات والأمن، ولا سيما خلال تصور البيانات. تعطي الخوارزميات الأولوية للمشتبه بهم الإرهابيين، وتقيم بشكل روتيني مخاطر ركاب السفر الجوي. ويمكن جمع المعلومات وتخزينها افتراضيا، لتحليلها في وقت لاحق بغية الكشف عن الأنماط والروابط التي تكشف الشبكات الإرهابية أو الأنشطة المشبوهة. تسمح أساليب التعلم الآلي بتفسير وتحليل الأنماط التي يتعذر الوصول إليها بكميات كبيرة من البيانات. قد تتضمن هذه الأساليب الترشيح أو تحليل العلاقات بين الكيانات أو أدوات التعرف على الصور أو الصوت الأكثر تطوراً[2].

وكالات الاستخبارات وأجهزة الأمن ليست وحدها التي تعترف بالقيمة التنبؤية للبيانات وتحاول إدراكها. وكانت النتيجة نقل الأساليب والقدرات إلى السلطات المدنية (مثل الشرطة). يعد تحليل الشبكات الاجتماعية للعصابات الحضرية، وأنظمة الإنذار على مستوى المدينة، والتنبؤ بموقع الجريمة، ومساعدات صنع القرار في الحجز، أمثلة على الأدوات التنبؤية التي يدعمها الذكاء الاصطناعي والتي تنطبق على مكافحة الإرهاب والتي تستخدمها بالفعل وكالات إنفاذ القانون.

بالإضافة إلى ذلك، تشارك الجهات التجارية أيضًا، أحيانًا نتيجة لمطالبة الحكومات باتخاذ إجراءات من قبل مقدمي خدمات الاتصالات لرصد واستبعاد النشاط الإرهابي على منصاتهم الخاصة. تستخدم بعض شركات التكنولوجيا مزيجًا من الخبرة البشرية والتدابير التنبؤية المتطورة بشكل متزايد لرصد وتعطيل النشاط الإرهابي على منصاتها. يمكن أن يشهد المستقبل مشاركة متزايدة من قبل هذه الأنواع من شركات التكنولوجيا في محاولة التصدي للإرهاب بنفسها، بدلاً من مجرد إغلاق المواقع أو ملفات تعريف المستخدمين غير المقبولة. كان تطوير استخدام الذكاء الاصطناعي في قطاع الخدمات المالية مدفوعًا بالإبلاغ الإلزامي عن النشاط المشبوه في المعاملات المالية. كما تشارك

(1)Ibid.p7.
(2)Ibid.p8.

ISNN : 1112-8518 EISSN : 6200-2600

شركات القطاع الخاص مشاركة كبيرة في تطوير البرامجيات وإتاحة مجموعات البيانات لكي يستخدمها القطاع العام في مجال إنفاذ القانون العام[1].

أظهرت تقنيات الذكاء الاصطناعي إمكانات كبيرة في مكافحة الإرهاب والعنف. يمكن استخدام هذه التقنيات لتحليل كميات كبيرة من البيانات، بما في ذلك منشورات وسائل التواصل الاجتماعي والاتصالات عبر الإنترنت ولقطات المراقبة، لتحديد أنماط ومؤشرات الأنشطة الإرهابية. يمكن تدريب خوارزميات التعلم الآلي على التعرف على سلوكيات أو أنماط محددة مرتبطة بالإرهاب، مما يتيح الكشف المبكر والتدخل. وبالإضافة إلى ذلك، يمكن للذكاء الاصطناعي أن نساعد في تحليل المعاملات والشبكات المالية، والمساعدة في الكشف عن مصادر التمويل غير المشروعة وتعطيل تمويل الإرهاب. وعموماً، يوفر الذكاء الاصطناعي أدوات قيمة لوكالات الاستخبارات وإنفاذ القانون في جهودها الرامية إلى مكافحة الإرهاب وحماية السلامة العامة "[2]

في حالة مكافحة الإرهاب، تقوم دوائر الاستخبارات والأمن تقليديا باتباع الطرق التحقيق المطبقة قبل وقوع الهجوم. وبوجه عام، تركز هذه الطرق على العمل بعيدا عن المؤامرات المكتشفة جزئيا أو المشتبه فيهم المعروفين من أجل العثور على أطراف أخرى متورطة أو تحديد الروابط المؤدية إلى تعمق المنظمات الإرهابية. ويتوقف منح إمكانية الوصول إلى البيانات المتعلقة بفرد معين على ارتباطه بتحقيق واحد أو أكثر من التحقيقات القائمة.

مما يختلف عن ذلك، والذي أصبحت معقولة مؤخرًا بسبب التطورات في الذكاء الاصطناعي، تحليل النشاط الروتيني لجميع الأفراد للتنبؤ بالأحداث الإرهابية، أو لتحديد الإرهابيين خلال التمييز بين ما هو متميز في نشاط مجموعة فرعية معينة. الكمية الهائلة من المعلومات الرقمية التي يولدها الآن الفرد العادي تعني أنه يمكن فهم المزيد من هذا النشاط الروتيني خلال التحليل. تشمل المصادر البيانات الوصفية للاتصالات وسجلات الاتصال بالإنترنت، ولكنها تمتد أيضًا إلى تتبع الموقع والنشاط والمشتريات ونشاط وسائل التواصل الاجتماعي. كثير من هذه المعلومات ليست في أيدي أجهزة المخابرات والأمن، مما يعني أن الجهات الفاعلة المشاركة في استغلالها متنوعة. ويرد أدناه وصف لبعض حالات الاستخدام الضيقة[3].

أ- توقيت الهجمات وموقعها:

قد كُرست جهود كبيرة، لا سيما من الأوساط الأكاديمية، لوضع نماذج تتنبأ بموقع الهجمات الإرهابية وتوقيتها. وقد تضمنت الطرق الأساسية «تأثير الهزة الارتدادية»، حيث تزداد فرصة وقوع حدث آخر في أعقاب هجوم (وهي

(1)Ibid.p8.
(2)Ben-Asher, N., & Gonzalez, C. (2018). Countering terrorism with Artificial Intelligence techniques. Journal of Defense Analytics and Logistics, 2(1), 5-22.
(3)Ibid.p9.

ISNN : 1112-8518 EISSN : 6200-2600

ظاهرة لوحظت أيضًا مع جرائم مثل السطو) لتقديم تنبؤات دقيقة بشكل مدهش حول الهجمات الإرهابية. وقد تنبأت طرق أخرى بتأثير العوامل الخارجية - مثل الظروف السياسية - على حدوث الهجمات. في عام 2015، على سبيل المثال، ادعت شركة PredictifyMe الناشئة في مجال التكنولوجيا أن نموذجها، الذي يحسب أكثر من 170 نقطة بيانات، كان قادرًا على التنبؤ بالهجمات الانتحارية بدقة 72 في المائة. ليس من الممكن التحقق من صحة هذا الادعاء، وتجدر الإشارة إلى أن الشركة الناشئة المعنية انهارت لاحقًا. ومع ذلك، في حالات أخرى، حققت النماذج المتطورة القائمة على معلومات مفتوحة المصدر والتي تهدف إلى التنبؤ بأنواع أخرى مختلفة من الأحداث نتائج بصيرة. تتضمن هذه النماذج بشكل متزايد بيانات مفتوحة المصدر تم إنشاؤها بواسطة الأفراد الذين يستخدمون وسائل التواصل الاجتماعي والتطبيقات على هواتفهم المحمولة. أحد الأمثلة على ذلك هو التعرف المبكر على الحدث القائم على النموذج باستخدام نظام البدائل (EMBERS)، والذي يتضمن نتائج عديد من النماذج التنبؤية المنفصلة من أجل التنبؤ بأحداث مثل تفشي الأمراض وأحداث الاضطرابات المدنية. المشروع عبارة عن تعاون بين المجتمعات الأكاديمية والتجارية ويتم تمويله من قبل برنامج مؤشرات المصدر المفتوح التابع لنشاط مشاريع الأبحاث المتقدمة للاستخبارات الأمريكية (IARPA). تشمل المدخلات، من بين أمور أخرى، خلاصات RSS من المواقع الإخبارية والمدونات وخلاصات تويتر وصفحات الأحداث على مواقع الشبكات الاجتماعية وتطبيقات حجز المطاعم[1] .

"إن تطبيق الذكاء الاصطناعي في جهود مكافحة الإرهاب يبشر بكثير ؛ غير أن هناك قيودا وعقبات مختلفة يتعين معالجتها. ويتمثل أحد التحديات في توافر البيانات ونوعيتها. تعتمد أنظمة الذكاء الاصطناعي على مجموعات بيانات كبيرة ومتنوعة للتدريب والتحليل الفعالين. التحدي الآخر هو قابلية تفسير نماذج الذكاء الاصطناعي. يعد فهم عملية صنع القرار في أنظمة الذكاء الاصطناعي أمرًا بالغ الأهمية لبناء الثقة ومعالجة التحيزات المحتملة. بالإضافة إلى ذلك، هناك اعتبارات أخلاقية وقانونية تحيط باستخدام الذكاء الاصطناعي في مكافحة الإرهاب، مثل الشواغل المتعلقة بالخصوصية واحتمال إساءة الاستخدام. على الرغم من هذه التحديات، فإن الذكاء الاصطناعي لديه القدرة على تعزيز جمع المعلومات الاستخبارية وتقييم التهديدات وقدرات الاستجابة في مكافحة الإرهاب. "[2]

ب- التعرض للتطرف

نظرًا لأن شركات التكنولوجيا تتولى بشكل متزايد واجبات تتعلق بحماية مستخدميها، فإن الأدوات التي تحدد مخاطر الانتحار أو التعرض لقضايا الصحة العقلية لديها إمكانيات لإعادة استخدامها كأدوات يمكن أن تقيم القابلية للإيديولوجيات المتطرفة العنيفة. بالنظر إلى التطرف على وجه التحديد، فإن شركة Jigsaw التابعة لشركة Alphabet .

([1])Ibid.p9.
([2])Alazab, M., Broadhurst, R., & Slay, J. (2018). Application of artificial intelligence to counter-terrorism: A review of limitations, impediments, and potentials. Terrorism and Political Violence, 30(5), 801-819.

ISNN : 1112-8518 EISSN : 6200-2600

Inc. (المعروفة سابقًا باسم Google Ideas) لديها رؤية معلنة تتمثل في كونها «حاضنة تبني التكنولوجيا لمواجهة بعض أصعب تحديات الأمن العالمي اليوم»، على سبيل المثال خلال تعطيل التطرف والدعاية عبر الإنترنت. من بين مشاريع Jigsaw «طريقة إعادة التوجيه»، التي تستهدف مستخدمي مواقع مشاركة الفيديو الذين قد يكونون عرضة للدعاية من الجماعات الإرهابية مثل الدولة الإسلامية في العراق وسوريا (داعش)، وتعيد توجيههم إلى مقاطع فيديو تتبنى رواية مضادة موثوقة[1].

ج - تحديد هوية الإرهابيين

التفاصيل المسربة لـ SKYNET التابعة لوكالة الأمن القومي الأمريكية، والتي يُزعم أنها استخدمت في باكستان في عام 2007، مفيدة في توضيح كيف يمكن للأساليب الكمية التنبؤ بالتورط في الإرهاب. كما ورد، تم استخدام الخوارزمية لتحليل البيانات الوصفية من 55 مليون مستخدم محلي للهاتف المحمول الباكستاني. كان هذا نموذجًا للتعلم الآلي تم بناؤه خلال التعرض لتلك البيانات ؛ وقامت بتصنيف مستخدمي الهاتف إلى مجموعتين منفصلتين، أظهرت إحداهما نمط استخدام مطابقا لنمط استخدام مجموعة صغيرة من الأشخاص المعروفين بأنهم سعاة إرهابيون، وتضم الأخرى بقية مستخدمي الهاتف المحمول. كان النموذج قادرًا على تضييق حجم السكان الكبير، وأفيد أنه حدد الأفراد بشكل خاطئ على أنهم سعاة محتملون في 0.008 في المائة فقط من الحالات. غير أنه من المهم ملاحظة أن حجم مجموعة البيانات الأولية بالنسبة لمجموع سكان باكستان (الذي كان يقترب في ذلك الوقت من 200 مليون نسمة) يعني ضمنا أن المعدل الإيجابي الزائف البالغ 0,008 في المائة من شأنه أن يؤدي إلى تحديد خاطئ لنحو 15000 فرد بوصفهم موضع اهتمام. بالإضافة إلي ذلك، لا يمكن تحقيق المعدل الإيجابي الخاطئ البالغ 0.008 في المائة إلا بمعدل دقة بنسبة 50 في المائة لتحديد الناقلين المعروفين، مما يعني أنه يمكن تحديد نصف الناقلين المعروفين باستخدام النموذج. من هذه الأرقام، من الواضح أن النموذج المستخدم لم يكن فاعلًا في حد ذاته، لكنه يوضح كيف أن البيانات التي تبدو غير حساسة قد تكون لها قيمة تنبؤية عند تحديد الروابط الوثيقة مع الإرهاب أو القيمة الاستخباراتية المحتملة[2] .

هذه الأمثلة المحدودة لحالات استخدام الذكاء الاصطناعي التنبؤي في مكافحة الإرهاب تشير إلى الإمكانيات، بدلاً من تقديم أي دليل موثوق به على المفهوم. ليس من الواقعي أن نتوقع من الذكاء الاصطناعي تقديم حلول فورية للأسئلة المعقدة. اكتشفت سلطات الهجرة والجمارك الأمريكية ذلك عند محاولة استخدام نماذج التعلم الآلي في التنقيب عن

([1])Ibid.p10.
([2])Ibid.p11.

ISNN : 1112-8518 EISSN : 6200-2600

البيانات عبر مصادر الإنترنت المختلفة للمساعدة في فحص طالبي التأشيرات. وتم التخلي عن السعي لإيجاد حل تقني لهذه المهمة بعد أن أصبح من الواضح أنه لا توجد قدرة من هذا القبيل متاحة للشراء الفوري.

باختصار، هناك بالفعل عديد من الأمثلة على الذكاء الاصطناعي التي تتنبأ بالإرهاب أو جوانب الإرهاب. في كثير من الأحيان، تكمن القدرة على تطوير أدوات الذكاء الاصطناعي لهذا الغرض في أولئك الذين لديهم إمكانية الوصول إلى البيانات، أو الذين هم أوصياء عليها بفضل الخدمة التي يقدمونها. عندما يكون الذكاء الاصطناعي التنبؤي مفيدًا لقوات الشرطة والسلطات الأخرى (مثل وكالات إنفاذ الحدود)، غالبًا ما يتم الاستعانة بمصادر خارجية لتطويره في صناعة البرمجيات. بافتراض استمرار اتجاه الرقمنة، وتحسن أداء الذكاء الاصطناعي، سيكون هناك مجال أكبر لاستخلاص تنبؤات دقيقة حول الإرهاب من الذكاء الاصطناعي في المستقبل، ومن المرجح أن يزداد استيعابه لاستخدام مكافحة الإرهاب[1].

4. التحديات المرتبطة بالاستخدام الحالي للذكاء الاصطناعي التنبؤي في مكافحة الإرهاب

إذن حظي استخدام تقنيات الذكاء الاصطناعي لأغراض مكافحة الإرهاب، لا سيما في التعرف على النشاط والأنماط، باهتمام كبير. يمكن لخوارزميات الذكاء الاصطناعي تحليل مصادر البيانات المختلفة، مثل لقطات المراقبة ووسائل التواصل الاجتماعي وشبكات الاستشعار، لاكتشاف الأنشطة المشبوهة وتحديد التهديدات المحتملة. خلال الاستفادة من تقنيات التعلم الآلي والتعلم العميق، يمكن لنماذج الذكاء الاصطناعي التعلم من البيانات التاريخية للتعرف على الأنماط المرتبطة بالأنشطة الإرهابية. بالإضافة إلي ذلك، يمكن للذكاء الاصطناعي تمكين الرصد والتحليل في الوقت الفعلي لتدفقات البيانات واسعة النطاق، مما يتيح اتخاذ تدابير استباقية وأوقات استجابة أسرع. ومع ذلك، لا تزال هناك تحديات من حيث قابلية التوسع والدقة ودمج أنظمة الذكاء الاصطناعي مع البنية التحتية الأمنية الحالية."[2]

يمكن استخدام الذكاء الاصطناعي لوضع تنبؤات حول الإرهاب بناءً على البيانات الوصفية للاتصالات ومعلومات المعاملات المالية وأنماط السفر وأنشطة تصفح الإنترنت، بالإضافة إلى المعلومات المتاحة للجمهور مثل نشاط وسائل التواصل الاجتماعي. وقد تؤدي إمكانية منع الهجمات الإرهابية إلى دفع زخم لزيادة استخدام هذه التكنولوجيا. في عام 2017، على سبيل المثال، شركة تشغيلية في المملكة المتحدة.

([1])Ibid.p11.
([2])Perera, G., & Zaslavsky, A. (2018). Counter-terrorism using artificial intelligence techniques for activity and pattern recognition. Journal of Parallel and Distributed Computing, 114, 178-187.

ISNN : 1112-8518 EISSN : 6200-2600

دعت مجلة Improvement Review، التي اكتملت في أعقاب أربع هجمات إرهابية، إلى تغيير تدريجي في القدرة على «استغلال البيانات للكشف عن النشاط المثير للقلق» فيما يتعلق بالموضوعين المعروفين سابقًا للأجهزة الأمنية وأولئك غير المعروفين لهم.

هناك عدد من التحديات القائمة أو الناشئة فيما يتعلق باستخدام الذكاء الاصطناعي التنبؤي في مكافحة الإرهاب. وينبغي أن يعالج تطبيقه نوعين من الشواغل: مشاكل حقوق الإنسان ؛ والآثار العملية[1].

مشاكل حقوق الإنسان:

عدم وجود معايير راسخة لاستخدام تكنولوجيا الذكاء الاصطناعي

في عام 2014، لاحظ تقرير مفوضية الأمم المتحدة لحقوق الإنسان (OHCHR) حول الحق في الخصوصية في العصر الرقمي أن «أمثلة المراقبة الرقمية العلنية والسرية في الولايات القضائية في جميع أنحاء العالم قد انتشرت، مع ظهور المراقبة الجماعية الحكومية كعادة خطيرة وليس كإجراء استثنائي». ويمكن استخدام الذكاء الاصطناعي لتسهيل المراقبة الجماعية ؛ تشير التطورات الأخيرة في تحليل الفيديو وتجهيز اللغات الطبيعية إلى أن التكنولوجيات المستقبلية من المرجح أن تجعل ذلك ممكنا بقدر أكبر مع احتمال انخفاض تكاليف الدخول.

أصبح الذكاء الاصطناعي معترفًا به على نطاق واسع كتكنولوجيا قد تحقق فوائد كبيرة بينما تشكل في الوقت نفسه مخاطر كبيرة، حيث تكرس عديد من المنظمات الموارد لاستكشاف هذه. نظر تقرير حديث متعدد المؤلفين حول الاستخدام الكيدي للذكاء الاصطناعي في تأثيره على الحرية السياسية، بما في ذلك السيناريو المستقبلي المحتمل لنظام «الاضطراب المدني» التنبؤي المصمم لاستباق التهديدات قبل أن تؤتي ثمارها. وفيما يتعلق بالتنظيم الخاص بقطاعات محددة بشأن استخدام الذكاء الاصطناعي من أجل السلامة العامة، لم يتم التوصل بعد إلى توافق في الآراء بشأن الأماكن التي ينبغي أن يتم فيها رسم الخط الفاصل بين استخدام هذه التكنولوجيات، سواء أكان ذلك من جانب دوائر الاستخبارات والأمن أم أجهزة إنفاذ القانون أم القطاع الخاص[2].

ترد تفاصيل بعض الحقوق والحريات المعنية في الإعلان العالمي لحقوق الإنسان، وهي موحدة في معاهدات مثل العهد الدولي الخاص بالحقوق المدنية والسياسية. تم اعتماد العهد الدولي الخاص بالحقوق المدنية والسياسية في عام 1966 ودخل حيز التنفيذ منذ عام 1976، وله نطاق عالمي، حيث بلغ عدد الدول الأطراف 173 دولة بحلول يوليو 2019. إنه يحمي الحقوق في الخصوصية وحرية الفكر والدين والتعبير وتكوين الجمعيات. أكثر ما يتصل بموضوع هذا الجزء هو قرار الجمعية العامة للأمم المتحدة بشأن الحق في الخصوصية في العصر الرقمي. يضع هذا القرار على عاتق

(1)Ibid.p12.
(2)Ibid.p12.

ISNN : 1112-8518 EISSN : 6200-2600

الدول مسؤولية ضمان امتثال أنشطتها للقانون الدولي، لكن التفسيرات المختلفة لمفاهيم مثل التدخل «التعسفي» أو حتى «غير القانوني» في خصوصية الفرد تعني أن القرار ضعيف نسبيًا كقاعدة ملزمة. وتساعد معاهدات حماية الحقوق الإقليمية على تعزيز ذلك في بعض المجالات، لا سيما عندما تضمن سلطة المحاكم فوق الوطنية. بصرف النظر عن المجالات التي يشملها اختصاص المحاكم ذات السلطة فوق الوطنية، توجد ضوابط ضد إساءة استخدام الذكاء الاصطناعي والمستودعات الواسعة للبيانات التي يعتمد عليها على مستوى الدولة. هناك اختلافات واسعة في جميع أنحاء العالم فيما يعد استخدامًا مقبولًا للذكاء الاصطناعي، من حيث الأساليب والغرض. تم الإبلاغ عن الصين، على سبيل المثال، على أنها تتبنى تقنية التعرف على الوجه والتحليل السلوكي بالفيديو على نطاق غير مسبوق، لمجموعة من الأغراض التي تشمل تحديد المتجولين والقبض على المجرمين المطلوبين في المناسبات العامة[1].

لا يزال الجمع الجماعي للبيانات المحلية والاحتفاظ بها وحدها، والذي من المحتمل أن يكون استخدام الذكاء الاصطناعي التنبؤي مشروطًا في شكل ما، نقطة متنازع عليها بشدة. في المحكمة الأوروبية لحقوق الإنسان (ECtHR)، على سبيل المثال، هناك عديد من القضايا المعلقة التي تؤكد أن دولًا بما في ذلك ألمانيا والسويد والمملكة المتحدة تنتهك الاتفاقية الأوروبية لحقوق الإنسان خلال اعتراضها والاحتفاظ بها واستخدام البيانات السائبة. تتمتع ولايات مختلفة أيضًا بسلطات الاحتفاظ بالبيانات التي تم تجريدها من الأحكام الصادرة عن محكمة العدل التابعة للاتحاد الأوروبي (CJEU). على سبيل المثال، في ديسمبر 2016، حكمت CJEU ضد قانون الاحتفاظ بالبيانات وسلطات التحقيق في المملكة المتحدة لعام 2014، مشيرة إلى أنها فشلت في تلبية الحقوق الأساسية التي يضمنها ميثاق الاتحاد الأوروبي. الطعون القانونية على التشريع البديل - قانون سلطات التحقيق لعام 2016 - جارية بالفعل، وقد أيدت المحكمة العليا المحلية الاعتراضات الأولية التي أدت إلى تعديل القانون[2].

كما هو الحال بالنسبة لمسألة القيود المفروضة على جمع البيانات والاحتفاظ بها وتحليلها عموما، لا يوجد موقف متفق عليه بشأن التناسب النسبي للتحليل الآلي والاهتمام البشري. في بعض الأحيان، كان استخدام التحليل الآلي يميل إلى تفاقم المخاوف بدلاً من تهدئتها. فعلى سبيل المثال، نشير إلى استخدام التحليل الآلي كجزء من السبب الذي يجعل نقل تم حظر بيانات سجل أسماء الركاب (PNR) إلى كندا من قبل الاتحاد الأوروبي من خلال رأي CJEU في يوليو 2017. وهذا يعكس النص السابق الذي أصدرته تلك المحكمة بأن الاستثناء والقيود المفروضة على حماية البيانات الخاصة يجب ألا تكون موجودة إلا بقدر الضرورة القصوى، وأن الحاجة إلى ضمانات لضمان ذلك «تزداد

(1)Ibid.p13.
(2)Ibid.p13.

ISNN : 1112-8518 EISSN : 6200-2600

كلما خضعت البيانات الشخصية للمعالجة التلقائية». وإلى جانب ذلك، لا يوجد سوى قدر ضئيل من الاجتهادات القضائية الدولية التي توضح أثر التحليل الآلي على التناسب.

إن القدرة على الوصول إلى بيانات المواطنين وجمعها وتخزينها بسبب عصر المعلومات يمكن أن تمثل تغييرًا في العلاقة بين الدول والمواطنين، وتطالب بمراجعة التدابير المصممة ليس فقط لحماية الخصوصية، ولكن للحريات الأخرى الحيوية للديمقراطية الأداء، مثل تلك الخاصة بالتعبير وتكوين الجمعيات. إن التطورات الأخرى في العصر الرقمي، مثل القدرة على أتمتة أجزاء كبيرة من تحليل تلك البيانات، تكرر هذا المطلب[1].

من بين المخاوف الرئيسة الأخرى المرتبطة بثورة المعلومات مسألة افتقاد الخصوصية، إن قدراً كبيراً من المعلومات يتم جمعه بالفعل فيما يختص بكل منا، سواء أكان خلال شركات خاصة، أم إدارات حكومية. ونحن لا نملك في معظم الأحيان أي فكرة عن كيفية استخدامها أو عما إذا كانت دقيقة أم لا؟ فإحصائيات مكتب الإحصاء السكاني تحتوي على كم كبير من التفاصيل، كذلك ترسم السجلات الطبية ومسجلات القيادة وسجلات المكينات، وسجلات المدارس، وسجلات المحاكم، وبيانات سوابق التسهيلات الإئتمانية، والسجلات الضريبية، والسجلات المالية، ومقابلات التوظيف، وفواتير المشتريات، وبطاقات الإئتمان... ترسم في مجملها صورة موجزة لحياتك التي قتد تنتهك إلكترونيا في أي لحظة .

رغم أن الطبيعة المتناثرة للمعلومات تحمى خصوصيتك بصورة تلقائية، فسوف يصبح بالإمكان عندما توصل الخازنات كلها معاً عن طريق المعلومات السريع، استخدام الكمبيوترات في الربط المحكم بينها، فبيانات الائتمان يمكن ربطها بسجلات المستخدمين، وسجلات معاملات البيع من أجل تكوين صورة دقيقة، ودون إذن منك عن أنشطتك الشخصية [2].

عند استخدام هذه السلطات والحد منها، يجب أن يكون من الممكن التمييز بين الدول الديمقراطية والاستبدادية. للمؤسسات الديمقراطية أدوار أساسية تؤديها في وضع الحدود والحفاظ عليها وفي خلق سياق واضح ومشرع لأي تدخل في خصوصية البيانات. في المملكة المتحدة، مراجعة التشريع الذي يحكم سلطات التحقيق لأجهزة الشرطة والاستخبارات في المملكة المتحدة - من قانون تنظيم سلطات التحقيق لعام 2000، إلى قانون الاحتفاظ بالبيانات وصلاحيات التحقيق لعام 2014، وبعد ذلك إلى قانون سلطات التحقيق لعام 2016 - محاولة لتحقيق ذلك. يُظهر الحكم الصادر في أبريل 2018 عن المحكمة العليا المحلية بتأييد الطعن في أجزاء من أحدث نسخة من القانون، ومطالبة بإعادة كتابتها إذا كانت قانونية، أن التعديل مستمر وليس يتم حله.

([1])Ibid.p14.

([2]) جيتس ،بيل جيتسي: المعلوماتية بعد الإنترنت، ترجمة عبدالسلام رضوان،عالم المعرفة،الكويت،1998.

ISNN : 1112-8518 EISSN : 6200-2600

سيعتمد الذكاء الاصطناعي التنبؤي على تحليل البيانات الخاصة بعامة الناس للتمييز بين السلوك المشبوه والسلوك الطبيعي، أو لتمييز الاتجاهات التي قد تساعد في التنبؤ بالهجمات. سيتم إنشاء الغالبية العظمى من البيانات قيد التحليل من قبل أشخاص ليسوا مهمين لأجهزة الاستخبارات[1].

لهذا السبب، فإن أحد مجالات القلق المحددة المرتبطة بتكنولوجيا الذكاء الاصطناعي التنبؤية هو أنها تشكل تدبيرًا للمراقبة مطبقًا على جميع السكان، وهذا من شأنه أن يجعلها عشوائية وبالتالي غير متناسبة بطبيعتها. كان هذا أيضًا أحد مجالات تركيز الاعتراضات على برامج جمع البيانات وتحليلها في الدول. وفي حين أن هذه البرامج لا ترتبط ارتباطاً مباشراً باستخدام الذكاء الاصطناعي، فمن المرجح أن يعتمد استخدام الذكاء الاصطناعي التنبؤي لمكافحة الإرهاب على القدرة على جمع البيانات وتحليلها بكميات كبيرة.

حتى جمع وتحليل البيانات التي تبدو غير حساسة لا يزال بإمكانها خلق تدخل كبير في الخصوصية. يصف قرار الجمعية العامة للأمم المتحدة 167/68 بشأن الحق في الخصوصية في العصر الرقمي «جمع البيانات الشخصية بشكل غير قانوني أو تعسفي» بأنه عمل تدخلي للغاية يمكن أن ينتهك «الحق في الخصوصية وحرية التعبير وقد يتعارض مع مبادئ المجتمع الديمقراطي». وذلك بسبب الاعتراف الطويل الأمد بأنه يمكن استنتاج معلومات شخصية مهمة من هذا النوع من البيانات، وأن تجميع البيانات وتحليلها يشكلان انتهاكًا للخصوصية حتى لو تم اتخاذ إجراءات في الأماكن العامة. لذلك لا يزال الجدل قائما، حتى لو تم جمع البيانات المعنية من مصادر مفتوحة[2].

مع بدايات القرن العشرين أصبح التقدم التكنولوجي يسير بسرعة فائقة، نتيجة لدخول تكنولوجيا الاتصالات ومعالجة البيانات عن طريق الحاسبات الإلكترونية، وهي ما أطلق عليها اسم «ثورة المعلومات التي تتعلق بجمع وتوصيل وتخزين واستعادة ومعالجة وتحليل المعلومات، وتقوم على الربط بين التكنولوجيا المبنية على الالكترونيات الدقيقة وصناعة المعلومات، وتتصف بسمات أهمها أنها ذات كثافة علمية شديدة، كما تتميز بشدة كثافة رأس المال فيها على النطاق العالمي [3].

فإذا كان الإنسان في ظل الثورة الصناعية قد نجح في صنع آلة تنوب عنه عضليا، فإنه لم يكتف بذلك، بل سعى إلى بناء آلة حاسبة تخفف عنه عبئاً ذهنياً، وقد شهد القرن التاسع عشر عدة محاولات لبناء آلة حاسبة من التروس

(1) McKendrick,K.p14.
(2) Ibid.p15.
(3) فؤاد المرسي: الرأسمالية تجدد نفسها، عالم المعرفة ، الكويت،1990، ص38.

ISNN : 1112-8518 EISSN : 6200-2600

والروافع، إلى أن خرج الكمبيوتر الرقمي في خمسينيات القرن العشرين وكان ثمرة لالتقاء علوم الفيزياء والرياضيات المنطقية والهندسة الإلكترونية، وقد أدى هذا التلاقي الخصب إلى ما نسميه الثورة التكنولوجية[1].

لقد أسهمت التطورات السريعة التي شهدتها تكنولوجيا الاتصال والمعلومات خلال السنوات الأخيرة، والتأثيرات المباشرة للثورة الرقمية على نمط الحياة الإنسانية، في حدوث «فجوة رقمية» بين الدول، حيث يشير هذا المصطلح إلى الفرق بين من يمتلك المعلومة ومن يفتقدها، وبين من يسهم ويشارك في صنع تكنولوجيا المعلومات والاتصالات واستغلالها ومن يتم استبعاده من إطار السباق المعلوماتي، وقد ظهر هذا المصطلح في الولايات المتحدة سنة ١٩٩٥م كتعبير عن اتساع الفجوة المعلوماتية بين الدول المتقدمة والدول النامية [2].

توفر بعض قوانين القانون الدولي مبادئ توجيهية لتقييم ما إذا كان أي انتهاك لخصوصية البيانات مبررًا. إن الحق في خصوصية البيانات محمي على وجه التحديد بموجب المادة 8 من ميثاق الاتحاد الأوروبي، ويغطيه أيضًا الحق في الخصوصية بشكل عام في المادة 8 من الاتفاقية الأوروبية لحقوق الإنسان. ولهذا السبب، أصدرت محكمة العدل الأوروبية والمحكمة الأوروبية لحقوق الإنسان الأحكام ذات الصلة. وبالنسبة لكلتا المؤسستين، فإن التدخل لابد أن يلبي معياراً ثلاثياً يتمثل في تحقيق هدف مشروع، وأن يتم التدخل ضمن إطار قانوني وتلبية شروط الضرورة والتناسب. وتعني الضرورة في هذا السياق أن الإجراء مناسب، حيث أن له علاقة سببية بهدف السياسة، وأنه لا ينتقص من الحقوق أكثر مما هو ضروري في ضوء الخيارات البديلة. وقد شددت محكمة العدل الأوروبية هذا الأمر إلى معيار الضرورة القصوى، مطالبة بأن تكون المراقبة مستهدفة؛ أنها محدودة أو تخضع للتمايز على أساس الهدف المنشود؛ وأنه يخضع لمبادئ توجيهية دقيقة وموضوعية؛ وأن توجد ضمانات كافية وفاعلة ضد إساءة الاستخدام [3].

عندما يتم إلغاء صلاحيات الدولة في الاحتفاظ بالبيانات وتحليلها من قبل محكمة العدل الأوروبية، في التحكيم بشأن تطبيق ميثاق الاتحاد الأوروبي، فذلك لأنها لم تستوف هذه المعايير. أوضحت محكمة العدل الأوروبية أن حكمها ضد المملكة المتحدة بشأن الاحتفاظ بالبيانات يمكن تفسيره على أنه "يستبعد التشريعات الوطنية التي تنص، لغرض مكافحة الجريمة، على الاحتفاظ العام والعشوائي بجميع بيانات حركة المرور والموقع لجميع المشتركين والمستخدمين المسجلين فيما يتعلق كافة وسائل الاتصال الإلكتروني". إن صلاحيات المملكة المتحدة في الاحتفاظ بالبيانات لم ترق إلى مستوى معايير الضرورة. قد تعد الأساليب التي تجمع وتحلل كل البيانات غير متناسبة، ليس لأن الاحتفاظ الشامل بها خطأ من حيث المبدأ، ولكن لأنه لا يمكن ربطها بهدف مشروع محدد له علاقة سببية واضحة بالسياسة[4].

([1]) نبيل علي : تحديات عصر المعلومات،الهيئة المصرية العامة للكتاب،القاهرة،2003،ص11.

([2]) المرجع نفسه،ص23.

([3]) McKendrick,K.p15.

([4]) Ibid.p15

ISNN : 1112-8518 EISSN : 6200-2600

تقدم عملية فحص أجريت في ألمانيا في محاولة لتحديد «الخلايا النائمة» الإرهابية مثالاً على الحالات التي لا ترقى فيها الطريقة التي تنطوي على تحليل البيانات في مستوى التدقيق فيما يتعلق بقدرتها على تحقيق هدف مشروع. تضمنت عملية الفحص إحالة مرجعية لمجموعة من الأفراد تم تحديدهم باستخدام خصائص ثابتة - مثل الانتماء الديني - مع قواعد بيانات أخرى. واعتبرتها المحكمة الدستورية الاتحادية الألمانية غير دستورية على أساس أنها تتدخل في «تقرير المصير الإعلامي للأشخاص الذين لا توجد شكوك ضدهم» في غياب تهديد محدد. تم اختيار الخصائص التي تم استخدامها لفصل هؤلاء الأفراد بناءً على الانطباعات عن الاتجاهات في الهجمات السابقة، والتي لم تكن قاعدة أدلة صارمة بما يكفي[1].

تلقي أحدث الأحكام الصادرة عن المحكمة الأوروبية لحقوق الإنسان مزيدا من الضوء على مشروعية نظم جمع البيانات بالجملة والاحتفاظ بها. في سبتمبر 2018، وجدت المحكمة أن المملكة المتحدة قد انتهكت الحق في الخصوصية بسبب عدم كفاية الضمانات والرقابة على نظام جمع البيانات بالجملة، لكنها رأت أيضًا أنه «في التوصل إلى هذا الاستنتاج، وجدت المحكمة أن تشغيل نظام الاعتراض بالجملة لا ينتهك في حد ذاته الاتفاقية». في يونيو 2018، رأت المحكمة الأوروبية لحقوق الإنسان أن اعتراض السويد بالجملة للإشارات الإلكترونية لا يتعارض بشكل مفرط مع حق المواطنين في الخصوصية، ويرجع ذلك جزئيًا إلى اقتصاره على الاتصالات التي تعبر الحدود السويدية. وفي هذه الحالة، تم قبول شرط واسع نسبيا بوصفه مقيدا بما فيه الكفاية في وجود هيئات رقابة مستقلة وتعريفا واضحا في القانون[2].

تميل التشريعات وأطر الحوكمة لاستخدام البيانات الشاردة إلى التركيز بشكل أساسي على صلاحيات الوصول إلى البيانات، مع وصف محدود لكيفية استخدام البيانات، أو الاعتبارات الطبيعية لكيفية حمايتها بشكل صحيح من إساءة استخدامها. ودون تقديم مزيد من التفاصيل عن استخدام البيانات، من الصعب إثبات الضرورة عن طريق الربط الواضح بين الاحتفاظ بالبيانات وبين شيء يمكن إثبات أنه هدف مشروع. إذا تم استخدام الذكاء الاصطناعي إلى حد أكبر، فيجب أن يثبت الإطار الذي يتم استخدامه بموجبه - أو يضمن بطريقة أخرى - إسهامه في هدف مشروع[3].

دور القطاع الخاص المتوسع ولكنه ضعيف التنظيم :

في البلدان التي تلزم فيها الحكومات نفسها بالتزامات قانونية صارمة نسبيًا، مارست الشركات الخاصة سلطة تقديرية أكبر بكثير حول كيفية استخدامها لبيانات العملاء. الطريقة التي يستخدم بها الذكاء الاصطناعي التنبؤي حاليًا في مكافحة الإرهاب ترى أن المسؤولية تقع على عاتق مجموعة واسعة من الجهات الفاعلة، أساسًا على أساس دورها

(1) Ibid.p16.
(2)Ibid.p16.
(3)Ibid.p16.

ISNN : 1112-8518 EISSN : 6200-2600

كأوصياء على البيانات. هذه الحرية النسبية جزء من السبب في أن نسبة كبيرة من الجهود المعلنة لاستخدام الذكاء الاصطناعي في التنبؤ بالإرهاب قد بدأت حتى الآن من قبل شركات التكنولوجيا[1].

قامت بعض الشركات، التي تعمل ضمن القيود القانونية على جمع البيانات وبيعها، بتحويل معلومات عن الجمهور إلى سلعة يمكن للشركات نفسها بيعها إلى وكالات إنفاذ القانون والأمن. وقد تشتري الحكومات بيانات تساعدها على الحفاظ على الأمن إذا لم تتمكن من الحصول عليها بصورة قانونية بوسائل أخرى، مثل اعتراض الاتصالات السلكية واللاسلكية. البيانات سلعة قيمة، مما يعني أن التزامات الشركات الخاصة لحماية خصوصية العملاء ليست دائمًا مبدئية كما قد تظهر. بينما منعت بعض شركات التكنولوجيا الحكومات صراحة من استخدام البيانات من منصاتها، تظل هذه البيانات نفسها متاحة لشركات خارجية ؛ وبالتالي، فإن هذه الشروط في الغالب بلاغية من حيث القيمة. تقود البراجماتية حول الوصول إلى الأسواق الكبيرة شركات التكنولوجيا إلى التراجع عن مبادئها المعلنة في بعض الولايات حيث تكون خصوصية المستخدم وحريته أكثر عرضة للخطر. بالإضافةإلى ذلك، هناك شفافية محدودة فيما يتعلق بمكان ومتى يفعلون ذلك. ففي البلدان التي توجد فيها سيطرة حكومية أكبر على الصناعة الخاصة، توجد فرص غير محدودة للحكومات لجمع وتحليل المعلومات الشخصية أو الحساسة عن مواضيعها[2].

في حين أن المرونة النسبية في القطاع الخاص قد تتيح الفرص، فإن إسناد قدر كبير من المسؤولية إلى الشركات التجارية يمكن أن يؤدي إلى عجز متزايد في المساءلة. على الرغم من أن بعض الشركات الخاصة تبذل جهودًا لتحقيق الشفافية، إلا أنها جزئية ويتم إجراؤها وفقًا لتقديرها الخاص. على الرغم من حقيقة أن الشركات الخاصة لها دور متزايد بحكم مسؤولياتها تجاه مستخدميها، فمن المشكوك فيه ما إذا كان ينبغي الاعتماد عليها لمواجهة الانتهاك المفرط للخصوصية وحرية التعبير من قبل الدول الاستبدادية، أو لتحقيق التوازن بين الأمن من الإرهاب والحق في الخصوصية نيابة عن الديمقراطيات[3].

- عدم التعويض :

إن الغموض المتأصل في أساليب استخدام الذكاء الاصطناعي التنبؤي في مكافحة الإرهاب، أو حتى في استخدام البيانات المحتفظ بها بشكل عام، يجعل من الصعب استحداث ضمانات قانونية للانتصاف. تحاول اللائحة العامة لحماية البيانات (GDPR) في الاتحاد الأوروبي، وهي واحدة من أكثر أنظمة حماية البيانات بعيدة المدى في العالم، تحقيق التوازن بين ذلك خلال تأمين حق الإنصاف في أي قرار مؤتمت بالكامل يتم اتخاذه. غير أنه من غير الواضح ما

(1)Ibid.p16.
(2)Ibid.p17.
(3)Ibid.p17.

ISNN : 1112-8518 EISSN : 6200-2600

إذا كان يمكن الوفاء بهذا المعيار باتخاذ قرارات تنطوي على مستوى تعسفي من الرقابة البشرية. بالإضافة إلي ذلك، يتضمن إعفاء للوكالات الحكومية.

تحاول أنظمة مثل محكمة سلطات التحقيق (IPT) في المملكة المتحدة توفير الإنصاف بشأن تصرفات الوكالات الحكومية، لكنها محدودة في القيام بذلك، مع إجراء بعض الإجراءات في الخفاء. على الرغم من أن IPT قد حكم ضد الحكومة، مشيرًا إلى استقلاليتها، فقد تعرض النظام لانتقادات لأنه لم يقدم سوى تعويضات محدودة، ويعتمد على الثقة في مؤسسات الحكومة ويصعب على عامة الناس الوصول إليها. ومع ذلك، وبسبب الحاجة إلى إجراء مقايضة بين الشفافية والأمن التشغيلي الذي هو نموذجي لأساليب مكافحة الإرهاب بشكل عام، فإن معاهدة منع انتشار الإرهاب تمثل حلاً وسطاً يجعله كثيرون عادلاً. وعلى الرغم من القيود المتأصلة في الشفافية في مكافحة الإرهاب، فإن أحد الجوانب المهمة للسياسة الناجحة لمكافحة الإرهاب يتمثل في تحقيق أقصى قدر ممكن من الشفافية. يمثل استخدام الذكاء الاصطناعي مشكلة ما إذا كان يشكل - أو يُنظر إليه على أنه يشكل - تهديدًا لتلك الشواغل العملية[1] .

"يمكن تطبيق الذكاء الاصطناعي على جوانب مختلفة من مكافحة الإرهاب، مثل استخبارات التهديدات وتقييم المخاطر والوعي بالأوضاع. يمكن لخوارزميات التعلم الآلي تحليل كميات كبيرة من البيانات لتحديد الأنماط والشذوذ والتهديدات المحتملة في الوقت الفعلي. يمكن أن تساعد تقنيات معالجة اللغة الطبيعية في مراقبة وتحليل الاتصالات عبر الإنترنت للمحتوى المتطرف. إن دمج الذكاء الاصطناعي مع التقنيات الأخرى، مثل تحليلات البيانات الضخمة والأمن السيبراني، يمكن أن يعزز فعالية جهود مكافحة الإرهاب. ومع ذلك، لا تزال هناك تحديات من حيث الشفافية الخوارزمية وخصوصية البيانات والاعتبارات الأخلاقية المرتبطة بنشر الذكاء الاصطناعي في هذا المجال. تشمل الاتجاهات المستقبلية تطوير نماذج الذكاء الاصطناعي القابلة للتفسير، واستخدام الذكاء الاصطناعي في الإجراءات الوقائية، والتعاون بين باحثي الذكاء الاصطناعي وصانعي السياسات والوكالات الأمنية لمواجهة التهديدات الناشئة."[2]

"اكتسب الذكاء الاصطناعي اهتمامًا كبيرًا في جهود مكافحة الإرهاب ومنع الجريمة. تم استخدام خوارزميات التعلم الآلي، مثل آلات ناقلات الدعم والشبكات العصبية، لتحليل مجموعات البيانات الكبيرة وتحديد الأنماط المشبوهة. تم استخدام تقنيات معالجة اللغة الطبيعية لتحليل النصوص وتحليل المشاعر في الاتصالات عبر الإنترنت.

([1])Ibid.p18.
([2])Alazab, M., Choo, K. K. R., & Layton, R. (2019). Artificial Intelligence for countering terrorism: Review and future directions. Computers & Security, 84, 53-67.

ISNN : 1112-8518 EISSN : 6200-2600

وقد أدى تكامل الذكاء الاصطناعي مع تكنولوجيات أخرى، مثل تحليل البيانات الضخمة وتحليل الشبكات الاجتماعية، إلى زيادة تعزيز فاعلية استراتيجيات مكافحة الإرهاب "[1]

- قدرة الذكاء الاصطناعي على تحقيق قيمة تنبؤية كافية :

إن قلة انتشار الإرهاب، وميل التكتيكات الإرهابية إلى التطور بسرعة إلى حد ما، يجعل من الصعب بناء نماذج تنبؤية جيدة. هناك أدوار مختلفة متعددة في الإرهاب، ومسارات متعددة للوفاء بهذه الأدوار. وهذا يعني أنه من المستحيل إدراج مؤشرات نهائية للتورط أو الاستبعاد من الأنشطة الإرهابية. وفي حين يبدو أن هناك بعض الاتجاهات الملحوظة في الخصائص المشتركة بين الإرهابيين، فإن العدد الضئيل من الإرهابيين في عموم السكان يجعل من الخصائص الواسعة النطاق القائمة على تحديد سمات لا قيمة تنبؤية لها. وعلى سبيل المثال، فإن احتمال إدانة شخص في المجموعة الفرعية من الذكور الذين اعتنقوا الإسلام بالإرهاب يقل عن ثلاثمائة في المائة، في حين أن أكثر من 90 في المائة من الإرهابيين المدانين ينتمون إلى خارج تلك المجموعة الفرعية. تعمل نماذج التعلم الآلي بشكل جيد عبر مجموعات سكانية كبيرة، ولكنها تكون ضعيفة بالسلوك الفردي[2].

إن الوعد بمزيد من الذكاء الاصطناعي المتطور هو أنه سيتمكن من إجراء توقعات أفضل بناءً على السلوكيات في مجموعة متنوعة من المجالات المختلفة، بدلاً من توصيف سطحي. ونظرًا لزيادة نشاط المنظمات الإرهابية عبر الإنترنت، أظهرت الأبحاث أنه من الممكن استخدام الذكاء الاصطناعي لتحليل الاتصالات واستنتاج سمات مثل درجة التطرف، والنية العدوانية، ونشوء حركات إرهابية، وحتى التنبؤ بوقوع هجمات عنيفة. يشير ذلك إلى أنه في حين كان من المستحيل في السابق توقع تورط الإرهابيين، قد لا يكون هذا هو الحال بعد الآن. يمكن تحسين دقة النماذج التنبؤية التي تعتمد على مصدر واحد من البيانات عن طريق دمج نتائج من مصادر بيانات أخرى. ومع ذلك، فإن إمكانية القيام بذلك تقتصر في الأغلب على وصول البيانات[3].

- الوصول إلى البيانات

كلما إزدادت البيانات، إزداد تحسين النماذج. تقتصر جودة النماذج الممكن تحقيقها على قيود على أنواع البيانات التي يمكن الوصول إليها وكيفية استخدام تلك البيانات. يتم فرض قيود على الوكالات الحكومية استناداً إلى التشريعات الوطنية وقوانين حقوق الإنسان الدولية أو الوصول الجسدي والقدرات التقنية. لهذا السبب، ترتبط الأمثلة السابقة المذكورة في هذه الوثيقة بوكالات المخابرات التي تعمل خارج بلدها الأصلي، أو الأوساط الأكاديمية، أو

([1])Tavana, M., Santos-Arteaga, F. J., & Di Caprio, D. (2020). Artificial intelligence for counter-terrorism and crime prevention: A bibliometric analysis. Technological Forecasting and Social Change, 155, 120032.
([2])Ibid.p18.
([3])Ibid.p19.

ISNN : 1112-8518 EISSN : 6200-2600

الجهات الخاصة ذات الوصول إلى البيانات عن طريق مهامها كمزودي خدمة. يؤكد هذا الجزء أن بعض القيود على الوصول، على النحو الذي هو عليه حالياً، لا توفر بالضرورة ضمانات للشرعية، في حين أن القيود المفروضة على كيفية استخدام البيانات قد تكون أفضل.

تقييد الوصول إلى البيانات يعتمد غالبًا على تمييز بين البيانات المحلية والأجنبية. تكون الصلاحيات القانونية لتحليل الاتصالات الأجنبية أشمل، وتشمل قدرات "الكشف" لتحديد التهديدات التي لم يتم اكتشافها مسبقًا. في الماضي، كان التمييز المستند إلى وجود عنصر أجنبي في الاتصالات ذا أهمية أكبر. كما لوحظ من قبل الأكاديمي فيليب بوبيت في عام 2008:[1]

كان ذكاء الإشارات في القرن العشرين يعني اعتراض الإشارات التناظرية التي تنقل عبر قنوات صوتية مخصصة. في القرن الحادي والعشرين، تكون الاتصالات رقمية بشكل رئيس: إذ تحمل مليارات حزم البيانات، وتُوجّه بطريقة متغيرة في حزم وتكون متصلة على مستوى عالمي.

يمكن أن يتم توجيه الاتصالات المحلية عبر خادم في بلد أجنبي فقط بناءً على أسباب التوفيق. بالإضافة إلي ذلك، في حين أن سوابق التمييز القانوني بين البيانات الأجنبية والمحلية تكمن في الحماية الأساسية ضد المراقبة ذات الدوافع السياسية، فإن التغييرات في طبيعة الاتصالات تعني أن التمييز على أساس منشأ تلك الاتصالات ووجهتها ليس بالضرورة قادرًا على توفير تلك الحماية[2].

الولايات المتحدة تستضيف حجمًا كبيرًا من البنية التحتية العالمية للإنترنت على أراضيها. تعطي هذه الحقيقة فرصة لامتلاك قدرات واسعة للتدخل الأجنبي. للامتثال لالتزامات وطنية لحماية خصوصية المواطنين، توجد إجراءات تقليص تلقائية لتصفية الاتصالات الداخلية للمواطنين التي تم اعتراضها بشكل غير مقصود، من دون خضوعها لمزيد من التحليل. يقبل هذا النشاط ضمنيًا تحليل البيانات الخاصة بالمواطنين الداخليين بشكل تلقائي (بهدف تصفيتها)، وتسمح حتى بحرية أوسع في تحليل البيانات الأجنبية.

الاختلاف في معاملة الاتصالات الأجنبية قد يسبب مشاكل في مشاركة المعلومات. على سبيل المثال، إذا تم تفسير اختلاف معاملة المواطنين الأجانب والمحليين بوصفه تعارضًا في احترام خصوصية هاتين المجموعتين، يبدو من المفهوم أن مزودي خدمات الاتصالات قد يكونون مترددين في الالتزام بمعايير غير متساوية ضد المواطنين من بلدانهم الأم. يمكن تفسير معدلات الامتثال المنخفضة لطلبات الوصول من قبل مزودي خدمات الاتصالات إلى الإنفاذ القانوني من دول أخرى بهذا الشكل. على المستوى الوطني، يمكن أن تكون العلاقات الاستخباراتية الوثيقة بين الدول إما معيقة بسبب

(1)Ibid.p19.
(2)Ibid.p19.

ISNN : 1112-8518 EISSN : 6200-2600

هذه القيود أو تقضي عليها تمامًا خلال السماح بمشاركة المعلومات المشتقة من انتهاك خصوصية المواطنين في الدول الأخرى[1].

تقتصر وكالات الحكومة على قدراتها التقنية لاعتراض الاتصالات. على سبيل المثال، يُعتقد أن الهيئة البريطانية للاتصالات الحكومية (GCHQ) تمتلك قدرات تدخل واسعة، ولكنها لا تزال قادرة فقط على الوصول إلى بعض الاتصالات الدولية التي تدخل أو تغادر المملكة المتحدة. وبالتالي، يمكن لـ GCHQ تحليل نسبة صغيرة من هذه الاتصالات. إذا تم الحصول على البيانات خلال هذه الأساليب للإلهام في النماذج التنبؤية، فإن القدرة التقنية هي قيد تعسفي بدلاً من أن تكون ضمان للشرعية. من الأفضل أن تكون هناك ترتيبات وصول أفضل مع مزودي خدمات الاتصالات، والتي تستند إلى شرعية الممارسات والأساليب المتورطة. كما هو الحال في الوقت الحالي، فإن الامتثال لهذه الطلبات من الشركات القائمة في دول أخرى غير مستقر، مما يترك التغطية غير مكتملة[2].

نظرًا للاعتماد على وصول البيانات لإنشاء نماذج تنبؤية جيدة، فإن قيود القدرة على الوصول واستغلال البيانات يقيد بدوره استخدام الذكاء الاصطناعي التنبؤي في مجال مكافحة الإرهاب. يمكن أن تكون القيود التقنية أو القانونية، أو يمكن أن تكون بسبب عدم وجود ثقة بين الجهات المعنية، مما يمنع تبادل المعلومات. من الضروري أن تكون القيود القانونية لمنع الاستغلال، ولكن القيود التي تركز فقط على الوصول إلى البيانات لها تأثير سلبي على جودة أي نماذج قد يتم تطويرها، في حين تفشل في تلبية الحاجة إلى معايير محددة تحكم كيفية استخدام البيانات بشكل مشروع. ويجب أن يكون الوصول إلى البيانات وطريقة استخدام هذه البيانات قانونيًا. ونظرًا لأن شرعية الوصول إلى البيانات تعتمد على شروط الضرورة، فهي مترابطة. الوصول إلى البيانات له ما يبرره اعتمادا على كيفية استخدامها[3].

"برز الذكاء الاصطناعي كأداة حاسمة في جهود مكافحة الإرهاب، حيث يوفر قدرات متقدمة للكشف عن التهديدات وتقييم المخاطر ودعم القرار. تم تطبيق تقنيات الذكاء الاصطناعي، مثل التعلم العميق والتعلم المعزز، بنجاح لتحليل مصادر البيانات المتنوعة، بما في ذلك وسائل التواصل الاجتماعي ومقاطع فيديو المراقبة وصور الأقمار الصناعية، لتحديد التهديدات المحتملة والتنبؤ بالأنشطة الإرهابية. يمكن للأنظمة القائمة على الذكاء الاصطناعي تعزيز الوعي بالحالة، وتسهيل دمج المعلومات، وتمكين استراتيجيات الاستجابة الاستباقية. ومع ذلك، يجب معالجة تحديات مثل جودة البيانات والتحيزات الخوارزمية والاعتبارات الأخلاقية من أجل الاستخدام المسؤول والفاعل للذكاء الاصطناعي في مكافحة الإرهاب. تتضمن وجهات النظر المستقبلية تطوير قابلية شرح الذكاء الاصطناعي، والتعاون بين

(1) Ibid.p20.
(2)Ibid.p20.
(3)Ibid.p20.

ISNN : 1112-8518 EISSN : 6200-2600

الإنسان والآلة، والتعاون بين الوكالات الحكومية والأوساط الأكاديمية والصناعة للاستفادة من تقدم الذكاء الاصطناعي في هذا المجال. "[1]

"يمثل الذكاء الاصطناعي تحديات وفرصًا في سياق الإرهاب. من ناحية، يمكن للإرهابيين استغلال الذكاء الاصطناعي لأغراض مختلفة، بما في ذلك تشفير الاتصالات ونشر الدعاية والأسلحة المستقلة. من ناحية أخرى، يمكن للذكاء الاصطناعي تعزيز جهود مكافحة الإرهاب من خلال تحليل البيانات الضخمة وتحديد الأنماط والتنبؤ بالأنشطة الإرهابية"[2]

- عدم وجود معايير مصادقة موحدة

على الرغم من أهمية الوصول إلى البيانات، إلا أنه في حد ذاته لا يضمن النجاح في بناء نماذج توقع دقيقة. التحقق والاختبار ضروريان لقياس الدقة التوقعية للنماذج وتقييم التناسب في استخدامها.

إحدى الدروس البارزة المستفادة من الخبرة في مجال مكافحة الجريمة التنبؤية هي أهمية تجريب الأنظمة واختبارها. تم وضع عدالة عديد من الخوارزميات المطورة تجاريًا لمكافحة الجريمة التنبؤية - أو تلك التي تؤثر على القرارات القانونية - تحت الشك، وكان يمكن تجنب ذلك خلال توظيف عملية تحقق أكثر شمولاً قبل استخدامها. قدمت دراسة نُشرت في عام 2013 حول مختلف أنواع برامج تقييم مخاطر المجرمين المستخدمة لتوجيه قرارات الكفالة في الولايات المتحدة النتائج غير المتوقعة التالية:

كان هناك نقص شديد في الولايات المتحدة بشأن تقييمات الصحة التوقعية للتقييمات التي تم إجراؤها باستخدام الأدوات التي تستخدم عادة في وكالات السجون في الولايات المتحدة. في معظم الحالات، لم تتم دراسة صحة القياس إلا في واحد أو اثنين من الدراسات التي أجريت في الولايات المتحدة، وغالبًا ما أجريت تلك الدراسات بالأشخاص أنفسهم الذين طوروا الأداة.

هذا يشير إلى غياب معايير يتم تطبيقها بشكل منهجي، وميل إلى الثقة بتقييمات مزودي البرمجيات التجارية لتقويم منتجاتها[3].

تهتم مجموعة بحثية حديثة بمدى ضعف الذكاء الاصطناعي في مواجهة التحيز، وتنفي فكرة أن نتائج الذكاء الاصطناعي التنبؤي يمكن جعلها علمية موضوعية. هناك عديد من مجالات التحيز. قد يكون التحيز موجودًا في البيانات التي يتم تدريب الذكاء الاصطناعي عليها، أو في جوانب التصميم مثل وجود حلقات ردود فعل مخفية، أو في

([1])Vashist, A., & Bhattacharya, S. (2021). Artificial intelligence for counter-terrorism: A comprehensive review and future perspectives. Journal of Defense Analytics and Logistics, 5(3), 338-357.
([2])Kshetri, N. (2020). Artificial intelligence and terrorism: Challenges, opportunities, and responses. Terrorism and Political Violence, 32(6), 1234-1255.
([3])Ibid.p21.

ISNN : 1112-8518 EISSN : 6200-2600

استخدام عوامل ثقافية متوسطة مثل الافتراضات المستندة إلى السفر إلى بعض البلدان، أو في المعاملة المتفاوتة للفرق الفرعية. قد تظهر الخوارزمية التي يبدو أنها تعمل بشكل فاعل تحيزًا، بل وحتى تزيد من هذا التحيز في العالم الحقيقي. للتخفيف من ذلك، يجب أن تشمل التقييمات العميقة للنماذج التوقعية تقييمات لجودة النموذج فيما يتعلق بالفئات الفرعية المختلفة.

نظرًا للمجموعة الواسعة من الجهات المشاركة، فإن المعايير المشتركة تصبح أكثر أهمية. زيادة استخدام تقنيات تُستخدم تقليديًا بواسطة وكالات المخابرات في إنفاذ القانون واستخدام الذكاء الاصطناعي من قبل القطاع الخاص يعني وجود عدد متزايد من الجهات المتورطة في تطوير واستخدام الذكاء الاصطناعي التنبؤي في مكافحة الإرهاب[1].

حاليًا ، تؤدي مجموعة متنوعة من الطرق إلى بعض النتائج غير المنطقية ، وتحديداً حذف البيانات الخاصة بالأفراد ذوي الأهمية الاستخباراتية الحقيقية جنبًا إلى جنب مع الاحتفاظ الشامل بالبيانات عن الأفراد الذين ليسوا كذلك. تقوم الجهات الفاعلة في القطاع الخاص بمراقبة المحتوى على منصاتهم بإزالة المواقع أو إغلاق الحسابات ، مما يؤدي أيضًا إلى حذف معلومات استخبارات قيمة بشكل حقيقي ومرتبطة بأنشطة إجرامية أو إرهابية. في قضية مقتل الجندي لي ريجبي في المملكة المتحدة في مايو 2013 ، قامت إحدى منصات التواصل الاجتماعي التي تستخدم الذكاء الاصطناعي في تحديد الحسابات المرتبطة بالإرهاب بإغلاق 11 حسابًا مرتبطًا بأحد الهجومين. واحدة من هذه الحسابات تحتوي على تبادل وصفته لجنة اختيار الاستخبارات البرلمانية بأنها الجزء الوحيد من الأدلة التي يمكن أن تحول دون وقوع الهجوم. هذا شيء يمكن أن يخفف منه وجود معايير التحقق المشتركة؛ خلال تحسين تبادل المعلومات على أساس الثقة[2].

هناك جهود على المستوى الوطني والدولي لتوحيد المعايير العامة وتشجيع تطوير أدوات مكافحة الإرهاب المفيدة. أمثلة على ذلك مشروع "التكنولوجيا ضد الإرهاب" الذي ترعاه الأمم المتحدة، وأداة حجب التطرف التي طورتها حكومة المملكة المتحدة لاستخدامها من قبل شركات التكنولوجيا التي ليس لديها الموارد لتطوير أداة خاصة بها. حتى الآن ، تعد هذه التدابير استشارية أو محدودة في نطاقها. في جميع القطاعات ، ينبغي أن يترافق الاستخدام المتزايد للذكاء الاصطناعي التنبؤي مع تنفيذ أنظمة التحقق والاختبار المناسبة. نظرًا لأن استخدام الذكاء الاصطناعي التنبؤي في مكافحة الإرهاب في مراحله الأولى، يمكن فهم غياب المحاولات لتقديم ضمانات لوجود وتطبيق معايير التحقق[3].

يتمثل الإرهاب الالكتروني للدول في إمكان النفاذ إلى شبكات التحكم في المرافق العامة، مما يتسبب في إحداث شلل تام للبنية التحتية الأساسية وذلك باستخدام الأسلحة البيولوجية المعلوماتية المتمثلة في جيوش الفيروسات التي

(1)Ibid.p21.
(2)Ibid.p22.
(3) Ibid.p22.

ISNN : 1112-8518 EISSN : 6200-2600

تخترق حدود الدول لتشيع الخراب والفوضى في أرجاء البنية المعلوماتية، وهناك إرهاب إلكتروني بغرض الأضرار بالمصالح الاقتصادية للدولة، وهو ما فعلته إسرائيل بهدف تشويه صورة السياحة المصرية [1].

إن الإشارة إلى أن ظهور التكنولوجيات الرقمية قد أعاد صياغة الفروق المألوفة بين الحروب «القديمة» والحروب «الجديدة» تؤدي إلى إثارة الجدل حول عدد من القضايا المثيرة للاهتمام. وقد نظر لهذا التمييز ماري كالدور(Mary) Kaldor ، التي تقدم تقييما ثاقبا لآثاره المفاهيمية المرتبة على التفكير مجدداً في الحرب في سياق ما بعد الحرب الباردة. باختصار، في تركيزها على الجوانب الجديدة في هذه الحروب «الجديدة»، تبادر ماري إلى الادعاء بأن ظهور هذه الحروب مرهون بشبكات مختلفة - تتسم في أغلب الأحيان بكونها غير رسمية وبدائية - تدافع عن القضايا الإقصائية وفي هذا الصدد، على سبيل المثال ما تبرز جماعات الشتات (Diaspora groups) إلى الواجهة [2].

بالإضافة إلى ذلك عادة ما تجلب الحروب الجديدة مجموعة من الجهات الفاعلة العالمية، في حين أنها تتركز عادة في المناطق التي تتفكك فيها الدولة الحديثة، وحيث لا يعود للفروق بين الداخلي والخارجي، والعام والخاص المعنى نفسه كما كان الحال في الحروب «القديمة». هذا يعني أن الظروف مهيأة لحدوث حروب جديدة في الأماكن التي فقدت فيها الدول الفاشلة أو الآيلة إلى الفشل أسس شرعيتها، وذلك عادة بسبب تدهور الاقتصاد (ومن ثم انهيار الاستثمار والإنتاج والضرائب) وزيادة الفساد. وعلى الفور تتوطد أوجه اللامساواة البنيوية، بما في ذلك ما يتعلق بالبطالة والهجرة من الريف إلى المدن، وذلك بطريقة قد تؤدي إلى إضعاف سيادة القانون. وتصبح الحرب نفسها، إذن، شكلا من أشكال التعبئة السياسية، كما تزعم كالدور؛ حيث تقول إن الغاية من العنف لا تتمثل في استهداف العدو بقدر ما تتمثل في توسيع شبكات التطرف». وتصبح أساليب الإرهاب أو التطهير العرقي أو الإبادة الجماعية بمنزلة استراتيجيات حرب متعمدة في السعي إلى تحقيق أهداف وغايات سياسية محددة. فالمعارك المريحة تصبح نادرة وبدلاً من ذلك، في الحروب الجديدة، يصبح العنف موجهاً بنحو رئيس ضد المدنيين، وتضيف قائلة: إن انتهاكات القانون الإنساني وقانون حقوق الإنسان ليست من الآثار الجانبية للحرب، بل هي المنهجية المركزية للحروب الجديدة». وبهذه الطريقة، إذن، تتحدى الحروب الجديدة تصورات الحرب السائدة نفسها. وينظر إلى المجالات المحلية والوطنية التي كانت سابقاً متباينة على أنها آخذة في التقارب، في حين أن الانقسامات التقليدية - لا سيما بين الحرب والجريمة - تصبح عمليا متداخلة فيما بينها ضمن سياسات الهوية التي تبرز الاختلافات وتركز على المصالح الخاصة .[3]

([1]) نبيل علي : تحديات عصر المعلومات،ص237-249.

([2]) ستيوارت ألن،رونالد ماتيسون: تقارير الحروب في العصر الرقمي،ضمن علم الإجتماع الرقمي،تحرير كيت أورتون،جونسونونيل بربور،ترجمة هاني خميس،عالم المعرفة،الكويت،2021،ص195.

([3]) المرجع نفسه،ص196.

ISNN : 1112-8518 EISSN : 6200-2600

- الأداء في بيئات متعارضة

أظهرت الأبحاث الحديثة في التعرف على الصور أن التغييرات الصغيرة في الصور يمكن أن تغير تمامًا كيفية إدراك الجهاز لتلك الصور، بينما قد يستمر الإنسان في إدراك محتواها الأصلي. بالإضافة إلى ذلك، هناك أمثلة موثقة بشكل جيد على تصنيف صور معينة بشكل خاطئ بمستويات ثقة عالية. إذا كان الخصم يحاول بشكل متعمد استدراج تطبيق التعرف على الصور، فهناك طرق فاعلة للقيام بذلك.

هذا الضعف في مواجهة التحديات مشكلة مستمرة وغير محلولة في بحوث الذكاء الاصطناعي. وهي مشكلة تستحق الاهتمام بشكل خاص عند استخدام الذكاء الاصطناعي في سياق الأمن. قد يسهم الإشراف البشري الملائم إلى حد ما في تخفيف الضعف، ولكن في الظروف التي يتم فيها استخدام الذكاء الاصطناعي للقيام بمهمة لا يمكن للبشر القيام بها ، فمن المستحيل أن يتم دعم أداء الجهاز بالإشراف البشري ببساطة بسبب قيود الوقت البشري. حتى في المجالات التي يمكن تنفيذ الإشراف البشري المباشر، تعتمد جودة هذا الإشراف على عوامل تتراوح من درجة تدريب المشغلين إلى كيفية تقديم النتائج. تسليم الإشراف البشري يتطلب النظر في التفاصيل والاعتبارات المتعلقة بالنظام. في معظم الحالات، يعني ذلك أن الذكاء الاصطناعي لن يكون حلاً كاملاً لمشكلة الأمن: فقط أداة إضافية يمكن أن تعزز دور البشر في معالجة تلك المشكلة بدلاً من استبداله[1].

5. هل يمكن استخدام الذكاء الاصطناعي التنبؤي بشكل مشروع كأداة للكشف عن الإرهاب ؟

قد نجمت التحديات المبينة أعلاه عن التطور غير المنهجي للذكاء الاصطناعي كوسيلة للتنبؤ بالإرهاب من جانب مختلف الوكالات العاملة في إطار تنظيمي مختلف، ولم يصمم أي منها خصيصاً لهذا الغرض.

ينظر هذا الجزء فيما إذا كان يمكن استخدام الذكاء الاصطناعي بشكل مشروع كأداة للدولة للتنبؤ بالإرهاب. قد يعني هذا منح الوكالات الحكومية وصولاً أوسع إلى البيانات العامة - بما في ذلك البيانات الخاصة بالمواطنين المحليين - ومرافقة هذا الوصول مع تنظيم أوضح حول كيفية استخدام البيانات. وفي إطار من هذا القبيل، قد يكون نشاط القطاع الخاص لمكافحة الإرهاب شرطا قانونيا تتولى الحكومة الإشراف عليه. أي واجب للإبلاغ مرتبط بهذه الصلاحيات وغيرها للوصول إلى البيانات بالجملة سيكون مرتبطًا مباشرة باستخدام الذكاء الاصطناعي التنبؤي.

يتطلب هذا النوع من الطرق قبول جمع وتحليل أجزاء من بيانات المواطنين المحليين بالجملة، وهو أمر لا تستمتع به الديمقراطيات الليبرالية حاليًا لأغراض مكافحة الإرهاب. وترد أدناه بمزيد من التفصيل للفرص التي يتيحها هذا النهج والمخاطر التي يشكلها[2].

(1)McKendrick,K.p23.
(2) Ibid.p23.

ISNN : 1112-8518 EISSN : 6200-2600

الفرص :

التشغيل الآلي يغير تقييمات التناسب :

حتى الآن، لم تعالج بشكل قاطع مسألة كيفية تغيير التحليل الآلي (مقابل الملاحظة البشرية) لتقييمات التناسب. ويمكن منح حقوق أوسع في الحصول على البيانات من جانب دوائر إنفاذ القانون والأمن لأغراض التحليل الآلي، استنادا إلى أن ذلك أقل تدخلا من الملاحظة البشرية.

إن ضرورة وتناسب استخدام نموذج تنبؤي لأتمتة تحليل البيانات العامة يتطلب إثبات الفاعلية (تأمين علاقة سببية مع هدف السياسة العامة)، وكذلك عدم وجود خيارات بديلة، وإثبات أن الفوائد تفوق التكاليف من حيث انتهاك الحقوق.

يتطلب تناول المعيار الأخير إجراء تقييم لنطاق اقتحام الحقوق المرتبط بتحليل البيانات. إن فكرة أن التحليل الآلي، عند مقارنته بالتحليل البشري، قد لا يصل إلى حد انتهاك الحق في الخصوصية هي حجة يقبلها ضمنيًا كثيرون في القطاع الخاص. وتجدر الإشارة إلى أن هذا لم يطرح بعد بنشاط لتلبية الشواغل المتعلقة بتناسب استخدام التحليل الآلي من قبل الحكومات، ولكنه شبه ضمني في قبول اعتراض الاتصالات بالجملة[1].

بالنسبة لغالبية السكان (الذين يتم تصفية معلوماتهم قبل إجراء مزيد من التحليل)، يتطلب استيفاء معيار التناسب القبول بأن تكون العملية الآلية لجمع وتحليل وحذف غالبية البيانات غير تدخلية ؛ أو أنه على الأقل يشكل اقتحامًا أقل من تخزين تلك البيانات لتحليلها لاحقًا من قبل الإنسان. هذا ليس سؤالًا مباشرًا، من حيث أن نوع البيانات وطبيعة التحليل تحدث فرقًا في مثل هذه الأحكام. ويتوقف قبول الحجج المتعلقة بتناسب الأساليب الآلية على وجود معايير لاستخدامها ؛ كما أنه يعتمد على القدرة على تقاسم تقييمات الثقة في تطبيق تلك المعايير.

في الوقت الحاضر، يتمثل النهج الافتراضي في الاحتفاظ الشامل بالبيانات، الذي يمكن استخدامه كأساس للمقارنة في تقييم التناسب. يمكن أن يؤدي التحليل الآلي المبكر إلى إزالة شرط الاحتفاظ بالبيانات التي من غير المحتمل أن تكون ذات أهمية استخباراتية، وتحسين الامتثال لمبدأ تقليل البيانات. ويمكن أن ينطبق الوصول إلى سبل الانتصاف على أولئك الذين يحتفظ ببياناتهم دون سبب ؛ ولكن بالمقارنة مع الاحتفاظ ببياناتهم ،على أي حال، سيتم تقليل المزيد من انتهاك الخصوصية[2].

(1) Ibid.p25.
(2) Ibid.p25.

ISNN : 1112-8518 EISSN : 6200-2600

يعد التأثير على الأفراد الذين تم تحديدهم بشكل خاطئ على أنهم موضع اهتمام خلال نموذج تنبؤي معين عاملاً مهمًا آخر في تقييم التناسب. يرتبط هذا ارتباطًا وثيقًا بجودة ودقة أي نموذج مستخدم. من المرجح أن تؤدي المعدلات الإيجابية الكاذبة المرتفعة إلى جعل النموذج الآلي غير متناسب إذا كانت تتطلب تدقيقًا بشريًا لعدد كبير بشكل غير معقول من هؤلاء الأفراد الذين تم تحديدهم بشكل خاطئ. قد تكون المشكلة الإيجابية الخاطئة مستعصية على الحل، أو قد تتحسن. ومن العوامل المهمة، مقارنة بالطرق الحالية، إمكانية قياسها ومقارنتها. وهذا يتيح إمكانية وضع تقييمات التناسب على أساس الأدوات الكمية فضلا عن الأحكام النوعية.

إلى جانب عدد المرات التي يكون فيها الذكاء الاصطناعي التنبؤي خاطئًا، فإن طبيعة التدخل المتصاعد على أساس أي تنبؤ له تأثير على التناسب. ركز تقييم بالغ الأهمية لفاعلية برنامج تنبؤي نفذته إدارة شرطة شيكاغو في عام 2013 لتحديد الأفراد الضعفاء على مدى ضعف التدخلات ذات الصلة، بدلاً من جودة التنبؤات[1].

يجب ألا يشكل ناتج الذكاء الاصطناعي التنبؤي معيار إثبات في حد ذاته ؛ بل ينبغي أن تكون إشارة إلى الاهتمام البشري. وقد يأذن هذا الاهتمام عندئذ بالنشاط الذي قد يولد أو لا يولد قاعدة أدلة لأي تدابير قسرية أو تقييدية تُفرض لاحقا. وفي حين أن عدم وجود رقابة بشرية مباشرة في المراحل الأولى من التحليل الآلي سيكون شرطا أساسيا لضمان التناسب، فإن هذا المستوى اللاحق من الرقابة البشرية سيكون ضروريا بالقدر نفسه لضمان التناسب في وقت لاحق من العملية. وينعكس ذلك في ضمانات الإنصاف على القرارات الآلية بالكامل التي توفرها اللوائح الأخيرة مثل اللائحة العامة لحماية البيانات الخاصة بالاتحاد الأوروبي. وبموجب تلك اللائحة، يجب أن يكون للقرارات الآلية أثر قانوني أو ذي شأن مماثل من أجل التأهل للحصول على أي ضمانات من هذا القبيل. ويعني ذلك أن التدخلات المهمة تتطلب رقابة بشرية، في حين أن الإجراءات الأقل أهمية لا تتطلب ذلك.

يمكن للتحليل الآلي أن يهدئ المخاوف بشأن التناسب، بشرط وجود الضوابط الصحيحة على الاستخدام - مثل الرقابة البشرية الكافية في الوقت المناسب، ومعايير جودة النموذج المستخدم[2].

التقييم الكمي لطرق إثبات الكفاية

يتيح استخدام الأساليب الآلية الفرصة لتقييم أداء النماذج بغية إثبات فاعليتها كمياً. يمكن استخدام مقاييس مثل الاستدعاء (أي النسبة المئوية للأوقات التي يحدد فيها النموذج بشكل صحيح حدثًا أو فردًا) والدقة، أو عدد الإنذارات الكاذبة، للإسهام في تقييمات التناسب - على وجه التحديد لإثبات أو دحض الارتباط بهدف مشروع،

(1) Ibid.p.25.
(2) Ibid.p25.

ISNN : 1112-8518 EISSN : 6200-2600

موصوف أعلاه على أنه المعيار الثاني للتناسب. تشمل المقاييس الأخرى طرقًا لتعديل النماذج بحيث يخفف الأداء عبر المجموعات الفرعية المختلفة من التمييز.

يحدد التحقق الكمي كشرط مسبق للاستخدام بين نموذج تنبؤي عامل و «رحلة صيد». فالطرق التي تقدم تحليلا مفصلا لنوعية نموذج تنبؤي معين قد توفر مبررا أكثر طمأنينة لاستخدامه من المبرر المتاح حاليا للاحتفاظ بالبيانات بالجملة[1].

ثمة مجال آخر للتحليل يتصل بالتناسب هو تأثير العوامل المختلفة على أداء النموذج. يسمح هذا باتخاذ قرار أوضح حول ما إذا كان هناك ما يبرر أي تدخل في الخصوصية في جمع البيانات التي تتكون منها هذه العوامل والاحتفاظ بها. أثناء مناقشة الشرطة التنبؤية، علق جون هوليوود المحلل في شركة RAND أن «الزيادات في القوة التنبؤية تميل إلى إظهار عوائد متناقصة» لأن العلاقات التي تقوم عليها الجريمة، خاصة تلك المرتبطة بالموقع والتوقيت، بسيطة نسبيًا ولا تتميز بعلاقات معقدة غير خطية يمكن استخدام الذكاء الاصطناعي بشكل أفضل لاستغلالها. هناك حد لمقدار التنبؤ المفيد الذي يمكن استخلاصه من البيانات، وإدراج المزيد من البيانات لا يحسن بالضرورة جودة التنبؤ. يمتد التحقق والاختبار إلى تحليل ما إذا كانت البيانات أو العوامل الإضافية تزيد بالفعل من تلك القيمة التنبؤية.

على الرغم من أن التحقق من الصحة ضروري، إلا أنه لا يزال مجالًا ناميًا. لا توجد طريقة موحدة أو متفق عليها لضمان أن يكون النموذج عادلاً. ويتسم العمل المتواصل بشأن التحقق الموضوعي بأهمية قصوى.

سيتطلب الأمر مقاييس كمية للأداء للإسهام في إثبات الضرورة. في حين أنهم لن يكونوا قادرين على إصدار أحكام التناسب بالكامل، فقد تعني أن هذه الأحكام مستنيرة بشكل أفضل[2].

نظام واحد

يميل تنظيم القدرات الجديدة إلى التخلف عن اعتمادها، ويؤدي إضفاء الطابع اللامركزي على القدرات إلى تفاقم ذلك. ومن شأن إضفاء الطابع المركزي على التحليل والقدرات والبيانات المصدرية، أو بدلا من ذلك على نتائج التحليل الذي تجريه وكالات مختلفة في إطار النظام التنظيمي نفسه ، أن يسهل تنظيم أنشطتها بصورة متسقة ويحسن القدرة على توجيه الموارد المناسبة إلى الأفراد المعرضين للخطر أو المعنيين.

لأسباب وجيهة، فإن فكرة معاملة الأشخاص المعرضين لخطر التطرف والإرهابيين الفعليين داخل النظام نفسه تسبب عدم الرضا. وإذا كان هذا النظام مميزا بما فيه الكفاية، فإنه لا يمكن الإبقاء على تمييز ذي مغزى بين هذه المجموعات الفرعية فحسب بل يمكن إثباته أيضا. إذا تخيلنا أنه في المستقبل، يمكن جعل الأنظمة التنبؤية القائمة

(1) Ibid.p26.
(2) Ibid.p26.

ISNN : 1112-8518 EISSN : 6200-2600

على تحليل البيانات المتولدة أو المخزنة رقميًا محايدة وقابلة للثقة وفاعلة حقًا، فيمكن استخدامها كطريقة أفضل لتوجيه التدخلات المبكرة غير القسرية (مثل تلك المضطلع بها لردع الشباب عن الانجذاب إلى الأيديولوجيات المتطرفة العنيفة) التي يمكن أن تحققها النظم الحالية، والتي تضع متطلبات الإبلاغ التي يمكن أن تهدد الثقة بين الأفراد. ولتقرير ما إذا كان هذا النوع من المراقبة يمكن أن يكون مستساغا في أي وقت من الأوقات، من الأهمية بمكان أن نفهم ما إذا كانت المشاكل تنشأ عن فكرة منع الإرهاب ذاتها خلال استهداف الأفراد، وليس من الأساليب التي ينطوي عليها تحديد هوية هؤلاء الأفراد وإدارتهم[1].

في حين أن المركزية قد يكون لها فوائد من حيث تحسين الدقة العامة، إلا أنها تحتوي أيضًا على عيوب، وقد تفوت بعض أشكال الحماية التي تأتي بشكل طبيعي مع التجزئة وتطوير مصادر منفصلة مضمونة للتحقق من النتائج. ومع ذلك، من الجدير بالذكر أن الحواجز التي تحول دون تبادل المعلومات الاستخباراتية قد قوضت بالفعل كثير من هذه الإمكانات. بالإضافة إلي ذلك، فإن وجود نظام واحد أو مجموعة من المعايير لا يعني بالضرورة وجود مخزون واحد ضخم من البيانات. وبدلاً من ذلك، يمكن تطوير النماذج وتطبيقها على مجموعات بيانات خاصة مختلفة، ويمكن اختبار نتائج هذه النماذج ودمجها مركزياً.

توجد حواجز أمام تبادل المعلومات بين أجهزة الاستخبارات وأجهزة إنفاذ القانون لمنع إساءة استخدام السلطات التي ينبغي أن تقتصر على أجهزة الأمن. يجدر النظر في أي نقطة يمكن استبدال بهذه التدابير الرقابية وغيرها ضمانات تقنية - مثل سجلات التدقيق والوصول - بالإضافة إلى القيود المفروضة على أنواع الوصول التي يتمتع بها المستخدمون المختلفون[2].

إمكانية الشفافية

قد يكون من الممكن إصدار مقاييس كمية لأداء النماذج دون تعريض أمن العمليات للخطر. إن إتاحة هذه المعلومات من شأنه أن يحسن الرقابة ويمكن أن يقطع شوطًا ما في معالجة المظالم بشأن الأساليب التي يُنظر إليها بخلاف ذلك على أنها تمييزية. فعلى سبيل المثال، إذا أمكن تحديد هوية الأفراد لإجراء «إيقاف وتفتيش» متعمق في المطارات استنادا إلى نموذج يدمج أنماط السفر المشبوهة، طرق الدفع غير العادية والعلامات الفسيولوجية لعدم الارتياح، وقد أدى ذلك بشكل واضح إلى انخفاض بنسبة 50 في المائة في العدد الإجمالي للأشخاص الذين يخضعون لعمليات التفتيش هذه، وربما أمكن إبلاغ المسافرين بهذه الحقيقة لتبديد المخاوف بشأن إمكانية أن تستند هذه الإجراءات فقط إلى التنميط بتحيز عرقي أو إثني. قد ينطبق الشيء نفسه على تدابير أخرى، مثل وضع كاميرات التعرف

(1) Ibid.p27.
(2) Ibid.p27.

ISNN : 1112-8518 EISSN : 6200-2600

التلقائي على لوحة الأرقام (ANPR). ومن الواضح أن أي تدابير من هذا القبيل للشفافية يجب أن تتم الوساطة فيها مع الشواغل الأمنية، ولكن إذا كانت المعايير التي يتعين تقاسمها تقيم الأداء العام، بدلاً من وصف طريقة ما بالتفصيل، فقد يكون ذلك ممكناً[1].

كما أن تقاسم المعايير الكمية يمكن أن ييسر الثقة ويهيئ الظروف لتبادل المعلومات على نحو أفضل بين الجهات الفاعلة والوكالات الدولية. فعلى سبيل المثال، قد يكون مقدمو خدمات الاتصالات الأجنبية أكثر قابلية للاستجابة لطلبات الوصول إذا أمكنهم التأكد من أن معايير هذه الطلبات عالية بما فيه الكفاية. ويمكن أن تتخذ تدابير الضمان هذه شكل إثبات أن الوصول مرتبط بهدف مشروع هو: إظهار كيفية مراجعة النماذج، وأن التدخلات القائمة على نتائجها متناسبة.

توفر المعايير الكمية مقياسا للشفافية التقنية. ومن المهم أيضا شفافية الإطار القانوني الذي يجري في إطاره التحليل التنبؤي. إن تركيز المسؤولية عن الإشراف على هذا التحليل والعمل عليه مع الوكالات الحكومية يحسن من إمكانية تحقيق فهم واضح ومتماسك حول ماهية التحليل الذي يتم إجراؤه ولماذا[2].

المخاطر:

الإمكانية التقنية:

بغض النظر عن مدى تطور الذكاء الاصطناعي، أو مقدار البيانات المتاحة، والتنبؤ بالتورط في الإرهاب، فإن حدوث الهجمات أو التعرض للتطرف بدقة كافية قد يثبت أنه يتجاوز حدود الاحتمال.

سيتعين اقتراح الأساليب وتجريبها وتقييمها مسبقا - وسحبها إذا تعذر الحصول على قيمة تنبؤية كافية. عديد من الأمثلة على الذكاء الاصطناعي للتعلم الآلي التي تم استخدامها بنجاح في العمل الصناعي خلال تحسين قدراتها التنبؤية عند استخدامها. إلى حد ما، ترتبط فوائد الطرق القائمة على التعلم الآلي بقدرتها على التكيف بشكل ديناميكي مع النظام الذي تقوم بتحليله، بما في ذلك التكيف مع التغييرات في بيانات الخلفية داخل هذا النظام. قد يؤدي فرض معايير التحقق قبل الاستخدام، والتحديث التدريجي للنماذج بناءً على البيانات الجديدة، بدلاً من السماح لها بالتكيف ديناميكيًا، إلى الحد من فائدتها. ويمكن القول إن هذا القيد ينبغي قبوله كضامن للاستخدام العادل[3].

إن الاحتياج لتطوير واختبار النماذج يعني أيضًا أنه يجب توافر مجموعات البيانات التاريخية للتجربة، مما يشكل تنازلًا عن خصوصية البيانات دون وجود رابط سببي فوري لهدف مشروع. هذا قد يكون مقبولًا، لكن فقط إذا

(1) Ibid.p28.
(2) Ibid.p28.
(3) Ibid.p28.

ISNN : 1112-8518 EISSN : 6200-2600

كان هناك فرصة معقولة لتطوير نموذج تنبؤ فاعل. يعد اتخاذ قرار بشأن متى وما إذا كان من الممكن قبول هذا النوع من التجارب شرطًا أساسيًا لاستخدام الذكاء الاصطناعي التنبؤي بغرض مكافحة الإرهاب بشكل متناسق.

المشكلة الأساسية في تحديد الإرهابيين أو تنبؤ الإرهاب بطرق أخرى لا يمكن حلها باستخدام الأساليب الحسابية وحدها. بالإضافة إلى بعض القيود التقنية الأساسية المعروفة سابقًا، مثل الضعف في مواجهة التحديات وعدم وجود فهم سياقي، يضع ذلك حدودًا نهائية على كيفية استخدام الذكاء الاصطناعي في توقع الإرهاب. على وجه التحديد، تقدم نتائج أي نظام تنبؤ فرصة وليس دليلاً، ويجب إيلاء اهتمام كبير للنظر في المجالات التي يحتاج فيها هذا النظام لدعم الأساليب القائمة بدلاً من استبدالها[1].

آثار المراقبة الجماعية

حتى الآن، تم مناقشة مبدأ التناسب على مستوى الفرد في اعتبار الانتهاكات في الخصوصية. ومع ذلك، فإن الحق في الخصوصية على هذا المستوى يستند إلى حقوق أخرى مثل حرية التعبير والتجمع، وله آثار اجتماعية مفيدة.

لقد قام عديد من الأكاديميين بدراسة كيف يمكن أن تسبب المراقبة الرقمية الواسعة الانتشار تأثيرًا "مخيفًا" على الانخراط في القضايا السياسية أو الأنشطة الحساسة، وكذلك على الرأي المعارض والتفكير النقدي، حيث يتغير سلوك الأفراد ليتوافق مع الأعراف الجماعية الملحوظة. لقد كان هذا الموضوع مصدر توتر لمجموعات المجتمع المدني، لا سيما بعد الكشف (المعروف باسم اكتشافات سنودن) في عام 2013 عن مدى برامج المراقبة الوطنية. لقد لاحظ علماء النفس أن مجرد إدراك الانتباه - حتى إذا كان مبنيًا على مشغل بسيط مثل صورة لزوج من العيون البشرية - يمكن أن يؤدي إلى تغيرات ملموسة في السلوك. بينما يمكن أن يقلل التحليل الآلي من انتهاك الخصوصية على مستوى الفرد، إلا أنه يفتح أيضًا الباب أمام إمكانية أن يشعر الجميع بأنهم يتم مراقبتهم في جميع الأوقات. وبسبب ذلك، قد يكون للتحليل الآلي تكاليف أعلى على حقوق أخرى مثل حقوق التعبير والتجمع، والتي يمكن أن تشعر بها بشكل أوضح عندما تجمع تغيرات السلوك الفردي على مستوى المجتمع[2].

لا يزال الشك موجودًا بشأن تأثير المراقبة على النشاط على الإنترنت، على الرغم من أن عددًا من الدراسات حاولت توثيقها كظاهرة قابلة للملاحظة تجريبيًا. تقدم الخبرة التاريخية في سلوك المواطنين تحت الأنظمة الشمولية أدلة قوية على ظاهرة التأثير المُخيف، على الرغم من أن من المستحيل تفكيك تأثير المراقبة بحد ذاتها عن تلك الإجراءات الأخرى المصممة لخلق الخوف وتغيير سلوك الأشخاص. في الآونة الأخيرة، أشار بعض المعلقين إلى استمرار المعارضة السياسية وحرية التعبير بعد كشف النقاب في عام 2013، وزيادة المشاركة الطوعية في مشاركة المعلومات

(1) Ibid.p29.
(2) Ibid.p29.

ISNN : 1112-8518 EISSN : 6200-2600

عبر وسائل التواصل الاجتماعي، كدليل على عدم وجود آثار ملموسة للتأثير المرعب. يعترف مؤيدو تأثير المراقبة المرعب بأنه من غير الممكن توقع طبيعة هذا التأثير بالضبط، أو قياسه. من الممكن أيضًا أن يكون التأثير الأكثر جدوى ليس رد فعل على المراقبة الحكومية، ولكن على المراقبة من قبل النظراء والمنافسين.

على الرغم من أنه يبدو منطقيًا أن احتمالية المراقبة المستمرة التي قد تقدمها التطورات في التشغيل التلقائي يمكن أن تؤدي إلى تأثيرات مرعبة، إلا أن ما إذا كانت ستحدث ذلك أم لا هو بالتأكيد تخمين في هذه المرحلة. سيكون على الحكومات مسؤولية تدشين هذه التأثيرات المحتملة عند تصميم ضوابط قانونية مناسبة على نشاط المراقبة. قد يكون معالجة هذا القلق المستقبلي تتطلب تطوير نماذج تقيّم الأضرار واسعة النطاق الناتجة عن انتهاكات الخصوصية الفردية بناءً على تأثيرها على المجتمع[1].

انحسار معايير البرهان

في حين أن التعامل مع معايير الأدلة التي تقل عن مستوى البرهان القطعي بالفعل سمة لعمليات مكافحة الإرهاب، إلا أن هناك مخاوف من أن "تزايد قابلية استخدام البيانات قد يؤدي إلى انحسار المعايير القائمة، مما يجعل تدخلات الشرطة والحكومة مشروعة لأن الحاسوب "قال ذلك" ". قد تتزامن القدرات المتاحة لجمع واستخدام البيانات مع انخفاض التسامح تجاه المخاطر وعدم اليقين على مستوى المجتمع، مما قد يؤدي إلى تركيز أكبر على الوقاية - وحتى على الاحتياط المسبق - مما كان موجودًا سابقًا. في الحد الأقصى، يشعر بعض المعلقين بالقلق من أنه:

"باستخدام تقنيات التنبؤ الجديدة، يصبح من الممكن جمع معرفة محددة عن المستقبل.

وفقًا لهذا المنطق، يمكن للسلطات معاقبة الأشخاص والتدخل قبل ارتكاب جريمة".

من الأمور الحاسمة للقضاء على هذا الشبح "الجريمة المسبقة" هو الاعتراف بأن نتائج أي نموذج تنبؤ يمثل دائمًا إمكانية وليس دليلاً قطعيًا. وبالتالي، يجب أن تستند التدخلات التي تتم استنادًا إلى نماذج التنبؤ في النهاية إلى قرار بشري يتخذه شخص ما مطلع بما فيه الكفاية على حدود وقدرات النموذج المستخدم.

- "التحيل الوظيفي"

هناك سابقة حيث تم اعتماد تدابير لمكافحة الإرهاب، ثم استخدمت لأغراضها العامة في مكافحة الجريمة. نظام وعي النطاق الذي تديره شرطة مدينة نيويورك هو مثال واحد. يتكامل النظام مع بيانات آلاف الكاميرات المغلقة وكاميرات تعرف لوحات السيارات بالإضافة إلى أجهزة استشعار أخرى. تم تثبيت النظام في الأصل - وغالبًا ما يُشدد عليه - بقيمته في مكافحة الإرهاب. ومع ذلك، فإن تقييم استخدامه يشير إلى أن هناك قليل جدًا من الأمثلة التي تم استخدامها في هذا الدور.

(1) Ibid.p30.

ISNN : 1112-8518 EISSN : 6200-2600

يمكن أن يكون حصد بيانات عن الجمهور العريض قيمة لا تُقدَّر بثمن في تحديد نقاط البداية للتحقيقات الجنائية، أو حتى لتوجيه عدد من التدخلات الاجتماعية المفيدة. إمكانية "التحيل الوظيفي" ضخمة وتتطلب وضع الإجراءات الواقية ضدها. يمكن أن يكون إجراء مناسب هو أن تستخدم قاعدة البيانات المعنية فقط للاستجواب بواسطة نماذج مسموح بها مسبقًا، بدلاً من كون البيانات متاحة للاستفسارات الموجهة المحددة من قبل المحللين. ويمكن أن يجعل ذلك قاعدة البيانات أسهل في السيطرة عليها، ويمكن أن يوفر أيضًا مستوى من الشفافية حول كيفية استخدام البيانات[1].

استمرار التعرض للاستغلال

حتى في وجود التنظيم والقيود، ستكون تفسيرات الحكومات ذات طابع استبدادي. يُطبق مصطلح "الإرهابي" عادة بمرونة لتلاءم الأغراض السياسية الكامنة. يحمل جمع البيانات العامة والسماح بتحليل هذه البيانات معها مخاطر سلبية. تعرض التدابير الوقائية مثل تجريد البيانات للخطر المتكرر في الربط بين البيانات وهويات الأشخاص المحددة.

ما إذا كانت هذه السلطات مقبولة يعتمد جزئياً على ثقة السكان في الحكومات وعلى ما إذا كانت قادرة على جني الدعم العام الكافي للسماح لها بممارسة تلك السلطات. تتزايد صعوبات الرقابة العامة كوسيلة للتحكم والتي تم الإشارة إليها أعلاه وتزيد من عدم فهم الجمهور لحجم البيانات التي يتم إنشاؤها وكيفية استخدامها.

لوائح حماية البيانات العامة (GDPR) لها تأثيرات على الذكاء الاصطناعي، ولكن وجود استثناءات للاستخدام القانوني للبيانات من قبل وكالات الحكومة والتركيز على استخدام البيانات لأغراض تجارية يعني أن التنظيم لا يُغطي بشكل كافي استخدام الذكاء الاصطناعي التنبؤي في مكافحة الإرهاب. من الضروري تنظيم استخدام البيانات بشكل أكبر لتوضيح التناسب وضمان الشفافية. على الرغم من أن هذا التشريع الإضافي قد يسهم في قيد استخدام التكنولوجيا التي يمكن استخدامها بشكل أقل دقة، إلا أنه لا يعالج بشكل كامل المخاطر المتعلقة[2].

الحفاظ على الدعم العام ليس ضمانًا في حد ذاته. إن القبول العام للحجة القائلة بأنه لا ينبغي أن يكون لدى الأفراد ما يخفونه يهمل مبدأ حماية الخصوصية كحق، ويمكن أن يؤدي إلى تبعات اجتماعية تنمو تدريجيًا عندما لا يتم مراعاة انتهاك الخصوصية. يمكن أن يقلل استعداد الجمهور لقبول التدابير الاستثنائية في مكافحة الإرهاب من قدرته على محاسبة الحكومة بشأن انتهاك الخصوصية. ويزداد هذا الأمر سوءًا بنقص وعي الجمهور العام بكمية

(1) I/bid.p31.
(2) Ibid.p31.

ISNN : 1112-8518 EISSN : 6200-2600

البيانات التي يولدها وكيفية استخدام هذه البيانات. مع تزايد رقمنة حياة الناس، طواعية أو غير ذلك، يجب نقل الضمانات التشريعية والإجرائية التي يتم وضعها من أجل منع حالة المراقبة في العالم الحقيقي بقوة إلى الفضاء الرقمي.

مع ذلك، لا ينبغي أن يجعل ذلك استخدام الذكاء الاصطناعي التنبؤي في مكافحة الإرهاب خارج الاستخدام. عديد من جوانب ممارسة مكافحة الإرهاب يمكن أن تتعرض بطبيعتها لسوء الاستخدام. تطوير صوتي وتنظيم إمكانات الذكاء الاصطناعي هو المفتاح لحماية ضد هذا الخطر. تلك الإمكانيات تتطلب عملية مستمرة للإدارة والمراقبة مماثلة لتلك التي تتبع فيها الممارسات الأخرى لمكافحة الإرهاب[1].

استخدام الذكاء الاصطناعي للأغراض التنبؤية في مكافحة الإرهاب ليس حسنًا بطبيعته ولا سيئًا بطبيعته. بل إن الطريقة التي يتم بها استخدام هذه القدرات هي الأمر الحاسم. يبدو أن البنى الحالية التي تنظم استخدام الذكاء الاصطناعي التنبؤي في مكافحة الإرهاب غير قادرة على الحماية من سوء الاستخدام أو تمكين الاستخدام الأكثر فائدة لهذه التقنيات، سواءأكان من حيث الأداء التشغيلي أم التزامها بمبادئ حقوق الإنسان.

إن متابعة المزيد من الجهود المتضافرة لاستخدام الذكاء الاصطناعي التنبؤي في عمليات مكافحة الإرهاب يتطلب التزامًا من حيث البحث والتجريب، من أجل تطوير نماذج جاهزة للاستخدام. إذا وصلت تقنيات الذكاء الاصطناعي للتنبؤ بالإرهاب إلى مرحلة النضج، فإن زيادة الوصول إلى البيانات والمركزية - في ظل ضمانات صارمة - يمكن أن توفر طريقة للتوسط في انتهاك الخصوصية لتحقيق غايات متناسبة[2].

في الوقت الحالي، تنظيم استخدام الذكاء الاصطناعي لأغراض التنبؤ بالانخراط في الإرهاب أو خطر الإرهاب جزئي أو مفقود تمامًا. عندما تكون هناك قيود، فإنها غالباً ما تركز على الوصول إلى البيانات وليس على كيفية استخدامها. بشكل متناقض، يمكن أن يقيد الوصول المحدود القدرة على تطوير نماذج جيدة يمكن أن تحسن التناسب وعدم التمييز. يمكن أن يكون الوصول المركزي أفضل تنظيمًا من وصول عرضي بتقدير ذاتي لأي جهة أو جهاز يمكنه الحصول عليه.

ستستخدم الحكومات الوسائل التكنولوجية الجديدة المتاحة لديها عند ملاحقة الأهداف الحساسة مثل السلامة العامة. حقيقة أن الذكاء الاصطناعي يجعل انتهاك الخصوصية على نطاق واسع أسهل بكثير يعني أن استخدام تلك التقنيات لا يزال مشكلة سياسية عامة. وهذا لا يعني أن استخدام الذكاء الاصطناعي للتنبؤ بالإرهاب من جانب الديمقراطيات الليبرالية يجب أن يكون محظورًا. في الواقع، يمكن أن تكون القدرات التنبؤية الجيدة التي تستند إلى التحليل التلقائي للبيانات الأقل تدخلاً جزءًا من قيود معقولة على استخدام تدابير غير متناسبة تشكل تهديدًا أكبر

(1) Ibid.p32.
(2) Ibid.p33.

ISNN : 1112-8518 EISSN : 6200-2600

للخصوصية والحريات المرتبطة الأخرى. يمكن أن تكون عملية صنع القرار، بأداء قابل للقياس، فيما يتعلق بالأفراد الذين يجب أن يخضعوا لمراقبة أكثر تدخلاً وجودة المحدودات التكنولوجية الجديدة، مفتاحًا لتقييد استخدام المراقبة الممكنة تقنيًا حيث من المحتمل أن تتآكل القيود العملية[1].

تعقيب

يُعد الإرهاب ظاهرة عالمية معقدة تُهدد الأمن والاستقرار في جميع أنحاء العالم .ولذلك، تبحث الدول والمنظمات الدولية عن أدوات جديدة لمكافحة هذه الظاهرة . ويُعد الذكاء الاصطناعي أحد هذه الأدوات الواعدة.

يُعد الذكاء الاصطناعي أداة قوية يمكن أن تؤدي دورًا مهماً في التنبؤ بمكافحة الإرهاب .ومع ذلك، يجب استخدام هذه الأداة بمسؤولية أخلاقية وضمان دقة البيانات المستخدمة في تحليلها.ضرورة التعاون الدولي في مجال استخدام الذكاء الاصطناعي لمكافحة الإرهاب.أهمية مشاركة البيانات والخبرات بين مختلف الدول.

ضرورة وضع معايير أخلاقية لضمان استخدام الذكاء الاصطناعي بشكل مسؤول.أهمية تدريب الكوادر البشرية على استخدام تقنيات الذكاء الاصطناعي بشكل فعال.

أرى أن الذكاء الاصطناعي يُعدّ أداة ثورية في مكافحة الإرهاب، لكن يجب استخدامه بحذر ودقة لضمان فعاليته وأخلاقياته.أُشير أيضًا إلى بعض المخاطر المحتملة لاستخدام الذكاء الاصطناعي في مكافحة الإرهاب، مثل إمكانية استخدامها من قبل الجماعات الإرهابية نفسها. إمكانية إساءة استخدامها من قبل الحكومات لانتهاك حقوق الإنسان.

(1) Ibid.p33.