تحديات وإشكاليات استخدام تقنيات الذكاء الاصطناعي في العمل الشرطي والقضائي

Challenges and problems of using artificial intelligence technologies in police and judicial work

إعداد

الدكتور / محمد نور الدين سيد

أستاذ مساعد القانون الجنائي

كلية الحقوق جامعة أسيوط

البريد الإلكترونى : Dr.mnour2018@gmail.com

الملخص العربي:

يهدف البحث إلى دراسة موضوع تحديات وإشكاليات استخدام تقنيات الذكاء الاصطناعي في العمل الشرطي والقضائي، موضحاً مفهوم الذكاء الاصطناعي وأنواعه، وأهم التقنيات المستخدمة، ودراسة متعمقة لأهم التحديات والإشكاليات التي تواجه استخدامها، مثل: حماية أمن المعلومات ومخاطر الإختراق الإلكتروني على الأمن السيبراني والأمن القومي، ثم بيان مشروعية هذا الاستخدام في الاجراءات التي يقوم رجل الشرطة ذات الطبيعة الأمنية أو الشرطية وتلك الأعمال والاجراءات التي يقوم بها بوصفه مأمور ضبط قضائي، وكذلك الاجراءات القضائية من سلطة التحقيق أو المحكمة.

توصل الباحث إلى عدة نتائج، منها ما يتعلق بأهمية استخدام الذكاء الاصطناعي في العمل الشرطي والأمني والنتائج المذهلة التي حققها في الحد من انتشار الجريمة والوقاية والتنبؤ بها، مثل: استخدام الطائرات بدون طيار (ذاتية التحرك) والسيارات المستقلة (ذاتية القيادة) والروبوتات فائقة الذكاء، وكذلك الأهمية القصوى لاستخدام هذه التقنيات في اجراءات التحقيق الابتدائي والمحاكمة خاصة في إصدار أوامر الحبس الاحتياطي والقبض والافراج المشروط، والعدالة التنبؤية. ومنها ما يتعلق بمدى مشروعية هذا الاستخدام ومدى كفاية النصوص الاجرائية الحالية في التعامل مع ذلك الاستخدام.

سعى الباحث إلى وضع بعض التوصيات من أهمها: قيام المشرع المصري بمعالجة الاختراق الإلكتروني لتقنيات الذكاء الاصطناعي والتلاعب في برمجيتها، وأنظمة

تشغيلها، بنصوص خاصة. كذلك تدخل المشرع بتنظيم الإجراءات التي يمكن الاستعانة فيها بالروبوت فائق الذكاء مستقلاً عن رجال الشرطة؛ هذا ما يقتضي النص على اعتبار هذا الروبوت من مأموري الضبط القضائي ذو طبيعة خاصة. كذلك وضع التنظيم التشريعي الاجرائي لاستخدام تلك التقنيات في العمل الشرطي، لمنع ارتكاب الجريمة والتنبؤ بها، أو في العمل القضائي من قبل النيابة العامة، أو من قبل المحكمة.

الكلمات الافتتاحية: الذكاء الاصطناعي، الطائرات المسيرة ذاتياً، السيارات المستقلة ، التنبؤ بالجريمة، العدالة التنبؤية.

Summary:

The research aims to study the challenges and problems of using artificial intelligence technologies in police and judicial work, explaining the concept of artificial intelligence and its types, the most important technologies used, and an in-depth study of the most important challenges and problems facing its use, such as: protecting information security and the risks of electronic penetration on cyber security and national security, then a statement. The legality of this use in the procedures carried out by the police officer of a security or police nature and those actions and procedures carried out by him in his capacity as a judicial arrest officer, as well as judicial procedures carried out by the investigating authority or the court.

The researcher reached several results, including those related to the importance of using artificial intelligence in police and security work and the amazing results it achieved in reducing the spread of crime, preventing and predicting it, such as: the use of (self-driving) drones, independent (self-driving) cars, and highly intelligent robots, As well as the paramount importance of using these techniques in primary investigation and trial procedures, especially in issuing orders for pretrial detention, arrest, conditional release, and predictive justice. Among them is what relates to the legality of this use and the adequacy of current procedural texts in dealing with that use.

The recommendations, the most important of which are: The Egyptian legislator should address electronic penetration of artificial intelligence technologies and tampering with their

software and operating systems, with special texts. The legislator intervened by regulating the procedures in which a highly intelligent robot can be used independently of the police. This requires stipulating that this robot be considered a judicial police officer of a special nature. It established procedural legislative regulation for the use of these techniques in police work, to prevent and predict the commission of crime, or in judicial work by the Public Prosecution, or by the court.

Key words: Artificial intelligence - autonomous drones - autonomous cars - crime prediction - predictive justice.

مقدمة:

إن الذكاء الاصطناعي جعل العالم على أعتاب ثورة جديدة على مختلف المستويات – لاسيما المستوى الأمني – ستغير هذه الثورة شكل البشرية؛ لأن تطبيقات الذكاء الاصطناعي تتعدد وتتزايد بصورة يصعب حصرها أو احتواءها، وأضحى الحديث عن الاستخدام الأمثل لهذه التطبيقات وقدراتها هو الشغل الشاغل لكافة الدول والحكومات؛ مما أثار الحديث عن تحديات استخدام تطبيقات الذكاء الاصطناعي في مختلف مجالات الحياة، لاسيما في مجال العمل الشرطي والقضائي، بهدف مكافحة الجريمة، والحد من انتشارها، سواء بالتنبؤ بها قبل ارتكابها للحيلولة دون ذلك، أو بعد ارتكابها والقيام بأعمال التحري والاستدلال عنها لضبط مرتكبيها، أو في مجال التحقيق والمحاكمة، والتي تعتبر من أكثر المجالات التي أثارت الجدل حول إيجابيات هذه التطبيقات وسلبياتها.

كما أثارت الجدل حول مدى مشروعيتها، ومدى ملائمة التشريعات الحالية لاستخدامها، هذا ما دفع البعض إلى القول بأن التشريعات الحالية أضحت غير ملائمة لمواجهة تحديات وإشكاليات الذكاء الاصطناعي وطالب بضرورة إعداد منظومة تشريعية أكثر ملائمة لتواكب تلك التحديات([1]).

وقد بادرت إمارة دبي بدولة الامارات العربية المتحدة بالمسارعة إلى إصدار القانون رقم ٩ لسنة ٢٠٢٣م بشأن تنظيم المركبات ذاتية القيادة في إمارة دبي، وقد أوضح

[1]) د/ محمد محمد خليفة، الذكاء الاصطناعي في ميزان التشريع، مجلة دبي القانونية، تصدرها النيابة العامة–دبي، العدد ٢٨، مارس ٢٠١٨م، ص٣٢.

المشرع بإمارة دبي أن من أهداف هذا القانون معالجة التحديات التنظيمية والقانونية الناجمة عن استخدامات الذكاء الاصطناعي في مجال النقل([1]).

وقد تعددت تطبيقات الذكاء الاصطناعي التي تزايد استخدامها في مجالات العمل الشرطي والقضائي وغيره من مجالات الحياة في مختلف القطاعات، وتعتمد هذه التطبيقات على قدراتها الهائلة في التعامل مع البيانات الكبيرة Big Data وتحليلها واتخاذ القرارات المناسبة دون تدخل الإنسان أو دعم القرارات التي يتخذها البشر في مجال معين.

أولًا– مشكلة البحث:

مما لاشك فيه أن تزايد الاعتماد على تطبيقات الذكاء الاصطناعي في الإجراءات الجزائية، يصاحبه العديد من الإشكاليات التي تثير الكثير من التهديدات، لاسيما على الأمن المعلوماتي والسيبراني، وحقوق الإنسان، لاسيما الحق في الخصوصية والحق في الصورة، بالإضافة إلى ما تثيره من إشكاليات تتعلق

[1]) الفقرة (٤) من المادة (٤) من القانون رقم ٩ لسنة ٢٠٢٣م بشأن تنظيم تشغيل المركبات ذاتية القيادة في إمارة دبي، الجريدة الرسمية لحكومة دبي، السنة ٥٧، العدد ٦١٣، ١٤ أبريل ٢٠٢٣م، ٢٣ رمضان ١٤٤٤هـ، ص١. جدير بالذكر أنه قد سبق هذا القانون صدور قرار المجلس التنفيذي لإمارة دبي رقم ٣ لسنة ٢٠١٩م بشأن تنظيم التجربة التشغيلية للمركبة ذاتية القيادة في إمارة دبي، ومن إهدافه:

- المُساهمة في تحقيق استراتيجيّة الإمارة للتنقُّل الذكي المُعتمد على استخدام المركبات ذاتيّة القيادة.
- تنظيم التجارب التشغيليّة للمركبات ذاتيّة القيادة للتحقُّق من سلامة استخدامها.
- الاستفادة من أفضل المُمارسات المُطبّقة عالمياً بشأن استخدام المركبات ذاتيّة القيادة.

بالمشروعية الإجرائية، التي تعتبر عماد الإجراءات الجزائية في العصر الحديث. هذا ما يدفعنا للحديث عن حدود تلك الإشكاليات، ومن ثم يمكن طرح التساؤلات الآتية: **ما هي التحديات التي تواجه استخدام تقنيات الذكاء الاصطناعي في العمل الشرطي والقضائي؟ وما هي الإشكاليات التي يثيرها هذا الاستخدام؟ وأخيراً، ما مدى ملائمة التشريعات الإجرائية الحالية في استيعاب هذا الاستخدام؟** من هذه التساؤلات الرئيسة تنبثق تساؤلات فرعية، نعرضها فيما يلي، مع السعي للإجابة عليها متبعا أصول وقواعد البحث العلمي والمنهج الملائم لموضوع البحث.

ثانيًا- تساؤلات الدراسة:

من التساؤلات المنبثقة عن مشكلة الدراسة:

- ما المقصود بالذكاء الاصطناعي وما أهم أنواعه؟
- ما هي تقنيات الذكاء الاصطناعي التي يمكن استخدامها في العمل الشرطي والقضائي؟
- ما هي إيجابيات وسلبيات استخدام هذه التقنيات في العمل الشرطي والقضائي؟
- ما هي التهديدات السيبرانية لاختراق أنظمة الذكاء الاصطناعي وتداعياتها الأمنية؟
- ما مدى مشروعية استخدام تقنيات الذكاء الاصطناعي في أعمال الاستدلال والتحقيق؟

- ما مدى فاعلية إستخدام تقنيات الذكاء الاصطناعي في إصدار الأحكام والقرارات القضائية؟

ثالثا– أهداف الدراسة: يستهدف البحث تحقيق الأهداف التالية:

- الوقوف على أهم الاستخدامات الحالية والمستقبلية للتقنيات الذكاء الاصطناعي في العمل الشرطي والقضائي.
- بيان الإشكاليات القانونية التي يثيرها هذه الاستخدامات، لاسيما ما يتعلق بحقوق الأفراد.
- الوقوف على مخاطر الاعتماد على هذه التقنيات في العمل الشرطي والقضائي لاسيما ما يتعلق بالاختراق الالكتروني والتهديدات السيبرانية.
- تقييم فاعلية استخدام تلك التقنيات في اصدار الأحكام والقرارات القضائية.

رابعًا– أهمية موضوع البحث:

يستمد موضوع البحث أهميته من الاشكالية التي عرضناها سلفًا؛ حيث أصبح استخدام تقنيات الذكاء الاصطناعي أمرا واقعيا يفرض نفسه في كافة مجالات الحياة البشرية، ولا يمكن تجاهل ذلك، وعلى الرغم من السلبيات التي تصاحب استخدامها؛ تسعى الدول إلى الاستفادة من هذه التقنيات إلى أقصى حد، وتعلن عن العديد من المبادرات لتفعيلها في كافة قطاعات الدولة– لاسيما القطاعات الحيوية– ومن ثم علينا أن نفكر جيدا فيما قد يواجه هذه الاستخدامات المتعددة من تحديات في شتى مناحي الحياة– لاسيما في نطاق العمل الشرطي والقضائي– الذي يعد من أكثر المجالات تعقيدًا وتداخلا مع الأفراد، ونفكر في سبل مواجهتها حتى يتسنى لنا الاستفادة من تلك

التقنيات بالشكل الذي يحقق الهدف المنشود منها، ومن ثم يمكن القول أن أهمية البحث تتنوع إلى:

أ) الأهمية النظرية:

يبدو ذلك من خلال ما يسعى إليه الباحث من دراسة التحديات والإشكاليات التي يثيرها استخدام تقنيات الذكاء الاصطناعي في الإجراءات الجزائية، ومن ثم يكتسب موضوع البحث أهميته النظرية والتي تتمثل في التعرف على مفهوم الذكاء الاصطناعي وتقنياته، وكذلك التعرف على كيفية الاستفادة من تلك التقنيات في العمل الشرطي والقضائي، مع استعراض الإيجابيات والسلبيات ومن ثم الوقوف على التحديات والإشكاليات التي تصاحب استخدامها وسبل المواجهة لاسيما ما يتعلق منها بالمشروعية الإجرائية، أو بحقوق الأفراد، لاسيما الحق في الخصوصية والحق في الصورة.

ب) الأهمية العملية:

يبدو ذلك من خلال ما أفرزه استخدام تقنيات الذكاء الاصطناعي في العمل الشرطي والقضائي من تجربة عملية فريدة حققت نتائج ايجابية في سبيل التنبؤ بالجريمة، والكشف المبكر لها، والتحري عنها، وضبط الجناة، وإقامة الدليل، والاستفادة منها في إجراءات التحقيق والمحاكمة؛ هذا ما قد يستتبع تحديات وإشكاليات قانونية كبيرة، ومن ثم يسعى الباحث إلى الوقوف على هذه التحديات وتلك الإشكاليات ودراستها سعيا وراء وضع تصور حدودها ونطاقها وسبل مواجهتها مع سعي الباحث إلى التوصل من دراسته إلى جملة نتائج وتوصيات قابلة للتطبيق العملي، بهدف الوصول إلى أفضل

الممارسات لتقنيات الذكاء الاصطناعي في العمل الشرطي والقضائي، وخاصة في الوقت الذي أصبح الحديث فيه عن الشرطي الروبوت، ووكيل الروبوت، والقاضي الروبوت.

خامسًا– منهج البحث:

يحاول الباحث الغوص في أصول وقواعد البحث العلمي للوقوف على المنهج الملائم لموضوع البحث، حتى يتوصل إلى معالجة جيدة لمشكلة الدراسة والتوصل إلى إجابات شافية لتساؤلاتها، ويعتقد الباحث أن المنهج الوصفي التحليلي وكذلك المنهج الاستباطي من أفضل مناهج البحث القانوني التي تلائم طبيعة موضوع البحث، وذلك من خلال وصف واقع استخدامات تقنيات الذكاء الاصطناعي في الإجراءات الجزائية، وتحليل الإشكاليات التي تواجه هذا الاستخدام، ومن خلال إنزال حكم القواعد الإجرائية العامة على استخدام الذكاء الاصطناعي في مجال العمل الشرطي للتنبؤء بالجريمة، ومكافحتها والحد منها، والتحري عنها، وضبط مرتكبيها ومحاكمتهم بما يضمن تحقيق العدالة، مع الإشارة إلى بعض التجارب العملية في هذا المجال، وكذلك محاولة إعمال القواعد والإحكام الإجراءات المنصوص عليها على توظيف واستخدام تقنيات الذكاء الاصطناعي في العمل القضائي، لاسيما خلال مرحلة التحقيق الابتدائي، ومرحلة المحاكمة، وما يتعلق بهاتين المرحلتين من إجراءات جزائية يتوقف عليها تحقيق العدالة المنشودة.

سادساً– خطة الدراسة:

المبحث التمهيدي: مفهوم الذكاء الاصطناعي والتقنيات المستخدمة في العمل الشرطي والقضائي.

الفصل الأول: مخاطر الاختراق الإلكتروني لتقنيات الذكاء الاصطناعي وصور مواجهته.

المبحث الأول: التعريف بالاختراق الإلكتروني وكيفية التصدي تقنياً وتشريعياً.

المطلب الأول: تعريف الإختراق الإلكتروني وأنواعه.

المطلب الثاني: مراحل الإختراق الإلكتروني وسبل المكافحة التقنية.

المطلب الثالث: صور المواجهة التشريعية للاختراق الإلكتروني.

المبحث الثاني: مخاطر الاختراق الإلكتروني على الأمن المعلوماتي.

المطلب الأول: تعريف الأمن المعلوماتي وعناصره.

المطلب الثاني: التمييز بين مفهوم الأمن المعلوماتي وغيره من المصطلحات المشابهة.

المطلب الثالث: مخاطر اختراق تقنيات الذكاء الاصطناعي على الأمن القومي وعلاقتها بالحروب الإلكترونية.

المبحث الثالث: تحليل التهديدات السيبرانية لأنظمة الذكاء الاصطناعي وصور الاختراقات الواقعة عليها

المطلب الأول: تحليل التهديدات السيبرانية والأثار الأمنية لاختراق أنظمة الطائرات المسيرة.

المطلب الثاني: تحليل التهديدات السيبرانية والأثار الأمنية لإختراق أنظمة المركبات ذاتية القيادة.

المطلب الثالث: صور الاختراق الإلكتروني لأنظمة الطائرات المسيرة ذاتياً والمركبات ذاتية القيادة.

الفصل الثاني: مشروعية استخدام تطبيقات الذكاء الاصطناعي في العمل الشرطي والقضائي

المبحث الأول: مدى مشروعية استخدام تقنيات الذكاء الاصطناعي من مأموري الضبط القضائي.

المطلب الأول: مدى مشروعية استخدام تقنية تمييز بصمة الوجه والصوت.

المطلب الثاني: مدى مشروعية استخدام الروبوتات فائقة الذكاء في العمل الشرطي.

المبحث الثاني: مدى مشروعية استخدام تقنيات الذكاء الاصطناعي في التحقيق الإبتدائي والمحاكمة.

المطلب الأول: استخدام الروبوتات فائقة الذكاء في التحقيق الإبتدائي.

المطلب الثاني: استخدام تقنية التحليلات التنبؤية في تحقيق العدالة الجنائية.

الخاتمة: تتضمن النتائج والتوصيات.

المبحث التمهيدي

مفهوم الذكاء الاصطناعي والتقنيات

المستخدمة في العمل الشرطي والقضائي.

تمهيد:

تعددت تعريفات الباحثين والمتخصصين للذكاء الاصطناعي، بعضها جاء موسعًا، وبعضها الآخر جاء مختصرًا، بيد أن جميع التعريفات تمحورت حول فكرة أن الذكاء الاصطناعي يقوم على محاولات العلماء في محاكاة الذكاء البشري، وقدراته الذهنية والعقلية، مثل: التفكير، والابداع، والتحليل، والتعليم الذاتي، بالإضافة إلى إكساب هذه التقنيات بعض المهارات، مثل: مهارة تبادل الحديث، والدردشة، والترجمة الفورية، وتحويل النصوص المسموعة إلى مكتوبة. وقد تعددت تقنيات الذكاء الاصطناعي التي شاع استخدامها في العمل الشرطي وأصبحت واقعا ملموساً، بالرغم من السلبيات التي قد تصاحب هذا الاستخدام.

إن البحث في الإشكاليات التي يثرها استخدام تطبيقات الذكاء الاصطناعي في العمل الشرطي والقضائي يتطلب منا الوقوف على مفهوم الذكاء الاصطناعي والتقنيات المستخدمة، مع استعراض إيجابياتها وسلبياتها، على أن نخصص لكل منها مطلبًا مستقلا.

تقسيم:

نتناول هذا المبحث في المطالب الثلاثة الآتية:

المطلب الأول: مفهوم الذكاء الاصطناعي.

المطلب الثاني: تقنيات الذكاء الاصطناعي المستخدمة في العمل الشرطي والقضائي.

المطلب الثالث: سلبيات وايجابيات الذكاء الاصطناعي وتقييم فاعليته.

المطلب الأول

مفهوم الذكاء الاصطناعي

للوقوف على حدٍ واضح للذكاء الاصطناعي([1]) نجد من الأهمية بمكان التعرض لتعريف الذكاء البشري بداية؛ حيث يعرف الذكاء البشري بأنه: "القدرة أو المهارة على وضع وإيجاد الحلول للمشكلات باستخدام الرموز وطرق البحث المختلفة، كذلك القدرة على استخدام الخبرة المكتسبة في التوصل إلى معلومات ومعارف جديدة، تؤدي إلى وضع أفضل الحلول للمشكلات التي تعترض مجالٍ معين من مجالات الحياة"([2]).

[1]) أشار البعض إلى أن مصطلح (الاصطناعي) مرجعه أن الحاسبات الآلية تُعد غير قادرة على التفكير والبرهنة في حد ذاتها، وهي إحدى وظائف الذكاء أو العقل البشري، وعلى ذلك فإن ذكاءها يُعد اصطناعياً. انظر: د/ عمر عبد الله نصيف، استخدام نظم الذكاء الصناعي كأداة للتميز في الجودة والتنافسية، دراسة ميدانية لقطاع المستشفيات الخاصة في محافظة جدة، مجلة الأندلس للعلوم الاجتماعية والتطبيقية، المجلد (٢)، العدد الخامس، فبراير ٢٠١٠م، ص ١٠.
ولكن من جانبنا نعتقد أن صفة الاصطناعية مرجعها تمييز القدرات الذكائية لهذه التطبيقات والحواسيب الآلية عن القدرات الذكائية للعقل البشري، طبيعي الخلقة.

[2]) انظر: د. أحمد ماجد، الذكاء الاصطناعي في دولة الامارات د/أحمد إبراهيم محمد إبراهيم، المسؤولية الجنائية الناتجة عن أخطاء الذكاء الاصطناعي في التشريع الإماراتي (دراسة مقارنة)، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، ٢٠٢٠م، ص٣١.

ويعتبر الذكاء البشري المسؤول الأول عن التطور والتفكير الإبداعي؛ ونظراً لأهميته نجد المتخصصين في حالة شغف شديد للبحث عن طبيعة هذا الذكاء، وكيفية قياسه، كما اهتم الباحثون بمحاولة فهم قدرة العقل البشري على معالجة البيانات والمعلومات المكتسبة، ومحاولة فهم الأسس العامة التي تقوم عليها قدراته الذهنية، بهدف وضع النماذج لمحاكاته، سواء اتخذ ذلك شكل برامج للحاسبات الآلية أو أنظمة رقمية([1]).

الفرع الأول

تعريف الذكاء الاصطناعي

ذكرنا أن هناك العديد من الحدود التي حُدَّت للذكاء الاصطناعي، ومنها أنه: علم إنشاء أجهزة وبرامج كمبيوتر قادرة على التفكير بالطريقة نفسها التي يعمل بها الدماغ البشري، تتعلم مثلما نتعلم، وتقرر كما نقرر، وتتصرف كما نتصرف"([2]). أو هو فرع من علوم الكمبيوتر يمكن بواسطته تصميم برامج حاسوبية تحاكي أسلوب الذكاء البشري حتى يتمكن الكمبيوتر من أداء المهام التي تتطلب قدرات التفكير والإدراك السمعي والبصري، والكلام التلقائي([3]) والتصرف بأسلوب منطقي ومنظم بدلًا

---

[1]) د/أحمد كاظم: الذكاء الصناعي، قسم هندسة البرمجيات، كلية تكنولوجيا المعلومات، جامعة الإمام الصادق، بغداد، ٢٠١٢م، ص٤.

[2]) شادي عبد الوهاب، وإبراهيم الغيطاني، وسارة يحيى: فرص وتهديدات الذكاء الاصطناعي في السنوات العشر القادمة، تقرير المستقبل، ملحق يصدر مع دورية "اتجاهات الأحداث"، العدد ٢٧، مركز المستقبل للأبحاث والدراسات المتقدمة، أبوظبي، ٢٠١٨م، ص٢.

[3]) مثال روبوت الدردشة بتقنية الذكاء الاصطناعي (Tay) الذي أطلقته شركة ميكروسوفت، فقد تم تطبيق الخوارزميات الذي يرتكز عليها (Tay) وتمكينها بالشكل الصحيح لتتحادث بطريقة بشرية

عن الإنسان([1]). في حين يعرفهJohn McCarthy تعريفا مختصرا بأنه: "علم وهندسة صنع آلات ذكية"([2]). أو هو "الذكاء الذي تمارسه الآلات أو تطبيقات بأسلوب يحاكي القدرات الذهنية للإنسان وطريقة عملها، مثل القدرة على التعلم والاستنتاج والاستدلال والتعقل ورد الفعل على أوضاع لم تبرمج في هذه الآلات أو التطبيقات"([3]).

ويمكن القول أن الذكاء الاصطناعي يتمحور في عملية محاكاة الذكاء البشري عبر أنظمة الحاسب الآلي وبرامجه، وباستخدام خوارزميات حسابية لمعادلات رياضية

مقنعة مع مستخدمي تويتر، له القدرة على التعلم والاستجابة لميول وتفضيلا المستخدمين من خلال استيعاب بياناتهم.

[1]) Jeff Crume, Doug Lhotka, Carma Austin, Security and Artificial Intelligence: FAQ, published by IBM Security, P:2, available at: https://www.ibm.com/downloads/cas/ZQROXRBK/7/1/2021

[2]) د/ سعيد خلفان الظاهري: الذكاء الاصطناعي "القوة التنافسية الجديدة"، مركز استشراف المستقبل ودعم اتخاذ القرار، شرطة دبي، العدد (٢٩٩)، دبي، نشرة شهر فبراير ٢٠١٧م، ص٣.

[3]) د. أحمد عادل جميل، د. عثمان حسين عثمان: إمكانية استخدام تقنيات الذكاء الصناعي في ضبط جودة التدقيق الداخلي "دراسة ميدانية في الشركات المساهمة العامة الأردنية"، بحث مقدم للمؤتمر العلمي السنوي الحادي عشر بعنوان "ذكاء الأعمال واقتصاد المعرفة"، جامعة الزيتونة الأردنية، كلية الاقتصاد والعلوم الإدارية، عمان، الفترة من ٢٣–٢٦ أبريل ٢٠١٢م، ص٢٤٠. كما ورد التعريف لدى: د. محمد محمد الطوخي، تقنيات الذكاء الاصطناعي والمخاطر الإلكترونية، مجلة الفكر الشرطي، مركز بحوث الشرطة، القيادة العامة لشرطة الشارقة، المجلد٣٠، العدد (١١٦) يناير ٢٠٢١م، ص٧٢.

Jeff Crume, Doug Lhotka, Carma Austin, Security and Artificial Intelligence: FAQ, op. cit., P: 3.

معقدة([1])، وبفضل جهود رواد الذكاء الاصطناعي أمثال (John McCarthy) and(Frank Rosenblatt) بدأ العمل على تزويد أنظمة الحوسبة بقدرات ذكائية، لاسيما القدرة على التكيف أو التعلم الاستقرائي من التجارب السابقة، التي تمثلها البيانات المدخلة. ويتحقق ذلك من خلال مجموعة من خوارزميات وإجراءات حوسبية تسلسلية محفوظة على مستوى متناهي الصغر. واستمرت الجهود –ومازالت– لتحقيق الهدف في ابتكار ذكاء اصطناعي مستقل عن البشر، قادر على استخدام خوارزميات التعلم المتطورة لينافس الذكاء البشري المرن ويتفوق عليه، كما حاولت الكثير من الخوارزميات الأولية أن تحاكي السلوكيات البيولوجية للبشر([2]).

[1]) يشتق اسم "خوارزميات" من اسم العالم العربي أبو عبد الله بن موسى الخوارزمي، الذي ابتكر إجراءات تفصيلية للتوصل إلى الحلول الحسابية للمعادلات، ثم توالت جهود علماء الذكاء الاصطناعي (Alonzo Church and Alan Turing) في وضع تعريف للخوارزمية، تحت مسميات مختلفة مثل: "قابلية الحوسبة" أو الدوال الحسابية" وانتهى التعريف إلى كون الخوارزمية متتالية محدودة من الأوامر الدقيقة القابلة للتنفيذ في الأنظمة الحاسوبية.

Osonde A. Osoba, William Welser IV, An Intelligence in Our Image, The Risks of Bias and Errors in Artificial Intelligence, Published by the RAND Corporation, Santa Monica, Calif., 2017, P:5.

[2]) Osonde A. Osoba, William Welser IV, An Intelligence in Our Image…, op. cit., P5.

الفرع الثاني

تصنيف تقنيات الذكاء الاصطناعي.

تتنوع تقنيات الذكاء الاصطناعي بحسب زواية البحوث في مجال الذكاء الاصطناعي، فقد اتجه البعض إلى تصنيفها بحسب قدراتها على التحليل والتفكير، أو بحسب نطاقها وأسلوب التعلم، ومن ثم نعرض لهذه الأنواع على اختلافها([1]).

أولًا– التصنيف بحسب القدرة على التعلم الذاتي:

١– آلات غير قادرة على التعلم:

هي أقدم أنظمة الذكاء الاصطناعي، تتمتع بقدرات محدودة، وتُحاكي وظيفة العقل البشري على الاستجابة للمثيرات والمحفزات الخارجية. ولكن لا تستطيع هذه الآلات توظيف قدرتها على التذكر، فلا تستطيع الاستفادة من خبراتها السابقة في توجيه خطواتها اللاحقة، ومن ثم ليس لديها القدرة على التعلم.

يرى البعض أن هذه الآلات هي أقرب إلى برمجية حاسوبية ليست من قبيل الذكاء الاصطناعي؛ لأن من أهم عناصر هذا الذكاء هو القدرة على التعلم، من خلال إمكانية جمع وتحليل البيانات والمعلومات ومعالجتها، ثم قدرتها على اتخاذ قرارات بناء على نتائج عملية التحليل([2]).

---

[1]) للمزيد راجع: مقال بعنوان "٧ أنواع للذكاء الاصطناعي.. تعرف عليها، مجلة الحكومية الرقمية، منشور على الموقع الإلكتروني للمجلة بتاريخ ١٨ أغسطس ٢٠١٩م، تاريخ الزيارة ٣/١١/٢٠٢٠م: https://digitalgov.sa/?p=2330

[2]) د. محمد محمد الطوخي، مرجع سابق، ص٧٤.

٢- آلات قادرة على التعلم العميق:

يراد بالتعلم العميق Deep learning مجموعة من الخوارزميات التي تنفذ شبكات عميقة توفر القدرة على التعلم غير الخاضع للإشراف([1])، أي التعلم الذاتي والتلقائي من خلال البيئة المحيطة والتجارب السابقة، ويعد التعلم العميق مستقبل الذكاء الاصطناعي؛ إذ يضمن لتطبيقاته التطور الذاتي بدون تدخل مبرمج بشري، ويكون لها المنطق الخاص بها القائم على التحليل والتنبؤ([2]). وتتمتع هذه الآلات بالذاكرة المحدودة بخلاف سابقتها، وتستطيع توظيف البيانات المخزنة فيها مسبقا في اتخاذ القرارات. ويمكن تدريب تلك الآلات بواسطة كميات هائلة من البيانات التي تُخزن في ذاكرتها كمرجع لحل المشكلات المستقبلية، ومثال ذلك: تستطيع تقنية التعرف على الوجه أن تُستخدم آلاف الصور ووصفها، وتتعلم هذه التقنية الربط بين الصور ومسمياتها. وبالتالي، عندما تعرض عليها صور جديدة فإنها تعتمد على الصور المستخدمة في التدريب في إدراك محتويات الصور الجديدة. وتُحدد تجربة التعلم العميق دقة هذه الأنظمة في تسمية الصور الجديدة، وكذلك من أمثلة الأنظمة القادرة على التعلم العميق: روبوتات الدردشة، وتطبيقات المساعدين الافتراضيين في الهواتف الذكية، والسيارات ذاتية القيادة.

---

[1]) See: Jeff Crume, Doug Lhotka, Carma Austin, Security and Artificial Intelligence, op. cit., P:3.

[2]) انظر: د. محمود سلامة عبد المنعم الشريف، الطبيعة القانونية للتنبؤ بالجريمة بواسطة الذكاء الاصطناعي ومشروعيته، المجلة العربية لعلوم الأدلة الجنائية والطب الشرعي، جامعة نايف العربية للعلوم الأمنية، المجلد الثالث، العدد ٢، ٢٠٢١م، ص٣٤٤.

٣– تقنيات تعتمد نظرية العقل:

خلافًا للنوعين السابقين، لا تزال الأنظمة المعتمدة على (نظرية العقل) في مرحلة التطوير. وتُمثل استشراف لمستقبل الذكاء الاصطناعي؛ حيث تستطيع هذه التقنيات فهم الكيانات التي تتفاعل معها بشكلٍ أفضل، وذلك من خلال تمييز الاحتياجات والعواطف والمعتقدات والعمليات الفكرية الخاصة بها.

٤– تقنيات ذات الوعي الذاتي:

تعد هذه التقنيات من المراحل الأخيرة لتطور أنظمة الذكاء الاصطناعي. وهي لم تتجاوز حدود افتراضات واجتهادات العلماء في هذا المجال. ويستهدف الذكاء الاصطناعي الواعي ذاتيًا بلوغ حدٍ قريبٍ من قدرات العقل البشري لدرجة تسمح له بإدراك وجوده وتطوير ذاته، تقوم هذه التقنيات على ما يعرف بالحوسبة المعرفية، وهي حقل فرعي من الذكاء الاصطناعي يبنى على الشبكات العصبية والتعلم العميق، يطبق العديد من العلوم المعرفية لبناء أنظمة تحاكي عمليات التفكير البشري، وتغطي هذه الحوسبة العديد من التخصصات مثل: التعلم الآلي، ومعالجة اللغة الطبيعية، والرؤية، والتفاعل بين الإنسان والحاسوب([1]).

[1]) ibid. P:4.

كما تشير تلك الحوسبة إلى الأنظمة التي تتعلم على نطاق واسع، وتتفاعل مع البشر بشكل طبيعي، فبدلاً من أن تتم برمجتها بشكل صريح، فإنها تتعلم من تفاعلاتها فيما بينها ومن خلال تجاربها مع بيئتها المحيطة بها([1]).

وتمثل هذه التقنيات الغاية المنشودة لبحوث الذكاء الاصطناعي، وإن كان لا يزال بحاجة إلى عقود قبل أن يتحقق على أرض الواقع، وسوف تكون هذه التقنيات قادرة على اكتساب العواطف، والميول، والرغبات، والمعتقدات، والاحتياجات الخاصة بما يحاكي البشر، وتثير تلك التقنيات مخاوفًا لدى البعض من خطرها على الجنس البشري؛ من منطلق وعيها بالمحافظة على وجودها وتعايشها مع البشر، وسوف تدافع عن وجودها ولو مَثَّلَ ذلك تهديدا للوجود البشري.

ثانياً- التصنيف بحسب حدود ونطاق الذكاء الاصطناعي:

١- الذكاء الاصطناعي المحدود:

يُشير هذا المصطلح إلى تقنيات الذكاء الاصطناعي التي تستطيع فقط القيام بأداء المهام المحدودة بشكل مستقل، وبواسطة إمكانات تُحاكي قدرات العقل البشري. ويعني ذلك أن هذه التقنيات محدودة في قدراتها، ولا تتجاوز بقدراتها حدود المهام المُصممة من أجلها، وبالرجوع إلى التصنيف الأول نجد هذه التقنيات تقابل الآلات محدودة

[1]) John E. Kelly, Computing, Cognition, and the Future of Knowing: How Humans and Machines are Forging a New Age of Understanding, September 2016, Vol. 28/No.8, available at: https://cra.org/crn/2016/09/computing-cognition-future-knowing-humans-machines-forging-new-age-understanding/8/1/2021

الذاكرة وغير القادرة على التعلم([١])، مثال: التقنيات القادرة على الكلام التلقائي([٢]) وتلك القادرة على التعرف على الصور والوجوه، والتي تعتمد على أسلوب التعلم العميق، وقد شّكلت ثورة البيانات الضخمة حافزا قويا يشجع على استخدام خوارزميات التعلم على نطاق واسع، وتوفر التدفق المستمر للبيانات متعددة الأنماط اللازمة لاستخلاص الرؤى القيّمة عبر خوارزميات التعلم([٣]).

٢– الذكاء الاصطناعي العام:

هنا تكتسب تطبيقات الذكاء الاصطناعي القدرة على التعلم والإدراك والفهم تمامًا مثل الإنسان من خلال محاكاة قدرات العقل البشري، ويصير بمقدورها بناء قدرات متنوعة والتوصل إلى روابط عبر عدة مجالات.

٣– الذكاء الاصطناعي الفائق:

يُمثل هذا النوع من التطبيقات أقصى مراحل تطوير الذكاء الاصطناعي الفائق أو الخارق، كما يعد هدفا بعيدا لذروة البحوث في مجال الذكاء الاصطناعي.

---

[١]) ايهاب خليفة، الذكاء الاصطناعي: تأثيرات تزايد دور التقنيات الذكية في الحياة اليومية للبشر، منصة المنهل، منشور على الرابط التالي، تاريخ الزيارة ٢٠٢١/١/١١:

http://platform.almanhal.com.uoseresources.remotexs.xyz/Reader/Article/100450

[٢]) مثال روبوت الدرشة بتقنية الذكاء الاصطناعي (Tay) الذي أطلقته شركة ميكروسوفت، فقد تم تطبيق الخوارزميات الذي يرتكز عليها (Tay) وتمكينها بالشكل الصحيح لتتحادث بطريقة بشرية مقنعة مع مستخدمي تويتر، له القدرة على التعلم والاستجابة لميول وتفضيلا المستخدمين من خلال استيعاب بياناتهم.

[3]) Brown, Brad, Michael Chui, and James Manyika, "Are You Ready for the Era of 'Big Data'?" McKinsey Quarterly, Vol. 4, No. 1, October 2011, P:25.

وإذا كانت تقنيات الذكاء الاصطناعي العام في حال تطويرها ستكون أكثر أشكال الذكاء قدرة على الأرض أي أكثر ذكاءً من البشر، فإن تقنيات الذكاء الاصطناعي الفائق سوف تفوق ذلك من حيث قدرتها اللامتناهية على الذاكرة والتعلم من تجاربها السابقة، وسرعة معالجة البيانات وتحليلها، والقدرة الفائقة على اتخاذ القرارات على نحو أفضل من البشر، وهذا ما يزيد من المخاوف تجاه وجودها بل ربما يُهدد وجود البشر أو يهدد أسس الحياة كما عهدها البشر، مما قد يصعب على مخيلة أي شخص أن يتصور عالم البشر بصحبة هذه الأشكال الأكثر تقدمًا من الذكاء الاصطناعي.

المطلب الثاني

تقنيات الذكاء الاصطناعي المستخدمة

في العمل الشرطي والقضائي

تنوعت تقنيات الذكاء الاصطناعي التي أصبح استخدامها واقعًا ملموسًا، ويرى الباحث أنه من الأهمية بمكان استعراض هذه التقنيات بما يخدم فكرة البحث والمشكلة البحثية التي يعالجها، فلا يتصور أن نبحث ونناقش التحديات والاشكاليات التي يثيرها استخدام تلك التقنيات في العمل الشرطي والقضائي دون التعرض لها تفصيلا على النحو التالي:

الفرع الأول

تقنية التحليلات التنبؤية

أولاً– مفهوم تقنية التحليلات التنبؤية:

أعلنت شركة (IBM) عن تقنيات الذكاء الاصطناعي ذات قدرات عالية على تحليل البيانات والمعلومات أو ما يطلق عليها تقنيات التحليلات التنبؤية([1]) والتي تساعد محللي العمليات الأمنية على مواجهة التهديدات والهجمات السيبرانية؛ حيث تمكن هذه التقنيات مثل التعلم الآلي([2]) المحللين من الاستجابة للتهديدات بقدر أكبر من السرعة والثقة، فقد ذكرت الشركة أنه بإمكان هذه التقنيات أن تتدرب من خلال استهلاك ملايين من البيانات من مصادر متنوعة، سواء أكانت محددة الهيكل أم كانت غير محددة الهيكل،

[1]) هي فرع من التحليلات المتقدمة التي تستخدم لعمل تنبؤات حول أحداث مستقبلية غير معروفة، تستخرج تقنيات التحليلات التنبؤية المعلومات من ملايين البيانات باستخدام تقنيات استخراج البيانات والإحصاءات والتعلم الآلي والذكاء الاصطناعي لتحليل البيانات الحالية لعمل تنبؤات حول المستقبل، وتتوقف قوتها التنبؤية على جودة وأهمية مجموعة البيانات المستخدمة، بالإضافة إلى دقة معالجة الخوارزمية لتلك البيانات.

See: Jeff Crume, Doug Lhotka, Carma Austin, Security and Artificial Intelligence, op. cit., P:7.

[2]) التعلم الآلي: هو حقل فرعي من الذكاء الاصطناعي وعلوم الكمبيوتر، له جذوره في الإحصاء. يغطي التعلم الآلي تقنيات التعلم الخاضع للإشراف وغير الخاضع للإشراف للتطبيقات في التنبؤ والتحليلات واستخراج البيانات. يمكن استخدام التعلم الآلي بشكل مستقل عن تقنيات الذكاء الاصطناعي أو التقنيات المعرفية الأخرى. في الواقع.

See: Jeff Crume, Doug Lhotka, Carma Austin, , op. cit., P: 3.

مثل المدونات والأخبار؛ فمن خلال التعلم الآلي وتقنيات التعلم العميق، يقوم الذكاء الاصطناعي بتحسين المعرفة لديه لفهم تهديدات الأمن السيبراني والمخاطر السيبرانية([1]).

كما يمكن استخدام هذه التقنية في تحليل وسائل التواصل الاجتماعي ومحتوى هذه الوسائل، لاسيما FaceBook، Twitter، Telegram، وغيرها؛ لاكتشاف ما يُعد من قبيل التحريض على الشغب والتظاهر غير السلمي، ومن ثَمَّ التنبيه على الجهات الأمنية بالتدخل الفوري، كما أشارت شركة (IBM) أنه يمكن الاعتماد على تلك التقنيات في جمع الآراء واستخدام التفكير المنطقي لتحديد العلاقات بين التهديدات، مثل الملفات الخبيثة أو عناوين IP المشبوهة، وقد يستغرق هذا التحليل ثوان أو دقائق معدودة، مما يسمح للمحللين الأمنيين بالاستجابة للتهديدات بسرعة أكبر ستين مرة من التحليل البشري التقليدي([2]).

كما أعلنت شركة (IBM) عن منصة (Watson) وهي من منصات الذكاء الاصطناعي والتعلم الآلي والحوسبة المعرفية توفر مجموعة واسعة من تقنيات الذكاء الاصطناعي لمعالجة كل من المعلومات المهيكلة وغير المهيكلة المستمدة من عدة مصادر، وتستطيع فهم ما تعنيه، وإضافة هذه المعلومات إلى مجموعة معارفها لاستخدامها لاحقًا، كما يمكنها بعد ذلك الرد على الأسئلة المعقدة باستخدام اللغة

[1]) https://www.ibm.com/ae-ar/security/artificial-intelligence/7/1/2021
[2]) Brown, Brad, Michael Chui, and James Manyika, "Are You Ready for the Era of 'Big Data'?", op. cit., P:26.

الطبيعية بناءً على هذه المجموعة، ويمكنها زيادة الذكاء البشري وتحسين الإدراك والكفاءة في المهام الحرجة([1]).

كما أعلنت الشركة عن تقنية (WPS) وهي ليست منتجًا واحدًا، ولكنها مجموعة من المكونات المتكاملة التي تتمتع بقدرات تحليلية متخصصة يمكن الاستفادة منها كمكونات فردية لتقديم حلول تدعم الذكاء الاصطناعي، توفر قدرات معرفية، ويستخدم بعضها التعلم الآلي أو التعلم العميق، والبعض الآخر يستخدم المزيد من التحليلات التقليدية([2]).

ثانياً– تحليل البيانات الكبرى والتنبؤ بالجريمة:

تعرف البيانات الكبرى (Big Data) بأنها: بيانات رقمية هائلة الحجم وتتميز بالتنوع والسرعة وتعدد مصادرها، ويسهل تحميلها وتخزينها ومعالجتها، ويمكن تحليلها باستخدام الخوارزميات وتقنية التحليلات التنبؤية، كما يمكن استخلاص نتائج تنبؤية دقيقة في قطاعات متنوعة مثل: القطاع الصحي، المالي، التعليمي، والأمني..... إلى آخره([3]). ويتم تجميع البيانات الكبرى من خلال وسائل التواصل الاجتماعي Social Media، وأجهزة تحديد المواقع العالمي (GPS) وكاميرات الفيديو المثبتة في الشوارع وأماكن التسوق، وقاريء لوحات السيارات الذكي، وبطاقات الائتمان،

[1]) Jeff Crume, Doug Lhotka, Carma Austin, op. cit., P:5.

[2]) ibid.

[3]) د/ حسن أحمد المومني، أهمية وأثر الذكاء الاصطناعي في مستقبل العمل الشرطي: البيانات الكبري نموذجًا، ورقة عمل مقدمة للمؤتمر الخامس والعشرين، جمعية المكتبات المتخصصة، فرع الخليج العربي، إنترنت الأشياء: مستقبل مجتمعات الإنترنت المترابطة، أبوظبي، في الفترة من ٥–٧ مارس ٢٠١٩م، ص٣٥٩.

وسجلات السفر، ووسائل الإعلام، كما يمكن استخلاصها من السجلات الطبية الالكترونية، وسجلات التأمين، والسجلات المصرفية، وبنوك المعلومات. كذلك قد يكون مصدرها الجهات الأمنية، مثل: سجلات المتهمين، الإجراءات المتخذة في حقهم، ومحاضر الاستدلال والتحقيق، والأحكام السابقة، بل إن من مصادر هذه البيانات التعليقات الخارجة على القانون عبر وسائل التواصل الاجتماعي، ومرات الولوج إلى المواقع والصفحات المشبوهة على الانترنت([1]).

وبياناً لأهمية البيانات الكبرى في عملية التنبؤ بالجريمة أشار البعض إلى أن هذه البيانات تمثل وقود للخوارزميات الرياضية، فكلما اتسع نطاق البيانات لمجرم معين كلما أصبح من اليسير التنبؤ باحتمالية ارتكابه جريمة في المستقبل([2]).

وقد عرض البعض للتجربة الهولندية في التنبؤ بالجريمة المعتمد على التحليل الزمني، بإنشاء شبكة من المجسات الذكية تقوم بجمع البيانات والمعلومات وتحليلها لأغراض المحافظة على الأمن([3]).

وقد تزايد الاعتماد على تحليل البيانات الكبرى في العمل الشرطي تحديدًا، وفي مجال العدالة الجنائية، فقد أشار البعض إلى أن: نظام العدالة الجنائية في الولايات

---

[1]) انظر: د. محمود سلامة عبد المنعم الشريف، الطبيعة القانونية للتنبؤ بالجريمة بواسطة الذكاء الاصطناعي ومشروعيته، مرجع سابق، ص٣٤٣.

[2]) المرجع السابق، ص٣٤٤.

[3]) د/عمار ياسر زهير، دور أنظمة الذكاء الاصطناعي في التنبؤ بالجريمة، مجلة الفكر الشرطي، مركز بحوث الشرطة، القيادة العامة لشرطة الشارقة، الإمارات العربية المتحدة، المجلد ٢٨، العدد ١١٠، يوليو ٢٠١٩م، ص٨٢.

المتحدة يلجأ بصورة متزايدة إلى استخدام أدوات خوارزمية في مرحلة إطلاق السراح المشروط([1]) كما قدم بعض المتخصصين تقريرا مفصلا عن نظام تقييم المخاطر الجنائية المتعلقة بأنماط إدارة الجناة الإصلاحية للعقوبات البديلة (COMPAS) ويستخدم هذا التطبيق في جلسات الحكم وإطلاق السراح المشروط. فقد عرض مؤلفو التقرير وقائع عديدة تم فيها تطبيق خوارزمية تقييم المخاطر، والتي يتم استخدامها لإبلاغ القرارات حول من يمكن إطلاق سراحه في كل مرحلة من مراحل نظام العدالة الجنائية؛ حيث يقدم التطبيق قرارا بنتيجة التنبؤ باحتمالية ارتكاب جريمة في المستقبل، مع تقييم احتياجات المجرم لإعادة التأهيل إلا أن هذا الاستخدام لتلك الخوارزميات في تقييم مخاطر احتمالية العودة إلى الإجرام كان محل انتقاد من قبل بعض المتخصصين، وسوف نعرض لهذا الانتقاد في بيان إشكاليات التنبؤ بالجريمة باستخدام تقنيات التحليلات التنبؤية للبيانات الكبرى في العمل الشرطي فيما بعد.

وقد أوضح المعهد الوطني للعدالة في الولايات المتحدة أن الشرطة التنبؤية تحاول تسخير قوة المعلومات والتقنيات الجغرافية المكانية للحد من الجريمة وتحسين السلامة العامة، هذا النهج يمكن أن ينقل إنفاذ القانون من الرد على الجرائم إلى عالم توقع ماذا وأين يحتمل حدوث شيء ما، ونشر رجال الشرطة وفقًا لذلك.

وفي سياق متصل طور الباحثون في جامعة (Carnegie Mellon) أداة برمجية للتنبؤ بالجريمة تسمى (CrimeScan) قبل عدة سنوات، تقوم على فكرة أساسية

[1]) Osonde A. Osoba, William Welser IV, An Intelligence in Our Image, The Risks of Bias and Errors in Artificial Intelligence, op. cit., P: 13.

مفادها: أن الجريمة العنيفة تشبه إلى حد ما المرض المعدي، تميل إلى الانتشار في مجموعات جغرافية معينة. وقد توصلوا –أيضًا– إلى الاعتقاد بأن الجرائم الأقل خطورة يمكن أن تكون نذيرًا لجرائم أكثر عنفًا؛ لذلك قاموا ببناء خوارزمية باستخدام مجموعة واسعة من بيانات المؤشر الرئيسي بما في ذلك تقارير الجرائم مثل: الاعتداءات البسيطة، والتخريب والسلوك غير المنضبط، وأن جوهر الفكرة هو: تتبع الشرر قبل اندلاع الحريق، فإن الاعتداءات البسيطة يمكن أن تفضي إلى اعتداءات جسيمة، أو قد يكون لدى الشرطة نمطا متصاعدا من العنف بين جماعتين إجراميتين متصارعتين([1]).

لا يُعد (CrimeScan) أول برنامج مصمم للشرطة التنبؤية، فقد تم إنشاء برنامج (PredPol) قبل ثمان سنوات من قبل علماء جامعة كاليفورنيا يعملون مع قسم شرطة لوس أنجلوس، بهدف معرفة كيف يمكن للتحليل العلمي لبيانات الجريمة أن يساعد في تحديد أنماط السلوك الإجرامي، يستخدم هذا البرنامج الآن من قبل أكثر من ستين قسم شرطة في جميع أنحاء البلاد، ويحدد (PredPol) مناطق أحد الأحياء التي من المرجح أن تحدث الجرائم الخطيرة خلال فترة زمنية معينة([2]).

وأكد بعض المتخصصين أن البرنامجين السابقين يمكن قصر تنبؤهما على الأماكن التي يمكن أن تحدث فيها الجرائم، وتجنب التنبؤ بمن قد يرتكبها، وهو نهج مثير

[1]) Randy Rieland, Artificial Intelligence Is Now Used to Predict Crime. But Is It Biased?, MARCH 5, 2018, available at: https://www.smithsonianmag.com/innovation/artificial-intelligence-is-now-used-predict-crime-is-it-biased-180968337/11/1/2021

[2]) ibid.

للجدل أنشأته مدينة شيكاغو حول الأشخاص الأكثر احتمالًا للمشاركة في عمليات إطلاق النار في المستقبل، سواء كمطلق للنار أو كضحية.

وقد أشارت الإحصاءات إلى أن العديد من الجرائم انخفضت نسبة ارتكابها بعد استخدام تقنية التنبؤ بالجريمة القائم على التعلم العميق، فقد انخفض العنف في مقاطعة Kent البريطانية بنسبة ٦% بعد تجربة برنامج (Predpol) لأربعة أشهر فقط. كما انخفضت جرائم السطو المسلح في مدنية Santa Cruz بولاية كاليفورنيا الأمريكية بنسبة ١٩%، كما انخفضت جريمة السرقة بنسبة ٦% في ستة أشهر فقط. كما ثبت أن معدل الجريمة في المدن التي طبقت برامج التنبؤ بالجريمة انخفض بنسبة ٣٥% عن المدن التي لم تطبقها([1]).

الفرع الثاني

تقنيات التعرف على الوجوه وبصمة الصوت

أولاً– تقنية التعرف على الوجوه:

١– مفهوم التقنية:

أكدت الدراسات أن الوجه البشري يتميز بملامح معينة تعد بصمة مميزة له، بما تتضمنه من ارتفاعات وانخفاضات تميزه عن غيره من الوجوه مثل: المسافة بين العينين، وطول الأنف، وشكل ومحيط الشفاه، وتباعد الأذنين وعرض الذقن، وغيرها،

[1]) انظر: د. محمود سلامة عبد المنعم الشريف، مرجع سابق، ص٣٤٤.

ومن ثم تقوم تقنية التعرف على بصمة الوجه من خلال تحويل هذه البصمة إلى بيانات رقمية، ثم مطابقة الوجه بدلالته الرقمية مع الصور المخزنة في قواعد البيانات في القطاعات الأخرى([1]). وقد تطور استخدام هذه التقنية للتعرف على شخصية صاحب الوجه بنسبة تطابق متطورة([2]) لذلك شاع استخدامها للتأكد من أن صاحب الصورة يمتلك الصلاحيات الكافية للدخول إلى موقع ما أو استخدام جهاز ما، كما يحدث عند جعل بصمة الوجه كما لو كانت كلمة مرور لنظام معلوماتي معين. وتتم هذه العملية في أجزاء من الثانية.

وقد أوضح بعض المتخصصين أن هذه التقنية تتم باستخدام خوارزمية (تحليل المكونات الأساسي)(PCA) والتي تسعى إلى تحديد هوية شخص ما تتواجد لدينا صورة له، وذلك تبعا للذاكرة المخزنة في قواعد البيانات والنظم المعلوماتية المخزنة عليها صور الأشخاص، وتكمن مهمة تقنية التعرف على الوجه في إيجاد شعاع الملامح الأكثر شبهاً والأقرب ضمن مجموعة التدريب إلى شعاع الملامح المستخلص

---

[1]) خلدون غسان سعيد " تقنيات متطورة للتعرف على الوجوه تصمم بنظم الذكاء الصناعي والتعلم العميق وتوظّف في استخدامات أمنية وطبية وتجارية، جريدة الشرق الأوسط، الثلاثاء – ١٧ جمادى الآخرة ١٤٤١ هـ – ١١ فبراير ٢٠٢٠ م، العدد ١٥٠٥٠، منشور على الموقع الإلكتروني التالي، تاريخ الزيارة ٢٠٢٠/١٢/١٣م.

https://aawsat.com/home/article/2125116/

[2]) واستطاعت خوارزمية طورها باحثون في جامعة هونغ كونغ الصينية في العام ٢٠١٤ التفوق على القدرات البشرية في التعرف على الوجوه، حيث استطاع النظام بالتعرف على الوجوه بنسبة ٩٨,٥٢ % مقارنة بـ٩٧,٥٣ % للتعرف البشري. واستطاعت «غوغل» في العام ٢٠١٥ تحقيق نسبة ٩٩,٦٣ % من التعرف الصحيح على الوجوه بعد مقارنتها بعدة صور وربط صاحب الصورة بصوره الأخرى. انظر: خلدون غسان سعيد، المرجع السابق.

من الصورة المقدمة للاختبار([١])، أي الصورة المطلوب تحديد هوية صاحبها عبر نظام التعرف([٢]).

وقد أشار البعض إلى جملة عوامل مؤثرة على قدرة تقنية التعرف على الوجه على اعتبار أن الوجه الإنساني ثلاثي الأبعاد، غير متصلب، يمكن أن يلاحظ بزوايا مختلفة، ومن هذه العوامل المؤثرة: ظروف الإضاة، النظارات والملابس والشعر، الشيخوخة والجراحات التجميلية في الوجه([٣]).

نشرت دائرة التقنية والعلوم التابعة لمركز الأمن القومي الأميركية عام ٢٠١٨م نتائج اختبارات تقنيات متعددة للتعرف على الوجه حصل أعلاها على نسبة ٩٩,٤٤ في المائة في أقل من خمس ثوان، وتم تطوير هذه التقنيات لدرجة أعلى؛ حيث بات

---

[١]) حيث يتم تشكيل واستخلاص ذاكرة تقنية التعرف على الوجه من مجموعة تدريب وهي عبارة عن مجموعة من الصور التي تقدم مسبقاً للنظام، وتتألف مجموعة التدريب هذه من أشعة الملامح المستخرجة من مجموعة معروفة من صور الوجوه لعدة أشخاص مختلفين. ويقصد بأشعة الملامح أي عبارة عن مصفوفة منتقاة من مصفوفات الصورة الاصلية، وتمثل القيم المهمة والاساسية ضمن الصور الاصلية، وبذلك يتم اختزال حجم الصور إلى أشعة تمثل خلاصة الصور.

[٢]) انظر: نور الصباحي، التعرف على الوجوه باستخدام خوارزمية " تحليل المكونات الأساسية" Principal Component Analysis PCA، منشور بواسطة Schwarz Tigers Weblog ، بتاريخ ٤ يناير ٢٠١٣م، على الموقع الإلكتروني التالي، تاريخ الزيارة ٢٠٢٠/١٢/١٤م:
https://schwarztiger.wordpress.com/tag/
وكذلك: على شائف محمد شعفل، جعفر زين العابدين، التعرف على تعبير الوجه باستخدام خوارزمية PCA، رسالة ماجستير، جامعة الخرطوم، كلية علوم الحاسوب وتقنية المعلومات، السودان، ٢٠١٣، ص٥٩.

[٣]) المرجع السابق، ص٤٢، ٤٣.

بإمكانها التعرف على مشاعر صاحب الوجه من صورة ثابتة له، وتحديد ما إذا كان سعيدًا أم غاضبًا أم مضطربًا أم حزينًا أم خائفًا أم غيرها من المشاعر الأخرى.

وقد ميز البعض بين تقنية التعرف على الوجه من خلال الشكل والملامح، وبين تقنية تحديد الوجه وهي تقنية قادرة على التعرف على الحالة النفسية التي يمر بها وجه الشخص من خلال تعابير الوجه من خلال عدة خوارزميات أكثر دقة وتعقيدًا من تلك المستخدمة في تقنية التعرف على الوجه([١])؛ حيث أكد بعض المتخصصين أنه يمكن تحميل تعابير الصور المراد التعرف عليها في مجلد بحيث تتم مقارنتها من قبل النظام مع تعابير الصور المخزنة في قاعدة البيانات، باستخدام خوارزمية (PCA) المشار إليها ثم يقوم النظام بإعطاء أقرب تعبير وجهي بالنسبة للصور المخزنة في قاعدة البيانات([٢]).

وقد أعلنت شرطة دبي أنه باستطاعة الشرطي الآلي كشف المشاعر وحركة الأجسام والتعرّف على الإيماءات وإشارات اليد عن بعد، كما يمكنه رصد تعابير السعادة والحزن والابتسام على وجوه الناس، كما يستطيع إرسال مقاطع فيديو إلى غرف العمليات في المراكز والإدارات الشرطية([٣]).

---

[١]) مقال بعنوان " تقنية التعرف على الوجه" مجلة العلوم والتكنولوجيا، منشور على الموقع الإلكتروني للمجلة، تاريخ الزيارة ١٤/١٢/٢٠٢٠م.
http://www.tqmagazine.net/Details.aspx?id=554

[٢]) على شائف محمد شعفل، جعفر زين العابدين، المرجع السابق، ص٨٠.

[٣]) الروبوت وتطبيقات الذكاء الاصطناعي، منشور على البوابة الرسمية لحكومة الإمارات العربية المتحدة، تاريخ الزيارة ٢٤/١٢/٢٠٢٠م:
https://u.ae/ar-ae/about-the-uae/digital-uae/robotics-and-ai-applications

٢– قدرات التقنية واستخداماتها الأمنية:

تشترك جميع تقنيات التعرف على الوجه في قدرتها على التعلم العميق من البيانات الواردة لها، ومع التقدم المستمر في مجال الذكاء الاصطناعي ومع ازدياد حجم عينات الصور التي يتم مطابقتها، ومع أسلوب التعلم العميق تستطيع تقنية التعرف على الوجه التعلم من الأخطاء التي يحدث أن تصدر منها، والتي يصححها لها البشر، ومع الوقت تعزز من إدراكها لآلية التحليل الصحيح في كل حالة، فيستطيع التحقق من اختلاف تحليل وجوه السيدات عن الرجال، وأصحاب البشرة الداكنة مقارنة بالبشرة الفاتحة([1]) وتقارب وجوه سكان جنوب شرقي آسيا من حيث الملامح، وتغير كمية الدهون الموجودة في وجوه المستخدمين بعد إكتساب أو فقدان الوزن، وغيرها من العوامل والمتغيرات الأخرى التي تحدث للوجه البشري مع تقدم العمر.

تتمحور كبرى الاستخدامات لتقنيات التعرف على الوجه في المراقبة الأمنية للمنافذ والمطارات، مثل إصدار الوثائق الثبوتية، ودوريات الشرطة الأمنية، والتعرف على هوية مرتكبي الجرائم والعمليات الإرهابية من خلال التسجيلات أو الصور الملتقطة في موقع الحادث.

---

[1]) جدير بالذكر أن البعض اعتبر هذا من قبيل التحيز حيث يؤكد هذا التحيز الآلي ، ما يدل على أن أنظمة التعرف على الوجه التجارية تتفوق في تحديد الذكور ذوي البشرة الفاتحة ، بمعدل خطأ أقل من ١ %. ولكن إذا كنت أنثى ذات بشرة داكنة ، فإن فرصة التعرف عليك بشكل خاطئ ترتفع إلى ما يقرب من ٣٥ %.

Osonde A. Osoba, Keeping Artificial Intelligence Accountable to Humans, August 20, 2018, available on internet, date of visit: 28/12/2020, https://www.rand.org/blog/2018/08/keeping-artificial-intelligence-accountable-to-humans.html

كما يمكن استخدامها في الطائرات المُسيّرة ذاتياً([1]) Drones التي تستطيع حمل كاميرات عالية الكفاءة في التعرف على المشتبه بهم في التجمعات الكبيرة من مسافات تصل إلى ثمانمائة متر بعيدا عنهم، وارتفاع مائة متر ومن زوايا مختلفة.

ويمكن ربط هذه الطائرة المُسيّرة بكابل متصل بمصدر للطاقة على الأرض تعمل لفترات طويلة جدا، مع نقلها للبيانات عبر كابلات متصلة بحواسيب على الأرض لحماية البيانات وضمان عدم اختراقها.

كما أصبح استخدام هذه التقنيات للأغراض الأمنية واقعا ملموسا نلاحظه في العديد من الشوارع والميادين في كبريات مدن العالم، وتحتل دولة الإمارات مرتبة متقدمة بين دول العالم التي اعتمدت هذه التقنيات للأغراض الأمنية([2]) فقد أعلنت إحدى شركات التقنية المشاركة في معرض (جيتكس ٢٠١٨م) أن مدنية دبي من أكثر مدن العالم استخداما لتقنيات التعرف على الوجه في أماكن التسوق لمراقبة سلوكيات الزوار وتحليلها، وفي مدرجات الأندية الرياضية أثناء المباريات لمراقبة

---

[1]) عرفتها المادة الأولى من القانون رقم ٧ لسنة ٢٠٢١م، بشأن تنظيم الرياضات الجوية الخفيفة في إمارة رأس الخيمة، بقولها: "طيارة بدون طيار يتم التحكم فيها عن طريق برمجتها والسيطرة على حركتها ذاتياً".

[2]) من ذلك نجد الصين تراقب الأفراد في الشوارع والميادين العامة باستخدام ٢٠٠ مليون كاميرا مراقبة في العام ٢٠١٨، مع خطتها لرفع العدد ليصل إلى ٦٢٦ مليونا في العام ٢٠٢٠. ويبلغ معدل الكاميرات لكل ألف شخص في مدينة تشونغكنغ الصينية ١٦٨، بينما يبلغ العدد ٦٨ لكل ألف شخص في لندن، وينخفض إلى ١٦ لكل ألف شخص في مدينة أتلانتا الأميركي. وتجدر الإشارة إلى أن ٨ مدن من أصل أكثر ١٠ مدن استخداما لكاميرات المراقبة هي مدن صينية، إضافة إلى مدينتي لندن وأتلانتا الأمريكية. كما دخلت موسكو العاصمة الروسية السباق باستخدام ٢٠٠ مليون كاميرا بنهاية العام ٢٠١٩ تستطيع التعرف على وجوه المارة لرفع مستويات الأمن العام.

سلوكيات الجمهور والتنبؤ بالأعمال التي يتوقع معها وقوع أعمال شغب جماهيري، وكذلك في تأمين المؤتمرات ومراقبة كل المشاركين وتحليل سلوكهم.

ثانياً– تقنية تحديد الهوية ببصمة الصوت:

١– مفهوم بصمة الصوت:

تعرف هذه البصمة بأنها: تسجيل سمعي للموجات الصوتية الخاصة بصوت الإنسان، والتي تكفي في تحديد هوية المتحدث أو مصدر الصوت([١]). كما عرفها البعض بأنها: تعيين هوية الإنسان عن طريق تحليل الصوت المتمركز في نواة أية خلية من خلايا جسمه([٢]). وتستمد بصمة الصوت أهميتها من كفايتها في تحديد هوية المتكلم؛ حيث أشار البعض إلى أن لكل صوت خصائص فردية([٣])، ولكل شخص صوت خاص به، لا يتصور صدروه من غيره بما يمكن تمييزه عن غيره من الأصوات التي

[١]) د/ عمر عبد المجيد مصبح، بصمة الصوت وأثرها في الإثبات الجنائي، مجلة البحوث الأمنية، المملكة العربية السعودية، العدد (٥٢) شعبان ١٤٣٣، ص٢٢. وقد أشار هذا الفقه إلى استخدام مصطلح (تحديد هوية المتكلم) أقرب إلى الصواب من مصطلح بصمة الصوت، بينما يفضل البعض استخدام مصطلح (فردية الصوت) على اعتبار أن الصوت لا يترك أثرًا، مثل بصمة الأصابع. انظر في هذا الرأي: د/ طارق ابراهيم الدسوقي، مرجع سابق، ص٣٠٤.

[٢]) نزار محمد معتصم، التعرف على الصوت، ٢٠١٠، القاهرة، ص ٢١٢، مشار إليه في بحث بعنوان " حجية البصمة الصوتية في الإثبات الجزائي" منشور على الرابط الإلكتروني التالي، تاريخ الزيارة ٢٠٢٠/١٢/١٠م.

http://aliqws4.simplesite.com/#_ftn5

[٣]) د/ عمر عبد المجيد مصبح، مرجع سابق، ص٢٢.

تصدر عن الآخرين؛ إذ الصوت هو من الحواس المميزة لشخصية الإنسان والتي تساهم إلى حد كبير في تحديد هوية المتكلم([1]).

كما تؤكد الدراسات أن لكل شخص جهازه الصوتي الخاص به؛ حيث يتعذر وجود شخصين متطابقين في القدرة وأسلوب تحريك اللسان والشفاة، كما أشار إلى بُعد احتمال أن يكون لدى شخصين ذات الاستعمال الديناميكي للجهاز الصوتي، الذي يتكون من أعضاء الجسم التي تساعد في إخراج الصوت مثل الفم، اللسان، الأسنان، القفص الصدري، والتي تتميز من حيث شكل وحجم الأعضاء وارتباط بعضها البعض([2]).

٢-القيمة الثبوتية للبصمة:

نظرا لارتباط الصوت ببعض الجرائم كما في جرائم السب والقذف، والتهديد، والعرض، سواء كان الصوت صادرا من الجاني أو من المجني عليه، فقد يكون الصوت دليلا قويا على براءة المتهم من التهمة المنسوبة إليه أو على العكس قد يكون دليلا قويا على إدانته، ومن ثم يمكن القول أن بصمة الصوت تندرج ضمن القرائن القوية التي تخضع لمبدأ الاقتناع الذاتي للقاضي، أي قاعدة حرية القاضي في تكوين عقديته أو اقتناعه.

[1]) عيسى غازي الذيب، د/ بارعة القدسي، دور البصمة الصوتية والبصرية ومدى مشروعيتهما في الإثبات الجزائي، مجلة جامعة البعث، سوريا، المجلد ٣٩، العدد ٥٢، ٢٠١٧، ص٩٢، ٩٣.

[2]) بحث بعنوان حجية البصمة الصوتية في الإثبات الجزائي، مرجع سابق، بدون صفحة.

مع التقدم في وسائل التعرف الآلي على البصمة الصوتية المميزة لهوية المتكلم بات واقعا ملموسًا استخدام البرامج الحاسوبية في التعرف على المتكلم؛ حيث يمكن لهذه البرامج مقارنة الأصوات، وتحديد ما إذا كان صوت شخص ما هو نفسه الصوت الذي تم تسجيله مسبقاً، مع تقليل احتمالات الخطأ أو الخداع في حالات تقليد الصوت؛ فالصوت المقلد يشبه الصوت الأصلي عند سماعه بالأذن البشرية، ولكن برامج الحاسب الآلي تستخدم ذكراة فائقة تختلف تماما عن الذاكرة البشرية مما يجعلها قادرة على التمييز بين الصوت الأصلي والصوت المقلد مع إعطاء نتيجة سريعة ودقيقة في تحديد هوية الشخص من خلال بصمة صوته، واتخاذ قرار سريع في تحديد هوية الشخص والتعامل معه على هذا الأساس. وبات الأمر أكثر دقة وسرعة، وبعيدا إلى حد كبير عن الأخطاء باستخدام خوارزميات الذكاء الاصطناعي في تحليل الأصوت؛ حيث أثبتت هذه التقنيات فاعلية عالية مقارنة بالبرامج الحاسوبية التقليدية التي لا تصل إلى إمكانيات الذكاء الاصطناعي.

الفرع الثالث

تقنية الطائرات المسيرة ذاتياً والسيارات ذاتية القيادة

أولاً- تقنية الطائرات المسيرة ذاتياً:

تجدر الإشارة إلى أن المشرع بإمارة دبي قد عرف الطائرة بدون طيار بأنها "طائرة تحلق في الجو دون وجود القائد على متنها، وتشمل الطائرة الموجهة بالعين المجردة، والطائرة الموجهة عن بعد، والطائرة المسيرة ذاتياً"([1]) ثم صدر المرسوم بقانون اتحادي رقم (٢٦) لسنة ٢٠٢٢ بشأن تنظيم الاستخدام المدني للطائرات بدون طيار والأنشطة المرتبطة بها([2])، حيث عرفها في المادة الأولى منه بأنها " الطائرة بدون طيار: أيّ آلة أو مركبة أو ما يماثلها من الأجسام تستطيع الطيران بدون وجود قائد لها على متنها ويتم التحكم فيها عن بعد أو بشكل ذاتي، وتعتبر أنظمة التحكم بها جزء منها وتستخدم للأغراض المدنية".

يشهد الاعتماد على تقنية الطائرات بدون طيار (Dornes) في الأغراض الأمنية تزايدا مضطردا، كما يشهد العالم تسابقا محمومًا في إنتاج وتسويق هذه التقنيات، بل أعلنت بعض الدول عن امتلاكها ما يشبه أسطول جوي من

---

[1]) المادة الأولى من قانون تنظيم الطائرات بدون طيار في إمارة دبي رقم ٤ لسنة ٢٠٢٠م. الجريدة الرسمية، دبي، السنة ٥٤، العدد ٤٧٩، ٧ يوليو ٢٠٢٠م، ١٦ ذو القعدة ١٤٤١هـ، ص٢.

[2]) https://laws.uaecabinet.ae/ar/materials/law/1587

الطائرات المسيرة بدون طيار، ووفقا لأحد التقديرات ستتجاوز مبيعات الطائرات بدون طيار أو ذاتية القيادة اثنتا عشرة مليار دولار بحلول ٢٠٢١م.

ونظرا لما تمتلكه هذه الطائرات من قدرات فائقة على التقاط الصور من مسافات بعيدة، وتحليل تلك الصور والفيديوهات التي تسجلها لتجمعات الأشخاص، شاع استخدامها في تأمين الاحتفالات والمهرجانات في الأماكن المفتوحة، التي يصعب فيها مراقبة جمهور الحضور بالعناصر البشرية.

كما شاع اعتماد إدارات الجمارك وحماية الحدود على استخدام منصات الطائرات بدون طيار في القيام بأنشطة الكشف عن البضائع المهربة، وتأمين الحدود ضد عمليات التسلل؛ كما يمكن استخدامها في المسح الكيميائي والبيولوجي والإشعاعي والنووي والمتفجرات في الموانيء.

وقد أوضحت المادة (٦) من المرسوم بقانون اتحادي رقم ٢٦ لسنة ٢٠٢٢م سالف الذكر استخدامات الطائرات بدون طيار ومنها ما ورد بالفقرة (هـ) بقولها:

هـ. تقديم بعض الخدمات العامة من قبل الجهات الحكومية والقيام بعملية الرقابة والتفتيش والمتابعة أو غيرها من الأنشطة المرتبطة بالمجالات التي تدخل في اختصاصاتها.

ثانيًا– تقنية المركبة المستقلة ذاتية القيادة:

عرفها قانون إمارة دبي رقم ٩ لسنة ٢٠٢٣م في شأن تنظيم تشغيل المركبات ذاتية القيادة في إمارة دبي، في المادة الأولى منه، بقولها: "مركبة تسير على الطريق

باستخدام نظام القيادة الآلي، تتوفر فيها المواصفات والمقاييس المعتمدة من الهيئة أو الجهات المختصة، ولا تشمل المركبة ذات الأنظمة المساعدة للسائق فقط، كالمساعدة في الحفاظ على المسار أو مثبت السرعة، أو الفرامل عند الطوارئ أو الركن الذاتي".

وتشير التقديرات الحالية إلى أن هذه التقنية ستساهم بشكل كبير في تحقيق أقصى درجات الأمن المروري، بالتقليل من خطورة حوادث الاصطدام، ومن ثم التقليل من الإصابات والوفيات، خاصة مع تصور أنه من النادر أن تكون هذه المركبات هي المتسببة في التصادم([1])

كما أشار دليل المركبات المستقلة ذاتية القيادة أن هذه التقنية تقدم إمكانية لتغيير عملية النقل تغييرا جذريًا، ومن المرجح أن يقلل تجهيز السيارات والمركبات الخفيفة بهذه التقنية من حوادث الاصطدام، ومن تكاليف الازدحام المروري([2]).

كما تشير الدراسات الحديثة أن المركبات ذاتية القيادة (AV) سوف تحدث ثورة في الكيفية التي يتنقل بها الناس وفي طرق معيشتهم وعملهم وتفاعلهم مع الآخرين. هذا ما يدفعنا إلى إعادة النظر في سُبل تصور وقياس وتنظيم

[1]) Laura Fraade-Blanar, Nidhi Kalra, Autonomous Vehicles and Federal Safety Standards, published by RAND Corporation, 2017, P: 1, available at: file:///C:/Users/HP/Downloads/RAND_PE258.pdf/2/1/2021

[2]) James M. Anderson and others, Autonomous Vehicle Technology, A Guide for Policymakers, Published by the RAND Corporation, Santa Monica, Calif., 2016, P: xiii.

السلامة المرورية على الطرق([1]). كما يمكن استخدام هذه التقنيات في إطلاق دورية شرطية ذكية، حيث يمكنها التجول استقلالا عن التدخل البشري، مع اتصالها الدائم بالمركز الذي يمكنه متابعة كل ما يحدث في بيئة المركبة.

الفرع الرابع

الروبوتات فائقة الذكاء

أولاً– تعريف الروبوت فائق الذكاء:

دخلت الروبوتات الذكية Intelligent robots، كافة جوانب الحياة البشرية في الوقت الحالي، فقد تغلغلت في تفاصيل حياتنا، حتى وصلت إلى أدقها وأخطرها، وينتظر أن تتوغل بشكل أكبر في المستقبل القريب دون أن نشعر بها، وقد تزايد الاعتماد عليها؛ لما تمتاز به من قدرات عالية على تقدير

[1]) Sean E. Goodison and others, Autonomous Road Vehicles and Law Enforcement, published by RAND Corporation, 2017, P: 1, available at: file:///C:/Users/HP/Downloads/RAND_RRA108-4.pdf/2/1/2021

حيث قدر معهد التأمين للسلامة على الطرق السريعة بالولايات المتحدة أن تزويد جميع المركبات بنظام تحذير الاصطدام الأمامي، ونظام التحذير من الانحراف عن مسار الطريق، وكذلك نظام الرؤية الجانبية، والمصابيح الأمامية، لو تم لكان من الممكن تجنب وقوع ثلث حوادث الاصطدام والوفيات، كما أشار التقرير إلى أن نظام المكابح التلقائي قد يقلل من حوادث الاصطدام خاصة عند استشعار وجود عائق في الطريق، وأخيرا تفعيل المستوى (٤) من نوعية هذه المركبات يقلل إلى حد كبير من حوادث الاصطدام التي مرجعها خطأ السائق مثل القيادة تحت تأثير الكحول.

James M. Anderson and others, op. cit., P: xiv.

المواقف واتخاذ القرارات مع أقل نسبة أخطاء مقارنة بالقرارات البشرية([1]). وقد عرف المشرع الاماراتي الروبوت الإلكتروني –كإنموذج للتشريعات العربية– بأنه "برنامج إلكتروني يتم إنشاؤه أو تعديله لغرض تشغيل المهام المؤتمتة بكفاءة وسرعة"([2]).

كما عرفه القانون الكوري–كإنموذج للتشريعات المقارنة– المتعلق بتطوير وتوزيع الروبوتات الذكية ٢٠٠٨م([3])، حيث عرفها في المادة الثانية من الفصل الأول المتعلق بالأحكام العامة، بأنها: "أداة ميكانيكية تدرك البيئة الخارجية بنفسها، وتميز الظروف، وتتحرك إرادياً أو ذاتياً".

وقد عرفه البعض([4]) بأنه "آلة مبرمجة ذاتياً، للقيام بعمل أو عدة أعمال، محددة، إما بإيعاز وسيطرة مباشرة من الإنسان، أو غير مباشرة من خلال

---

[1]) محمد عبد الحفيظ المناصير، إشكالية الشخصية الإلكترونية القانونية للروبوت، دراسة تأصيلية تحليلية مقارنة في إطار التشريعين المدني العماني والأوروبي، المجلة العربية للعلوم ونشر الأبحاث، المجلد٦ ، العدد١، ٣٠مارس٢٠٢٠م، ص٤٥.

[2]) المادة الأولى من المرسوم بقانون اتحادي رقم ٣٤ لسنة ٢٠٢١م في مكافحة الشائعات والجرائم الالكترونية، منشور على الرابط الالكتروني:
https://laws.uaecabinet.ae/ar/materials/law/1526

[3]) See: CHAPTER I GENERAL PROVISIONS, Art. (2), INTELLIGENT ROBOTS DEVELOPMENT AND DISTRIBUTION PROMOTION ACT, No. 9014, Mar. 28, 2008, Amended by Act No. 9161, Dec. 19, 2008, Act No. 13744, Jan. 6, 2016, available at:
https://elaw.klri.re.kr/eng_mobile/viewer.do?hseq=39153&type=lawname&key=robot

[4]) د. عمرو طه بدري، النظام القانوني للروبوتات الذكية، المزودة بتقنية الذكاء االصطناعي (الإمارات العربية المتحدة كأنموذج) (دراسة تحليلية مقارنة)، مجلة الدراسات القانونية والاقتصادية، جامعة مدينة السادات، المجلد ٧، العدد ٢، ديسمبر ٢٠٢١ (ملحق ديسمبر)، ص٢٨، ٢٩.

برامج الكترونية تم وضعها، وخصصت لذلك، وتعمل على تجسيد الذكاء الاصطناعي للعالم الخارجي، من خلال قدرتها على فهم الأشياء والتواصل مع البشر، ومع بعضها البعض، ومجهزة بقدرات تنبؤية، وقرارية، استناداً إلى خبرتها الخاصة".

ثانياً– توظيف الروبوتات فائقة الذكاء:

أ) الخصائص والسمات المميزة للروبوتات الذكية:

لا تقف صناعة الروبوتات الذكية عند حد معين، بل في تتطور بشكل مستمر وبدرجة مذهلة، ومن ثم تتطور الخصائص والسمات المميزة لهذه الروبوتات، بحيث يتم إكسابها خصال وسمات لم تكن تتمتع بها من قبل، يرجع ذلك إلى التقدم المذهل في البرامج والتقنيات التي يمكن تزويد الروبوتات بها.

ويمكن الإشارة إلى أهم الخصائص والسمات التي تتمتع بها الروبوتات الذكية أو فائقة الذكاء([1])، ومنها:

- القدرة على التحكم الذاتي والاستقلالية الذاتية، متعمدة على أجهزة الاستشعار المزودة بها، والتي تجعلها تتبادل البيانات مع البيئة الخارجية، ومعالجة هذه البيانات وتحليلها.
- القدرة على التعلم الذاتي، من خلال التجربة والتفاعل مع المواقف التي تتعرض لها، معتمدة على شبكات التعلم العميق.

[1]) المرجع السابق، ص٢٩، ٣٠.

- القدرة على تغيير وتكييف ظروفها مع البيئة الخارجية المحيطة بها.

ب) تنوع استخدامات الروبوتات الذكية:

تنوع توظيف الروبوتات من الاستخدامات المدنية إلى الاستخدامات العسكرية([1]) والأمنية، ومن الاستخدامات الشخصية إلى الاستخدامات الصناعية والحكومية، حتى أصبح للروبوتات سوقا عالمية رائجة تمثل اقتصادا غير محدود([2]).

يشهد العديد من دول العالم استخدامًا متصاعدًا للربوتات المستقلة، والتي تُعدُّ تطورا متقدما في العمل الأمني بالاعتماد على عناصر شرطية غير بشرية ومستقلة تماماً عن تدخل البشر، ويمكن الاعتماد على هذه الروبوتات في المواقف التي تتضمن خطرا على سلامة الشرطيين البشريين، كما في حالات تفكيك العبوات الناسفة، وتأمين الطرق([1]). وقد انتشر استخدام الروبوتات في الأعمال الأمنية المتكررة والتي تتطلب دقة عالية وسرعة فائقة، وقد تصيب

---

[1]) يوسف جمعة الحداد، الذكاء الاصطناعي .. كيف غير من مفاهيم الردع وتوازن القوى وحروب المستقبل؟، مجلة درع الوطن، صادرة عن مديرية التوجيه المعنوي، القيادة العامة للقوات المسلحة، الإمارات العربية المتحدة، بتاريخ ٢٠٢٠/٣/١م، منشور على الرابط الإلكتروني التالي، تاريخ الزيارة: ٢٠٢١/١/١٦م.

http://www.nationshield.ae/index.php/home/details/research/

[2]) إيهاب خليفة، اقتصاديات الروبوت، تصاعد الاهتمام العالمي بتطبيقات الذكاء الاصطناعي، المنهل، مجلة اتجاهات الأحداث، تحليلات المستقبل، العدد٨، مارس ٢٠١٥م، ص٢.

http://platform.almanhal.com.uoseresources.remotexs.xyz/Reader/Article/80873/11/1/2021

[1]) د. عادل عبد النور: أساسيات الذكاء الاصطناعي، منشورات مواقف، بيروت، ٢٠١٧م، ص١٠١.

الإنسان بالملل، مثل روبوت الدردشة الذي يستخدم في الرد على تساؤلات العملاء المتكررة والمتشابهة، فقد يصاب المجيب البشري ببعض الملل أو الضجر أو الغضب في الرد على بعض التساؤلات السطحية أو التافهة من بعض العملاء، كما سبق استخدامها في مجالات فنية دقيقة مثل: تشخيص الأمراض، ووصف الدواء، وإجراء الجراحات الدقيقة جداً([٢]).

ولا يقف استخدام روبوتات الذكاء الاصطناعي عند حد القيام ببعض المهام المادية بل يمكن الاستعانة به في الأغراض التوعوية؛ لما يتمتع به من سلالة في التعامل مع الأشخاص والرد على تساؤلاتهم بمعلومات متعمقة عن موضوع الحملة التوعوية؛ حيث يمكنه البحث في ثوان معدودة في شبكات المعلومات والرد بأسلوب علمي وعملي مما يكون له مردود في إقناع الأفراد بموضوع الحملة التوعوية، من قبيل ذلك أعلنت شرطة دبي عام ٢٠١٧م عن إطلاق أول روبوت ذكاء اصطناعي في المنطقة العربية للتوعوية بمخاطر المخدرات بأسلوب مبتكر([١]).

---

[٢] ك. إريك دريكسلر، وكريس بيترسون، وجايل برجاميت: استشراف المستقبل "ثورة التكنولوجيا النانوية"، ترجمة وتقديم: رؤوف وصفي، المركز القومي للترجمة، القاهرة، الطبعة الأولى، ٢٠١٦م، ص٧.

[١] شيرين فاروق، شرطة دبي تُطلق الروبوت «أمل» للتوعية بمخاطر المخدرات، مقال منشور في جريدة البيان بتاريخ ٣١ ديمسبر ٢٠١٧م، على الرابط الإلكتروني:
https://www.albayan.ae/across-the-uae/news-and-reports/2017-12-31-1.3146756

المطلب الثالث

إيجابيات وسلبيات الذكاء الاصطناعي وتقييم فاعليته

لا تخرج دراسة إيجابيات وسلبيات تقنيات الذكاء الاصطناعي عن كونها من ثمار الثورة التكنولوجية وما صاحبها من إيجابيات وسلبيات مرتبطة بحقوق وحريات الأفراد، أو بالأمن المجتمعي، أو بالمصالح العليا للدولة، بيد أن تقنيات الذكاء الاصطناعي قد تكون أفضل في إيجابياتها وأسوأ في سلبياتها.

الفرع الأول

إيجابيات تقنيات الذكاء الاصطناعي

١- يلعب الذكاء الاصطناعي دورًا مهمًا في الكثير من المجالات الحساسة مثل: المجال الطبي بالاعتماد عليه في تشخيص الأمراض، ووصف العلاج([1]) وإجراء بعض الجراحات الدقيقة، وقد ظهر مصطلح (الروبوت الجراحي)([2])

---

[1]) على سبيل المثال، يتم استخدام IBM Watson في جامعة North Carolina في Chapel Hill Cancer Center من أجل تحديد خيارات العلاج والتوصية بها للمرضى الذين لم يستجيبوا للعلاجات القياسية. مع نشر ما يقرب من ٨٠٠٠ ورقة بحثية طبية جديدة يوميًا، فمن المستحيل على الطبيب أو حتى فريق الأطباء مواكبة أحدث التطورات. ومع ذلك، يمكن لـ Watson أن يستعرض كل بحث جديد ثم يطبقه بسرعة لتحسين نتائج المرضى. وفي اختبار شمل ١٠٠٠ مريض تطابقت توصيات Watson مع توصيات الخبراء بنسبة ٩٩% من الوقت. والأهم من ذلك وجدت Watson خيارات علاجية أخرى في حوالي ٣٠ % من الحالات التي لم يحددها الخبراء.
Jeff Crume, Doug Lhotka, Carma Austin, op. cit., P:6.

[2]) انظر: د/ أبو بكر خوالد، د/ خير الدين بوزرب، فاعلية استخدام تطبيقات الذكاء الاصطناعي الحديثة في مواجهة فيروس كورونا (coved-19): تجربة كوريا الجنوبية نموذجًا، مجلة بحوث

وسيتم إدخال روبوتات النانو داخل الجسم البشري لتوصيل الدواء إلى الخلايا المريضة، أو لغرض إجراء العمليات الجراحية الخطيرة.

٢- بزر استخدام تقنيات الذكاء الاصطناعي في مجال الاستشارات القانونية، فقد ظهر مصطلح (المحامي الروبوت) و(القاضي الروبوت) و(والمحقق الروبوت) كما برز استخدامه في مجال التعليم التفاعلي والبحث العلمي، حيث أعلن عن قيام الروبوت (بيتا) بتأليف كتاب ليكون أول كتاب من تأليف الذكاء الاصطناعي، فقد استخدمت خوارزمية متطورة ذات قدرات عالية على تصنيف وتحليل البحوث العلمية والتي بلغ عددها خمسة وثلاثين ألف بحث من قاعدة البيانات الضخمة([1]).

٣- كما برز استخدام تطبيقات الذكاء الاصطناعي في المجال العسكري، من ذلك استخدام الطائرات المقاتلة بدون طيار، والروبوتات المقاتلة، وإتخاذ القرارات العسكرية الحاسمة في وقت نشوب المعارك، وتحليل المواقف وإعداد الخطط والإشراف على تنفيذها؛ فقد ذكر بعض الخبراء([2]) أن الروبوتات المقاتلة

الادارة والاقتصاد، جامعة زيان عاشور بالجلفة، الجزائر، مجلد ٢، عدد خاص٢، (٢٠٢٠)، ص٤٠.

[1]) مقال بعنوان طرح أول كتاب من تأليف الذكاء الاصطناعي، مجلة الإعمار والاقتصاد، عدد ٣٥٠، السنة ٢٦، ٣١ آيار ٢٠١٩، شركة الأوائل للتوزيع، بيروت، لبنان، ص١٥.

[2]) د/ تي إكس هارمز، الروبوتات المقاتلة: كيف سيغير الذكاء الاصطناعي طبيعة الحروب القادمة؟ منشور على منصة المنهل، على الرابط الإلكتروني:

http://platform.almanhal.com.uoseresources.remotexs.xyz/Reader/Article/105668/11/1/2021

والطائرات بدون طيار سوف تغير ملامح الحرب الحديثة، وستغير كذلك من الاستراتيجيات العسكرية المتبعة في حماية المجتمعات([1]).

٤- كذلك الحال في مجال التصنيع، حيث يمكن لتقنيات الذكاء الاصطناعي القيام بعمليات مراقبة الإنتاج، والإحلال محل العمال في الظروف البيئية الصعبة([2]) فقد ساهم الروبوت في أداء وظائف تصنيع يصعب على الانسان القيام بها مثل: العمل داخل أفران الحديد والصلب العملاقة، وداخل المفاعلات النووية، مما زاد من خطوط الإنتاج مع ضمان سلامة العنصر البشري([3]).

٥- يمكن الاعتماد على تطبيقات الذكاء الاصطناعي في المجالات شديدة التعقيد، والتي تحتاج تركيز عقلي مستمر، وحضور ذهني متواصل، وقرارات حساسة، وحاسمة، وسريعة لا تحتمل التأخير والخطأ وأوضح مثال على ذلك بروز دور الذكاء الاصطناعي في مكافحة الأوبئة والكوارث الطبيعية، فقد نجد الفرق الطبية تنهار تحت ضغط العمل المتواصل ليلًا ونهارًا، في مكافحة

---

[1]) يوسف جمعة الحداد، الذكاء الاصطناعي .. كيف غير من مفاهيم الردع وتوازن القوى وحروب المستقبل؟ مرجع سابق.

[2]) د/ محمد محمد خليفة، مرجع سابق، ص٣١.

[3]) إيهاب خليفة، اقتصاديات الروبوت، تصاعد الاهتمام العالمي بتطبيقات الذكاء الاصطناعي، مرجع سابق، ص٢.

الوباء بالإضافة إلى الاحتمالية المتزايدة لتعرضهم للعدوى([1])، كذلك فرق الدفاع المدني قد تنهار وتخسر العديد من أفرادها تحت ضغط العمل الخطير في إنقاذ الأرواح لاسيما في حالات الحرائق والزلازل.

٦- كما تساهم الأنظمة الرقمية الذكية في المجالات التي تحتاج صنع القرار؛ إذ إن هذه الأنظمة تتمتع بالاستقلالية والدقة والموضوعية، ومن ثم تكون قراراتها سريعة ودقيقة وأقرب إلى الصواب، وأبعد عن الخطأ، والانحياز والتأثر بالمشاعر، أو التطرف والعنصرية، والأحكام السابقة والتدخلات الخارجية أو الشخصية، ومثال ذلك: قرارات التعيين في الوظائف المتقدمة في الهيكل الإداري، ودعم القرارات المالية والاقتصادية الحساسة التي تعتمد على دراسات جدوى دقيقة ومتأنية، ومعتمدة على تجارب الدول والأنظمة المالية والاقتصادية الأخرى، كما هو الحال في رسم السياسات الضريبية.

٧- فيما يتعلق بالأمن السيبراني، نجد أن تقنيات الذكاء الاصطناعي ذو وجهين في تأثيرها الإيجابي والسلبي على الأمن السيبراني، حيث أعلنت شركة (IBM) عن إمكانية استخدام الذكاء الاصطناعي والتقنيات المعرفية في تحديد التهديدات والهجمات السيبرانية والاستجابة لها بسرعة أكبر، مما يقلل بشكل كبير من مضارها، فقد استوعبت تقنية (Watson) للأمن السيبراني أكثر من مليارين مستند في مجموعة المستندات، وتقوم بإضافة آلاف أخرى

[1]) للمزيد عن فاعلية استخدام تطبيقات الذكاء الاصطناعي في مواجهة الأوبئة والأمراض المعدية راجع: د/ أبو بكر خوالد، خير الدين بوزرب، مرجع سابق، ص٤٣، ٤٤.

كل يوم، ولقد قللت هذه التقنية من الوقت اللازم لتحليل بيانات تلك المستندات بحيث لا يستغرق الأمر دقائق معدودة، مما أدى إلى تسريع عملية التحليل بشكل كبير وتقليل التأثيرأت السلبية لهذه التهديدات على المؤسسة([1]).

٨- في المجال الأمني والشرطي، برز استخدام تقنيات الذكاء الاصطناعي في مجال الأمن على اختلاف أنواعه، سواء الأمن العام، أو الشامل، والأمن القومي، والبيئي، والصحي، والمالي، والاقتصادي، والغذائي، والدوائي..... إلى آخره. وقد أعلنت شرطة دبي عن أول روبوت ذكاء اصطناعي٢٠١٧م يستطيع التعامل مع البشر في تقديم الشكاوى والرد على تساؤلاتهم، ويحسن التفاعل معهم، مثل الشرطي البشري، ويمتاز هذا الروبوت بعدم حاجته إلى بعض التعقيدات الإدارية مثل الموظفين البشريين، كما لا يحتاج إلى ساعات تدريبية طويلة ومكلفة مثلهم، ويمكنه أداء المهام المكلف بها على أكمل وجه وبكفاءة عالية.

٩- كما برز استخدام تقنيات الذكاء الاصطناعي في العمل الشرطي لاسيما تقنية التحليلات التنبؤية والتعرف على الوجه والصوت لتحديد الهوية، فقد أثبتت جدارة في التنبؤ بالعديد من الأعمال الإجرامية أو التجمعات والتحركات المشبوهة ، وأصبح توجه وزارات الداخلية والجهات الشرطية إلى إنشاء مركز إدارة الجريمة والذي يستخدم تقنيات تحليل البيانات والتنبؤ التحليلي، حيث يحتوي المركز على مستودع معلومات الجرائم التي تحدث في المدينة، ويقوم

[1]) Jeff Crume, Doug Lhotka, Carma Austin, op. cit., P:6.

النظام بتحليل البيانات الكبرى وتقييم المخاطر المحتملة؛ وذلك للتنبؤ باحتمال وقوع الجرائم في المستقبل، سواء في أماكن معينة أو من أشخاص معينين، والاستعداد لها وتحسين زمن الاستجابة من خلال تكثيف وتوزيع الدوريات في الأماكن الأكثر عرضة لحدوث الجرائم، كما يتم استخدام هذه التطبيقات في مراقبة حركة المرور للتنبؤ بدقة عالية بالحوادث المرورية وتفاديها، والتنبؤ بالاختناقات المرورية، واتخاذ قرار حلها والعمل على السيولة المرورية([1]).

١٠- كما يمكن إسناد مهمة المتابعة والرصد لشاشات الدوائر التليفزيونية المتصلة بكاميرات المراقبة لخوارزميات الذكاء الاصطناعي، حيث يمكنها مراقبة عدد كبير من الشاشات بشكل أفضل من إسناد هذه المهمة لشخص واحد أو عدة أشخاص؛ حيث يمكن للخوارزمية تحليل سلوكيات الأفراد، وطريقة مشيهم وتحركهم، ومدى دلالة هذا على توقع سلوك غير مشروع منهم، كما يمكنها التعرف على الأشخاص وتحديد هويتهم([2]).

---

[1]) للمزيد راجع: د/ عادل عبد النور، مدخل إلى عالم الذكاء الاصطناعي، مدينة الملك عبد العزيز للعلوم والتقنية، المملكة العربية السعودية، ٢٠٠٥م، ص٩، منشور على الموقع الإلكتروني التالي، تاريخ الزيارة ٢٠٢٠/١٠/٢٧م:

https://www.noor-book.com/-pdf

[2]) انظر: إيهاب خليفة، الذكاء الاصطناعي: تأثيرات تزايد الاعتماد على التقنيات الذكية على الحياة اليومية للبشر، مرجع سابق، ص٣.

الفرع الثاني

سلبيات تقنيات الذكاء الاصطناعي

أشار بعض المتخصصين إلى العديد من تداعيات استخدام تقنيات الذكاء الاصطناعي في العمل؛ حيث يمثل ذلك تهديدا للعمالة البشرية، بتقليل الأيدي العاملة في المصانع التي تعتمد بشكل كبير على الروبوتات الآلية، كما قد تضطر الإدارات إلى إصدار قرارات بالاستغناء عن بعض العمالة لعدم الخبرة الكافية في التعامل مع الميكنة الذكية للتصنيع([1]) وهناك بعض قطاعات التصنيع التي تعتمد بشكل أساسي على الروبوتات الذكية مثل: صناعة السيارات، والأدوات الكهربائية، فقد تشهد انخفاضا حادا للعمالة البشرية.

وقد يصل الأمر إلى إحلال الذكاء الاصطناعي محل البشر في قطاع كبير من الوظائف والأعمال، مثل: سائقي التاكسي، موظفي الاستقبال، حراس الأمن، عمال التوصيل، موظفي المكتبات، والحسابات والمبيعات، الاستشارات الإدارية والمصرفية والمالية، هذا الأمر يلقي على عاتق الحكومات عبئًا ثقيلًا بضرورة وضع الخطط والسياسات في رفع الكفاءة المهنية للموظفين، وتأهيلهم بشكل يواجه تحدي مزاحمة الذكاء الاصطناعي للعناصر البشرية في العديد من قطاعات العمل([2]).

وتشير دراسة من معهد ماكينزي العالمي إلى أنه بحلول عام ٢٠٣٠، يمكن أن يحل العملاء والروبوتات الذكية محل ما يصل إلى ٣٠% من العمالة البشرية الحاليّة في

---

[1]) إيهاب خليفة، اقتصاديات الروبوت....، مرجع سابق، ص٥.

[2]) انظر: د/ سعيد خلفان الظاهري: الذكاء الاصطناعي "القوة التنافسية الجديدة"، مرجع سابق، ٤.

العالم. وتعتقد شركة ماكنزي أنه اعتمادًا على سيناريوهات التبني المختلفة، ستحل آلية التشغيل الآلي محل ما بين ٤٠٠ و٨٠٠ مليون وظيفة بحلول عام ٢٠٣٠، مما يتطلب ما يصل إلى ٣٧٥ مليون شخص لتبديل فئات الوظائف بالكامل([1]).

وقد نبه البعض([2]) إلى التداعيات الأمنية لاستخدام تقنيات الذكاء الاصطناعي، فقد يمثل بعضها خطرا على حياة الأفراد وحرياتهم، حال إساءة استخدامها، فقد ذكر أن الروبوتات المقاتلة وكذلك الطائرات بدون طيار المقاتلة قد تستخدم في القتل خارج إطار القانون، لاسيما إذا تم اختراق أنظمة التشغيل والتحكم فيها عن بعد، أو حال حدوث خطأ من الروبوت في تقدير الموقف المحيط به فاتخذ قرارا عدوانيا بناء على ذلك، فقد أشار البعض أنه في عام ١٩٨١م قُتل موظف ياباني في مصنع للدراجات بواسطة روبوت ذكاء اصطناعي؛ حيث قدرالروبوت على نحو خاطئ الحالة التي فيها الموظف وفسره على أنه يمثل تهديدا أو عائقا يحول دون إتمام مهمته، فقام بدفعه إلى آلة قريبة أدى إلى قيام الآلة بتحطيم رأس الموظف بذراعها الهيدروليكي، ومات على الفور، ثم واصل الروبوت مهامه كأن شيئا لم يكن([3]).

---

[1]) طه الراوي، مقال بعنوان "الذكاء الاصطناعي وأثره على الاقتصاد" نون بوست، بتاريخ ٢٠٢٠/١٠/٤م، منشور على الرابط الالكتروني التالي، تاريخ الزيارة ٢٠٢١/٣/١٤م:
https://www.noonpost.com/content/38443

[2]) إيهاب خليفة، الذكاء الاصطناعي: تأثيرات تزايد الاعتماد على التقنيات الذكية...، مرجع سابق، ص٣.

[3]) انظر: د/أحمد إبراهيم محمد إبراهيم، المسؤولية الجنائية الناتجة عن أخطاء الذكاء الاصطناعي في التشريع الإماراتي (دراسة مقارنة)، مرجع سابق، ص٨٨.

وعلى المستوى الاجتماعي أشار البعض إلى أن الإفراط في التعامل مع الالآت الذكية قد يؤثر سلبا على العلاقات الاجتماعية بين الأفراد، حيث تبعدها تدريجيا عن الجانب المعنوي والإغراق بها في الجانب المادي، كذلك التحول في العلاقة البشرية إلى النمطية المملة، والبعد عن التعقيد المفيد للعلاقات([1]). في حين نبه البعض إلى أنه من المتوقع أن تستفيد دولة الإمارات العربية المتحدة من تعزيز الذكاء الاصطناعي في تقليص أعداد العمالة الوافدة؛ ومن ثم تعديل الخلل بهيكل التركيبة السكانية وسوق العمل؛ وبناء عليه تراجع حجم التحويلات الماليه المتسربة للخارج من اقتصاد الدولة([2]).

كما أشار البعض إلى أن الاعتماد المفرط على الالآت الذكية قد يؤدي إلى إنفصال الإنسان عن محيطه الاجتماعي وبيئته، وانفصاله عن غيره، فيغرق في فرديته المفرطة، وقد وصل التخوف لدى البعض إلى القول بهيمنة الالآت الذكية واندثار الإنسان، ونهاية الجنس البشري، وقد تتمكن الالآت الذكية من التواصل فيما بينها وتكوين عقل خاص بها، وتشرع في التمرد والخروج عن سيطرة الإنسان، وإذا لم يكن ذلك تصرف ذاتي لهذه الالآت فقد يكون من خلال تنظيم إجرامي إلكتروني يتلاعب في شبكات التواصل بين الالآت الذكية ويغير في برمجتها، ويسيطر عليها؛ بحيث تنفذ مخططاته الإجرامية، وقد يصل الأمر إلى الكارثة إذا حدث ذلك بالنسبة

[1]) إيهاب خليفة، الذكاء الاصطناعي: تأثيرات تزايد الاعتماد على التقنيات الذكية...، مرجع سابق، ص٣.

[2]) أحمد ماجد، مرجع سابق، ص١٨.

للروبوتات المقاتلة والطائرات بدون طيار المزودة بأسلحة مدمرة، ولاشك أن هذا التخوف تغلب عليه المبالغة في تقدير خطر تقنيات الذكاء الاصطناعي على البشر([1]).

ومع ذلك فقد صرح بعض المتخصصين في مجال هذه التقنيات بضرورة الحد من تطور قدرات الذكاء الاصطناعي، ووضع ضوابط وقيود على فكرة استقلاليته عن تدخل الإنسان. وقد لفت البعض الانتباه إلى أن خوارزميات التعلم في تقنيات الذكاء الاصطناعي تنطوي على ثغرات في تغذية البيانات؛ حيث ذكر أنها ليست محصنة ضد الاختراق، مما يقتح الباب أمام هجوم المستخدمين من أصحاب الأغراض الخبيثة([2]).

ويمكن التأكيد على أن أهم وأخطر تداعيات استخدام تقنيات الذكاء الاصطناعي في كافة جوانب الحياة: الشخصية والحكومية، المهنية والترفيهية، المدنية والعسكرية،

[1]) انظر: سعيد عبيدي، خطر الالآت الذكية على الإنسان، مجلة الوعي الإسلامي، السنة ٥٥، العدد ٦٣٣، جمادى الأولى، ١٤٣٩هـ، يناير ٢٠١٨م، ص٢٩، د/ سعيد خلفان الظاهري، مرجع سابق، ص٦.

[2]) مثال على ذلك: في تطبيق روبوت الدردشة (Tay) فإن قدرته على التعلم والاستجابة لميول وتفضيلات المستخدمين مكنت مستخدمي تويتر من التلاعب بتقنية (Tay) مما تتسبب في إصدار الروبوت سلسلة من العبارات والألفاظ البذيئة؛ وفسر بعض المتخصصين ذلك بأن هذه التقنية في تجربتها لم تأخذ بعين الاعتبار الحداثة في سياقها الجديد.

Lee, Peter, "Learning from Tay's introduction" blog, Microsoft website, March 25, 2016. As of December 5, 2016:
http://blogs.microsoft.com/blog/2016/03/25/learning-tays-introduction/#sm.0001
v8vtz3qddejwq702cv2annzcz

الشرطية والقضائية يتمثل في قابلية برمجة هذه التقنيات إلى الاختراق وتعرضها للتهديدات والهجمات السيبرانية، فلنا أن نتخيل حجم الكارثة المترتبة على هذه الاختراقات والهجمات على كافة الأصعدة والمستويات، نعتقد أن الأمر يفوق تخيلاتنا المحدودة، وعلى سبيل المثال، مدى تخيل الأثار الأمنية المترتبة على اختراق تقنيات الذكاء الاصطناعي على الأمن القومي، كذلك الحال اختراق برمجة المركبات المستقلة ذاتية القيادة، ومدى خطورتها في تعريض حياة الأفراد للخطر، لاسيما إذا أدى الاختراق إلى تعطيل أجهزة الاستشعار، أو الكبح، أو نظام تحديد المواقع العالمي (GPS)، وعلى مستوى حقوق الأفراد، نجد أن الاختراق السيبراني يمثل تهديدا خطيرا لحق الأشخاص في الخصوصية وحرمة الحياة الخاصة، كما لو حدث اختراق لتقنية التعرف على الوجه، ومدى تهديد حق الأشخاص في الصورة.

كما أشارت شركة (IBM) إلى أن تطبيق Watson للأمن السيبراني يحتاج إلى التدريب باستخدام البيانات لتقديم رؤى واضحة لتحديد سيناريوهات التهديدات والهجمات السيبرانية المحتملة، وهناك كثيرون مهتمون بإساءة استخدام الذكاء الاصطناعي لتحقيق غاياتهم الخاصة؛ لذلك نجد أن تطبيقات الذكاء الاصطناعي هي مجرد أداة يمكن الاستفادة منها للعمل الجيد أو الضار([1]).

ما يؤكد خطورة قابلية تقنيات الذكاء الاصطناعي للاختراق، حرص المشرع بإمارة دبي على إفراد نصاً خاصاً أدرج فيه أفعال التدخل غير المشروع التي تعرض سلامة الطيران المدني والنقل الجوي للخطر، ومنها السيطرة على الطائرة بدون طيار أو

[1]) Jeff Crume, Doug Lhotka, Carma Austin, op. cit., P:6 .

اختراق أنظمة تشغيلها بصورة غير مشروعة([1]). كما أفرد نصاً خاصاً لحظر استخدام تقنية الطائرات بدون طيار في انتهاك الخصوصية وسرية البيانات التي تتمتع بالحماية القانونية([2]). كما صدر المرسوم بقانون اتحادي رقم ٢٦ لسنة ٢٠٢٢م في شأن تنظيم الاستخدام المدني للطائرات بدون طيار والأنشطة المرتبطة بها، وقد نص في المادة (٩) على الأفعال والأنشطة المحظورة بما يضمن الحفاظ على الخصوصية ومنها في البند (٣): "تركيب أو تجهيز الطائرات بدون طيار بآلات التصوير أو أيّ أجهزة أو معدات أخرى قد تستخدم للتصوير أو التسجيل".

الفرع الثالث

تقييم فاعلية وموضوعية نتائج تقنية التحليلات التنبؤية

على الرغم من أن الكثيرين يضعون ثقتهم في فاعلية وموضوعية تقنية التحليلات التنبؤية في مجال العدالة الجنائية في تحديد درجة احتمالية العودة للإجرام، خاصة عن إصدار قرار بإطلاق السراح المشروط، كما يضعون ثقتهم في فاعلية وموضوعية نتائج تقنيات التنبؤ بالجريمة، بالنسبة للأشخاص الذين يحتمل ارتكابهم جرائم، أو بالنسبة للأماكن والمناطق السكنية التي يحتمل وقوع جرائم معينة فيها وفق بيانات تتعلق بسلوكيات الأشخاص المقيمين فيها، وطبائعهم، ودخولهم، ومستواهم الثقافي والإجتماعي إلى غير ذلك– على الرغم من ثقة هذا الجانب في نتائج هذه التقنيات

[1]) المادة (٣٥) من قانون تنظيم الطائرات بدون طيار بإمارة دبي رقم ٤ لسنة ٢٠٢٠م.

[2]) المادة (٣٦) من القانون المذكور.

نجد في جانب آخر من يثيرون المخاوف من مخاطر تقييم التقنيات التحليلية التنبؤية باحتمالية العودة للإجرام أو التنبؤ بارتكاب جريمة من شخص أو أشخاص معينين.

أولًا- تقييم فاعلية وموضوعية تقنيات احتمالية العودة للإجرام:

أشرنا من قبل أن استخدام تقنيات الذكاء الاصطناعي في مجال التنبؤ بالجريمة أضحى من أسس العمل الشرطي في العديد من دول العالم، ومنها: دولة الإمارات العربية المتحدة، التي اعتمدت العديد من خوارزميات الذكاء الاصطناعي للأنشطة التنبؤية بالجرائم والأفعال غير المشروعة، لاسيما التحريض على الإرهاب والعنف، إلا أن العديد من الدراسات التي أجريت على تجربة الولايات المتحدة في تطبيق تقنيات التنبؤ بالجريمة قد حذرت من مخاطر التحيز غير المنصف لخوارزميات هذه التقنيات.

كما أشرنا إلى أن نظام العدالة الجنائية في الولايات المتحدة يلجأ بصورة متزايدة إلى أدوات خوارزمية في مرحلة إطلاق السراح المشروط([1]) وقد أشرنا إلى أن التقرير المفصل عن نظام تقييم المخاطر الجنائية المتعلقة بأنماط إدارة الجناة الإصلاحية للعقوبات البديلة (COMPAS) ويستخدم هذا التطبيق في جلسات الحكم وإطلاق السراح المشروط، نجد من الأهمية الوقوف على بعض ما جاء بهذا التقرير لأهميته في وضع اليد على مخاطر الاعتماد على تقنيات الذكاء الاصطناعي في التنبؤ

[1]) Osonde A. Osoba, William Welser IV, op. cit., P: 13.

بالجريمة أو العودة إلى الإجرام باعتباره أحد أهم الأنشطة الشرطية في مكافحة الجريمة والحد من انتشارها في المجتمع([1]).

عرض مؤلفو التقرير وقائع عديدة تم فيها تطبيق خوارزمية تقييم المخاطر والتي يتم استخدامها لإبلاغ القرارات حول من يمكن إطلاق سراحه في كل مرحلة من مراحل نظام العدالة الجنائية؛ حيث يقدم التطبيق قرارا بنتيجة التنبؤ باحتمالية ارتكاب جريمة في المستقبل، مع تقييم احتياجات المجرم لإعادة التأهيل.

وقد حذر المدعي العام الأمريكي عام ٢٠١٤م، من أن تقييم المخاطر قد يؤدي إلى تحيز المحاكم، ودعا لجنة القضاء الأمريكي إلى دراسة استخدامها، وذكر أنه على الرغم من أن هذه الإجراءات قد صيغت بنوايا حسنة، إلا أنني أشعر بالقلق من أنها قد تقوض –عن غير قصد– جهودنا لضمان العدالة الفردية والمتساوية، كما أضاف أنها قد تؤدي إلى تفاقم التباين غير المبرر وغير المنصف الذي أصبح شائعا جدا في نظام العدالة الجنائية في مجتمعنا.

وقد أشار التقرير أنه بالحصول على تقييمات المخاطر المخصصة لأكثر من سبعة آلاف شخص تم القبض عليهم في مقاطعة برووارد بولاية فلوريدا في عامي ٢٠١٣ م و ٢٠١٤م وبالفحص لمعرفة عدد المتهمين بارتكاب جرائم جديدة على مدار العامين

[1])Angwin, Julia, Jeff Larson, Surya Mattu, and Lauren Kirchner, "Machine Bias: There's Software Used Across the Country to Predict Future Criminals. And It's Biased Against Blacks," ProPublica, May 23, 2016. As of December 5, 2016:
https://www.propublica.org/article /machine-bias-risk-assessments-in-criminal-sentencing

المقبلين، وهو نفس المعيار الذي استخدمه مبتكرو الخوارزمية؛ ثبت أن النتيجة غير موثوقة بشكل ملحوظ في التنبؤ بجرائم العنف: فقط ٢٠% من الأشخاص الذين توقعوا ارتكاب جرائم عنيفة استمروا في فعل ذلك. كما اكتشف وجود فوارق عرقية كبيرة في نتائج التقييم، تمامًا كما كان يخشى المدعي العام الأمريكي؛ حيث تم تصنيف المتهمين البيض بشكل خاطئ على أنهم منخفضو المخاطر أكثر من المتهمين السود.

ونظرا لأن القرارات الرئيسية في نظام العدالة الجنائية في أيدي البشر الذين يسترشدون بغرائزهم وتقديراتهم وتحيزاتهم الشخصية بينما إذا تمكنت برامج الحاسب الآلي من التنبؤ بدقة أكثر بالمتهمين الذين من المحتمل أن يرتكبوا جرائم جديدة في المستقبل فقد يكون نظام العدالة الجنائية أكثر إنصافاً، بينما إذا كان هناك خطأ في تقييم المخاطر فقد يؤدي ذلك إلى إطلاق سراح المجرم الخطير، في حين قد يؤدي إلى تلقي شخص ما بشكل غير عادل لحكم أقسى، أو انتظار فترة أطول للإفراج المشروط عما هو مناسب لخطورته.

وقد تناول (Larson) وآخرون التقرير السابق بالدراسة والتحليل واكتشفوا أن التقرير يؤكد على أن خوارزمية تقييم المخاطر واحتمالية العودة للجريمة انتابها التحيز وعدم الانصاف؛ حيث إن المتهمين السود كانوا أكثر عرضة لسوء التصنيف من المتهمين البيض بمقدار النصف في بحث ارتفاع احتمالات معادوة الإجرام العنيف، بينما تمت

إساءة تصنيف معاودي الإجرام من البيض كمصدر خطر متدني بنسبة ٦٢,٣% في كثير من الأحيان عن المتهمين السود([1]).

وقد علق كل من (Osonde A. Osoba, William Welser IV) على أن التقدم الحالي في مجال تقنيات الذكاء الاصطناعي ربما سيجعل من إضفاء الصفات البشرية عليها أقرب إلى الوضع الطبيعي السائد. ولعل هذا سيسفر عن منافع غير متوقعة مثل تعزيز فهم المتعاملين مع تقنيات الذكاء الاصطناعي بوصفها غير منزهة عن التحيزات، مثلها مثل البشر([2])؛ حيث بدأت تتلاشى وبسرعة فكرة الآلات الذكية الخالية من المشاعر والتي تتخذ قرارات خالية من التحيز، هذا ما دفع البعض الى التساؤل مرة أخرى هل تقنيات الذكاء الاصطناعي في التنبؤ بالجريمة عادلة أم متحيزة؟

ربما كان أكثر العيوب العامة لهذا التصور هو تحقيق ProPublica لعام ٢٠١٦ الذي خلص إلى أن البيانات التي تقود تقنيات الذكاء الاصطناعي التي يستخدمها القضاة لتحديد ما إذا كان من المحتمل أن يرتكب المجرم المدان المزيد من الجرائم في المستقبل بدت متحيزة ضد الأقليات. ورغم معارضة شركة Northpointe، الشركة التي أنتجت الخوارزمية المعروفة باسم COMPAS، تفسير ProPublica للنتائج،

[1]) Larson, Jeff, Surya Mattu, Lauren Kirchner, and Julia Angwin, "How We Analyzed the COMPAS Recidivism Algorithm," ProPublica, May 23, 2016. As of December 6, 2016:
https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm

[2]) Osonde A. Osoba, William Welser IV, op. cit., P: 26.

مما أثار جدلاً وتحليلاً حول مقدار الثقة في نتائج تقييم تقنيات الذكاء الاصطناعي التنبؤية([1]).

ثانياً تقييم فاعلية وموضوعية تقنيات التنبؤ بالجريمة:

لا يقف الأمر عند استخدام خوارزميات الذكاء الاصطناعي في تقييم مخاطر احتمالية ارتكاب جريمة في المستقبل في جلسات إطلاق السراح المشروط وإصدار الأحكام، وإنما تلجأ أجهزة الشرطة إلى أدوات خوارزمية للقيام بأعمال الشرطة التنبؤية بالجريمة وتخصيص وتوزيع قوات ضبط وإنفاذ القانون؛ إلا أن نتائج هذه الخوارزمية قد تكون غير منصفة.

ويعرض كل من (Osonde A. Osoba, William Welser IV) مثالا على أن الخوارزمية المقبولة رياضيا قد تؤدي إلى سلوك غير منصف لأعمال الشرطة، مثل الخوارزمية الرياضية التي تعتمد على البيانات التاريخية للجرائم يمكن أن تؤدي إلى سلوك غير منصف. مثال على ذلك: نفترض أن لدينا مجموعة من السكان مقسمة بشكل طبيعي إلى فئات (مثل الموقع، الجنس، نوع الجريمة، أو أي معيار آخر) وأن لدينا قوات محدودة لإنفاذ القانون لا يمكنها اكتشاف جميع الحوادث الإجرامية والاستجابة لها وبالتالي بالنسبة لسكان يعانون من معدل جريمة معين، سنكتشف انتهاكات وسنطبق القانون باحتمالية معينة ويحدد مقياس الاحتراس مقدار الاهتمام

[1]) Randy Rieland, Artificial Intelligence Is Now Used to Predict Crime. But Is It Biased?, MARCH 5, 2018, available at: https://www.smithsonianmag.com/innovation/artificial-intelligence-is-now-used-predict-crime-is-it-biased-180968337/11/1/2021

الذي نوليه في مختلف الفئات، ومن ثم احتمال الاكتشاف الناجع للجرائم ومقاضاة مرتكبيها حال ارتكابها، وتتكيف درجة احتراس النظام باستخدام الخوارزمية الرياضية فيزيد النظام من درجة الاحتراس في المناطق التي تزداد فيها ملاحظة النزعة الإجرامية أو في المناطق التي يرتفع فيها نشاط إنفاذ القانون استنادا إلى بيانات الإنفاذ المسجلة سابقا([1]).

إن الخوارزمية الموصوفة هي أكثر من مجرد أداة توضيحية، فهي تحاكي تأثير المراقبة غير المنصفة والمجردة من المبادئ التي تقوم بها الدولة استنادا إلى السجلات التاريخية، وتفيد المحاكاة بأن ازدياد المراقبة التي تقوم بها الدولة ليس أداة محايدة خاصة إذا لم تطبق بشكل موحد، وعلى مستوى الشرائح السكانية ككل، يمكن أن يؤدي ذلك إلى التجريم غير المنصف؛ حيث يكون للمجرمين من مختلف الخصائص الديموغرافية احتمالات مختلفة بشكل منهجي للاعتقال وأحكام بالسجن متفاوتة الشدة، ويرى بعض فقهاء القانون أن التجريم غير المنصف بات هو الموقف السائد في الولايات المتحدة، وغالبا ما يتم تبريره استنادا إلى سجلات تاريخية للجريمة، كما كان الحال في نظام أنماط إدارة الجناة الإصلاحية للعقوبات البديلة (COMPAS) وقد عثرت وزارة العدل الأمريكية (٢٠١٦)على مزيد من الأدلة على هذه المراقبة وهذا التجريم غير المنصفين في التحقيق الذي أجرته مؤخرا في جهاز شرطة بالتيمور([2]).

[1]) Osonde A. Osoba, William Welser IV, op. cit., P: 14.
[2]) ibid, P: 15.

وقد أثار الاتحاد الأمريكي للحريات المدنية [ACLU] ومركز (Brennan) للعدالة والعديد من منظمات الحقوق المدنية تساؤلات حول مخاطر التحيز في البرمجيات، يؤكد النقاد أن البيانات المستمدة من ممارسات الشرطة يمكن أن توجد حلقة تغذية راجعة feedback تتخذ من خلالها الخوارزميات التنبؤية قرارات تعكس وتعزز المواقف حول أي المناطق السكنية سيئة وأيها صالحة؛ هذا هو السبب في –من وجهة نظرهم– أن الذكاء الاصطناعي المستند إلى بيانات الاعتقالات يحمل في طياته خطرًا أكبر من التحيز – فهو أكثر انعكاسًا لقرارات الشرطة([1]).

إذا كانت هناك أداة تنبؤية تثير توقعات الجرائم في منطقة سكنية معينة، فهذا يطرح تساؤلا في غاية الأهمية، هل ستكون الشرطة التي تقوم بدوريات في هذه المنطقة–بناء على هذه التنبؤات– أكثر عدوانية أو تحيزا في تنفيذ الاعتقالات؟ إن معالجة قصور تقنيات الذكاء الاصطناعي سيتطلب المزج بين المقاربات التقنية وغير التقنية، وثمة جهود حديثة تُجرى لتطوير أساليب تعلم آلي عادلة ومسؤولة وشفافة، اقترح (Dwork) وآخرون استخدام مقاييس المسافة أو التشابه المعدلة عند التعامل مع بيانات الأشخاص، والهدف من مقاييس التشابه هو تطبيق قيود عدالة صارمة عند مقارنة الأشخاص في مجموعات البيانات([2]).

---

[1]) Randy Rieland, Artificial Intelligence Is Now Used to Predict Crime. But Is It Biased?op. cit.

[2]) Dwork, Cynthia, Moritz Hardt, Toniann Pitassi, Omer Reingold, and Richard Zemel, “Fairness Through Awareness,” Proceedings of the 3rd Innovations in Theoretical Computer Science Conference, Cambridge, Mass., January 8–10, 2012, pp. 214–226.

كما اقترح (Sandvig) وآخرون عددا من خوارزميات إجراءات التدقيق التي تقارن بين مخرجات الخوارزميات والسلوك المنصف المتوقع، فيمكن أن تكون عمليات التدقيق المعتمدة على الخوارزميات أكثر جدوى ودقة عندما تكون رموز وإجراءات الخوارزميات مفتوحة المصدر([1]).

وطرح (DeDeo) مقاربة خوارزمية لضمان أن نماذج التعلم الآلي تفرض الاستقلالية الإحصائية بين النتائج والمتغيرات المحمية([2]). وينتهي كل من (Osonde A. Osoba, William Welser IV) في تقريرهما إلى القول بأن الأبحاث التقنية في مجال خوارزميات الذكاء الاصطناعي والتعلم الذاتي ينتظرها الكثير، كما أن مسألة التحيز والأخطاء الخوارزمية تتطلب منهجاً مختلفا من مصممي هذه الخوارزميات، مع ضرورة قيام هؤلاء بتنويع الخصائص الديموغرافية عند دمجها في الخوارزمية، مع تنويع خيارات التصميم.

هذا مع ضرورة وجود جرعة من القيود التنظيمية من أجل تحقيق التوازن مع التوجه نحو تدابير معالجة التحيز في الخوارزميات، فأي نوع من العلاج سيتطلب أن تلتزم الخوارزميات بصورة أوثق بالقيمة الاجتماعية. فما هذه القيم؟ ومن سيقررها؟ فمع

[1]) Sandvig, Christian, Kevin Hamilton, Karrie Karahalios, and Cedric Langbort, "Auditing Algorithms: Research Methods for Detecting Discrimination on Internet Platforms," paper presented to the Data and Discrimination: Converting Critical Concerns into Productive Inquiry preconference of the 64th Annual Meeting of the International Communication Association, Seattle, Wash., May 22, 2014.

[2]) DeDeo, Simon, "Wrong Side of the Tracks: Big Data and Protected Categories," Ithaca, N.Y.: Cornell University Library, May 28, 2015. As of March 7, 2017:
https://arxiv.org/pdf/1412.4643v2.pdf

استغراق المجتمع أكثر وأكثر في هذا المجال، سينبغي تناول مسائل حرية التعبير، والرقابة، والإنصاف، وغيرها من المعايير الأخلاقية المقبولة([1]).

[1]) Osonde A. Osoba, William Welser IV, An Intelligence in Our Image, The Risks of Bias and Errors in Artificial Intelligence, op. cit., P: 24.

الفصل الأول
مخاطر الاختراق الإلكتروني لتقنيات الذكاء الاصطناعي وصور مواجهته.

تمهيد:

يعد الاختراق الالكتروني من أهم وأخطر التحديات التي تواجه الاستخدامات المتزايدة لتقنيات الذكاء الاصطناعي، بل يمثل تهديداً جسيماً قد يجعل هذه الاستخدامات، لاسيما في العمل الشرطي والقضائي، مصدر قلق شديد للدول التي اتجهت بقوة للاعتماد عليها.

وجدير بالذكر أن أغلب التشريعات الجزائية رصدت عقوبات مغلظة لأفعال الاختراق الالكتروني للأنظمة المعلوماتية، والشبكات، ومنها قانون مكافحة جرائم تقنية المعلومات المصري، رقم١٧٥ لسنة ٢٠١٨م، والذي جرم الولوج غير المصرح به أو غير المسموح به لأنظمة تقنية المعلومات أو لشبكات المعلوماتية، أو الولوج بتجاوز حدود التصريح أو الإذن، كذلك القانون الإماراتي رقم ٣٤ لسنة ٢٠٢١م، في شأن مكافحة الشائعات والجرائم الإلكترونية، وعليه نخصص هذا الفصل لدراسة مخاطر الاختراق الالكتروني الواقع على تقنيات الذكاء الاصطناعي، من خلال الوقوف على تعريفه، وأنواعه، ومراحله، مع البحث عن صور المواجهة التقنية والتشريعية.

تقسيم:

نقسم هذا الفصل على النحو الآتي:

المبحث الأول: التعريف بالاختراق الإلكتروني والمكافحة التقنية والتشريعية.

المبحث الثاني: مخاطر الاختراق الإلكتروني على الأمن المعلوماتي والقومي.

المبحث الثالث: المواجهة التشريعية للاختراق الإلكتروني لتقنيات الذكاء الاصطناعي.

المبحث الأول

التعريف بالاختراق الإلكتروني وكيفية التصدي تقنياً وتشريعياً.

تمهيد:

جدير بالذكر أن الكثير من التشريعات الخاصة بمكافحة الجرائم الإلكترونية حرصت على وضع تعريف تشريعي محدد للإختراق الإلكتروني، مع الاختلاف في المصطلح المستخدم، فقد عبر عنه البعض بمصطلح (الاختراق الالكتروني) بينما عبر عنه البعض بمصطلح (الدخول غير المشروع) أو (الدخول غير المصرح به). كما حرص الفقه الجنائي إلى وضع تعريفات فقهية لمصطلح الاختراق الإلكتروني، كما عرض المختصصون في مجال تقنية المعلومات أنواع الإختراق بالنظر إلى الأجهزة محل الاختراق. وسعياً وراء بيان مخاطر الاختراق الإلكتروني الواقع على تقينات الذكاء الاصطناعي وصور مكافحته يرى الباحث أنه من الأهمية بمكان الوقوف على تعريفه وأنواعه، على التقسيم الآتي:

تقسيم:

نقسم هذا المبحث إلى المطالب الثلاثة الآتية:

المطلب الأول: تعريف الإختراق الإلكتروني وأنواعه.

المطلب الثاني: مراحل الإختراق الإلكتروني وسبل المكافحة التقنية.

المطلب الثالث: صور المواجهة التشريعية للاختراق الإلكتروني.

المطلب الأول

تعريف الإختراق الإلكتروني وأنواعه.

إن وضع تعريف محدد للاختراق الإلكتروني من الموضوعات التي حظت بإهتمام المتخصصين في مجال تقنية المعلومات، ورجالات الفقه الجنائي، ثم حرص العديد من التشريعات الخاصة بجرائم تقنية المعلومات أو الجرائم الإلكترونية على وضع تعريف محدد لمصطلح الاختراق أو الدخول غير المصرح به، من هذه التشريعات المرسوم بقانون اتحادي رقم ٣٤ لسنة ٢٠٢١م في شأن مكافحة الشائعات والجرائم الالكترونية، وقانون مكافحة جرائم تقنية المعلومات المصري رقم ١٧٥ لسنة ٢٠١٨م، نعرف في الفرع الأول من هذا المطلب لتعريفات الاختراق الالكتروني، ثم نعرض لأنواعه على النحو الآتي.

الفرع الأول

تعريفات الاختراق الإلكتروني

أولاً– التعريف الفقهي:

عرفه البعض بأنه الدخول غير المصرح به لنظام معلوماتي أو شبكة معلوماتية أو أي وسيلة من وسائل تقنية المعلومات، وبطريقة غير مشروعة، لتحقيق أغراض غير مشروعة، سواء لغرض الحصول على المعلومات، أو إفشاءها أو محوها أو تحريفها والتلاعب فيها أو لغرض تدمير النظام المعلوماتي أو تعطيله أو تعطيل خدمات الشبكة المعلوماتية أو وسيلة تقنية المعلومات، حيث يمكن للمخترق التلاعب بمحتوى

النظام المعلوماتي أو تدميره، أو رزع برامج خبيثة على الشبكة المعلوماتية تنتقل إلى الأجهزة المستخدمة للشبكة([1]).

نلاحظ أن المخترقين المخربين لنظم المعلومات والشبكات المعلوماتية ووسائل تقنية المعلومات يطلق عليهم (Crackers) وهو مصطلح مأخوذ من فعل (Crack) يعني الكسر والتحطيم، بينما يطلق مصطلح (Hackers) على المخترقين بغرض الحصول على المعلومات أو البيانات الحكومية أو الشخصية بهدف انتهاك سريتها وخصوصيتها دون المساس بها أو اتلافها.

ثانياً- التعريف التشريعي:

عرفه المشرع المصري بأنه: "الدخول غير المرخص به أو المخالف لأحكام الترخيص، أو الدخول بأي طريقة غير مشروعة إلى نظام معلوماتي أو حاسب آلي أو شبكة معلوماتية وما في حكمها"([2]). نفس التعريف ورد بالقانون الاماراتي، مع اختلاف بسيط في الصياغة، حيث عرفه بأنه: "الدخول غير المرخص به أو المخالف لأحكام الترخيص أو الدخول بطريقة غير مشروعة أو البقاء بصورة غير مشروعة في نظام معلوماتي أو حاسب آلي أو نظام تشغيل جهاز أو آلة أو مركبة أو شبكة معلوماتية وما في حكمها"([3]). نلاحظ أن المشرع الإماراتي فصّل في صور النظم

---

[1]) انظر: د/ عماد عبد الستار طه زيدان، الثغرات الأمنية فى مواقع الويب: دراسة تطبيقية على مواقع أقسام المكتبات والمعلومات المصرية، المجلة الدولية لعلوم المكتبات والمعلومات، الجمعية المصرية للمكتبات والمعلومات والأرشيف، المجلد ٥، العدد ٤، ديسمبر ٢٠١٨م، ص١٧٥.

[2]) المادة الأولى من القانون رقم ١٧٥ لسنة ٢٠١٨م في شأن مكافحة جرائم تقنية المعلومات.

[3]) المرسوم بقانون اتحادي رقم ٣٤ لسنة ٢٠٢١م في شأن مكافحة الشائعات والجرائم الالكترونية.

المعلوماتية التي تكون عرضة للاختراق، وفي مجال بحثنا نجد المشرع الإماراتي يذكر صراحة، الاختراق الواقع على جهاز أو آلة أو مركبة، بما يشمل اختراق تقنيات الذكاء الاصطناعي التي تعتمد على النظم المعلوماتية، مثل: الروبوت الذكي، السيارة ذاتية القيادة، والطائرة المسيرة ذاتياً.

بينما نجد المشرع الكويتي يستعمل مصطلح (الدخول غير المشروع) للتعبير عن الاختراق الإلكتروني، وعرفه بأنه "النفاذ المتعمد غير المشروع لأجهزة وأنظمة الحاسب الآلي أو لنظام معلوماتي أو شبكة معلوماتية أو موقع إلكتروني من خلال اختراق وسائل وإجراءات الحماية لها بشكل جزئي أو كلي لأي غرض كان بدون تفويض في ذلك أو بالتجاوز للتفاوض الممنوح"([1]).

الفرع الثاني

أنواع الاختراق الإلكتروني

يتنوع الاختراق الالكتروني بالنظر إلى محل الاختراق، سواء شمل الأجهزة الخادمة أو الأجهزة الشخصية، وسواء وقع الاختراق على الشبكة المعلوماتية إلى:

أ) اختراق الأجهزة الخادمة:

يشير المتخصصون في علوم تقنية المعلومات والحاسبات إلى أن اختراق الأجهزة الخادمة يتم بأسلوب المحاكاة، وهو أسلوب يتضمن انتحال شخصية مسموح بها

[1]) المادة الأولي من القانون الكويتي رقم ٦٣ لسنة ٢٠١٥م في شأن مكافحة جرائم تقنية المعلومات.

بالدخول إلى هذه الأجهزة باستخدام طريقة يطلق عليها (مسارات المصدر) ويتم فيها إعطاء حزم IP شكلا معينا لتبدو وكأنها صادرة عن كمبيوتر شخص مسموح له الدخول إلى تلك الأجهزة([1]). وقد أشارت دراسة حول مخاطر اختراق أنظمة الطائرات بدون طيار إلى إمكانية قيام شخص ما ليس مخولا بالانتحال مدعيا بأنه الجهاز المتلقي المعتمد لبيانات الطائرات بدون طيار، وفي حالة الأمن السيبراني المرتبط بأنظمة الطائرات بدون طيار قد تكون هذه الطائرات هدفًا للاختراق الإلكتروني([2]).

ب) اختراق الأجهزة الشخصية:

نظرا لتقصير العديد من أصحاب الأجهزة الحاسوبية الشخصية في توفير الحماية التقنية لأجهزتهم بل تفريطهم في ذلك إلى حد إهمال وضع برامج حماية تقنية لذلك نجد هذا النوع من الاختراق سريع الانتشار.

ت) اختراق الشبكات المعلوماتية:

هو من أكثر أنواع الاختراق شيوعا بسبب تزايد المستخدمين لشبكات الإنترنت وشبكات الاتصالات، وبسبب ما تتضمنه من كم لا حصر له من المعلومات، وغالبا من يتم الاختراق في صورة اعتراض مراسلات البريد الإلكتروني الحكومية منها والشخصية، كذلك اعتراض مواقع الشراء والتسوق الإلكتروني بغرض الاستيلاء على أرقام بطاقات الائتمان الخاصة بالعملاء([3]).

---

[1]) د/ صلاح الدين محمد علي الفرجاني، مخاطر إختراق المواقع الإلكترونية، مجلة المصرفي، بنك السودان المركزي، العدد ٨٣، مارس ٢٠١٧م، ص٢٥.

[2]) KATHARINA LEY BEST and Others, op. cit., P: 7.

[3]) د/ صلاح الدين محمد على الفرجاني، المرجع السابق، ص٢٥.

المطلب الثاني

مراحل الاختراق الإلكتروني وسبل المكافحة التقنية

أهم ما يميز الاختراق الإلكتروني هو ارتكابه على مراحل معينة، ولاشك أن الإلمام بهذه المراحل يكفل الفهم الصحيح لمكافحته التقنية، على النحو التالي:

الفرع الأول

مراحل الاختراق الإلكتروني

يمر الاختراق الإلكتروني بعدة مراحل منها([1]):

أ) مرحلة الاستطلاع:

حيث يقوم المخترق بجمع أكبرقدر ممكن من المعلومات والبيانات عن الموقع المراد اختراقه، ويضع استراتيجية للهجوم، واختيار الاسلوب المناسب والطريقة المناسبة، ويتطلب هذا من المخترق تحليل البيانات والمعلومات التي حصلها حتى يتمكن من وضع يده على الثغرة الموجودة في نظام الحماية للموقع أو النظام المعلوماتي المراد اختراقه، وغالبا ما يقوم المخترق باستكشاف الموقع أو النظام المعلوماتي من الداخل أو الخارج، خاصة بالمناسبة للمواقع والأنظمة المعلوماتية التي يسمح للأفراد بالولوج إليها بقدر معين، ويحظر أكثر من ذلك، ومن خلال ذلك يحاول المخترق انتحال

[1]) عرضت بعض الدراسات مراحل الهجوم السيبراني أو الإلكتروني في سبع مراحل، وهي: الاستطلاع، التسليح، التسليم، الاستغلال، التركيب، القيادة، السيطرة، الإجراءات – للهجوم الإلكتروني. تمثل هذه المراحل سلسلة مرتبة حيث تمثل كل مرحلة إجراءً يتخذه الخصم بشكل حاسم. KATHARINA LEY BEST and Others, op. cit., P: ١٠.

شخصية أحد الأشخاص المخولين بالولوج أكثر للموقع أو النظام المعلوماتي، أو يحاول اختراق البريد الإلكتروني لأحد هؤلاء بغرض البحث عن معلومات خاصة باسم المستخدم وكلمة سر الخاصين بصاحب البريد الإلكتروني، وهنا يتم التحذير دائما من ترك هذه الرسائل المهمة على البريد الإلكتروني، سواء في صندوق الوارد أو حتى في سلة المهملات أو الرسائل المحذوفة أو الأرشفة([1]).

ب) مرحلة الفحص:

يتم ذلك بفحص الشبكة أو النظام المعلوماتي المراد اختراقه، وذلك باستخدام المعلومات والبيانات التي تم تجميعها في مرحلة الاستطلاع، وتستهدف مرحلة الفحص الوقوف على ثغرة في تأمين أو حماية الشبكة أو النظام المعلوماتي، وقد يستغرق هذا المزيد من الوقت والجهد والإصرار من المخترق، خاصة بالنسبة للشبكات والنظم المعلوماتية المؤمنة، وتعد مرحلة العثور على ثغرة في الشبكة هي المرحلة الأصعب والأهم لبدء الهجوم بالاختراق([2]).

ث) مرحلة الهجوم:

إذا تمكن المخترق مع العثور على ثغرة أو ثغرات في تأمين وحماية الشبكة أو النظام المعلوماتي المراد اختراقه يقوم بالهجوم على الشبكة سواء أكانت شبكة محلية تربط مجموعة من المستخدمين في نطاق معين، أو شبكة عامة، وسواء أكانت المواقع أو

[1]) د/ عماد عبد الستار طه زيدان، الثغرات الأمنية فى مواقع الويب...، المرجع السابق، ص٧٧.

[2]) د/ عماد عبد الستار طه زيدان، المرجع السابق، ص٧٧، د/ صلاح الدين محمد على الفرجاني، المرجع السابق، ص٢٧.

النظم المعلوماتية المراد اختراقها حكومية أم خاصة بالأفراد أو المؤسسات التجارية الخاصة([1]).

ج) مرحلة الولوج والبقاء:

بعد نجاح المخترق في شن الهجوم على الشبكة أو النظام المعلوماتي المراد اختراقه وتحديد نقاط الضعف وثغرات الحماية والتأمين يتمكن المخترق من الولوج إلى الشبكة أو النظام المعلوماتي بأسلوب أو أكثر من الأساليب والحيل المستخدمة في ذلك، ولا يقف الأمر عند حد الولوج وإنما يسعى المخترق إلى ضمان البقاء في الشبكة أو النظام المعلوماتي أطول مدة ممكنة حتى يتمكن من تحقيق مآربه وأغراضه، سواء كانت مجرد الحصول على البيانات والمعلومات الحساسة التي يسعى إليها، وإفشاؤها أو التغيير فيها أو تدمير وإتلاف البيانات والمعلومات التي يحتويها النظام المعلوماتي أو التلاعب فيها أو تدمير وإتلاف النظام المعلوماتي نفسه، أو الإضرار بالشبكة وتعطيل خدماتها([2]).

ح) مرحلة مسح أثر الولوج:

يشير المتخصصون([3]) إلى أن هذه المرحلة من الأهمية بمكان حيث تمكن المخترق من تكرار هجومه أكثر من مرة، خاصة المخترقين غير المخربين، أولئك الذين يسعون

---

[1]) د/ صلاح الدين محمد على الفرجاني، مخاطر اختراق المواقع الإلكترونية، مرجع سابق، ص٢٦.

[2]) د/ عماد عبد الستار طه زيدان، المرجع السابق، ص٧٨.

[3]) الموضع السابق.

إلى الحصول على البيانات والمعلومات بشكل مستمر من النظام المعلوماتي دون المساس بها أو التعدي على النظام نفسه، وبهذا يمكنه إذا استطاع أن يخفي أثر هجومه الأول ولم يتمكن مسؤول الحماية التقنية للشبكة أو النظام المعلوماتي من اكتشاف الهجوم الحاصل في هذه الحالة يستطيع المخترق تكرار هجومه دون رادع، خاصة إذا كان المسؤول عن الحماية والتأمين غافلا عن تحديث سبل الحماية والتأمين من حين لآخر. وفي دراسة أمريكية حديثة([1])عن مخاطر اختراق أنظمة الطائرات بدون طيار (UAS) أشارت إلى أنه مع تزايد انتشار الأجهزة الحاسوبية المتصلة، يزداد خطر حدوث الاختراق بأسلوب حقن دودة (أحد برامج الاختراق) بطائرات بدون طيار أو حدوث هجوم إلكتروني مماثل، كما أشارت إلى أن الهجوم قد لا يقتصر على شبكات وزارة الأمن الداخلي (DHS) والأجهزة المتصلة، وإنما قد يوجه إلى الأجهزة الشخصية لموظفي وزارة الأمن الداخلي (DHS) أو الشبكات المنزلية التي يمكن أن تكون نقاطا للوصول إلى رمز الدخول إلى أنظمة (DHS) إما لاسلكيًا أو عن طريق موظف يربط جهازًا مصابًا بأجهزة وزارة الأمن الداخلي (DHS).

الفرع الثاني

سبل المكافحة التقنية للاختراق الإلكتروني

تعتبر تقنيات الأمان الإلكتروني من الأدوات الحاسمة في مكافحة الاختراق والتهديد السيبراني المحتمل، وتساعد هذه التقنيات في حماية البيانات والأنظمة والشبكات

[1]) KATHARINA LEY BEST and Others, op. cit., P:xii.

المعلوماتية من خطر الهجمات السيبرانية المتطورة باستمرار، ومن أساليب المكافحة التقنية:

يعد أسلوب اختبار الاختراق من أكثر الأساليب فاعلية في مكافحة الاختراق الإلكتروني؛ حيث يستهدف الفحص المستمر للنظام المعلوماتي والشبكة المعلوماتية مدى قوة الحماية والتأمين، وهي طريقة تقنية من أجل تقييم النظام الأمني للشبكة المعلوماتية أو النظام المعلوماتي، وتتم باستهداف الحواسيب بمجموعة من الهجمات الإلكترونية المختلفة للتأكد من مدى قدرة النظام على التعامل مع هذه الهجمات بدون أدنى تأثير على أداءه وخدماته، ودون المساس بالمعلومات والبيانات التي يحتويها النظام؛ بحيث تكشف تلك الهجمات المفتعلة عن نقاط الضعف والثغرات التي تعتري النظام المعلوماتي أو الشبكة المعلوماتية المحمية([1]).

ومن اختبارات الاختراق الشائعة: اختبار الاختراق الأبيض، اختبار الاختراق الأسود، اختبار الاختراق الرمادي. يتم استخدام هذه التقنيات لتقييم قوة النظام الأمني وتحديد الثغرات التي يمكن استغلالها من قبل المهاجمين. يعتبر فهم هذه التقنيات واستخدامها أمرًا ضروريًا لفهم ومكافحة التهديدات السيبرانية بنجاح.

وقد عرضت دراسة عام ٢٠٢٠م عن مخاطر اختراق أنظمة الطائرات بدون طيار بعض السيناريوهات ضمن مكافحة الهجوم الإلكتروني؛ حيث ذكرت أنه يوجد تنوع كبير في كيفية اكتشاف تعرض الطائرة بدون طيار لخطر الاختراق الإلكتروني؛

[1]) د/ عماد عبد الستار طه زيدان، مرجع سابق، ص٧٦.

حيث يتخذ صانعو القرار موقف الخصم المهاجم في تحديد التهديدات التي لم يتم الكشف عنها، وتتيح سلسلة تهديد الأمن السيبراني للمستخدم تحديد متى وكيف يكون نظام معين عرضة للخطر ضمن سيناريو ما، وقد يتيح ذلك تصميم دفاع مستنير ضد تهديد سيبراني معين، وقد عرضت هذه الدراسة سبع مراحل للهجوم الإلكتروني، وهي: الاستطلاع، التسليح، التسليم، الاستغلال، التركيب، القيادة، السيطرة، والإجراءات. وتقدم كل مرحلة – من زاية أخرى– فرصة لاكتشاف الهجوم على نحو ما سبق([1])؛ ونظرًا لأن هذه المراحل متسلسلة، يرتبط الاكتشاف المبكر للهجوم السيبراني في أنظمة الطائرات بدون طيار بعواقب أقل اضطرابًا وإصلاحات أقل تكلفة؛ إذ إن الإجراء الدفاعي المناسب يعتمد على تحديد مكان وجود إجراء معين في السلسلة، وأن تحديد مكان وجود الطائرة بدون طيار في سلسلة قتل الأمن السيبراني يسهل اعتماد تدابير أمنية فعالة([2]).

بالإضافة إلى أسلوب اختبار الاختراق الإلكتروني يمكن الاستعانة بطرق وأساليب إلكترونية أخرى في سبيل مكافحة الاختراق سواء باستخدام تطبيقات الجدران النارية، بتأمين المنافذ التي تحصل من خلالها على خدمات الإنترنت، بما يشمل نظم التشغيل والتطبيقات المستخدمة. تعمل برمجيات الجدران النارية كمصفاة تمنع وصول الطلبات

[1]) KATHARINA LEY BEST and Others, op. cit., P:10.
[2]) ibid.

المشبوهة إلى الأجهزة المزودة. ويشير البعض إلى أن تطبيقات الجدارن النارية ليست الحل السحرى في الحماية من الاختراق، ويجب تطبيق سبل أخرى([1]).

المطلب الثالث

المواجهة التشريعية للاختراق الإلكتروني

ذكرنا –من قبل– أن العديد من التشريعات الجزائية ومنها القانون المصري في شأن مكافحة جرائم تقنية المعلومات، ونظيره القانون الاماراتي في شأن مكافحة الشائعات والجرائم والإلكترونية، وغيرهما من التشريعات التي واجهت الإختراق الإلكتروني بنصوص جزائية، عاقبت عليه بعقوبات وتدابير جزائية تتدرج بحسب خطورة فعل الإختراق على البيانات والمعلومات والمواقع محل الإختراق، والنتيجة المترتبة عليه، مع التمييز بين الإختراق الواقع على نظم معلوماتية حكومية أو الاختراق الواقع على نظم معلوماتية خاصة الأفراد، حيث غلظ عقوبة الأول، بالنظر إلى خطورته وجسامته.

الفرع الأول

مواجهة الإختراق الالكتروني في القانون المصري

نلاحظ أن المشرع المصري ميز في المعالجة بين اختراق المواقع والنظم المعلوماتية الخاصة بالأفراد والأشخاص الاعتبارية الخاصة، وبين اختراق تلك المواقع والنظم

[1]) للمزيد حول أساليب الحماية من الاختراق الإلكتروني راجع: د/ محمد محمد الألفي، الحماية القانونية لقواعد البيانات في نظم المعلومات، مرجع سابق، ص١٩٠ وما بعدها.

المعلوماتية التي تدار بمعرفة أو لحساب الدولة أو أحد الأشخاص الاعتبارية العامة أو مملوكا لها أو يخصها، حيث وصل بالتجريم في الفرض الثاني إلى حد الجناية، وعاقب على فعل الاختراق بالسجن والغرامة المغلظة.

فقد نصت المادة (١٤) من القانون المصري في شأن مكافحة الجرائم تقنية المعلومات([1]) على تجريم فعل الدخول غير المشروع لموقع أو حساب خاص أو نظام معلوماتي محظور الدخول عليه. وقررت عقوبة الحبس مدة لا تقل عن سنة ولا تزيد على ثلاث سنوات، والغرامة التي لا تقل عن ٥٠ ألف جنيه ولا تجاوز ١٠٠ ألف جنيه، أو إحدى العقوبتين.

وقد يقع ذلك الاختراق على نظم تقنيات الذكاء الإصطناعي والأنظمة الرقمية المملوكة للأفراد، أو المؤسسات والشركات الخاصة، من ذلك: أنظمة تشغيل الطائرات المسيرة ذاتياً، أو المركبات ذاتية القيادة، أو السفن والقطع البحرية ذاتية القيادة، والروبوتات الذكية التي تعمل في المنازل أو الشركات والمؤسسات الخاصة. وقد يقف فعل الجاني عند حد الاختراق دون تحقيق أي من النتائج المشددة للعقوبة، أي أن الجريمة تقف عند حد الدخول العمدي غير المصرح به، أو الدخول خطأً مع البقاء في النظام بدون وجه حق.

[1]) جاء بنصها: "يعاقب بالحبس مدة لا تقل عن سنة وبغرامة التي لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه أو بإحدى العقوبتين كل من دخل عمداً، أو بخطأ غير عمدي وبقى بدون وجه حق، على موقع أو حساب خاص أو نظام معلوماتي محظور الدخول عليه".

نلاحظ على معالجة المشرع المصري لجريمة الاختراق الالكتروني للنظم المعلوماتية أنه جعل من الجريمة جنحة مشددة، عاقب عليه بعقوبة سالبة للحرية قد تكون مناسبة لجسامة الفعل، خاصة أن العقوبة مقررة لمجرد الدخول غير المشروع دون أن يترتب عليه اتلاف أو تدمير أو نسخ أو أية صورة من صور النتيجة المشددة للعقوبة المنصوص عليها في الفقرة الثانية من المادة المذكورة.

كما نلاحظ أن المشرع المصري ساوى في العقوبة بين الدخول العمدي والدخول غير العمدي، إذا قام الجاني بالبقاء في النظام المعلوماتي بدون وجه حق، وعليه؛ يمكن القول بحسن مسلك المشرع في هذه الجزئية، بالنظر إلى أنه قد يحدث عملاً الدخول خطأً بغير عمد من الجاني، ولكنه يبقى في النظام المعلوماتي رغم علمه بعدم أحقيته أو بعدم مشروعية دخوله لهذا النظام، ومن ثم يكون بقائه في النظام مساوياً في التجريم لفعل الدخول المتعمد بدايةً.

ثم عاقب المشرع المصري بعقوبة أشد على فعل الدخول غير المشروع لنظام معلوماتي إذا نتج عنه إتلاف أو محو أو تغيير أو نسخ أو إعادة نشر للبيانات أو المعلومات الموجودة على ذلك الموقع أو في الحساب الخاص أو النظام المعلوماتي؛ حيث جعل العقوبة الحبس مدة لا تقل عن سنتين، وغرامة لا تقل عن مائة ألف جنيه، ولا تجاوز مائتي ألف جنيه، أو بإحدى هاتين العقوبتين.

هنا يمكن تصور حصول الدخول غير المشروع لنظم تقنيات الذكاء الاصطناعي بقصد تحقيق صورة من النتائج المشددة للعقوبة، لاسيما إتلاف أو محو أو تغيير البيانات، على سبيل المثال: السيارات ذاتية القيادة، لنا أن نتخيل حجم الخطورة إذا

حصل الاختراق مع إتلاف البيانات أو محوها أو تغييرها التي تتضمنها أو تعتمد عليها أنظمة تشغيل هذه النوعية من المركبات. كذلك لنا أن نتخيل حجم الضرر إذا حصل الاختراق مع القيام بنسخ البيانات التي تتضمنها أنظمة الروبوتات الذكية، وما يعد انتهاكا صارخاً للحق في خصوصية من له الحق في هذه البيانات والمعلومات، لاسيما روبوتات الخدمة المنزلية أو روبوتات الشركات والمؤسسات الخاصة؛ وعليه، نعتقد أن عقوبة الغرامة المقررة للجريمة غير متناسبة مع جسامة الفعل، لاسيما إذا نتج عن الفعل اتلاف أو محو أو تغيير أو نسخ أو إعادة نشر البيانات والمعلومات الموجودة على أنظمة تقنيات الذكاء الاصطناعي؛ لما قد يترتب عليه من خطورة أو ضرر لحق ذوي الشأن في الخصوصية وسرية البيانات والمعلومات المتعلقة بهم، لذا نوصي المشرع المصري بتغليظ مقدار الغرامة بما يتناسب مع جسامة وخطورة الجريمة.

بينما عالجت المادة (٢٠) من القانون المذكور في فقرتها الأولى جريمة الاختراق الالكتروني الواقع على موقع أو حساب أو نظام معلوماتي يدار بمعرفة الدولة أو لحسابها أو بمعرفة أو لحساب شخص من الأشخاص الاعتبارية العامة أو مملوكاً لها أو خاصاً بها، حيث عاقبت على فعل الدخول غير المصرح به المتعمد أو البقاء بدون وجه حق أو تجاوز حدود الحق في الدخول من حيث الزمان أو مستوى الدخول بالحبس مدة لا تقل عن سنتين والغرامة التي لا تقل عن خمسين ألف جنيه ولا تجاوز مائتي ألف جنيه، أو بإحدى هاتين العقوبتين. ثم شدد العقوبة في الفقرة الثانية منها إذا كان الاختراق بقصد الاعتراض أو الحصول بدون وجه حق على بيانات أو معلومات

حكومية؛ حيث جعل العقوبة السجن، والغرامة التي لا تقل عن مائة ألف جنيه، ولا تجاوز خمسمائة ألف جنيه، ثم شددت العقوبة أكثر في الفقرة الثالثة إذا ترتب على فعل الاختراق إتلاف هذه البيانات أو المعلومات، أو ترتب عليه تدميرها أو تشويهها أو تغييرها أو تغيير تصاميمها، أو نسخها أو تسجيلها أو تعديل مسارها أو إعادة نشرها، كلياً أو جزئياً؛ حيث غلظ المشرع عقوبة الغرامة، بحيث لا تقل عن مليون جنيه ولا تجاوز خمسة ملايين جنيه.

وقد يقع ذلك الاختراق على نظم تقنيات الذكاء الإصطناعي والأنظمة الرقمية المملوكة للدولة، أو الوزارات والهيئات الحكومية أو العامة، من ذلك: أنظمة تشغيل الطائرات المسيرة ذاتياً، أو المركبات ذاتية القيادة، أو السفن والقطع البحرية ذاتية القيادة، والروبوتات الذكية التي تعتمد عليها المؤسسات الحكومية والوزارات، من ذك: روبوتات الشرطة التي تقدم بعض الخدمات الشرطية للأفراد، مثل: تلقي البلاغات والشكاوى، سداد الفواتير والغرامات، كذلك المركبات الشرطية ذاتية القيادة في الدوريات الذكية.

لنا أن نتخيل حجم الخطر والضرر الذي قد ينجم عن اختراق أنظمة هذه التقنيات الذكية، وما قد يترتب عليه من تعرض البيانات والمعلومات الحكومية السرية للاتلاف أو المحو أو التغيير أو النسخ أو إعادة النشر، لاسيما البيانات الخاصة بالوزارات التي أخذت في الاعتماد بشكل متزايد على تقنيات الذكاء الاصطناعي والأنظمة الرقمية، مثل: وزارة الداخلية، والدفاع، والعدل، وغيرهم.

نلاحظ أن المشرع المصري لم يكتفِ بالعقوبات الأصلية السابق ذكرها، وإنما نص على بعض العقوبات الفرعية والتدابير الجنائية، من ذلك ما ورد النص عليه في المادة

(٣٨) من قانون مكافحة جرائم تقنية المعلومات، بوجوب الحكم بعقوبة المصادرة عند الإدانة([1])، ولكن بتحليل نص المادة المذكورة نجد أن معالجة المشرع المصري للمصادرة جاءت محل نظر، إذ أنه اشترط للقضاء بها عدم الإخلال بحقوق الغير حسن النية، يفهم من ذلك أن المشرع يأخذ في اعتباره حق الشخص حسن النية على الأشياء محل المصادرة، كما أنه من زاوية أخرى قصر القضاء بها في حالة الحكم بالإدانة،

الفرع الثاني

مواجهة الإختراق الإلكتروني في القانون الإماراتي

عالج المشرع الإماراتي جريمة الاختراق الإلكتروني بموجب نص المادة (٢) من المرسوم بقانون اتحادي رقم ٣٤ لسنة ٢٠٢١م؛ حيث جاء بنصها: "١- يعاقب بالحبس والغرامة التي لا تقل عن (١٠٠,٠٠٠) مائة ألف درهم ولا تزيد على (٣٠٠,٠٠٠) ثلاثمائة ألف درهم، أو بإحدى هاتين العقوبتين، كل من اخترق موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة معلومات أو وسيلة تقنية معلومات.

٢- وتكون العقوبة الحبس مدة لا تقل عن (٦) ستة أشهر والغرامة التي لا تقل عن (١٥٠,٠٠٠) مائة وخمسون ألف درهم ولا تزيد على (٥٠٠,٠٠٠) خمسمائة ألف

[1]) جاء بنصها: "مع عدم الإخلال بحقوق الغير حسن النية، على المحكمة في حالة الحكم بالإدانة في أي جريمة من الجرائم المنصوص عليها في هذا القانون أن تقضي بمصادرة الأدوات والآلات والمعدات والأجهزة مما لا يجوز حيازتها قانونا، أو غيرها مما استخدم في ارتكاب الجريمة أو سهل أو ساهم في ارتكابها".

درهم، أو بإحدى هاتين العقوبتين، إذا ترتب على الاختراق إحداث أضرار أو تدمير أو إيقاف عن العمل أو تعطيل موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة معلومات أو وسيلة تقنية المعلومات، أو إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو نسخ أو نشر أو إعادة نشر أو الحصول على أي بيانات أو معلومات أو خسارة سريتها.

١– وتكون العقوبة الحبس مدة لا تقل عن سنة والغرامة التي لا تقل عن (٢٠٠,٠٠٠) مائتي ألف درهم ولا تزيد على (٥٠٠,٠٠٠) خمسمائة ألف درهم، أو بإحدى هاتين العقوبتين، إذا كان الاختراق بغرض الحصول على البيانات أو المعلومات لتحقيق غرض غير مشروع".

من النص السابق نلاحظ أن المشرع الإماراتي استخدم مصطلح (اختراق) بخلاف المشرع المصري وغيره من المشرعين، ومنهم المشرع الكويتي، استخدم مصطلح الدخول غير المصرح به، ونعتقد أن حسن مسلك المشرع الإماراتي، بالنظر إلى المصطلح الأول أكثر دقة في التعبير عن مضمون السلوك الإجرامي المكون للجريمة، كما أن لفظ (اختراق) يعبر بذاته عن عدم مشروعية الولوج إلى الموقع أو النظام المعلوماتي، لا يحتاج إلى عبارة أو إية إضافة تعبر عن ذلك، كما هو الحال عند استخدام لفظ (الدخول) أو (الولوج) لابد من إضافة عبارة (غير مشروع) أو (غير مصرح به) أو (بدون حق).

كما نلاحظ أن المشرع الإماراتي –كما فعل نظيره المصري– خص المادة الثانية للاختراق الواقع على المواقع والأنظمة المعلوماتية الخاصة بالأفراد أو الأشخاص

الاعتبارية الخاصة، على الرغم من أن المشرع لم ينص على ذلك صراحة، إلا أنه يستوضح ذلك بمفهوم المخالفة، إذ أن المادة التالية (م٣) من ذات المرسوم عالج فيها المشرع الإماراتي الاختراق الواقع على المواقع والأنظمة الخاصة بمؤسسات الدولة، يراد بها الأشخاص الاعتبارية العامة، حيث جاء بنصها: "١. يعاقب بالسجن المؤقت والغرامة التي لا تقل عن (٢٠٠,٠٠٠) مائتي ألف درهم ولا تزيد على (٥٠٠,٠٠٠) خمسمائة ألف درهم، كل من اخترق موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة معلومات أو وسيلة تقنية معلومات عائدة لمؤسسات الدولة.

٢. وتكون العقوبة السجن مدة لا تقل عن (٥) خمس سنوات والغرامة التي لا تقل عن (٢٥٠,٠٠٠) مائتين وخمسين ألف درهم ولا تزيد على (١,٥٠٠,٠٠٠) مليون وخمسمائة ألف درهم، إذا ترتب على الاختراق إحداث أضرار أو تدمير أو إيقاف عن العمل أو تعطيل موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة معلومات أو وسيلة تقنية المعلومات، أو إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو نسخ أو نشر أو إعادة نشر أي بيانات أو معلومات أو خسارة سريتها أو وقعت الجريمة نتيجة لهجمة إلكترونية.

٣. وتكون العقوبة السجن مدة لا تقل عن (٧) سنوات والغرامة التي لا تقل عن (٢٥٠,٠٠٠) مائتين وخمسين ألف درهم ولا تزيد على (١,٥٠٠,٠٠٠) مليون وخمسمائة ألف درهم، إذا كان الاختراق بغرض الحصول على البيانات أو المعلومات الخاصة بتلك الجهات المنصوص عليها بالفقرة الأولى من هذه المادة".

قد يعتقد البعض أن الغرامات المنصوص عليها في المادة السابقة مناسبة لخطورة فعل الاختراق الواقع على المواقع والأنظمة المعلوماتية الخاصة بمؤسسات الدولة، مما يضفي على الغرامة القيمة الرادعة، ولكن المتفحص للأمر يجد أن هذه الغرامات بحديها الأدنى والأقصى قد تكون غير مناسبة لخطورة وجسامة الأضرار الهائلة التي قد تنجم عن فعل الاختراق إذا ترتب عليه تعطل أو تدمير و اتلاف أو نسخ أو نشر أو إعادة النشر البيانات أو المعلومات السرية التي يتضمنها الموقع أو النظام المعلوماتي الحكومي، وما قد يترتب عليه من خسائر وأضرار مالية قد تصل بالمليارات، أو مئات الملايين من الدراهم، بالنظر إلى توسع المؤسسات الحكومية بدولة الامارات العربية المتحدة في الاعتماد كليةً على النظم المعلوماتية، التي تعد بلا مبالغة عصب الحياة وشريانها الذي تسري فيه مظاهر الحياة للدولة ذات الحكومية الإلكترونية، ليس ذلك فحسب، بل إن الدولة تسارع الزمن في بلوغ أقصى درجات الاستفادة من امكانيات وقدرات الذكاء الاصطناعي في كافة المجالات، لاسيما تلك المجالات المتعلقة بالأمن، ومنع ارتكاب الجرائم والتنبؤ بارتكابه، وضبط محتوى الاعلامي على مواقع التواصل الاجتماعي، بالإضافة إلى الاعتماد سلاسل الكتل المعروفة بمصطلح (Blockchin)، في إدارة بعض أوجه العمل القضائي في وزارة العدل.

لذلك يوصي الباحث بأن ينتهج المشرع الإماراتي–على وجه الخصوص– أسلوب الغرامة النسبية، بحيث ينص على عقوبة الغرامة بوضع حد أدنى لها، مع ترك الحد الأقصى لتقدير القاضي في ضوء من حققه الجاني أو حاوله تحقيقه من ربح أو فائدة

مالية من ارتكاب الجريمة، أو ربطه بما تسبب فيه الجاني من خسائر مالية للمؤسسة التي اخترق موقعها أو نظامها المعلوماتي.

المبحث الثاني
مخاطر الاختراق الإلكتروني على الأمن المعلوماتي.

تمهيد:

مما لا شك فيه أن هذا الحجم الهائل من المعلومات والبيانات في تطبيقات الذكاء الاصطناعي وما قد تتعرض له من اختراق يهدد كافة قطاعات الدولة لاسيما القطاع الأمني والشرطي، والقطاع الصحي، والقطاع المالي، وغير ذلك من القطاعات الحكومية، وغير الحكومية، ينطوي على خطر كبير على الأمن المعلوماتي والسيبراني وارتباطهما الوثيق بالأمن القومي، ومن ثم تكون حماية أمن المعلومات ومواجهة الاختراق الإلكتروني أو السيبراني هو في ذات الوقت حماية للأمن القومي.

تقسيم:

نتناول هذا المبحث في المطالب الثلاثة الآتية:

المطلب الأول: تعريف الأمن المعلوماتي وعناصره.

المطلب الثاني: التمييز بين مفهوم الأمن المعلوماتي وغيره من المصطلحات المشابهة.

المطلب الثالث: مخاطر اختراق تقنيات الذكاء الاصطناعي على الأمن القومي وعلاقتها بالحروب الإلكترونية.

المطلب الأول

تعريف الأمن المعلوماتي وعناصره.

ظهر مصطلح (الأمن المعلوماتي) مع شيوع الاعتماد على المعلوماتية وتكنولوجيا المعلومات والحواسيب الآلية، وشبكات المعلومات؛ حيث اتجه العالم في ظل ثورة المعلوماتية إلى التفكير جليا في المخاطر التي قد تواجه هذه المعلومات، والأثار المترتبة عليها، من هنا ظهرت الحاجة إلى حماية أمن المعلومات، وقد ظهر مصطلح (الأمن المعلوماتي) واختلط به مصطلحين آخرين وهما (الأمن الإلكتروني) و(الأمن السيبراني)، ومن ثم وجب التمييز بينهم. وقد عرض الباحثون في أمن المعلومات مجموعة عناصر تقوم عليها فكرة الأمن المعلوماتي، ومن ثم نعرض في هذا المطلب لتعريف الأمن المعلوماتي في فرع أول، ثم نعرض لعناصر الأمن المعلوماتي في فرع ثان.

الفرع الأول

تعريف الأمن المعلوماتي

يشبر البعض([1]) إلى أن مفهوم الأمن المعلوماتي مر بعدة مراحل؛ أدت إلى ظهور مصطلح (أمنية المعلومات)، ويدور المصطلح الجديد حول تأمين الوصول إلى المعلومات، وتحديد طرق الوصول غير المشروعة والحد منها ومكافحتها، ومع اعتماد

[1]) هاني مطر أبو سعود، عباسة طاهر، ارتباطات الأمن المعلوماتي بالأمن القومي، مجلة الدراسات الحقوقية، جامعة سعيدة الدكتور مولاي الطاهر، الجزائر، المجلد ٧، العدد٢، جوان ٢٠٢٠م، ص٢١٠، ٢١١.

العالم على الحواسيب الآلية وشبكة الإنترنت في كل مجالات الحياة، وما أسفر عن ذلك من بزوغ أهمية المعلومات والبيانات، التي أصبحت من مظاهر قوة الدول، وتحكمها في مجريات الأحداث؛ هذا ما جعل الدول والشركات الضخمة تتسابق فيما بينها إلى الاستحواذ على المعلومات والبيانات، وأضحى تأمين المعلومات والبيانات خاصة الحكومية أمراً في غاية الأهمية.

يعرف الأمن المعلوماتي من الناحية الأكاديمية بأنه: العلم الذي يبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها وأفعال الاعتداء عليها. بينما يعرف من الناحية التقنية بأنه: الوسائل والإجراءات اللازم توفيرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية. ويعرف من الناحية القانونية بأنه: مجموعة من الإجراءات والمعالجات التي تستخدمها الدولة بهدف حماية أنظمتها الإلكترونية من الهجمات الإلكترونية المختلفة أو من الوصول غير المصرح به لأي نظام معلوماتي حيوي في الدولة([1]).

كما عرف بأنه: ذلك الحقل الذي يهتم بدراسة طرق حماية البيانات والمعلومات المخزنة على الحواسيب الآلية، إضافة إلى الأجهزة الملحقة وشبكات الاتصالات

[1]) انظر في هذه التعريفات: د/ محمد محمد الألفي، الحماية القانونية لقواعد البيانات في نظم المعلومات، ورقة عمل لندوة أمن المعلومات والتوقيع الإلكتروني، المنظمة العربية للتنمية الإدارية، القاهرة، ٢٠٠٧م، ص١٨٦. هاني مطر أبو سعود، عباسة طاهر، ارتباطات الأمن المعلوماتي بالأمن القومي، مرجع سابق، ص٢١١.

والتصدي للمحاولات الرامية إلى الدخول غير المشروع إلى قواعد البيانات المخزنة أو تلك الرامية إلى نقل أو تغيير أو تخريب المخزون المعلوماتي لهذا القواعد([1]).

كما يراد بالأمن المعلوماتي مجموعة التدابير اللازمة لحماية سرية وسلامة محتوى توفر المعلومات ومنع كل وصول غير مصرح به لهذا المحتوى، أو إساءة استغلاله في الاعتداء على خصوصية الأفراد أو على مصالح الشركات التجارية الكبرى، أو الاعتداء على الأمن القومي للدول.

من التعريفات السابقة يمكن القول:إن الأمن المعلوماتي يقوم على عدة محاور أهمها:

- حماية المعلومات من الاستيلاء عليها واستغلالها بشكل غير مشروع.
- حماية المعلومات من التعدي عليها سواء بالإتلاف أو التحريف أو التغيير أيا كان مصدره.
- تمكين الأنظمة المعلوماتية في المؤسسات الحيوية بالدولة من العمل بشكل آمن.
- ضمان استمرار المؤسسات الحيوية بالدولة على أداء وظيفتها بشكل آمن.

[1]) د/ أمين أعزان، د/ عبد السلام جاكيمي، الحماية التقنية والجنائية للنظم المعلوماتية، المجلة المغربية للقانون الجنائي والعلوم الجنائية، مركز الدراسات والبحوث الإنسانية والإجتماعية، المغرب، العدد الثالث، ديسمبر ٢٠١٦م، ص٢٢.

الفرع الثاني

عناصر الأمن المعلوماتي

يشير البعض([1]) إلى أن استراتيجيات ووسائل أمن المعلومات سواء التقنية منها والتشريعية مضمون بتوافر العناصر التالية:

١- السرية والموثوقية:

يراد بها: التأكد من أن المعلومات محل الحماية لا يتم الكشف عنها أو الاطلاع عليها من قبل أشخاص غير مخولين. مع ملاحظة أن السرية ليست متطلبة لكل المعلومات، بل إن هناك معلومات مسموح الإطلاع عليها. كما أن المعلومات الخاصة بمنشآة معينة ليست على نفس القدر من الأهمية؛ حيث تسمح المنشآت للأفراد بالوصول إلى بعض المعلومات التي ترى أهمية لذلك، مع حظر الوصول بالنسبة لمعلومات أخرى.

بل إن البيانات الحكومية تدور بين السرية والإفصاح؛ حيث تنقسم إلى: البيانات الحكومية المفتوحة، تلتزم الحكومات بالإفصاح عنها للأفراد، من ذلك: البيانات الخاصة بالخدمات الحكومية، والاحصاءات الوطنية، والقوانين والقرارات الوزارية، والمعلومات الخاصة ببعض الوزارات، مثل: وزارة التعليم والصحة، وهيئة الضرائب. بل أن الحكومات تنشئ منصات مفتوحة للأفراد، للوصول إلى بعض البيانات الخاصة بهم، مثل: بوابة الحكومة المصرية المتاحة على شبكة الانترنت. البيانات الحكومية

[1]) د/ محمد محمد الألفي، الحماية القانونية لقواعد البيانات في نظم المعلومات، مرجع سابق، ص١٨٧.

السرية، تلتزم الحكومات بضمان سريتها وتأمينها، وتجريم الوصول إليها بدون تصريح. من ذلك: البيانات المتعلقة بالأمن القومي، وتلك المتعلقة ببعض الوزارات، مثل: وزارة الدفاع والداخلية([1]).

قد يحدث ذلك في مجال تقنيات الذكاء الاصطناعي من ذلك أنظمة الطائرات بدون طيار، فقد يتم الكشف عن المعلومات وانتهاك مبدأ السرية، حيث ينشر الوكيل معلومات إلى شخص ليس لديه بيانات الاعتماد المناسبة لتلقيها، ويمكن أن تشمل تهديدات الكشف عن المعلومات التسلل إلى نظام بيانات مستشعر أنظمة الطائرات بدون طيار(UAS) للوصول إلى الفيديوهات أو التسجيلات الصوتية أو البيانات الأخرى، كما يمكن للوكيل –أيضًا– الكشف عن المعلومات ثم إنكار ما حدث للتنصل من المسؤولية([2]).

٢– التكاملية وسلامة المحتوى:

يراد بها: التأكد من أن محتوى المعلومات صحيح ولم يتم تعديله أو العبث به، في أي مرحلة من مراحل الحماية أو المعالجة، سواء من خلال التعامل الداخلي مع المعلومات أو من خلال التدخل غير المشروع.

---

[1]) د. يحيي ابراهيم دهشان، الحماية الجنائية للبيانات في ظل التحول الرقمي، مجلة الدراسات القانونية والاقتصادية، جامعة مدينة السادات، المجلد ٩، العدد ٣، سبتمبر ٢٠٢٣م، ص١٥٢٢، ١٥٢٣.

[2]) KATHARINA LEY BEST and Others, How to Analyze the Cyber Threat from Drones, Background, Analysis Frameworks, and Analysis Tools, Published by the RAND Corporation, Santa Monica, Calif. 2020, P:8.

٣- استمرارية توفر المعلومات والخدمة:

يراد بها: التأكد من استمرارية عمل النظام المعلوماتي والقدرة على التفاعل مع المعلومات، وتقديم الخدمة للمواقع المعلوماتية باستمرار، وقد يحدث رفض الخدمة حال الاختراق لأنظمة الطائرات بدون طيار عندما تكون هذه الأنظمة مستهدفة، ويمكن أن تتضمن إصابة برامج التحكم في الطائرة لجعل الأجهزة لا تستجيب لتوفر الخدمة([1]).

٤- الإقرار بالتصرف المرتبط بالمعلومات:

بمعنى ضمان عدم إنكار الشخص الذي تصرف بشكل أو بآخر على نحو متصل بالمعلومات أو المواقع المعلوماتية أنه من قام بهذا التصرف أو ذاك، مما يوفر المقدرة على إثبات حدوث تصرف ما من شخص ما في وقت معين. وقد أشار البعض إلى التنصل؛ حيث يرفض المهاجمون تحمل المسؤولية عن عمل ما، هذا التهديد هو الأقل صلة بمجال الأمن السيبراني المتعلق بالطائرات بدون طيار، وأحد الأمثلة المحتملة على التنصل هو إساءة استخدام ضوابط النظام من الداخل. على سبيل المثال، يمكن لمشغل طائرة بدون طيار أن يدعي أنه لم يتعمد تعطل الجهاز عن طريق إلقاء اللوم على فقدان السيطرة على عيب في تصميم شبكة الاتصالات([2]).

وهو ما أشارت إليه بعض الدراسات المتخصصة حول مخاطر الإنترنت على الأمن القومي لاسيما إنترنت الأجسام (Internet of Bodies) أنه غالبا ما يتم تصنيف

---

[1]) ibid.
[2]) KATHARINA LEY BEST and Others, op. cit., P:7.

المخاطر من حيث الأمن الإلكتروني ضمن ثلاث فئات تعرف بتسمية ثلاثي السرية، والسلامة، والتوفر. تعني السرية :أن الكيانات المصرح لها هي الوحيدة المخول لها الاطلاع على البيانات. وتعني السلامة: أنه لم يتم التلاعب بالبيانات التي تم جمعها. ويعني التوفر: أنه يتم الوصول إلى البيانات متى وحيث وجدت الحاجة إلى ذلك([1]).

المطلب الثاني

التمييز بين مفهوم الأمن المعلوماتي وغيره من المصطلحات المشابهة

ذكرنا من قبل أن ثمة خلط في مفهوم كل من مصطلحات الأمن المعلوماتي، والأمن الإلكتروني، والأمن السيبراني، ومن ثم وجب التمييز بينهم على النحو التالي:

الفرع الأول

التمييز بين مفهوم الأمن المعلوماتي والأمن الإلكتروني

حرص المشرع الإماراتي على وضع تعريف محدد للأمن الإلكتروني بأنه: "تأمين وحماية الشبكة المعلوماتية وشبكة الاتصالات ونظم المعلومات وعمليات جمع

[1]) Center for Internet Security, “EI-ISAC Cybersecurity Spotlight— CIA Triad,” webpage, undated. As of April 27, 2020:
https://www.cisecurity.org/spotlight/ei-isac-cybersecurityspotlight-cia-triad/30/12/2020
MARY LEE and others, The Internet of Bodies, Opportunities, Risks, and Governance, published by The RAND Corporation, 2020.
https://www.rand.org/pubs/research_reports/RR3226.html/30/12/2020

المعلومات باستخدام أي من الوسائل الإكترونية"([1]). وقد ميز البعض بين مفهوم الأمن المعلوماتي وبين مفهوم الأمن الإلكتروني المنصوص عليه في قانون إنشاء الهيئة الوطنية للأمن الإلكتروني بدولة الإمارات العربية المتحدة؛ حيث يرى أن مفهوم الأمن المعلوماتي ينحصر نطاقه في إطار أو منظور فكرة حماية (النظام المعلوماتي، والشبكة المعلوماتية، والبيانات والحاسوب، وبرامجه والموقع المعلوماتي) بمفهومها المجرد؛ من حيث مضمونها ومحتواها كقيمة مادية أو معنوية بالمعني الضيق، وليست من منظور أمني سيادي أو دفاعي يتعلق بمصالح قومية عليا([2]). بينما نجد مفهوم الأمن الإلكتروني أوسع نطاقا؛ حيث يشمل إلى جانب فكرة الحماية فكرة تأمين البيئة الإلكترونية وعناصرها ومقوماتها؛ من شبكات الاتصالات ونظم التحكم الإلكتروني والشبكة المعلوماتية ونظم المعلومات وغيرها من مجالات البيئة الافتراضية بمفهومها الضيق من الوجهة التقنية والمعلوماتية ومعالجة البيانات والأجهزة وغيرها([3]).

[1]) المادة الأولى من قانون ٣ لسنة ٢٠١٢ بشأن إنشاء الهيئة الوطنية للأمن الإلكتروني.

[2]) د/ حازم حسن أحمد الجمل، الحماية الجنائية للأمن السيبراني في ضوء رؤية المملكة ٢٠٣٠م، مجلة البحوث الأمنية، كلية الملك فهد الأمنية – مركز الدراسات والبحوث، المجلد ٣٠، العدد ٧٧، أغسطس ٢٠٢٠م، ذوالحجة ١٤٤١هـ، ص٢٥٤، ٢٥٥.

[3]) الموضع السابق.

الفرع الثاني

التمييز بين مفهوم الأمن المعلوماتي والأمن السيبراني

أشار البعض إلى أن مفهوم الأمن السيبراني أوسع نطاقا من مفهوم كل من الأمن المعلوماتي والأمن الإلكتروني سالفي الذكر؛ لأنه يزيد على فكرة الحماية في الأمن المعلوماتي، وفكرة التأمين في الأمن الإلكتروني ويشمل فكرة الدفاع السيبراني، كأساس وإطار ومبرر لحماية المصالح الحيوية والوطنية ذات الصلة بسيادة الدولة على فضائها الإلكتروني، والتصدي للاعتداءات من خلال مجموعة من القوانين والتشريعات والنظم والخطط والتدابير والاستراتيجيات والأدوات والسياسات والأساليب الحيوية للحفاظ على الأمن القومي والنظام العام وسياسات الدولة في المجالات الاقتصادية والاجتماعية والتقنية ومنشآتها ومؤسساتها الحيوية([1]).

ويرادف الأمن السيبراني أمن الفضاء الإلكتروني، أو أمن البيئة الافتراضية الإلكترونية، المعبرة عن سيادة وحق الدولة في الدفاع وحماية فضائها السيبراني المتعلق بالأمن القومي والمصالح والأهداف الحيوية، وينطوي الأمن السيبراني بهذا المفهوم على قدرة الدولة في حماية استخدام الفضاء السيبراني والدفاع عنه من الهجمات والتهديدات السيبرانية([2])، وهو ما يبرر حق الدولة في التدخل والدفاع عن

---

[1]) الموضع السابق.

[2]) في سياق الأمن السيبراني، يتضمن التنبؤ بالتهديدات السيبرانية البحث في كميات كبيرة من البيانات لتحديد الجهات الهجومية والتهديدات التي تتعرض لها البنية التحتية المعلوماتية في المؤسسة، فالهدف هو منع الهجمات قبل حدوثها والقضاء على آثارها أو تقليلها.

أمنها السيبراني كمظهر من مظاهر السيادة على فضائها السيبراني([1]). ويقصد بالأخير النطاق العالمي لبيئة المعلومات، والتقنيات، ويتألف من شبكة مترابطة من البنى التحتية لنظم المعلومات بما في ذلك الإنترنت، وشبكات الاتصالات، وأنظمة الحاسوب، والمعالجات، وأجهزة التحكم المضمنة([2]).

Jeff Crume, Doug Lhotka, Carma Austin, Security and Artificial Intelligence: FAQ, op. cit., P: ٧.

[1]) د/ حازم حسن أحمد الجمل، المرجع السابق، ص٢٥٣.

[2]) المرجع السابق، ص٢٥٤.

المطلب الثالث

مخاطر اختراق تقنيات الذكاء الاصطناعي على الأمن القومي وعلاقتها بالحروب الإلكترونية.

ذكرنا أن حماية الأمن المعلوماتي ترتبط ارتباطا وثيقا بالأمن القومي، بالنظر إلى أن الأخير يعتمد بشكل ما على ما تتمتع به النظم المعلوماتية وشبكات الاتصالات والمعلومات من الحماية التقنية والأمنية، ومن ثم يمثل اختراق أو انتهاك الأمن المعلوماتي مصدر تهديد جسيم للأمن القومي، كما يرتبط هذا بالحروب الإلكترونية باعتبارها صورة حديثة للحرب الأشد فتاكا وضراوة من الحرب التقليدية.

الفرع الأول

مخاطر اختراق تقنيات الذكاء الاصطناعي على الأمن القومي

أثار الحديث عن مخاطر الاعتماد المتصاعد على تقنيات الذكاء الاصطناعي على الأمن القومي نقاشا مطولا بين أعضاء فريق عمل تابع لمؤسسة RAND([1])؛ حيث تعرضوا لبحث المخاطر المرتبطة بالذكاء الاصطناعي في محاور مألوفة؛ إذ يمكن – على سبيل المثال– لعملية صنع القرار المعتمدة على تقنيات الذكاء الاصطناعي في مجال الأمن القومي أن تؤدي إلى أخطاء مكلفة وخسائر كبيرة، فلنا أن نتخيل حجم

[1]) Osonde A. Osoba, William Welser IV ,The Risks of Artificial Intelligence to Security and the Future of Work, RAND, Saint Monica, California, USA, 2017, P:5-6, available at internet, date of visit: 24/12/2020, file:///C:/Users/HP/Downloads/RAND_PE237.pdf

الخسائر الناجمة عن أي خلل في منظومة الأسلحة النووية المؤمنة، وكذلك الأسلحة التي تعمل بتقنيات الذكاء الاصطناعي بعيداً عن تدخل البشر.

وفي بيان مخاطر اختراق تقنيات الذكاء الاصطناعي على الأمن القومي حدد فريق العمل موضوع الأمن الإلكتروني كمجال خصب بشكل خاص لمواطن الضعف الناجمة عن الذكاء الاصطناعي؛ حيث إن أبرز وظائف الأدوات الاصطناعية الإلكترونية، هو التلاعب الفعال بالمعلومات، مما قد يدفع إلى حروب المعلومات بين الدول. كما يمكن تعزيز البرامج الضارة التي تستهدف إنترنت الأشياء من خلال الذكاء الذي يحسن من قدراتها وإمكاناتها الاستراتيجية، مما يُمكن هذه البرامج أن تكون فعالة ودقيقة في أهدافها الاستراتيجية كما يُصعب من اكتشافها إبقاء سعة تلك البرامج صغيرة، مع توقع أن تسفر التطورات المستقبلية في مجال الذكاء الاصطناعي عن برامج ضارة صغيرة الحجم وذات آثار مدمرة.

كما حدد فريق العمل نقطة تخوف أخرى، تتمثل في وجود ضعف في ماهية البيانات المغذية في نظم التعلم المستقلة الحالية؛ إذ تتسم نظم الذكاء الاصطناعي بجودة البيانات نفسها التي تدرب على أساسها، ويمكن لهذه النظم أن تبلور أي تلاعب أو أكاذيب يتم العثور عليها ببيانات تدريبها.

ومن ثم يفتح تطبيق الذكاء الاصطناعي في المراقبة والأمن الإلكتروني وجهة للهجوم الإلكتروني على الأمن القومي قائمة على ضعف في البيانات المغذية، ومما يزيد الأمر خطورة أن المهاجمين قد يتعلموا كيفية تغذية نظم المراقبة العاملة في مجال الذكاء الاصطناعي بمعلومات مضللة بشكل منهجي، فينشؤون عميلا آليا مزدوجا

بشكل سري. كما ظهر موطن ضعف آخر مؤثرا على الأمن القومي مرتبطا بالذكاء الاصطناعي، ويتمثل في استخدام تقنيات الذكاء الاصطناعي التي تستغلها جهات خارجية للتدخل في الشبكات؛ فقد أعلنت وكالات الاستخبارات الأمريكية على اعتقادها بتعرض الانتخابات الأمريكية عام ٢٠١٦م لتدخل أجنبي من خلال هجمات إلكترونية خارجية، ألمحت بإتهام دول متورطة في هذه الهجمات ومنها: روسيا والصين، أثرت تلك الهجمات على آراء الناخبين.

كما يمكن تصور وقوع العبث بسلامة تقنيات الذكاء الاصطناعي ذاتها مثل: حالة الأمن السيبراني المرتبط بأنظمة الطائرات بدون طيار، فقد يتم استخدام الطائرات بدون طيار كسلاح إلكتروني، ويمكن أن يحدث التلاعب إذا تم استخدام الطائرة لإيصال برامج ضارة إلى جهاز كمبيوتر مستهدف عبر شبكة لاسلكية غير آمنة. ويمكن أن تصيب مثل هذه البرامج الضارة الآلات عالية القيمة، مثل معدات المصانع أو محطات الطاقة، وقد تهاجم أهدافًا عالية التأثير مثل أنظمة المياه وشبكات الطاقة([1]).

الفرع الثاني

علاقة اختراق تقنيات الذكاء الاصطناعي بالحروب الإلكترونية

إن توجه العالم إلى تطبيق الحكومة الإلكترونية E-Government معتمدا في ذلك على تقنيات الذكاء الاصطناعي بشكل أساسي دفع إلى إعطاء الحروب

[1]) KATHARINA LEY BEST and Others, How to Analyze the Cyber Threat from Drones, Background, Analysis Frameworks, and Analysis Tools,op. cit., P:7.

الإلكترونية Electronic wars بعداً أكثر خطورةً وشراسةً من ذي قبل، بداية نشير إلى أن مصطلح الحرب الإلكترونية ظهر مع تنامي الاعتماد على البيئة الرقمية في كافة المجالات، وتنامي الاعتماد على الحواسيب الآلية وشبكات الاتصالات والمعلوماتية، ومن ثم لا يظن البعض أن مصطلح الحرب الإلكترونية ارتبط ظهوره بالذكاء الاصطناعي، بل إنه ارتبط بالمعلوماتية وشبكات الإنترنت والاتصالات بشكل أساسي([1]).

ومع ذلك نؤكد على أن تعاظم خطورة الحرب الإلكترونية وشراستها على مصالح الدول واقتصادها ارتبط بالاعتماد الكبير على نظم الذكاء الاصطناعي، ومنها البيانات الكبرى (Big Data) والبلوك تشين (Block Chain) والطائرات بدون طيار (Drones) لاسيما المسيرة ذاتياً، والروبوتات المقاتلة(Robots Fighting)، إلى غير ذلك من تطبيقات الذكاء الاصطناعي(AI).

تعرف الحرب الإلكترونية بأنه حرب افتراضية ذات طبيعية غير ملموسة تحاكي الواقع بشكل شبه تام، تتلخص أدوات الصراع في الموجهات الإلكترونية والبرمجيات التقنية، وجنودها من برامج إلكترونية حاسوبية تدميرية أو تخريبية، لذلك فهي حرب بلا إراقة دماء، تستهدف تدمير النظم المعلوماتية في الدول، وانهيار اقتصادياتها، وقطاعاتها التي تعتمد على هذه النظم المعلوماتية، مثل القطاع

[1]) د/ عبد الفتاح الطاهري، الأمن المعلوماتي وعلاقته بالأمن القومي، مجلة الباحث للدراسات القانونية والقضائية، عدد١٠، فبراير ٢٠١٩م، ص٣١.

العسكري، النووي، الصحي، المالي، التجاري، الضريبي أو المصرفي، وغير ذلك من القطاعات الحيوية في الدولة المستهدفة([1]).

ومن أسلحة الحرب الإلكترونية: التجسس المعلوماتي بالتنصت على الشبكات المعلوماتية والنظم المعلوماتية واعتراض المراسلات الإلكترونية الحكومية لاسيما العسكرية منها أو الأمنية، بل واعتراض المحادثات والمراسلات عبر الهواتف المحمولة. والاختراق الإلكتروني بالدخول غير المصرح به لأي نظام معلوماتي أو شبكة معلومات أو البقاء فيه على نحو غير مشروع، وقد يكون بهدف الحصول على المعلومات دون المساس بها، وقد يكون بهدف اتلاف المعلومات التي يتم الوصول إليها وتدميرها مما يصيب كافة قطاعات الدولة المتحاربة بالشلل التام. وغالبا ما يتم هذا بزرع فيروسات أو برامج خبيثة مدمرة. كما يعد الاعلام الرقمي الجديد من أهم أسلحة الحروب الإلكترونية، لما يتمتع به من تأثير سريع ومنتشر بين ملايين المستخدمين للمواقع المعلوماتية سواء المقروءة أو المرئية والمسموعة، حيث يمكن بث معلومات مغلوطة أو مقاطع فيديو انهزامية أو تحريضية أو تخريبية مع ضمان سرعة انتشارها بين المستخدمين([2]).

ولاشك في أن أوضح سلاح معلوماتي للحرب الإلكترونية مرتبط بتقنيات الذكاء الاصطناعي هو الطائرات المسيرة أو بدون طيار (Drones) والروبوتات

[1]) انظر: د/ عبد الفتاح الطاهري، المرجع السابق، ص٣٢، ٣٣.

[2]) المرجع السابق، ص٣٥–٣٨.

المقاتلة(Fighting Robots). وفي دراسة أمريكية([1]) عن مخاطر الاختراق الإلكتروني لتقنيات الذكاء الاصطناعي، ومنها أنظمة الطائرات بدون طيار، أشارت إلى أن جميع مكونات ومكاتب وزارة الأمن الداخلي تقريبًا يمكن أن تصبح ضحايا لاختراق البيانات؛ حيث تحتوي جميع هذه المكاتب والمكونات على مواقع معلوماتية تحتوي على كم هائل من البيانات الحساسة والشبكات اللاسلكية، مما يجعلها أهدافًا لهذه الأنواع من الهجمات الإلكترونية.

كما أشارت الدراسة إلى أن أنظمة الطائرات بدون طيار تقدم طرقًا جديدة للهجمات الإلكترونية، حيث تعمل أنظمة هذه الطائرات نفسها كـ "أسلحة إلكترونية" تهدف إلى تقديم محتوى ضار أو تأثيرات مدمرة؛ إذ يمكن لأسراب الطائرات بدون طيار التي تحمل متفجرات بأعداد كبيرة لمهاجمة أهداف محددة([2])، هذا مع التأكيد على صعوبة التنبؤ بكيفية ترجمة التقنيات الناشئة إلى أنواع جديدة من تهديدات الأمن السيبراني لمساعدة صانعي السياسات على فهم أفضل لكيفية قيام أنظمة الطائرات بدون طيار بتغيير مجال التهديد السيبراني، ومن ثم تقدم هذه الدراسة عدة مناهج لتصور التهديدات المتعلقة بأنظمة هذه الطائرات كأهداف إلكترونية أو أسلحة إلكترونية. وتمكن الأساليب المستخدمين من تحديد وتصنيف التهديدات المتعلقة بتكنولوجيا بتلك الطائرات، وتصور مساحة التهديد لفهم طبيعة التهديدات والفرص المتاحة لتحسين الأمن السيبراني المرتبط بأنظمتها([3]). يرى الباحث أن محاولة تقييم المخاطر

[1]) KATHARINA LEY BEST and Others, op. cit., P:xii.
[2]) ibid, P: 1.
[3]) ibid.

والتهديدات المتعلقة بالأمن السيبراني لأنظمة الطائرات بدون طيار، توجب على صانعي القرار التعامل مع الموضوع من عدة زوايا؛ حيث يمكن أن تكون أنظمة الطائرات بدون طيار بمثابة أهداف أو تهديدات للأمن السيبراني، كما سنوضح في المبحث التالي.

المبحث الثالث

تحليل التهديدات السيبرانية لأنظمة الذكاء الاصطناعي

وصور الاختراقات الواقعة عليها

تمهيد:

يعد التلاعب في برمجة تقنيات الذكاء الاصطناعي من أهم وأخطر التحديات التي تواجه استخدام هذه التقنيات في العمل الشرطي والقضائي، ويقع على عاتق قطاع الأمن الإلكتروني أو السيبراني مسؤولية جسيمة في توفير الحماية الأمنية والتقنية للمعلومات والبيانات التي تعتمد عليها خوارزميات الذكاء الاصطناعي، وذلك بسد كافة الثغرات التقنية التي يمكن من خلالها للمخترق الوصول إلى تلك البيانات والمعلومات بشكل غير مشروع دون المساس بها، أو الوصول إليها بغرض التلاعب فيها والمساس بها بأي صورة كانت، سواء بالإتلاف أو التدمير أو التغيير أو التعديل([1]).

ولنا أن نتخيل ما قد يسفر عنه وصول المخترق إلى بيانات تقنية التعرف على الوجه لتحديد الهوية أو نظم تشغيل السيارة ذاتية القيادة أو الطائرة بدون طيار أو الروبوتات الطبية أو الروبوتات المقاتلة، وما قد يسفر عنه التلاعب في هذه البيانات من أشكال التخريب والتدمير والاعتداء على الأرواح والممتلكات، بل وعلى السياسات العامة

[1]) د/ أيمن محمد السيد الأحول، د/ أحمد دسوقي، التحديات الأمنية المعاصرة للظواهر الإجرامية المستحدثة، الفكر الشرطي، القيادة العامة لشرطة الشارقة، مركز بحوث الشرطة، المجلد ٢٢، العدد ٨٦،يوليو ٢٠١٣، ص١٧٥.

لأغلب قطاعات الدولة، ليس ذلك فحسب، بل على الأمن القومي بكافة صوره لاسيما الأمن العسكري والاقتصادي أو المالي.

وسوف نقصر الحديث عن مخاطر التلاعب في برمجة تقنية الطائرات المسيرة ذاتياً، وتقنية السيارات ذاتية القيادة؛ نظرا لأن العالم في طريقه إلى الاعتماد على هاتين التقنيتين بشكل متسارع مما يزيد من مخاطر التلاعب ببرمجتهما.

تقسيم:

نتناول في هذا المبحث المطالب الثلاثة الآتية:

المطلب الأول: تحليل التهديدات السيبرانية والأثار الأمنية لاختراق أنظمة الطائرات المسيرة.

المطلب الثاني: تحليل التهديدات السيبرانية والأثار الأمنية لإختراق أنظمة المركبات ذاتية القيادة.

المطلب الثالث: صور الاختراق الإلكتروني لأنظمة الطائرات المسيرة ذاتياً والمركبات ذاتية القيادة.

المطلب الأول

تحليل التهديدات السيبرانية والأثار الأمنية

لاختراق تقنية أنظمة الطائرات المسيرة.

مع تزايد الاعتماد على تقنية الطائرات بدون طيار، لاسيما تلك المسيرة ذاتياً، في الأغراض الأمنية يقابل هذا تزايداً في احتمالية التهديدات والانتهاكات للأمن

السيبراني، لذلك نجد من الأهمية بمكان الوقوف على الأثار الأمنية للنمو السريع لهذه التقنية، مع بيان نقاط الضعف الحالية والمستقبلية، والتي تمثل تغرات أمنية في أنظمتها تقتضي المواجهة.

الفرع الأول

تحليل التهديدات السيبرانية لتقنية الطائرات المسيرة ذاتياً.

مع التوقع بأن تصبح الطائرات بدون طيار أكثر تكاملًا مع وظائف الأمن وتنفيذ القانون؛ خاصة في ظل التطورات الجديدة في تكنولوجيا الأنظمة الجوية بدون طيار (UAS)، بما في ذلك إدخال برامج تحكم أكثر تطورًا واستقلالية([1]). وفي عرض لتجربة الولايات المتحدة نجد أن وزارة الأمن الداخلي قد استخدمت هذه الطائرات من قبل خفر السواحل الأمريكي، الجمارك وحماية الحدود(CBP)، وكالة إدارة الطوارئ الفيدرالية (FEMA)، ووكالة الأمن السيبراني وأمن البنية التحتية(CISA). وفي دراسة([2]) عن مخاطر تهديد الاختراق الإلكتروني لأنظمة الطائرات بدون طيار على استخدامها في المجالات السابقة أشارت إلى أن ضعف هذه الأنظمة على صد الهجوم الإلكتروني يفقدها القدرة على القيام بما يلي:

[1])Divya Joshi, "Commercial Unmanned Aerial Vehicle (UAV) Market Analysis – Industry Trends, Companies and What You Should Know," Business Insider, August 8, 2017.
Nick Statt, "Skydio's AI-Powered Autonomous R1 Drone Follows You Around in 4K," TheVerge, February 13, 2018.
[2])KATHARINA LEY BEST and Others, op. cit., P:xi.

- مراقبة الجمارك والحدود (CBP) وقدرات الاستخبارات والمراقبة والاستطلاع(ISR)، مما يخلق نقاطًا عمياء بصرية في اكتشاف التهريب أو الأنشطة الإجرامية الأخرى على الحدود والموانئ. وقد تعتمد الجمارك وحماية الحدود(CBP) على استخدام منصات الطائرات بدون طيار في القيام بأنشطة أخرى في المستقبل؛ على سبيل المثال: استخدامها في المسح الكيميائي والبيولوجي والإشعاعي والنووي والمتفجرات في الموانيء، حيث يمكن أن يمنع اختراق أنظمة (UAS) وكلاء (CBP) من القيام بواجباتهم على أكمل وجه، كما قد يتسبب في أضرار مالية كبيرة عن طريق تأخير حركة البضائع أثناء إصلاح النظام، أو يمكن القيام بإرسال قراءات خاطئة للبضائع الخطرة. يمكن أن يؤدي اختراق أنظمة (UAS) أيضًا إلى مخاطر غير معروفة خاصة إذا كان مشغل (CBP) غير مدرك لحدوث الاختراق.
- قد يقلل اختراق الأنظمة الجوية بدون طيار (UAS) من قدرة وكالة إدارة الطوارئ الفيدرالية (FEMA) على تحديد أو الوصول للأفراد المعرضين للخطر في مناطق الكوارث. يحدث ذلك؛ لأن أنظمة (UAS) المخترقة لم تعد قادرة على القيام بمهامها.
- قد يقلل اختراق أنظمة (UAS) من قدرة وكالة الأمن السيبراني وأمن البنية التحتية (CISA) على إجراء عمليات تفتيش أساسية للبنية التحتية في بعض الحالات، ويمكن استخدام هذه الأنظمة المخترقة في هجوم مادي إلكتروني لإلحاق الضرر بالبنية التحتية الحيوية التي كان من المفترض مسحها. كما

يمكن أن يؤدي الاختراق إلى مخاطر غير معروفة إذا كان مشغل (CISA) غير مدرك لحدوث الاختراق.

أشرنا فيما سبق إلى أن مراحل الهجوم السيبراني على أنظمة الطائرات بدون طيار (UAS) تمثل سلسلة مرتبة، يمكن الاستعانة بها في تحديد التهديدات التي لم يتم الكشف عنها في أنظمة (UAS) وتتيح هذه السلسلة للمستخدم تحديد كيف ومتى يكون نظام معلوماتي معين عرضة لخطر الهجوم السيبراني، وقد يتيح ذلك تصميم دفاع مستنير ضد هذا التهديد السيبراني؛ إذ إن الإجراء الدفاعي المناسب يعتمد على تحديد مكان وجود التهديد ضمن مراحل الهجوم السيبراني، ومن ثم فإن تحديد مكان نظم تشغيل الطائرة بدون طيار في سلسلة الهجوم السيبراني يسهل اعتماد تدابير أمنية دفاعية فعالة، فقد يتم اتخاذ إجراء هجوم سيبراني (تكتيك دفاعي) ضد الطائرة نفسها للسيطرة عليها أو على أنظمتها الفرعية، لالتقاط أو تغيير بياناتها، أو تغيير مسارها، أو تدمير جهاز التحكم، ويطلق المختصصون على هذا البديل من الهجمات السيبرانية (التكتيك الدفاعي) التي تدعم أنظمة الطائرات بدون طيار مصطلح (الطائرة بدون طيار كهدف) (Drone as a Target) باعتبار أن الطائرة تمثل هدفا في ذاته للمخترق([1]).

وتشير الدراسة إلى أنه في الهجمات الأخرى التي تدعم أنظمة الطائرات بدون طيار، يستغل المهاجمون الخصائص الفريدة لأنظمة هذه الطائرة كوسيلة لمهاجمة هدف غير الطائرات بدون طيار. في مثل هذه الحالات، يتم استخدام الطائرة بدون طيار كرابط

[1]) KATHARINA LEY BEST and Others, op. cit., P:10.

وسيط أو رابط نهائي لتسهيل الهجوم، ومن ثم يتم استخدام (UAS) كوسيلة لتحقيق غاية في الهجوم السيبراني على أهداف أخرى، ويطلق المختصصون على دور أنظمة الطائرات في هذه الحالة مصطلح (الطائرات بدون طيار كوسيط أو ناقل للهجوم) (Drones as an Attack Vector)([1]) باعتبار أنها ليست هدفاً في ذاته للمخترق، وإنما وسيطاً يتمكن منه المخترق الوصول إلى هدف أبعد، كما لو أراد اختراق الأنظمة المعلوماتية الأخرى المتصلة بنظام تشغيل الطائرة بدون طيار المستهدفة.

كما تشير الدراسة([2]) إلى أن قناة الاتصال بين المشغل البشري والطائرة بدون طيار تتولى تشغيل الطائرة والتحكم فيها عن بعد. ومن ثم يكون الرابط الأول في أنظمة هذه الطائرات هو شخص يمكن اعتباره المشغل الأساسي للطائرة، ومع ذلك قد يتم إرسال الأوامر البشرية إلى الطائرة عبر مجموعة متنوعة من أجهزة الحوسبة على سبيل المثال، قاعدة الشحن مع تعليمات جدول الرحلة، الخادم المستند إلى السحابة لأوامر الطيران، وحدة التحكم المادية، الهاتف الخلوي، الكمبيوتر المحمول، أو الكمبيوتر اللوحي.

وتركز قناة الاتصال بين الطائرة وبيئتها التشغيلية بشكل أقل على الاتصالات اللازمة للتحكم فيها، وأكثر تركيزًا على المعلومات التي يتم جمعها من بيئة التشغيل. ويمكن أن يتضمن جمع المعلومات الحسية بواسطة الطائرة مجموعة متنوعة من المصادر لالتقاط مجموعة متنوعة من العوامل البيئية مثل إشارة نظام تحديد المواقع العالمي

[1]) ibid.
[2]) ibid., P:11-13.

(GPS)، وبيانات الارتفاع، والمستشعر المرئي، وغير ذلك من البيانات. وقد عرضت الدراسة أن خمسة أسئلة يتم الإجابة عليها لتوضيح موجهات الهجوم على أنظمة الطائرات بدون طيار، وهي: ما الخلل البرمجي (السلاح السيبراني) (Cyber Weapon)؟ كيف وصل إلى هناك (ناقل الهجوم) (Attack Vector)؟ من أين وصل (نقطة وصول النظام)؟ ما الذي فشل (الثغرة الأمنية)(Security Vulnerability)؟ ماذا حدث (النتيجة) (Result)؟

كما يمكن القول بانطباق ذلك على الطائرات المسيرة ذاتياً، التي لا يتم التحكم فيها بشرياً، ولكن يتم برمجتها مسبقاً، مع منحها الذاتية والاستقلالية في تحديد مسار الرحلة بما يحقق الأهداف من اطلاقها، في هذا النوع يمكن المهاجم أو المخترق أن يصل إلى كافة الأنظمة المعلوماتية المتصلة بالطائرة، مما يفرض على العامل البشري، لاسيما التقني عبء ثقيل في مراقبة ما قد تتعرض له الطائرة من هجوم سيبراني قد يؤدي إلى هجوم أكثر خطرا أو أوسع نطاقاً على أنظمة أخرى.

الفرع الثاني

الثغرات والآثار الأمنية لاختراق تقنية الطائرات المسيرة ذاتياً.

يكشف فحص عمليات الاستغلال الموثقة([1])عن العديد من الثغرات المنتشرة عبر جميع الأنظمة الفرعية الأساسية لأنظمة الطائرات بدون طيار، لاسيما المسيرة

[1]) رصد بعض المتخصصين قائمة تضم ٢٦ حالة موثقة من حالات استغلال الطائرات بدون طيار، انظر:

Sander Walters, "How Can Drones Be Hacked? The Updated List of Vulnerable Drones and Attack Tools," available at:

ذاتياً، على سبيل المثال: استهدفت عمليات الاستغلال الناجعة تأمين كلمة مرور ضعيفة(Weak Password)، وإعدادات افتراضية معروفة، وشبكات مخصصة غير محمية(Unprotected Networks). فيما يتعلق بالنظم الفرعية، تم استغلال الثغرات الأمنية في أنظمة الطائرات بدون طيار نفسها بالإضافة إلى أجهزة الاستقبال (Receivers)، أجهزة الاستشعار الضوئية (Optical Sensors)، وحدات التحكم(Controllers)، تطبيقات الملاحة (Navigation Applications)، وجميع روابط الاتصالات (Communications Links) التي تربط هذه الأنظمة الفرعية([1]). وفيما يتعلق بالمهارة التكنولوجية المطلوبة للمهاجم، وجدنا أن معظم عمليات استغلال أنظمة الطائرات بدون طيار لا تتطلب درجة عالية من التطور، حيث سيطر أحد المستغلين على (UAS) باستخدام جهاز كمبيوتر بدائي ورخيص الثمن يهدف إلى تعليم الكفاءة الحاسوبية الأساسية([2]).

حقيقة أن أساليب تنفيذ استغلال الطائرات بدون طيار متاحة للأفراد؛ حيث يوثق المسؤولون عن الهجوم أو الاختراق أو الاستغلال لأنظمة الطائرات بدون طيار منهجيتهم وأساليبهم الناجعة على مواقع الويب مثلYouTube أو المدونات الشخصية([3]). كما أن هذه الثغرات ليست مقتصرة على الأجيال الأولى من أنظمة

https://medium.com/@swalters/how-can-drones-be-hacked-the-updated-list-of-vulnerable-drones-attack-tools-dd2e006d6809, 1/1/2021.

[1]) Fernando Trujano, Benjamin Chan, Greg Beams, and Reece Rivera, "Security Analysis of DJI Phantom 3 Standard," op. cit., P:3

[2]) KATHARINA LEY BEST and Others, op. cit., P:16.

[3]) ibid, P:15.

الطائرات بدون طيار منخفضة التكلفة، فقد استهدفت تلك الثغرات الأجيال الأحدث والأعلى تكلفة.

كما تم استغلال وحدات التحكم عالية الجودة بنجاح؛ حتى أن أحد مستشاري أمن تكنولوجيا المعلومات خطف طائرة من الدرجة الأولى تتراوح قيمتها بين ٢٥٠٠٠ دولار و ٣٥٠٠٠ دولار ، يتم استخدامها في إنفاذ القانون([1]). ليس ذلك فحسب بل تم العثور على أدلة إضافية تؤكد ضعف أنظمة الطائرات بدون طيار من قبل باحثين متخصصين؛ حيث قاد أحد الأبحاث في جامعة تكساس فريق الاستعداد للطوارئ الحاسوبية عام ٢٠١٧م إلى إصدار مذكرة تثبت ضعف مجموعة من المروحيات الرباعية التي يمكن اختطافها بشكل مجهول عبر الشبكة المحلية.

ويمكن إجمال الثغرات الأمنية التي أظهرها باحثون جامعيون والتي تؤكد ضعف أنظمة الطائرات بدون طيار (UAS) المطروحة تجاريًا لمجموعة واسعة من الهجمات لجمع البيانات، ورصد مواقع الطائرات وتتبعها، واختطافها أو تعديل البرامج للسماح بدخول أنظمة (UAS) المجال الجوي المحظور بواسطة لجنة الاتصالات الفيدرالية، مثل هذه الثغرات الأمنية تسمح للمهاجم باختطاف وسرقة الطائرة بدون طيار أو التدخل في عملها بطريقة تتسبب في سقوطها مدويةً على الأرض([2])؛ ومن ثم ندرك

---

[1]) ibid.

[2]) Andrew J. Kerns, and others, "Unmanned Aircraft Capture and Control Via GPS Spoofing," Journal of Field Robotics, Vol. 31., No. 4, July/August 2014; Fernando Trujano, and others, "Security Analysis of DJI Phantom 3 Standard," Massachusetts Institute of Technology, May 11, 2016, P:3, 1/1/2021, available at:

أهمية تأمين البيانات الناتجة عن الطائرة بدون طيار؛ يتضمن ذلك سجلات الرحلات، والوسائط التي التقطتها الكاميرا، ويمثل الوصول غير المصرح به إلى أيٍّ منهما انتهاكًا للسياسة الأمنية للطائرات بدون طيار. علاوة على ذلك، فإن القدرة على تعديل أو إدراج أي بيانات إضافية ستجسد انتهاكًا أمنيًا أكبر([1]).

وقد انتهت الدراسة إلى ضرورة التعاون فيما بين صانعي الطائرات بدون طيار وخبراء الأمن السيبراني ووكالات إنفاذ القانون لوضع استراتيجية واضحة لأنظمة هذه الطائرات.

المطلب الثاني

تحليل التهديدات السيبرانية والأثار الأمنية

لإختراق أنظمة المركبات ذاتية القيادة.

مما لاشك فيه أن تقنية المركبات ذاتية القيادة (Autonomous Vehicle Technology) أحد أهم وأبرز تطبيقات الذكاء الاصطناعي التي يتوقع منها أن تقوم بدور فعال في تحقيق هدف السلامة المرورية وأمن الطرق، باعتباره أحد المهام الجسيمة الملقاة على عاتق الإدارات المرورية في وزارة الداخلية، إلا أن هذه التقنية على الرغم من إيجابياتها وأهدافها المتوقعة في السلامة المرورية قد يصاحبها العديد

https://courses.csail.mit.edu/6.857/2016/files/9.pdf. Junia Valente and Alvaro E. Cardenas, "Understanding Security Threats in Consumer Drones Through the Lens of the Discovery Quadcopter Family," Proceedings of the 2017 Workshop on Internet of Things Security and Privacy, Dallas, Tex.: Association for Computing Machinery, 2017.

[1]) Fernando Trujano, and others, op. cit., P:3

من المخاطر أثناء التشغيل والاستخدام الفعلي على الطرق، من قبل الأفراد والمؤسسات، من أبرز هذه المخاطر ما قد ينجم عن اختراق النظام الإلكتروني للمركبة، وهو ما يندرج ضمن مخاطر المساس بالأمن الإلكتروني (Electronic Security) أو الأمن السيبراني (Cyber Security).

الفرع الأول

فاعلية تقنية المركبات ذاتية القيادة مرهون باتباع معايير السلامة

أشارت بعض الدراسات حول فاعلية المركبات ذاتية القيادة أنها سوف تحدث ثورة في الكيفية التي يتنقل بها الناس، في طرق معيشتهم، وعملهم وتفاعلهم مع الآخرين. لكن هناك ثورة أكثر هدوءا تحدث في الوقت الذي تدفعنا تقنية المركبات ذاتية القيادة إلى إعادة النظر في سُبل تصور وقياس وتنظيم السلامة المرورية، وتشير دراسة أجريت عام ٢٠٢٠م([1]) إلى ضرورة الاستعداد أمنيا وتشريعيا للمشكلات التي ستتسبب فيها هذه المركبات وكيفية التعامل معها لاسيما فيما يتعلق بحركة المرور، وهناك تحدي

[1]) Sean E. Goodison and others, Autonomous Road Vehicles and Law Enforcement, published by RAND Corporation, 2017, P: 1, available at: file:///C:/Users/HP/Downloads/RAND_RRA108-4.pdf/2/1/2021

حيث قدر معهد التأمين للسلامة على الطرق السريعة بالولايات المتحدة أن تزويد جميع المركبات بنظام تحذير الاصطدام الأمامي، ونظام التحذير من الانحراف عن مسار الطريق، وكذلك نظام الرؤية الجانبية، والمصابيح الأمامية، لو تم لكان من الممكن تجنب وقوع ثلث حوادث الاصطدام والوفيات. كما أشار التقرير إلى أن نظام المكابح التلقائي قد يقلل من حوادث الاصطدام خاصة عند استشعار وجود عائق في الطريق، وأخيرا تفعيل المستوى (٤) من نوعية هذه المركبات يقلل إلى حد كبير من حوادث الاصطدام التي مرجعها خطأ السائق مثل القيادة تحت تأثير الكحول.

James M. Anderson and others, op. cit., P: xiv.

يتمثل في فهم هذه المشكلات بل والفرص التي ستنشئها تلك المركبات ووضع الخطط والاستراتيجيات لمواجهتها.

تبدو حاجة إدارات إنفاذ القانون إلى التواصل بشكل آمن مع المركبات ذاتية القيادة؛ حيث إنه من المخاطر الأمنية لانتشار استخدام هذه المركبات ما قد يقوم به بعض المجرمين من ارتكاب بعض الأفعال الإجرامية بمساعدة تلك المركبات مثل: استخدامها في تهريب الأشخاص والمخدرات، انتهاك الخصوصية، مهاجهة المركبات الأخرى باستخدام برامج حاسوبية؛ لذلك يعد تحدياً كبيراً تدريب أفراد إدارات إنفاذ القانون على التكيف مع هذه السلوكيات والسيناريوهات المتوقعة واتخاذ الإجراءات المناسبة بشأنها([1]).

وتجدر الإشارة إلى أن المركبات ذاتية القيادة لديها القدرة على جمع البيانات، وتفسير محيطها، واتخاذ قرار بشأن المسار المناسب، وتنفيذ هذا القرار لفهم بيئتها، وتستفيد من مجموعة قوية من أجهزة الاستشعار، مثل كاميرات الفيديو، وكشف الضوء والمدى، وأجهزة استشعار الرادار، والموجات فوق الصوتية، والأشعة تحت الحمراء([2]). وعلى الرغم من توفر أجهزة الاستشعار المتطورة إلا أن عدم قدرة المركبات في

[1]) Sean E. Goodison and others, op. cit., P: 2.

[2]) كما أشار دليل المركبات المستقلة ذاتية القيادة أن التطور في أجهزة الاستشعار المتقدمة لجمع المعلومات عن البيئة المحيطة بالسيارة، والخوارزميات المتطورة لمعالجة بيانات الاستشعار والتحكم بالسيارة، والقوة الحسابية لتشغيل هذه الأجهزة في الزمن الفعلي، كل هذا أدى إلى تقليل الحوادث التي قد تعزى إلى أتمتة السيارة، فقد قطعت سيارة (غوغل) التي تعمل بشكل مستقل مسافة ٥٠٠,٠٠٠ ميل بدون أي حادث اصطدام يعزى إلى الأتمتة.

James M. Anderson and others, op. cit., P: 58-59.

التعرف على البشر والحيوانات والأشياء الأخرى بشكل دقيق يمثل عقبة كبيرة أمام انتشارها على نطاق واسع([1]).

كما ورد بالدليل أن هناك نقص في فهم التهديدات الإلكترونية ضد المركبات المملوكة للقطاع الخاص أو المركبات التجارية. كما أن هناك نقص في الفهم بشأن التهديدات السيبرانية لأنشطة إنفاذ القانون، على سبيل المثال: توقف حركة المرور، وتحديد الهوية(Identification)، ومفتاح القفل عن بُعد (Remote Lock Key)، واستخراج البيانات (Data Extraction)([2]). ونظرًا لتضخم عدد المركبات الخاصة والتجارية التي تتمتع بقدرات الأتمتة، يتوقع الخبراء أن تزداد الأمور المتعلقة بالسلامة العامة تعقيداً. كما ستظهر أنواع جديدة من الجرائم، مثل استخدام المركبات المستقلة في نقل المواد المهربة، واختراق أنظمة هذه المركبات لجمع بيانات السائقين، أو استخدامها في تعريض سلامة الآخرين وحياتهم للخطر([3]).

وبالنسبة لسيناريوهات العمل الشرطي فيما يتعلق بالمركبات المستقلة ذاتية القيادة، ناقش الخبراء أربعة سيناريوهات تتضمن التفاعلات المتوقعة بين إدارات إنفاذ القانون والمركيات ذاتية القيادة: ١- توقف حركة المرور أو حدوث اختناقات مرورية. ٢- الاصطدامات أو حدوث تصادمات بسيطة. ٣- حالات الطوارئ مثل: التحويلات،

[1]) Quain, John R., "These High-Tech Sensors May be the Key to Autonomous Cars," New York Times, September 26, 2019. Siddiqui, Faiz, "What Self-Driving Cars Can't Recognize May Be a Matter of Life and Death," Washington Post, November 11, 2019.
[2]) Sean E. Goodison and Others, Autonomous Road Vehicles and Law Enforcement, op. cit., P:8.
[3]) ibid, P:9.

عمليات إخلاء بعض الطرق. ٤– التفاعلات العرضية مثل: المركبات المستقلة ذاتية القيادة كمصدر للأدلة أثناء التحقيق. وقد أشار أعضاء لجنة الخبراء إلى أن الانتقال التدريجي نحو المركبات ذاتية القيادة سيتم خلال سنوات عديدة؛ حيث ستتشارك هذه المركبات وغيرها من المركبات الأخرى في الطريق، مما يعني أن إدارات إنفاذ القانون ستحتاج إلى مواصلة الأساليب الحالية لضبط السيارات التي تعمل بالسائق المباشر أثناء تعلم المهارات والتقنيات لمعالجة المركبات الآلية([1]).

وقد أشار الخبراء([2]) إلى أنه من المتوقع أن تستجيب الشرطة لحوادث المرور، سواء كانت تصادمات طفيفة مع أضرار محدودة في الممتلكات أو تصادمات كبيرة مع خسائر محتملة في الأرواح؛ نظرًا لأن المركبات الآلية قد تخفف أو تقضي على العوامل البشرية للتصادمات المرتبطة بالقيادة مثل: الإرهاق، والإلهاء، وقلة الخبرة، والقيادة العدوانية؛ ومع ذلك يؤكدون أنه من المحتمل آلا يؤدي استخدام إمكانيات المركبات ذاتية القيادة (AV) إلى القضاء على الاصطدامات التي ترجع لأسباب متنوعة، بما في ذلك الخطأ الميكانيكي، أو فشل أجهزة الاستشعار، أو تعطلها، أو اختراقها، أو إساءة استخدام الإنسان لهذه الإمكانيات.

وقد أثيرت تساؤلات للنقاش ومنها: ما الذي يحتاجه الضباط أو المستجيبون الأوائل للتصادم لمعرفته أو فعله مع مركبة ذاتية القيادة متعطلة؟ لا سيما في المواقف التي يصبح فيها سلوكها غير متوقع بسبب فشل المكونات الإلكترونية؟ كيف يحدد

[1]) Sean E. Goodison and Others, op. cit., P:11.
[2]) ibid.

المسؤولون نطاق المسؤولية بين السائقين أو الشركات المصنعة؟ من يمتلك البيانات التي تجمعها المركبات ذاتية القيادة الفعلية؟ وما وسائل حماية الخصوصية التي يجب أن يتوقعها المالكين أو الركاب؟

كما أشار الخبراء([1]) إلى أن التفاعل بشكل صحيح مع المركبات المستقلة ذاتية القيادة يتطلب أن تكون إدارة إنفاذ القانون قادرة على تحديد ما إذا كانت السيارة قادرة على العمل بشكل مستقل وما إذا كان مصرحًا لها القيام بذلك. قد يكون هذا أمرًا صعبًا بسبب تنوع الشركات المصنعة، وأنواع السيارات وطرازها، ومستويات التشغيل الآلي. وقد اقترح الخبراء إمكانية وضع ملصق على لوحة الترخيص كوسيلة لتقييم قدرات المركبات لاسيما القدرة على التوجيه والكبح، ويجب دمج هذه القدرات في التسجيلات الإلكترونية.

ومن الأمور التي يتوقف عليها نطاق المسؤولية القانونية فيما يتعلق بالمركبات ذاتية القيادة تحتاج إدارات إنفاذ القانون إلى تحديد ما إذا كانت هذه المركبات تعمل بدون تحكم بشري ونظام تشغيلها، وهذا أمر بالغ الأهمية؛ لأن كيفية عمل السيارة يمكن أن تأخذ في الاعتبار في تحديد السبب المحتمل للحادث. على سبيل المثال: قد يكون لدى الضابط مبررا قانونيا لإيقاف واعتقال شخصا مخمورا يمارس بعض السيطرة على مركبة من المركبات ذاتية القيادة لكن من المستويات([2])

---

[1]) ibid, P:12.

[2]) يشير دليل المركبات المستقلة ذاتية القيادة أن درجة الاستقلالية أو الخضوع للسائق البشري تختلف باختلاف درجة المستوى، حيث أنه في المستوى (٠) تخضع السيارة لسيطرة كامل من السائق البشري، بينما في المستوى (١) هناك وظيفة من وظائف السيارة ذاتية التشغيل، وفي

من (٠ إلى ٣)؛ حيث يمكن للشخص التدخل في عمل المركبة وتشغيلها والتحكم في مسارها، بينما إذا الشخص نفسه في مركبة تعمل من تلقاء نفسها أي في المستويين (٤ أو٥) لا يمكنه التدخل في عملها أو التحكم في مسارها، فلا ينسب إليه ارتكاب أي جريمة ، ولا يوجد مبرر قانوني لإيقافه، في هذا المثال، يحتاج الضباط إلى معرفة متى تعمل السيارة بدون سيطرة بشرية لمواصلة من عدمه، وقد ناقش الخبراء فكرة تمكين المركبات من إرسال إشارة إلكترونية يمكن قراءتها بواسطة إدارات إنفاذ القانون لتحديد ما إذا كانت السيارة تعمل بشكل مستقل بدون تدخل بشري أم لا.

وقد اقترح المشاركون طرقًا مختلفة لإدارات إنفاذ القانون للتواصل مع المركبات ذاتية القيادة مثل: مطالبتها بالتوقف عند التعرف على الأضواء الساطعة الحمراء والزرقاء لسيارة الدورية أو أصوات صفارات الإنذار منها ومع ذلك، هناك مشكلة محتملة تتمثل في أن الكاميرات الموجودة على المركبات الذاتية قد لا تتمكن من تمييز أضواء الشرطة عن الأضواء الساطعة الأخرى، وقد ذكروا أن التحدي

المستوى (٢) هناك أكثر من وظيفة من وظائف السيارة ذاتية التشغيل في ذات الوقت، مثل الإسراع أو التوجيه، مع بقاء السائق البشري في حالة يقظة وانتباه دائما، وفي المستوى (٣) تكون وظائف السيارة كاملة ذاتية التشغيل بما يسمح للسائق البشري أن يشعر بالأمان ويمارس بعض النشاطات الأخرى، وفي المستوى (٤) تعمل السيارة باستقلالية بحيث يمكنها القيادة بنفسها دون وجود السائق البشري.

See: James M. Anderson and others, op. cit., P: 2-3.

وقد أضاف البعض أن الاختلاف بين إمكانات المستوى (٤) والمستوى (٥) يتمثل في أن الأول يسمح بالقيادة المستقلة للمركبة بنفسها دون سائق بشري، مع فرض بعض القيود، مثل ما يتعلق بالوقت والمكان، في حين يسمح المستوى (٥) باستقلالية القيادة دون أية قيود من هذا القبيل.

Sean E. Goodison and Others, op. cit., P:٥.

المحتمل الآخر يتمثل في التباين والاختلاف في كيفية تجهيز سيارات الدوريات بأشرطة ضوئية وصفارات الإنذار، وقد ناقش الخبراء إمكانية تمكين سيارات الدوريات من إرسال إشارة إلكترونية إلى المركبات الآلية تطلب منها التوقف، كما أوضح خبراء إنفاذ القانون أن التوقف المروري يتطلب طريقة اتصال قوية بين الضباط والمركبات ذاتية القيادة. على سبيل المثال، قد يطلب الضباط من المركبة التوقف في مكان معين أو بطريقة معينة، ويمكن للضابط توصيل أمر التوقف بسهولة عبر مكبر صوت عندما تكون السيارة تخضع لسيطرة الإنسان، لكن الضباط ليس لديهم حاليًا طريقة قوية لتوصيل أوامر التوقف إلى المركبات ذات القيادة المستقلة عن تحكم البشر، وقد أشار الخبراء إلى أن بعض المحاولات لتطوير أنظمة الاتصال المرئي بائت بالفشل([1]).

كما أكد الخبراء أن أنظمة الاتصالات الرقمية يجب أن تسمح بحدوث تواصل متفاعل عبر قنوات اتصال موحدة بين جميع سيارات الدوريات والمركبات ذاتية القيادة بحيث يكون الاتصال ثنائي الإتجاه ممكنًا([2]) بحيث يمكن للمركبات أو المالكين لها التواصل مع دوريات إنفاذ القانون للتبليغ عن عدم قدرة المركبة على التوقف، كما لو كان بسبب كسر جهاز الاستشعار أو إذا كانوا بحاجة إلى وقت إضافي لتنفيذ التوقف بأمان، يعتقد المشاركون في الدراسة أن المركبات لن تستفيد من القدرة على التعرف

---

[1]) Sean E. Goodison and Others, op. cit., P:12.

[2]) ذكر تقرير المركبات المستقلة ذاتية القيادة أن توفير قنوات للتواصل بين المركبة ذاتية القيادة ومركبة أخرى أو بينها وبين البنية التحتية يواجه تحديات عملية وتكنولوجية.
See: James M. Anderson and others, op. cit., P: 67.

على أوامر الكلام أو إيماءات اليد بسبب القيود التكنولوجية ومخاطر الانتحال؛ حيث إن أية أنظمة اتصال تم تطويرها من أجل التواصل مع المركبات المساعدة يجب أن تكون آمنة بحيث لا يتم الوصول إليها من قبل جهات غير الشرطة لأغراض خبيثة، ويجب أن تكون هناك آلية داخل هذه الأنظمة لمصادقة الأوامر الصادرة للمركبات للتأكد من أنها من أفراد إنفاذ القانون المخولين، ينطبق هذا القلق –أيضًا– على كل طرق الاتصال التي تتضمن الأضواء أو صفارات الإنذار، والتي يمكن تصنيعها باستخدام الأجهزة المتاحة تجاريًا من قبل جهات غير شرطية لسحب المركبات المساعدة([1]).

فيما يتعلق بالتدريب على التعامل مع المركبات ذاتية القيادة:

كان من الواضح من مناقشة الخبراء في ورشة العمل أن هناك حاجة ماسة لبروتوكولات معيارية وأنظمة تدريب يتم وضعها للتحكم في تفاعلات التعلم الذاتي مع المركبات ذاتية القيادة. وعلى الرغم من أن المشاركين في الورشة اتفقوا على أن المركبات ذاتية القيادة عالية الإمكانيات التقنية (أي المستوى ٤) من المحتمل ألا تكون مصدر قلق كبير لإدارات إنفاذ القانون خلال السنوات الخمس المقبلة، وأن هذا هو الوقت المناسب لتطوير التدريب بشكل استباقي. كما أعرب الخبراء عن الحاجة إلى التأكد من أن جميع المركبات ذاتية القيادة المملوكة للقطاع الخاص، وتلك المملوكة للقطاع الحكومي مبرمجة لتتصرف بنفس الطريقة في كل تفاعل مع المستجيبين الأوائل حتى لا تضطر الإجراءات إلى التغيير بناءً على طراز السيارة

[1]) Sean E. Goodison and Others, op. cit., P:12.

هذه أو تلك، وأوضحوا أن الإجراءات يجب أن تكون سهلة ومباشرة لتحقيق أقصى قدر من سلامة الضباط. كما يجب أن يكون الضباط قادرين على فهم كيف ولماذا تتصرف السيارة بطريقة معينة؟ ([1]). ومن الأهمية بمكان بالنسبة لرجال إنفاذ القانون والمطورين للمركبات المستقلة ذاتية القيادة العمل معًا لتحديد كيفية حدوث هذه التفاعلات بين رجال إنفاذ القانون وبين تلك المركبات.

أوصى المشاركون في ورشة العمل بضرورة إنشاء هيئة أو سلطة لوضع معايير وطنية لصناعة هذه المركبات، وشدد الخبراء على إلزام الشركات التي تشغل المركبات المستقلة ذاتية القيادة بوضع وسائل قياسية للتفاعل مع إنفاذ القانون قبل تسيير مركباتها على الطرق([2]). كما أوصوا بضرورة عقد ورش عمل للعاملين في مجال إنفاذ القانون لرفع مستويات المعرفة فيما يتعلق بالمركبات ذاتية القيادة مع ضرورة إجراء مسح لخبراء إنفاذ القانون لتحديد نوع المعلومات الأكثر فائدة لهم في مجال هذه.

في سياق متصل نجد المشرع بإمارة دبي، بدولة الامارات العربية المتحدة، يصدر القانون رقم (٩) لسنة ٢٠٢٣م سالف الذكر، في شأن تنظيم تشغيل المركبات ذاتية القيادة في إمارة دبي، والذي نص على منح هيئة الطرق والمواصلات بإمارة دبي الاختصاص بكل ما يتعلق بالمركبات ذاتية القيادة، وحدد اختصاصاتها بموجب المادة (٣) من القانون، من أهمها: ٣- اعتماد المعايير الفنّية والتشغيليّة ومعايير الأمن

[1]) Sean E. Goodison and Others, op. cit., P:15.
[2]) ibid.

والسّلامة وتقييم أداء المُشغِّل، الواجب توفُّرها لسير المركبة ذاتيّة القيادة على الطّريق، ومُراجعتها بشكلٍ دوري.

١٣–التعاون والتنسيق مع الجهات المُختصّة، وتشكيل فرق العمل المُشتركة في كُل ما من شأنِه تحقيق أهداف هذا القانون.

١٥–عقد الاتفاقيّات وتأسيس الشّراكات مع الجهات المُختصّة والمُنظّمات والمُؤسّسات والهيئات الدوليّة المعنيّة بالمركبات ذاتيّة القيادة، من أجل ضمان تحقيق أهداف هذا القانون". ([1]).

---

[1]) من المهام والصلاحيات الممنوحة للهيئة بموجب نص المادة (٣) من القانون مايلي:

١- وضع السِّياسات والخطط الإستراتيجيّة لرفع كفاءة وتشغيل وتطوير المركبات ذاتيّة القيادة في الإمارة.

٢- تحديد فِئات وأنواع وأصناف المركبات ذاتيّة القيادة، وفقاً للمعايير والمُواصفات والضّوابط المُعتمدة من الجهات المُختصّة.

٣- اعتماد المعايير الفنّية والتشغيليّة ومعايير الأمن والسّلامة وتقييم أداء المُشغِّل، الواجب توفُّرها لسير المركبة ذاتيّة القيادة على الطّريق، ومُراجعتها بشكلٍ دوري.

٤- تحديد مراحل تشغيل المركبة ذاتيّة القيادة في الإمارة، بناءً على خطط التشغيل التي يصدُر باعتمادِها قرار من رئيس المجلس التنفيذي.

٥- تحديد الطُّرق والمناطق والمسارات التي يُسمَح بتشغيل المركبة ذاتيّة القيادة فيها، وكذلك تحديد سُرعتِها، وغير ذلك من المسائِل المُرتبِطة بتنظيم سيرها على الطّريق.

٦- تجهيز البنى التحتيّة اللازمة لتشغيل المركبة ذاتيّة القيادة، وفقاً للمعايير والمُواصفات المُعتمدة في هذا الشأن.

٧- وضع الحلول المروريّة والقواعد والإجراءات اللازمة للحفاظ على سلامة أنظمة السّير والمُرور في الإمارة، بما في ذلك القواعد المُتعلِّقة بالمُشاة والمركبات، بما فيها المركبة ذاتيّة القيادة، بما يضمن سلامة مُستخدِمي الطّريق، وتقليل نِسَب المُخالفات المُروريّة.

٨- ترخيص المركبة ذاتيّة القيادة، وفقاً للشُّروط والإجراءات المُعتمدة لديها في هذا الشأن.

الفرع الثاني

الثغرات والأثار الأمنية لاختراق تقنية المركبات ذاتية القيادة

من التحديات الأمنية للمركبات المستقلة ذاتية القيادة (AV) التأكد من موثوقية البرمجيات والخوارزميات والأنظمة المعقدة في المركبة، فقد تحتاج هذه البرمجيات والأنظمة إلى التحسينات التي تضمن تغلبها على الثغرات الأمنية التي قد

٩- جراء الفحص الفنّي للمركبة ذاتيّة القيادة، وفقاً للمعايير والضّوابط والإجراءات المُعتمدة لديها في هذا الشأن.

١٠- تحديد الأنشِطة التي يُسمَح فيها باستعمال المركبة ذاتيّة القيادة، بالتنسيق مع الجهات المُختصّة في الإمارة، ورفعها إلى رئيس المجلس التنفيذي لاعتمادِها، وإصدار التصاريح اللازمة لمُزاولتِها، وفقاً للشُّروط والإجراءات المُعتمدة لديها في هذا الشأن.

١١- جمع وتصنيف البيانات النّاتِجة عن تشغيل وقيادة المركبة ذاتيّة القيادة في الإمارة.

١٢- الرّقابة والتفتيش على المُصرَّح له، للتأكُّد من التزامِه بأحكام هذا القانون والقرارات الصّادرة بمُوجبِه.

١٣- التعاون والتنسيق مع الجهات المُختصّة، وتشكيل فرق العمل المُشتركة في كُل ما من شأنِه تحقيق أهداف هذا القانون.

١٤- تلقّي الشّكاوى المُقدَّمة بحق المُصرَّح له، والتحقيق فيها، واتخاذ الإجراءات اللازمة بشأنِها.

١٥- عقد الاتفاقيّات وتأسيس الشّراكات مع الجهات المُختصّة والمُنظّمات والمُؤسّسات والهيئات الدوليّة المعنيّة بالمركبات ذاتيّة القيادة، من أجل ضمان تحقيق أهداف هذا القانون.

١٦- وضع الخطط والإستراتيجيّات والإجراءات اللازمة لتسهيل الاستثمار في الأنشِطة المُرتبِطة بالمركبات ذاتيّة القيادة، بالتنسيق مع الجهات المُختصّة.

١٧- أي مهام أو صلاحيّات أخرى تكون لازمة لتحقيق أهداف هذا القانون، يتم تكليفُها بها من الحاكم أو رئيس المجلس التنفيذي.

تعرضها للهجوم الإلكتروني أو السيبراني؛ حيث يشترط أن تكون هذه التحسينات متوافقة مع أحدث الإصدارات في نماذج المركبات المستقلة خاصة أجهزة الاستشعار ونظام الملاحة، وقنوات الاتصال قصيرة المدى، كما ينبغي أن تكون تلك التحسينات تعمل على منصات متغيرة على نحو متزايد، مما يضفي عليها أقصى درجات الموثوقية والجودة([1]).

ويشير دليل المركبات المستقلة ذاتية القيادة إلى أن مسألة إدخال التحسينات على برمجيات المركبات يسلط الضوء على مسألة في غاية الخطورة والأهمية ألا وهي مسألة أمن النظام؛ إذ إن المركبات المتصلة ببعضها البعض (اتصال مركبة بمركبة أخرى) أو بالبنية التحتية أو بالإنترنت (قنوات الاتصالات) يجعلها أكثر عرضة للهجمات والاختراقات الإلكترونية([2])، وقد أشار بعض الخبراء في السلامة المرورية على الطرق السريعة إلى أن هذا التطور (المركبات المستقلة) يجلب معه تحديات متزايدة، في مجال موثوقية النظام والأمن الإلكتروني، الذي يبدو خطرا أكثر فأكثر؛ إذ إن هذه المركبات أصبحت متصلة أكثر بمجموعة من المنتجات، سواء أكان المدخل إلى تلك المركبات عبر الإنترنت، أم كان عبر الأجهزة الأخرى المتوفرة في الأسواق، أم عبر منافذ الناقل العام (USB) أم عبر الهواتف الذكية، كل هذه المنافذ أو المداخل للمركبات المستقلة تجلب معها تحديات كبيرة.

---

[1]) James M. Anderson and others, Autonomous Vehicle Technology, A Guide for Policymakers, op. cit., P: 70.

[2]) Manar Abu Talib and Others, Systematic literature review on Internet-of-Vehicles communication security, International Journal of Distributed Sensor Networks, Vol. 14(12), 2018, P:2.

ويشير الدليل إلى أن المركبات غير الموصولة -أيضاً- ليست بمنأى عن الخطر؛ إذ إن تحسينات البرمجيات تتطلب الاتصال عبر شبكة الإنترنت، مما يجعلها عرضة لهجوم فيروسي باستخدام برامج حاسوبية مخربة أو مدمرة للنظام، فقد يتمكن شخص أو أشخاص من اختراق أنظمة التشغيل، والاستيلاء على مركبة أو أكثر من المركبات المستقلة ذاتية القيادة، واستغلالها في ارتكاب أعمال إجرامية أو إرهابية([١]).

بالإضافة إلى احتمالية قيام المخترق أو المهاجم بالتشويش على أنظمة الملاحة أو النظام العالمي لتحديد المواقع (GPS) أو تعطيل أجهزة الاستشعار، أو التأثير على دقتها في التعرف على البيئة المحيطة بالمركبة المستقلة، وقد يؤدي إلى تعطيل نظام الكبح أو عجلة القيادة مما قد يتسبب في حوادث تصادم([٢]). والأخطر من ذلك أنه من الصعب اكتشاف الرسائل المزيفة التي أرسلها المخترق ودفعت أجهزة الاستشعار إلى إعطاء قراءات كاذبة([٣]). كما يمكن أن يؤدي نشر المعلومات المزيفة التي تم إنشاؤها بواسطة المهاجمين حول وجود اختناقات أو وقوع حوادث طرق غير موجودة إلى تحويل حركة المرور بشكل ضار، قد يكون لأغراض السرقة أو الاختطاف أو إختفاء السيارات، وقد يضر بالسائقين أو بسلامة المركبات وأمنها([٤]).

كما أشار دليل صانعي المركبات ذاتية القيادة إلى أن السلوك الفضولي لبعض المستخدمين أو المالكين في القيام بإجراء تعديل على نظام الحماية لتغيير بعض

---

[1]) James M. Anderson and others, op. cit., P:70.
[2]) Manar Abu Talib and Others, op. cit., P:٣.
[3]) James M. Anderson and others, op. cit., P:71.
[4]) Manar Abu Talib and Others, op. cit., P:٢.

البرمجة لوظائف المركبة دون تخويل ذلك من الشركة المصنعة قد يتسبب في إحداث خلل في نظم التشغيل والتأمين، والإخلال بمعايير السلامة لدى المركبة، كما أكد الدليل على أن تقنية هذه المركبات مثلها مثل أي تقنية أخرى قابلة للاختراق والفشل في ظروف معينة، بيد أن نظم هذه المركبات قادرة على اكتشاف أي من هذه الحالات والتعامل معها بأمان، إما بتحويلها إلى نظام سلامة بسيط يخضع للرقابة الشديدة، وإما بالتوقف كلية عن العمل([1]).

[1]) James M. Anderson and others, op. cit., P:71.

المطلب الثالث

صور الاختراق الإلكتروني لأنظمة الطائرات المسيرة ذاتياً والمركبات ذاتية القيادة

عرضنا فيما سبق لإمكانية تعرض تقنيات الذكاء الاصطناعي ومنها: الطائرات بدون طيار، لاسيما المسيرة ذاتياً، وكذلك المركبات المستقلة ذاتية القيادة للاختراق من قبل المهاجمين السيبرانيين، ونعتقد أن الاختراق الإلكتروني لأنظمة هذه الطائرات أو المركبات يكتسب أهمية خاصة؛ نظرا لتزايد الاعتماد عليها في العديد من القطاعات لاسيما القطاع الشرطي، ومن ثم قد يستهدف المهاجمون إساءة استغلال تلك التقنيات في القيام بأفعال إجرامية خطيرة جداً تهدد الأمن القومي؛ عن طريق اختطاف الطائرة المسيرة واستغلالها في أعمال هجومية أو إرهابية، كما قد تستخدم المركبة ذاتية القيادة في ارتكاب بعض الأفعال الإجرامية مثل: تهريب المخدرات، قتل ودهس الأشخاص أو ارتكاب أعمال إرهابية، وقد يحدث ذلك بالتلاعب في أنظمة الملاحة أو النظام العالمي لتحديد المواقع (GPS) مما قد يترتب عليه تعطيلها أو تعطيل أجهزة الاستشعار، وأجهزة تعرف المركبة ذاتية القيادة على البيئة المحيطة بها (أجهزة الاستشعار) مما يؤدي حتماً إلى وقوع تصادمات أو حوادث مرورية تهدد سلامة وأرواح الأفراد للخطر.

الفرع الأول

اختطاف الطائرة المسيرة ذاتياً بالاختراق الإلكتروني لأنظمة تشغيلها

يعد الاختطاف الالكتروني من أخطر الأفعال الإجرامية التي يمكن تصور وقوعها على أنظمة تشغيل الطائرات المسيرة، ومن ثم يقتضي الأمر بحثه من الناحية التقنية، وكيفية حدوثه، كذلك بحثه من الناحية القانونية، والوقوف على ما يثيره فعل اختطاف الطائرة المسيرة إلكترونياً من صور تجريمية وفق قانون العقوبات أو أي قانون آخر.

أولًا– إمكانية حدوث الاختطاف الإلكتروني للطائرة المسيرة تقنياً:

أشار البعض إلى واقعة اختطاف طائرة بدون طيار في منتصف رحلتها؛ حيث قام المهاجم بحذف نظام الملفات بأكمله، وهو ما تسبب في تعطل الطائرة([1])؛ فقد استغرق أربعة باحثون من معهد ماساتشوستس للتكنولوجيا شهرًا في تحديد الثغرات الأمنية على طائرة بدون طيار شهيرة من نوع (DJI Phantom 3). وتحديد صور إساءة استغلالها. وقد استخدم الباحثون أدوات رسم خرائط الشبكة لالتقاط الحزم الصادرة من الأنظمة الفرعية الرئيسية الثلاثة: الطائرة بدون طيار، والكاميرا، ووحدة التحكم الخاصة بها، وقد حصل الباحثون على حق الوصول إلى المصدر من خلال استغلال ضعف تأمين كلمة مرور الجهاز. ومن ثم الوصول إلى نظام ملفات الطائرة بدون طيار ومن ثم تعديلها، والذي بدوره يسمح للمهاجم بتعديل مسارات الطيران.

[1]) Fernando Trujano and others "Security Analysis of DJI Phantom 3 Standard," op. cit.

كما يمكن الوصول إلى الكاميرا؛ ومن ثم الوصول إلى الصور ومقاطع الفيديو للقيام بحذفها أو نسخها. وأخيرًا، حدد الباحثون ثغرة أمنية في تطبيق (Android) للطائرة بدون طيار، والتي من شأنها أن تسمح للمهاجمين بتجاوز القيود المفروضة على دخول المجال الجوي المحظور من قبل لجنة الاتصالات الفيدرالية.

ثانياً- الوصف الجنائي لفعل الاختطاف الإلكتروني للطائرة المسيرة:

يثير فعل اختطاف الطائرة بدون طيار، خاصة المسيرة ذاتياً مدى انطباق وصف جريمة الهجوم على طائرة أو سفينة المنصوص عليه في الفقرة الأولى من المادة (٣٣٨) من قانون الجرائم والعقوبات الاماراتي([1])، والتي نصت على عقوبة السجن المؤبد لكل من هاجم طائرة أو سفينة بقصد الاستيلاء عليها أو على البضائع التي تحملها أو إيذاء أحد فيها أو تحويل مسارها بغير مقتضى. يمكننا التأكيد على أن الجريمة السابقة تدخل ضمن جرائم الاعتداء على وسائل المواصلات والمرافق العامة، إذ ينصرف مقصد المشرع إلى الطائرات التقليدية المستخدمة في النقل الجوي للأشخاص أو البضائع، ومن ثم لا ينصرف التجريم إلى فعل الاختطاف الإلكتروني للطائرة المسيرة؛ حيث إنها لا تعد من قبيل وسائل المواصلات أو النقل العام. كما لا ينطبق وصف التجريم المنصوص عليه في المادة (٣٣٩) من قانون الجرائم والعقوبات، والتي تعاقب بالسجن المؤقت كل من عرض عمدا للخطر -بأية وسيلة

[1]) تنص هذه المادة على أنه "يعاقب بالسجن المؤبد كل من هاجم طائرة أو سفينة بقصد الاستيلاء عليها أو على كل أو بعض البضائع التي تحملها أو بقصد إيذاء واحد أو أكثر ممن فيها أو بقصد تحويل مسارها بغير مقتضى".

كانت– سلامة سفينة أو طائرة أو أي وسيلة من وسائل النقل العام، يقابله نص المادة (١٦٧) من قانون العقوبات المصري رقم ٣ لسنة ١٩٣٧م وفق أحدث تعديلاته([1]).

بيد أنه يمكن انطباق وصف جريمة الاعتداء على الآلات أو الأدوات اللازمة لمنع الحوادث أو كاميرات المراقبة، المنصوص عليها في الفقرة الأول من المادة (٣٤٤) من قانون الجرائم والعقوبات الاماراتي، سواء اتخذ فعله صورة نزعها أو كسرها أو إتلافها جعلها غير صالحة للاستعمال أو عطلها بأية كيفية كانت([2])، وذلك على اعتبار الطائرة بدون طيار، لاسيما المسيرة ذاتياً، من قبيل التقنيات الذكية التي تستخدم في مراقبة الطرق والتجمعات والاحتفالات والمهرجانات لأغراض أمنية منها: منع الحوادث، أو مراقبة الحركة المرورية، أو التنبؤ بارتكاب جرائم. مع ملاحظة أن هذا الوصف لا ينطبق إذا اتخذ فعل الجاني صورة اختطاف الطائرة أو الاستيلاء عليها، ولكن ينطبق إذا ترتب على فعل الاختراق الالكتروني لأنظمة التشغيل تعطل الطائرة عن العمل.

ويمكن بحث المسألة من زاوية جرائم الاعتداء على الأموال، على اعتبار الطائرة المسيرة مالاً مملوكاً للغير، ومن ثم تقوم بفعل الخاطف جريمة السرقة، إذا كان غرضه

[1]) جاء بنصها: "كل من عرض للخطر عمداً سلامة وسائل النقل العامة البرية أو المائية أو الجوية أو عطل سيرها يعاقب بالسجن المشدد أو بالسجن".

[2]) نصت على أنه "يعاقب بالحبس مدة لا تقل عن سنة وبالغرامة التي لا تقل عن (٥٠,٠٠٠) خمسين ألف درهم كل من نزع عمدا إحدى الآلات أو الأدوات أو الإشارات اللازمة لمنع الحوادث أو كاميرات المراقبة، أو كسرها أو أتلفها أو جعلها غير صالحة للاستعمال، أو عطلها بأية كيفية كانت".

الاستيلاء عليها بنية تملكها. هذا بالإضافة إلى جريمة الاختراق الإلكتروني لنظام معلوماتي أو وسيلة تقنية معلومات أو شبكة معلوماتية والمنصوص عليها في المادة (٢) من المرسوم بقانون اتحادي رقم ٣٤ لسنة ٢٠٢١م سالفة الذكر، مع ملاحظة أن هذه الجريمة تعد من الجرائم المرتبطة ارتباطاً لا يقبل التجزئة بجريمة سرقة الطائرة بدون طيار، باعتبار أن الاختراق كان وسيلة الاستيلاء عليها.

وفي هذا المقام يشير الباحث إلى موقف المشرع بإمارة دبي حيث أفرد نصاً خاصاً لبيان أفعال التدخل غير المشروع التي تقع على الطائرات بدون طيار، وذكر منها، فعل الاستيلاء على طائرة بدون طيار، بيد أنه لم يقرر عقوبة جزائية، مكتفياً بالإشارة إلى أن مخالفة ذلك يوقع مرتكبها تحت طائلة المساءلة القانونية([1])، دون أن يوضح صورة المسؤولية، وما إذا كانت تقتصر على المساءلة المدنية أم تمتد إلى المساءلة الجزائية دون وصف صور وحدود المسؤولية. ومن ثم نوصي بضرورة تدخل المشرع بالنص صراحة على تجريم فعل اختطاف الطائرة بدون طيار بنص خاص.

الفرع الثاني

اختطاف المركبة ذاتية القيادة

بالاختراق الإلكتروني لأنظمة تشغيلها

يعد الاختطاف الالكتروني من أخطر الأفعال الإجرامية التي يمكن تصور وقوعها على أنظمة تشغيل المركبة ذاتية القيادة، ومن ثم يقتضي الأمر بحثه من الناحية

[1]) المادة (٣٥) من قانون تنظيم الطائرات بدون طيار بإمارة دبي، رقم ٤ لسنة ٢٠٢٠م.

التقنية، وكيفية حدوثه، كذلك بحثه من الناحية القانونية، والوقوف على ما يثيره فعل اختطاف المركبة ذاتية القيادة إلكترونياً من صور تجريمية وفق قانون العقوبات أو أي قانون آخر.

أولاً– إمكانية حدوث الاختطاف الإلكتروني للمركبة المستقلة تقنياً:

أشار دليل المركبات المستقلة ذاتية القيادة إلى إمكانية تعرضها للاختطاف الإلكتروني من قبل مخترقي أنظمة التشغيل؛ حيث تكون المركبة عرضة لخطر الهجوم الإلكتروني على برمجيات التشغيل بإدخال برامج تبدو في ظاهرها غير ضارة، ولكنها مخادعة؛ يستطيع المهاجم من خلالها زرع فيروسات حاسوبية تمكنه من الاستيلاء على المركبة أو مركبات أخرى متصلة بها، سواء كان الاختراق غرضًا في حد ذاته أم كان بهدف السيطرة عليها لغرض ارتكاب أفعال إجرامية أو عمليات إرهابية([1]).

ثانياً– الوصف الجنائي لفعل الاختطاف الإلكتروني للمركبة ذاتية القيادة:

على خلاف ما أثير بالنسبة لفعل اختطاف الطائرة المسيرة، يمكن القول بانطباق وصف الجريمتين المنصوص عليهما في المادتين (٣٣٨)، (٣٣٩) من قانون الجرائم والعقوبات الاماراتي سالفتا الذكر، بالنظر إلى أن المركبة ذاتية القيادة يمكن اعتبارها من قبيل وسائل النقل، حال تشغيلها في نقل الأشخاص كسيارة أجرة؛ كما أعلنت هيئة الطرق والمواصلات بإمارة دبي عام ٢٠٢٢م([2])، بخلاف الحال في

[1]) James M. Anderson and others, Autonomous Vehicle Technology, A Guide for Policymakers, op. cit., P:70.

[2]) تم بالفعل تسيير مركبات ذاتية القيادة من انتاج شركة (تسلا) كسيارات أجرة للأشخاص في إمارة دبي بدولة الامارات العربية المتحدة فقط أعلنت هيئة الطرق والمواصلات دبي «RTA» بتاريخ

القانون المصري؛ حيث لا يمكن اعتبار السيارة ذاتية القيادة من وسائل النقل العام؛ حيث لم يعلن عن استخدام تلك السيارات ضمن منظومة سيارات الأجرة؛ كما هو الحال في إمارة دبي؛ ومن ثم يمكن القول بعدم انطباق وصف الجريمة الوارد بالمادة (١٦٧) من قانون العقوبات المصري، سالفة الذكر.

وفي إطار معالجة فعل الاختطاف الإلكتروني للسيارة ذاتية القيادة في ضوء أحكام قوانين مكافحة الارهابية، يمكن القول بانطباق وصف الجريمة المنصوص عليها في المادة (٥) من المرسوم بقانون اتحادي رقم (٧) لسنة ٢٠١٤م في مكافحة الجرائم الإرهابية الاماراتي، والتي تعاقب على فعل اختطاف وسيلة من وسائل النقل لغرض إرهابي([1]). كذلك الحال، بالنسبة لوصف الجريمة المنصوص عليها في المادة (٦) من المرسوم ذاته، والتي تعاقب على فعل إتلاف أو تعطيل أو التعريض عمداً سلامة وسيلة من وسائل النقل لغرض إرهابي([2]).

---

٣ يوليو ٢٠٢٢م عن البدء بتشغيل سيارة «تسلا ٣ – Tesla 3» ضمن أسطول تكسي دبي بهدف تجربة مدى فعالية استخدام السيارات الكهربائية كسيارات أجرة داخل دبي، بعد النجاح الذي حققه استخدام ١٧٢ سيارة «Tesla» منذ عام ٢٠١٧ في خدمة الليموزين التابعة لمؤسسة تكسي دبي.
آفاق حياري، مقال بعنوان، الإمارات: هيئة الطرق والمواصلات تشغل سيارة تسلا ٣ كسيارة تكسي في دبي، منشور على موقع سولارابيك، بتاريخ ٦ يوليو ٢٠٢٢م، على الرابط الآتي:
https://solarabic.com/latest/2022/07/tesla-3-

[1]) حيث جاء بنصها "١-يُعاقب بالسجن المؤبد كل من اختطف لغرض إرهابي وسيلة من وسائل النقل الجوي أو البري أو المائي".

[2]) ١ – يعاقب بالسجن المؤبد كل من أتلف أو عطل أو عرض عمداً للخطر وسيلة من وسائل النقل الجوي أو البري أو المائي او إحدى منشآت الملاحة الجوية أو البرية أو المائية أو عرقل الخدمات فيها وكان ذلك لغرض إرهابي.

ولكن يشترط لإعمال نص المادتين السابقتين أن يكون فعل الاختطاف الإلكتروني في المادة الأولى، وأفعال الإتلاف أو التعطيل أو التعريض للخطر في المادة الثانية لتحقيق غرض إرهابي، ومن ثم لا ينطبق وصفي التجريم السابقين إذا ارتكب الفعل لأغراض أخرى، وقد حدد المشرع الإماراتي مفهوم الغرض الارهابي في المادة الأولى من المرسوم بقانون رقم ٧ لسنة ٢٠١٤م سالف الذكر([1]).

لكن يدق الأمر بالنسبة لفعل الاختطافالإلكتروني لسيارة ذاتية القيادة تستخدم من قبل الأجهزة الأمنية وإدارات الشرطة مثل: الدوريات الذكية؛ حيث لا يمكن اعتبارها من وسائل النقل، ومن ثم لا ينطبق التجريم السابق على هذا الفعل، ولكن يمكن القول بانطباق نص المادة (٣٤٣) من قانون الجرائم والعقوبات الاتحادي، والتي عاقبت في فقرتها الثانية على فعل التعريض عمداً سلامة وسيلة من وسائل النقل الخاصة بالأجهزة الأمنية والشرطية للخطر، أياً طريقة كانت([2]).

ولا شك أن السيارات ذاتية القيادة التي تستخدمها دوائر وإدارات الشرطة في الدوريات تعد من وسائل النقل الخاصة بالأجهزة الشرطية المذكورة بالنص السابق، كما يمكن القول أن المشرع الإماراتي لم يحدد طريقة معينة للتعريض للخطر، ومن ثم تقع

[1]) حيث عرفه بأنه "اتجاه إرادة الجاني الى ارتكاب فعل أو الامتناع عن فعل، متى كان هذا الارتكاب أو الامتناع مجرماً قانوناً وذلك بقصد إحداث نتيجة إرهابية مباشرة أو غير مباشرة أو علم الجاني بأن من شأن الفعل أو الامتناع عن الفعل، تحقيق نتيجة إرهابية".

[2]) جاء بنصها "يعاقب بالحبس كل من عرض للخطر عمداً سلامة وسيلة من وسائل النقل الخاص بأية طريقة كانت. وتكون العقوبة السجن المؤقت إذا وقع الفعل عمداً على وسائل النقل الخاصة بالأجهزة الأمنية أو الشرطية".

الجريمة بأي طريقة، ومنها الاختراق الإلكتروني لأنظمة التشغيل، والذي يفترض فيه أن يقع عمداً، وهو ما اشترطه المشرع في كون الجريمة من الجرائم العمدية صراحةً.

برغم ما تقدم، نجد أن النص السابق يعالج فقط تعريض سلامة وسيلة النقل للخطر، لكن لا يمتد إلى فعل اختطاف السيارة أو الإستيلاء عليها، ومن ثم نوصي بضرورة تدخل المشرع الإماراتي بالنص صراحة على جريمة الاختطاف الإلكتروني للسيارة ذاتية القيادة بنص خاص.

الفرع الثالث

تعطيل نظام تحديد المواقع العالمي (GPS)

أولاً- الإمكانية التقنية لتعطيل نظام تحديد المواقع:

أظهر اختبار ميداني أن حدوث هجوم مخادع (Deceptive Attack) لنظام تحديد المواقع العالمي (GPS) ضد الطائرات بدون طيار أمرًا ممكنًا تقنيًا وعمليًا([1])؛ فقد اقترح أربعة باحثين في جامعة (Texas) في (Austin) طريقة للسيطرة على طائرة بدون طيار ونفذوها عن طريق إرسال إشارة GPS خادعة. وفي الهجوم المقترح يتلقى جهاز الانتحال إشارات صحيحة من أقمار GPS الصناعية؛ ثم يُولّد المخادع سلسلة من الإشارات المزيفة التي تجبر جهاز استقبال الطائرة على إرسال إشارات السرعة والوضع الوهمي؛ ثم بمجرد أن يمارس المخادع السيطرة على الجهاز، يمكنه التلاعب بمسار رحلة الطائرة.

[1]) Kerns, Andrew J., Daniel P. Shepard, Jahshan A. Bhatti, and Todd E. Humphreys, "Unmanned Aircraft Capture and Control Via GPS Spoofing," Journal of Field Robotics, Vol. 31, No. 4, July/ August 2014, pp. 617–636.

كما يمكن أن تكون المركبات ذاتية القيادة معرضة لخطر التشويش على نظام الملاحة العالمي (GPS) بإرسال رسائل تشويش لتعطيل أجهزة الاستشعار أو إرسال قراءات مزيفة أو كاذبة لهذه الأجهزة في المركبة، بما يؤثر على تحليل المركبة لعناصر البيئة المحيطة، والتعرف على معوقات السير مما قد يتسبب في حوادث تصادم([1]).

ثانياً– الجرائم المرتبطة بفعل تعطيل نظام تحديد المواقع:

بحسب الغرض الذي يسعى إليه المخترق لأنظمة الملاحة أو تحديد المواقع العالمي أو أجهزة الاستشعار تتحدد المسؤولية الجنائية له، بمعنى إذا تعمد من فعله دهس أحد الأشخاص كنا بصدد جريمة عمدية مكتملة الأركان، بغض النظر عن وسيلة القتل، بينما يسأل عن قتل غير عمدي إذا جاء فعله على سبيل التفاخر بقدرته على التحكم في السيارة ذاتية القيادة عن بعد، أو كان على سبيل المزاح، ثم يتسبب في دهس أحد المارة لعجز المركبة عن التعرف عليه بسبب تشويش أو خلل في أجهزة الاستشعار.

بينما يسأل عن جريمة إتلاف إذا كان غرضه مجرد تدمير السيارة أو إتلافها بحدوث تصادم بينها وبين مركبات أخرى، أو تسبب في سقوطها من مكان مرتفع بسبب خلل في أنظمة تحديد المواقع. هذا بالإضافة إلى جريمة تعريض الغير للخطر إذا سيطر على المركبة أثناء رحلتها بوجود الركاب فيها، وتحكم في مسارها بشكل يعرضها للخروج عن المسار ويعرضها للجنوح.

[1]) James M. Anderson and others,, op. cit., P:71.

الفصل الثاني

مشروعية استخدام تطبيقات الذكاء الاصطناعي

في العمل الشرطي والقضائي

تمهيد:

من الإشكاليات التي تواجه استخدام تقنيات الذكاء الاصطناعي في العمل الشرطي والقضائي ما يتعلق بوجوب تمتع هذا الاستخدام بالمشروعية، وفق ما استقر عليه العمل بقانون الإجراءات الجنائية، وإعمالاً لمبدأ الشرعية الإجرائية الذي يقتضي أن تكون كافة الإجراءات من رجال الشرطة وسلطات التحقيق تحت مظلة قانون الإجراءات الجنائية. من ذلك ما أثاره استخدام تقنيات الطائرات بدون طيار، لاسيما المسيرة ذاتياً، والمركبات ذاتية القيادة، المزودة بتقنيات التعرف على الوجه والصوت، وكذلك الروبوتات فائقة الذكاء في العمل الشرطي والقضائي من نقاش حول مشروعيته مع اختلاف الحكم بين استخدامها مع جمهور الناس بغرض التنبؤ بارتكاب جريمة، والحيلولة دون ذلك، واستخدامها بموجب إذن من سلطة التحقيق مع المطلوبين أو الصادر بشأنهم أمرًا بالقبض عليهم، كذلك ما أثاره استخدام الروبوتات فائقة الذكاء في القيام بأعمال القبض والتحفظ على الأشخاص في حالات التلبس بالجرائم.

ولما كان الهدف من الدراسة الوقوف على الإشكاليات التي تواجه استخدام تقنيات الذكاء الاصطناعي في الإجراءات الجنائية، سواء من قبل مأموري الضبط القضائي أو من قبل سلطات التحقيق والمحاكمة، من

تقسيم:

نقسم هذا الفصل إلى المبحثين التاليين:

المبحث الأول: مدى مشروعية استخدام تقنيات الذكاء الاصطناعي من مأموري الضبط القضائي.

المبحث الثاني: مدى مشروعية استخدام تقنيات الذكاء الاصطناعي في التحقيق الإبتدائي والمحاكمة.

المبحث الأول

مدى مشروعية استخدام تقنيات الذكاء الاصطناعي

من مأموري الضبط القضائي.

تمهيد:

ذكرنا أن استخدام تقنيات الذكاء الاصطناعي في الإدارات الشرطية والأمنية أضحى واقعًا ملموسًا، بل أصبح ضرورة عملية لضمان أداء مهام هذه الإدارات على الوجه الأكمل، من ذلك: استخدام تقنية التعرف على الأشخاص من خلال تمييز بصمة الوجه والصوت، كذلك الاعتماد على الطائرات بدون طيار، لاسيما المسيرة ذاتياً، لمراقبة التجمعات البشرية، والطرق، وتأمين بعض المنشآت، والأماكن، والأشخاص، وكذلك الاعتماد على هذه التقنيات في التعامل مع الكم الهائل من البيانات والمعلومات الشرطية والقضائية من خلال معالجتها وتحليلها والخروج منها بنتائج دقيقة، أكثر دقة وأسرع من تحليل الذكاء البشري؛ ومن ثم أصبح مفتاح نجاح

الإدارات الشرطية والمؤسسات الأمنية في تطوير وتحسين خدماتها يعتمد على استخدام تلك التقنيات في التحليل الاستباقي للبيانات الكبرى (Big Data)([1]).

ولا يقف الأمر عند هذا الحد، بل يجب التطرق إلى تطالعات الإدارات الشرطية والمؤسسات القضائية مستقبلاً في الاعتماد بشكل كبير على الروبوتات فائقة الذكاء أو ما يعرف بـ(الشرطي الروبوت)، في القيام ببعض الأعمال الشرطية مستقلاً عن التدخل البشري، سواء في التعامل مع المطلوبين أو أولئك الخطرين على الأمن، أو التعامل مع أي تجمع بشري أو تجمهر ينبئ بوقوع جريمة، إلى غير ذلك من مجالات استخدام الروبوتات فائقة الذكاء في العمل الشرطي. أو في صورة الاعتماد مستقبلاً على هذه الروبوتات وغيرها من تقنيات وأنظمة الذكاء الاصطناعي في العمل القضائي، حيث ظهر مصطلح (وكيل النيابة الروبوت) و(القاضي الروبوت).

تقسيم: نتناول في هذا المبحث المطالب التالية:

المطلب الأول: مدى مشروعية استخدام تقنية تمييز بصمة الوجه والصوت.

المطلب الثاني: مدى مشروعية استخدام الروبوتات فائقة الذكاء في العمل الشرطي.

[1]) د/ حسن أحمد المومني، أهمية وأثر الذكاء الاصطناعي في مستقبل العمل الشرطي: البيانات الكبري نموذجًا، مرجع سابق، ص٣٥١.

المطلب الأول

مدى مشروعية استخدام تقنية تمييز بصمة الوجه والصوت.

إن تقنية تمييز بصمة الوجه والصوت Face and Voice Fingerprint Recognitionمن أهم الاكتشافات العلمية الحديثة في سبيل التعرف على هوية الأشخاص في المطارات، والموانئ، والشوارع، والميادين العامة، فقد ساهمت في كشف غموض العديد من الجرائم التي لم يكن من السهل إقامة الدليل على مرتكبيها؛ لذلك كان لزاما على المشرع الجنائي الإجرائي التوجه إلى تقنين العمل بهذه التقنية، ووضع شروط وضوابط استعمالها في الإثبات الجنائي، مع العمل على الاعتراف الكامل بحجيتها كدليل، وقيمتها الثبوتية على النحو الذي يكفل حماية حقوق الأفراد من خطر إساءة استخدامها، لاسيما الحق في الخصوصية (Right to Privacy) والحق في الصورة (Right in the Photo)، هذا ما يدفعنا لبحث مشروعية استخدام تقنية تمييز بصمة الوجه والصوت في التعرف على الأِشخاص في ضوء النصوص الإجرائية السارية.

ونتناول مسألة المشروعية من زاوية المخاطر التي تشوب استخدام تقنية التعرف على الأشخاص من خلال بصمة الوجه والصوتFace and Voice Fingerprint ، ومدى نسبة تحققها من هوية الشخص (Identity of the Person) ، ثم نستعرض من زاوية أخرى للخلاف الفقهي حول مشروعية استخدام هذه التقنية في الإجراءات الجنائية Criminal Procedur .

الفرع الأول

إنشاء قاعدة بيانات بالبصمات الحيوية.

في عالم يتزايد فيه الاعتماد بشكل كبير على وسائط التخزين الإلكترونية تشتد الحاجة إلى حماية وتأمين تقنية هذه الوسائط من الاختراقات، مما يحقق أكبر قدر من السرية في حفظها ومنع تداولها. وقد تزايد الاعتماد على البصمات الحيوية (Biometric Fingerprints) ومنها البصمة الوراثية (Genetic Fingerprinting) في التحقق من الشخصية.

وقد أشار البعض([1]) إلى أن كفاءة هذه التقنيات ونجاحها في تحديد هوية الأشخاص في العمليات البنكية مثل استخدام البطاقات الائتمانية (Credit Cards)، والخزانات الشخصية في البنوك دفع إلى توظيفها في أغراض أخرى، يغلب عليها الطابع الأمني، من ذلك: تعقب أثر الأفراد عند دخولهم أو خروجهم من بعض المؤسسات الأمنية ذات الإجراءات المشددة، وتأمين بعض الشبكات الإلكترونية الحاسوبية ذات الأهمية القصوي التي لا يكفي تأمينها بالاعتماد على كلمات المرور passwords التقليدية المكونة من حروف Letters أو أرقام Numbers أو رموز Symbols .

وقد تعرض البعض إلى دراسة أهمية إنشاء بنك وطني للحامض النووي DNA يحوي قاعدة بيانات من نتائج عينات الحامض النووي لجميع الأفراد، في كشف الحقيقة في

---

[1]) د/ صفوت عبدالحليم علي، توظيف تكنولوجيا التصوير التليفزيوني المعاصر لتسجيل بصمة العين ودورها في الكشف عن الأدلة الجنائية، مجلة علوم وفنون، جامعة حلوان، مصر، المجلد ٢٠ ،ع ١، يناير ٢٠٠٨م، ص١٥.

العديد من الجرائم لاسيما جرائم العرض، وقضايا الأحوال الشخصية المتعلقة بإثبات النسب، وقضايا المفقودين، والهجرة، إلى غير ذلك من القضايا التي تلعب البصمة الوراثية فيها دوراً مهماً في كشف الحقيقة بشأنها وإقامة الدليل عليها بالإثبات أو النفي([1]).

كما أشار إلى الصعوبات التي تواجه إنشاء بنك عينات الحامض النووي، سواء أكانت صعوبات اجتماعية في مدى تقبل الأفراد فكرة أخذ العينة وحفظ نتائج تحليلها في قاعدة بيانات حاسوبية مركزية، تتمتع بالسرية، أو صعوبات اقتصادية، تتعلق بتكلفة إنشاء هذا البنك، كما قد تكون هذه الصعوبات مادية أو فنية، وقد تكون صعوبات إدارية أو تدريبية تتعلق بتوفير الكوادر الفنية المدربة على التعامل مع قاعدة البيانات المزمع إنشاؤها، وضمان سريتها، وتأمينها بكفاءة عالية، وأخيرا عرض البعض للصعوبات التشريعية التي تتمثل في وضع التنظيم التشريعي، وكذلك المعالجة الإجرائية لكيفية الحصول على العينة وإلزام الأفراد بتقديمها([2]).

وعليه، يمكن القول أن التحدي الأكبر الذي يواجه الدول في تفعيل الاعتماد على البصمات الحيوية في الأغراض الشرطية، والعدالة الجنائية هو إنشاء قاعدة بيانات كبيرة تتضمن كافة البصمات الحيوية لكافة الأفراد في الدولة مواطنين ومقيمين، حتى

[1]) د/ محمد فوزي إبراهيم، البنك الوطني للحامض النووي ودوره في كشف غموض الحوادث المجهولة، مجلة الفكر الشرطي، أكاديمية العلوم الشرطية بالشارقة، الإمارات العربية المتحدة، المجلد ٢٧، العدد ١٠٤، يناير ٢٠١٨م، ص٢٢٤-٢٢٧.

[2]) المرجع السابق، ص٢٣٣-٢٥١.

يمكن الوصول إلى أعلى درجات الفاعلية والدقة في تحديد هوية الأفراد بواسطة هذه البصمات.

وقد فطنت دولة الإمارات العربية المتحدة إلى أهمية إنشاء هذه القاعدة، وتأمينها وحمايتها فأصدرت المرسوم بقانون اتحادي رقم ٣٩ لسنة ٢٠٢٣م بشأن تنظيم قاعدة بيانات البصمة الوراثية الاتحادية([1]). وقد حدد المرسوم استخدامات هذه القاعدة في المادة (٤)، ومنها:

١. التحقيق في الجرائم والتعرف على مرتكبيها.
٢. التعرف على ضحايا الأزمات والكوارث والحوادث.
٣. التعرف على هوية الجثث والبقايا والأشلاء البشرية المجهولة.
٤. التعرف على مجهولي الهوية والمفقودين.
٥. أي أغراض أخرى يصدر بها قرار من مجلس الوزراء.

كما حرص المشرع الإماراتي على ضمان حماية البيانات التي تحويها القاعدة المنصوص على إنشائها، فنص في المرسوم على سرية البيانات والمعلومات التي يتم تغذية القاعدة بها، وحظر إفشاء أو تداول أو نشر هذه البيانات والمعلومات في غير الأحوال المصرح بها قانوناً([2]). وقرر عقوبة مغلظة جزاء مخالفة هذا الحظر؛ حيث نص في المادة (١٤) على عقوبة السجن المؤقت والغرامة التي لا تقل (٢٠,٠٠٠)

[1]) نص في المادة (٣) على أنه "تنشأ في الوزارة قاعدة بيانات تسمى "قاعدة بيانات البصمة الوراثية الاتحادية" ويصدر الوزير ضوابط وشروط وإجراءات تغذية واستخدام قاعدة البيانات.
ووفقا للمادة الأولى من المرسوم، يقصد بالوزارة: وزارة الداخلية، ويقصد بالوزير: وزير الداخلية.

[2]) المادة (٥) من المرسوم بقانون.

عشرين ألف درهم عن ولا تزيد على (١٠٠,٠٠٠) مائة ألف درهم كل من: ٣. أفشى أو تداول أو نشر أو أفصح عن البيانات الموجودة في قاعدة بيانات البصمة الوراثية الاتحادية بالمخالفة للأحكام المنصوص عليها في هذا المرسوم بقانون.

ومما لاشك فيه أن مخاطر تعرض القاعدة المنصوص على إنشائها للاختراق الالكتروني تمثل تحدياً كبيراً أمام الجهات المعنية والمسؤولة عن هذه القاعدة، ومن ثم تأتي الحماية التي كفلها المرسوم بقانون اتحادي رقم ٣٤ لسنة ٢٠٢١م بشأن مكافحة الشائعات والجرائم والإلكترونية، بالعقاب المغلظ على اختراق الأنظمة المعلوماتية الخاصة بمؤسسات الدولة، والمنصوص عليها في المادة (٣) من المرسوم سالف الذكر؛ حيث عاقب على هذا الاختراق بالسجن المؤقت والغرامة التي لا تقل عن ٢٠٠ ألف درهم ولا تزيد على ٥٠٠ ألف درهم([1])، وتكون السجن المؤقت بما لا يقل عن ٥ سنوات، والغرامة التي لا تقل عن ٢٥٠ ألف درهم، ولا تزيد على ١,٥٠٠,٠٠٠ درهم، إذا ترتب على الاختراق إلغاء أو تدمير أو إفشاء أو إتلاف أو تغيير أو نسخ أو نشر أو إعادة نشر أي بيانات أو معلومات أو خسارة سريتها...([2]).

وشدد العقوبة أكثر؛ بحيث تكون العقوبة السجن المؤقت الذي لا يقل عن ٧ سنوات؛ إذا كان الاختراق بغرض الحصول على البيانات والمعلومات الخاصة بمؤسسات الدولة([3]).

---

[1]) الفقرة الأولى من المادة المذكورة.

[2]) الفقرة الثانية من المادة (٣) من المرسوم بقانون.

[3]) الفقرة الثالثة من المادة (٣) من المرسوم بقانون سالف الذكر.

الفرع الثاني

مدى تعارض استخدام تقنية التعرف على الوجه

مع الحق في الصورة.

من الثابت أن عمل مأموري الضبط القضائي في أعمال التحري والاستدلال يتم تحت مظلة المشروعية الإجرائية واحترام حقوق الإنسان، فعلى الرغم من الأهمية القصوى للعمل الشرطي في المجتمع وما تبذله الإدارات الشرطية في سبيل حفظ الأمن والوقاية من الجريمة والحد من انتشارها إلا أن ذلك لا يعد مشروعاً وغير مقبول إذا نال من الاحترام الواجب لحقوق الإنسان، ومن ثم يقترن الحديث عن دور الإدارات الشرطية في حفظ الأمن ومكافحة الجريمة مع الحديث عن حقوق الانسان وضمان الاحترام الواجب لها. في هذا الخصوص نتناول مشروعية استخدام تقنيات التعرف على الوجه والصوت من زاوية احترام حقوق الإنسان، ومنها: حق الانسان في الصورة.

أولًا- استخدام تقنية التعرف على الوجه مع المشتبه فيهم والمطلوبين أمنيًا:

بداية نؤكد على مشروعية استخدام هذه التقنية في الأماكن التي تشترط لدخولها التعرف على وجه الشخص وتحديد هويته، مثل دخول بعض المؤسسات الأمنية، والمطارات، والمنافذ، وغيرها، وذلك استنادا إلى الرضاء الصحيح، سواء كان رضاءً صريحاً أو ضمنياً من الشخص طالب الدخول إلى هذه الأماكن؛ إذ إن التعرف على الوجه بالتقاط صورة للشخص بغرض تحديد هويته من متطلبات ومستلزمات

الدخول([1])؛ ومن ثم إذا امتنع الشخص أو رفض الاستجابة إلى استخدام هذه التقنية بالتقاط صورته يمنع من الدخول، دون أن يجبر على ذلك، كما يحدث في المطارات، إذا لم يستجب الشخص القادم من الخارج لمتطلبات تقنية التعرف على الوجه لتحديد هويته، كما لو رفض الوقوف أمام الكاميرا مباشرة لالتقاط صورة، أو تعمد التحرك أمام الكاميرا أو ارتداء شيئا يؤثر على دقتها في التقاط الصورة يمنع من عبور المطار ودخول الدولة، كذلك الحال إذا امتنع عن الامتثال لالتقاط صورة قبل الدخول إلى أحدى المؤسسات الأمنية التي تشترط ذلك.

كما نؤكد على مشروعية استخدام تلك التقنية حال استيقاف أحد الأشخاص الذي وضع نفسه محل ريبة وشك من قبل رجل الشرطة، حيث يجوز للأخير أن يصطحبه إلى مركز الشرطة لاستيضاح أمره، وكشف حالة الريبة والشك التي أوجد نفسه فيها طواعيةً واختياراً، ويكون استخدام الشرطي لتقنية التعرف على الوجه لتحديد هويته مشروعاً استنادًا إلى سلطة رجل الشرطة في استيضاح أمر من يضع نفسه طواعيةً واختيارًا محل ريبة وشك.

كما نؤكد على مشروعية استخدامها حال تلقي بلاغاً من أحد الأشخاص يفيد بوجود أحد المطلوبين أو الفارين في مكان ما، ثم تتوجه قوة من الشرطة إلى المكان المذكور فيجوز لها استخدام التقنية في سرعة التأكد من صحة البلاغ، والتحقق في ثوان معدودة من شخصية المبلغ ضده، دون احتمال وقوع أخطاء مقارنةً بالتحقق بشريًا من

[1]) في تفصيل استخدام تقنية التعرف على الوجه في المطارات راجع: د/عمار باسر زهير، دور أنظمة الذكاء الاصطناعي في التنبؤ بالجريمة، مرجع سابق، ١٠٥، ١٠٨.

هوية الشخص بفحص جميع الصور أو أوامر القبض الصادرة في دائرة الاختصاص، فضلاً عن أن تقنية التعرف على الوجه تضمن إمكانية التحقق من هوية الأشخاص الممنوعين من السفر بأمر من سلطة التحقيق أو المحكمة؛ لصلتهم بجرائم تستدعي بقاءهم في الدولة وعدم مغادرتها، إلا بإذن من السلطة مصدرة الأمر.

وتكتسب تقنية التعرف على الوجه أهمية خاصة في تفعيل بعض المبادرات الذكية([1])، التي تعتمد بشكل كبير على الاستفادة من تقنيات الذكاء الاصطناعي إلى أقصى درجة في تحقيق أعلى مستويات الأمن للمطارات والمنافذ الحدودية للدولة.

ومما يزيد من فاعلية تقنية التعرف على الوجه الاعتماد على تقنية Blockchain أو (سلسلة الكتل) والتي تعرف بأنها: نوع جديد من قواعد البيانات غير التقليدية واللامركزية، توفر إدارة قائمة متزايدة باستمرار من السجلات التي تسمى (كتل) تتضمن كل كتلة معلومات وبيانات هائلة، منها: بيانات زمنية وروابط إلى الكتلة السابقة، فتكون سلسلة من البيانات لا يمكن تعديلها أو التلاعب بها، وفي حالة الرغبة بالقيام بذلك يجب أن يكون هناك توافق لا مركزي من قبل مختلف عناصر

[1]) ومن هذه المبادرات: مبادرة "الكفالة الذكية" التي أطلقتها نيابة دبي بديلاً عن إجراء حجز جوازات السفر لأطراف محل المساءلة في القضايا البسيطة والجنح المعروضة على النيابة، وهي مبادرة ذكية تتيح تخزين بيانات الأشخاص الموقوفين وأصحاب القضايا البسيطة في قوائم الممنوعين من السفر إلكترونيا دون الحاجة إلى حجز جوازات سفرهم.
انظر: د/علي حميد بن خاتم، الكفالة الذكية ضمانة إلكترونية تلغي إجراء حجز جوازات السفر، مجلة دبي القانونية، صادرة عن النيابة العامة بدبي، عدد (٣٠) يناير، ٢٠١٩م، ص٣٢.

الشبكة.([1]) وتعتبر Blockchain حاليا أكبر قاعدة بيانات موزعة عالميا بين الأفراد([2]).

كما تعرف بأنها: عبارة عن قاعدة بيانات موزعة تمتاز بالقدرة على إدارة قائمة متزايدة باستمرار من السجلات المسماة (كتل) بحيث تحتوى كل كتلة على الطابع الزمنى، مع رابط إلى كتلة سابقة، بحيث تتشكل سلسلة من الكتل المترابطة. والهدف من إنشاء هذه السلسلة إتاحة البيانات لجميع المستخدمين مع الحفاظ على أمانها، دون القدرة على تعديل تلك الكتل([3]).

وقد أشار بعض المتخصصين إلى أن أهم ما يميز (Blockchain) هو الأمان أي تأمينها؛ حيث يتم منع كل عملية تزوير للبيانات القديمة وتغيير طريقة حماية البيانات الجديدة من خلال عملية التشفير والتخزين اللامركزي. وكذلك عدم القابلية للاختراق؛

([1]) رنا إبراهيم، استراتيجية "البلوك تشين" المستقبل الآمن لتسريع المعاملات الحكومية، مجلة دبي القانونية، صادرة عن النيابة العامة بدبي، عدد (٣٠) يناير، ٢٠١٩م، ص٣٥.

أشار هذا الفقه إلى إطلاق تقنية "الهوية الرقمية" Digital identity التي تتمتع بمواصفات الأمان والمصداقية الرقمية والقدرة على تخزين البيانات عبر وحدات آمنة، كما يحتوي هذا التطبيق Application على توقيع رقمي Digital signature مزود بالأمان والموثوقية.

انظر: المرجع السابق، ص٣٧.

([2]) تم استخدام نظام Blockchain أول مرة عام ٢٠٠٨م، وذلك باعتبارها المنصة الرئيسية لعملة Bitcoin، والتي استمدت قوتها وثقة المتعاملين فيها، بفضل نظام Blockchain للمزيد حول هذه التقنية وعناصرها تفصيلا راجع: إيهاب خليفة، البلوك تشين: الثورة التكنولوجية القادمة في عالم المال والإدارة، أوراق أكاديمية صادرة عن مركز المستقبل للأبحاث والدراسات المتقدمة، أبوظبي، الإمارات العربية المتحدة، العدد ٣، ٢٠ مارس ٢٠١٨م، ص١–٨.

([3]) أشرف شهاب، مصطفى الدمرداش، ثورة البلوك تشين على أعتاب التغيير، مجلة الأهرام للكمبيوتر والإنترنت والاتصالات، ملف بعنوان (لغة العصر) العدد ٢١٥، نوفمبر ٢٠١٨م، ص٣٢.

حيث أن اختراق سجلات Blockchain أشبه بالمستحيل؛ وقد تتطلب قدرات حاسوبية خالية لتنفيذها([1]).

يؤكد الباحث على أن استخدام تقنية التعرف على الوجه -على النحو السابق بيانه- لا يتضمن انتهاكاً لحق الإنسان في الصورة([2])على اعتبار أن استخدام هذه التقنية من قبل الشرطة ما هي إلا وسيلة لضمان السرعة، والدقة في تحديد الهوية، وينسب الإجراء إلى الشرطي الذي استخدم التقنية، بمعنى أنه ما دام الإجراء جائز من الشرطة حال قيامه بالتعرف على الوجه وتحديد الهوية بنفسه فإنه يجوز له استخدام هذه كمجرد وسيلة من منطلق الاستفادة من التكنولوجيا الحديثة.

ثانيا- استخدام تقنية التعرف على الوجه مع جمهور الأفراد:

إن القدرات الفائقة لتقنية التعرف على الوجه في تحليل الصور والفيديوهات للمساعدة على تحديد هوية شخص ما متورط بالضلوع في ارتكاب جريمة ما أو عمل إرهابي من خلال ظهور صورته في فيديو تم تسجيله بواسطة كاميرا مثبتة في أحد الشوارع أو على أحد المباني في محيط مسرح الجريمة أو العمل الإرهابي، حتى ولو كانت جودة

---

[1]) أشرف شهاب، مصطفى الدمرداش، المرجع السابق، ص٣٣.

[2]) يعرف الحق في الصورة بأنه الحق الذي يكون للشخص الذي تم تصويره بإحدى الطرق الفنية أن يعترض على نشر صورته.

KAYSER (P.), Le droit à l›image, Mélanges SAVATIER, D. 1961, N 22.

لدى د/ جميل عبد الباقي الصغير، الحق في الصورة والإثبات الجنائي، مجلة كلية القانون الكويتية العالمية، العدد ١٠، ٢٠١٤، ص٣٠٧. نعتقد أن مفهوم الحق في الصورة أوسع وأشمل من مجرد منح الشخص حق الاعتراض على نشر صورته، وإنما يتضمن منحه الحق في الاعتراض على التقاط صورته ابتداءً.

التصوير منخفضة جدا بسبب ظروف المكان أو الزمان([1])، كل هذا جعل من استخدام تقنيات الذكاء الاصطناعي في تحليل الصور والفيديوهات أمراً في غاية الأهمية والفاعلية في العمل الأمني أو الشرطي تحديداً.

إلا أن هذا يثير الجدل حول مشروعية استخدام تقنية التعرف على الوجه مع عامة الناس، كما يحدث في الأماكن العامة، والشوارع، وأماكن التسوق، والاحتفالات، سواء تم ذلك باستخدام روبوتات قادرة على تمييز الوجوه، أو باستخدام الطائرات بدون طيار، المزودة بكاميرات ذكية؛ حيث تستطيع هذه التقنيات التعامل بسرعة مع الحالات الخطرة المحتملة، من خلال مراقبة الشوارع والأماكن المفتوحة، مع إمكانية التقاط صوراً بجودة عالية لأي شخص وتحديد هويته، والتعرف على سوابقه الإجرامية، ومدى درجة خطورته أمنياً، ومن ثم التعامل معه مباشرة – إذا مُنحت ذلك– أو إبلاغ مركز التحكم في الإدارات الشرطية، مما يكون له أبلغ الأثر في الحد من الجريمة والوقاية منها([2]).

ونعتقد أن مصدر الجدل حول هذه المسألة هو: مدى تعارض استخدام هذه التقنية مع حقوق الإنسان، لاسيما حقه في الصورة التي تمثل أحد مكونات الخصوصية أو الحياة

[1]) د/ عمار باسر زهير، دور أنظمة الذكاء الاصطناعي في التنبؤ بالجريمة، مرجع سابق، ص٨٨.

[2]) فقد أشار البعض إلى أن استخدام الطائرات بدون طيار في المكسيك أدى إلى انخفاض الجرائم بنسبة ١٠% عن معدلاتها الطبيعية، إذ إن وجود الطائرات بدون طيار أصبح أمرا رادعا للجريمة. د/ عمار باسر زهير، المرجع السابق، ص٩٠.

الخاصة. يقتضي البحث في تلك المسألة الوقوف في عجالة على مضمون هذا الحق، ثم نتطرق لبحث مدى تعارض أو توافق استخدام تقنية التعرف على الوجوه معه.

في دراسة لفريق عمل مؤسسة RAND عام ٢٠١٧م أثار استخدام تقنيات الذكاء الاصطناعيAI في مراقبة المدنيين من قبل الحكومات مخاوف الفريق، لاسيما فيما يتعلق باستخدام خوارزميات الذكاء الاصطناعي في التنبؤ الشرطي وحدود استخدامها في إنفاذ القانون، كما صدر تقرير منظمة (ProPublica) فيما يتعلق باستخدام خوارزميات الذكاء الاصطناعي في مجال العدالة الجنائية عام ٢٠١٦م، حيث وصف التقرير استخدام خوارزمية (COMPAS) لتقييم احتمالية العودة إلى الإجرام في جلسات استماع اطلاق السراح المشروط. ومع تنامي استخدام تطبيقات الذكاء الاصطناعي في إنفاذ القانون تزايدت المخاوف بشأن حقوق الأفراد الأساسية، لاسيما الحق في الخصوصية([1])، وسوف نعرض لهذه المخاوف في معرض الحديث عن استخدام تقنيات العدالة التنبؤية في المطلب الآخير من البحث.

جدير بالذكر أن الحق في الصورة يواجه تحدياً كبيراً في مواجهة التقدم التكنولوجي في العصر الرقمي (Digital Age)، فقد يتعرض الشخص للتصوير بكاميرات متطفلة دون أن يشعر، ثم يفاجئ بوجوده في مقطع فيديو لا يرغب الظهور فيه، أو يجد له صورة على هيئة أو في وضعية لا يرغب فيها؛ هذا ما يفرض على الدولة بكافة أجهزتها واجب حماية حق الأفراد في الصورة من سلوكيات المتطفلين. ولكن يكون

[1]) Osonde A. Osoba, William Welser IV ,The Risks of Artificial Intelligence to Security and the Future of Work, op. cit. P: 7-8.

الأمر أكثر خطورة وتعقيداً، عندما تقع أفعال التصوير للأشخاص بكاميرات تستخدمها أجهزة الدولة، لاسيما الإدارات الشرطية والسلطات القضائية، مستغلة في ذلك القدرات التقنية العالية لبعض الكاميرات التي يتم زرعها في أماكن تجمعات بشرية، تقوم بتصوير جميع المتواجدين فيها، دون موافقة صريحة منهم.

بيد أن هذا يثير الحديث عن مدى تجريم فعل التقاط صورة للغير دون رضاء صريح منه في الأماكن العامة، حيث اتجه جُل التشريعات الجنائية إلى عدم التجريم، ومنها قانون العقوبات المصري([1])، بالنظر إلى أن الحق في الصورة يتطلب وجود الشخص في مكان خاص، ثم يتم التقاط الصورة له دون رضاه، ومن ثم يكون ما يقع من تصوير للأفراد في الأماكن العامة، مثل الحدائق وأماكن التسوق، وغيرها لا يمثل أي إعتداء على حقهم في الصورة، ومن ثم يكون بعيدا عن نطاق التجريم.

في المقابل، نجد المشرع الإماراتي يعاقب على الفعل سواء وقع في مكان عام أم خاص([2])، وذلك بموجب نص المادة (٢١) من المرسوم بقانون اتحادي رقم ٣٤ لسنة

---

[1]) بموجب المادة (٣٠٩) مكرر(١) بقولها: "يعاقب الحبس مدة لا تزيد على سنة كل من اعتدى على حرمة الحياة الخاصة للمواطن، وذلك بأن ارتكب أحد الأفعال الآتية في غير الأحوال المصرح بها قانوناً أو بغير رضاء المجني عليه.

(ب) التقط أو نقل بجهاز من الأجهزة أياً كان نوعه صورة شخص في مكان خاص".

[2]) بينما نجد المرسوم بقانون اتحادي رقم ٣١ لسنة ٢٠٢١م بإصدار قانون الجرائم والعقوبات من التشريعات التي اشترطت ارتكاب الفعل في مكان خاص، مع عدم التجريم إذا ارتكب في مكان عام، وذلك بموجب (٤٣١) بقولها "يعاقب بالحبس والغرامة كل من اعتدي على حرمة الحياة الخاصة أو العائلية للأفراد وذلك بأن ارتكب أحد الأفعال الآتية في غير الأحوال المصرح بها قانونا أو بغير رضاء المجني عليه:

٢٠٢١م في شأن مكافحة الشائعات والجرائم الإلكترونية والتي عاقبت بالحبس مدة لا تقل عن ستة أشهر والغرامة التي لا تقل عن ١٥٠ ألف درهم ولا تجاوز ٥٠٠ ألف درهم، أو بإحدى هاتين العقوبتين كل من استخدم شبكة معلوماتية أو نظام معلومات إلكتروني، أو إحدى وسائل تقنية المعلومات، بقصد التعدي على خصوصية شخص أو حرمة الحياة الخاصة أو العائلية للأفراد من غير رضا وفي غير الأحوال المصرح بها قانوناً بإحدى الطرق الآتية:

٢. التقاط صور الغير في أي مكان عام أو خاص أو إعداد صور إلكترونية أو نقلها أو كشفها أو نسخها أو الاحتفاظ بها.

بينما نجد المشرع المصري لم يكن بهذا الوضوح في حسم الخلاف والجدل حول مدى اشتراط ارتكاب فعل التقاط الصورة باستخدام وسائل تقنية المعلومات في مكان خاص([1])؛ حيث جرم التعدي على حرمة الحياة الخاصة باستخدام هذه الوسائل، وعاقب عليه بموجب المادة (٢٥) من القانون رقم ١٧٥ لسنة ٢٠١٨م في شأن

٢- التقط أو نقل بجهاز أيا كان نوعه صورة شخص في مكان خاص".

[1]) اتجه جانب من الفقه إلى القول بتحقق الجريمة فقط في المكان الخاص، مستبعداً تحققها أثناء تواجد الشخص في مكان عام بين الأفراد، واستند هؤلاء إلى أن حق الخصوصية لا يعطي صاحبه حق الاعتراض على التقاط أي صورة له أثناء وجوده في مكان عام، تأسيساً على أن تواجد الشخص في مكان عام يجعله جزءً من عمومية المكان، وإنما يعطيه الحق في عدم نشرها. بينما يتجه البعض إلى أن التمييز بين التقاط صورة للشخص في مكان عام بشكل عرضي وبين استهداف صورة الشخص بالتصوير بشكل مباشر؛ حيث لا يتطلب الإذن في الفرض، بعكس الفرض الثاني.

انظر في ذلك: محمد نور الدين سيد، الحماية الجنائية للحق في خصوصية المكالمات الهاتفية دراسة في القانونين الكويتي والاماراتي، مجلة كلية القانون الكويتية العالمية، العدد ١٠، ٢٠١٤، ص٥٧٧، ٥٧٨.

مكافحة جرائم تقنية المعلومات([1]) دون أن يوضح طبيعة المكان، ودون أن يحدد الأفعال التي تمثل تعدياً على حرمة الحياة الخاصة، وبالرجوع إلى قانون العقوبات نجده يُعدّد هذه الأفعال، ومنها التقاط صورة للغير في مكان خاص.

لكن من زاوية أخرى، يمكن القول أن هناك انسجاماً وتوافقاً بين منظومة التشريعات المصرية، يتبين ذلك من خلال المقاربة بين معالجة المشرع المصري للاعتداء على حرمة الحياة الخاصة، في قانون العقوبات، ومعالجته إياها في قانون مكافحة جرائم تقنية المعلومات. بينما لا نجد هذا الانسجام والتوافق في منظومة التشريعات الاماراتية؛ حيث اشترط المشرع الاماراتي المكان الخاص في قانون الجرائم والعقوبات، بينما نص على تجريم فعل التعدي على الحياة الخاصة سواء في مكان عام أو خاص، في قانون مكافحة الشائعات والجرائم الالكترونية.

ولاشك أن علة التجريم لاسيما ما يقع على مكان خاص تتمثل في حماية الحق في الخصوصية في مواجهة الأخطار التقنية في صورة التقاط صورة للغير بتقنية عالية، وفي خفاء تام، بحيث قد لا يلاحظ المجني عليه ما تم من التقاط صورة له، مع وجود العديد من البرامج الحاسوبية التي تمكن من التلاعب في الصورة أو تعديلها بما يسيء للمجني عليه بتقنية عالية جداً([2]). لكن ذلك لا يمنع من إضفاء جانباً من التمتع

---

[1]) منشور بالجريدة الرسمية، العدد ٣٢ مكرر (ج)، ١٤ أغسطس ٢٠١٨م، ص١٨.

[2]) أسماء على سالم الشامسي، جرائم الاعتداء على حرمة الحياة الخاصة للأشخاص في ظل المرسوم بقانون رقم ٥ لسنة ٢٠١٢م، بشأن مكافحة جرائم تقنية المعلومات، دراسة مقارنة، رسالة ماجستير، جامعة الإمارات العربية المتحدة، ٢٠١٨م، ص٣٦.

بالخصوصية للأفراد أثناء تواجدهم في أماكن عامة؛ لاسيما إذا كان محلاً وحيداً للصورة، فلا يقبل أحد أن يتم تصويره وعائلته من قبل الغير بوسائل التقنية الحديثة ولو كان في مكان عام، مثل: مطعم، أو مكان للتسوق، أو التنزه، أو شاطئ([١]).

إن المغايرة السابقة في موقف المشرع المصري عن نظيره الإماراتي تترتب عليها مغايرة في مدى مشروعية الدليل المستمد من تصوير الأفراد في الأماكن العامة بوسائل تقنية المعلومات، إذ يعتبر الإجراء صحيحاً، ويكون الدليل مشروعاً، يصلح للإدانة([٢]) وفق صراحة القانون المصري في اشتراط المكان الخاص لتجريم التصوير بدون موافقة، بل يرى هذا الاتجاه جواز التصوير الحاصل في مكان خاص من خلال مكان عام، كما يحدث بواسطة الطائرات بدون طيار، إذا كان ما تم تصويره مرئياً للعامة من الخارج، ومن ثم لا يمثل التصوير تعدياً على الخصوصية مادام المشهد أو الصورة مرئية لأي شخص في الخارج([٣]).

بينما يكون الإجراء غير صحيح، والدليل مستبعداً، لا يصلح للإدانة وفق صراحة القانون الاماراتي في تجريم الفعل سواء وقع في مكان عام أم خاص، باستخدام وسائل تقنية المعلومات. وينطبق ذلك في حالة التقاط صورة قريبة لشخص بواسطة تقنية

---

[١]) في ذات الاتجاه انظر: د/ محمود عبد الرحمن محمد "نطاق الحق في الحياة الخاصة دراسة في القانون الوضعي والشريعة الإسلامية" دار النهضة العربية، ١٩٩٦.، ص٢٤١.

[2]) T. Pol. Paris, 25 Mai 1984, Gaz. Pal. 1984, 2, P. 632, obs. LEVASSEUR ; R.S.C. 1986, P. 856 ; Crim., 5 Février 1986, Jurisps. auto 1986, P. 203 ; Crim., 25 Janvier 1995, Jurisps. auto.1995, P. 221

مشار لهذه الأحكام لدى: د/ جميل عبد الباقي الصغير، الحق في الصورة والإثبات الجنائي، المرجع السابق، ص٣٣٧.

[٣]) د. جميل عبد الباقي الصغير، المرجع السابق، ص٣٣٧.

التعرف على الوجه لتحديد هويته، حيث يكون الشخص موضوعاً وحيداً للصورة، تركز عليه بشكل دقيق جداً، لتحديد نقاط الوجه المميزة له، من ارتفاعات وانخفاضات والمسافة بين العينين وحجم ومساحة الأنف، وشكل عظام الخدين ومساحتهما، إلى غير ذلك من النقاط المميزة للوجه.

ولكن نعتقد أنه حسماً لهذا الجدل والخلاف يمكننا القول أنه لا يكفي لقيام الجريمة توافر الفعل المكون للركن المادي، بل لابد من توافر الركن المعنوي، فلا جريمة بدون ركن معنوي، ولما كانت جريمة الاعتداء على خصوصية الأفراد تفترض ارتكاب فعل التقاط صور الغير عمداً وبقصد التعدي على هذه الخصوصية([1])، وهو ما تأكد باتجاه قضاء المحكمة الاتحادية العليا، حيث تطلبت أن يتوفر لدى الجاني قصد الاعتداء على خصوصية الأشخاص، وقصد الإساءة إلى سمعتهم([2]).

في هذا المقام تجدر الإشارة إلى مسلك المشرع بإمارة دبي؛ حيث نظم استخدام الطائرات بدون طيار في أعمال التحري والاستدلال المتعلقة بالجرائم في الأماكن الخاصة بشرط الحصول على إذن مسبق من النيابة العامة، وبناء على معلومات جدية([3])، مع شرط قيام مأمور الضبط بنفسه باستخدام الطائرة بدون طيار في أعمال

---

[1]) أسماء على سالم الشامسي، المرجع السابق،ص٧٦.

[2]) حكم المحكمة الاتحادية العليا، الطعن رقم ١٥٦ لسنة ٢٠١٨م، الدائرة الجزائية، جلسة بتاريخ ٧ مايو ٢٠١٨م.

[3]) فقرة (أ) من المادة (٣٤) من قانون تنظيم الطائرات بدون طيار بإمارة دبي، رقم ٤ لسنة ٢٠٢٠م.

المراقبة، وله في سبيل ذلك الاستعانة بالفنيين كلما اقتضت أعمال المراقبة ذلك([1])، وبمفهوم المخالفة، يمكن القول بجواز الاستعانة بهذه الطائرات في الأماكن العامة دون اشتراط الحصول على إذن من النيابة العامة، سواء استخدمها بنفسه أو بواسطة غيره من رجال السلطة العامة أو الفنيين من غير مأموري الضبط. وخيراً فعل المشرع بإمارة دبي، مع التوصية بأن يسلك المشرع المصري نفس النهج وينص صراحة على تنظيم استخدام الطائرات بدون طيار لاسيما المسيرة ذاتياً في أعمال التحري والإستدلال وغيرها من تقينات الذكاء الاصطناعي بقانون خاص.

الفرع الثالث

استخدام تقنية بصمة الصوت والحق في خصوصية المحادثات.

نتناول في هذا الفرع فرضية استخدام تقنية تمييز بصمة الصوت Voice fingerprint في تحديد الهوية Identifying ومدى توافقها مع الحق في خصوصية المحادثات الخاصة سواء أثناء التحقيق، أو مع جمهور الأفراد وتسجيل المحادثات الخاصة التي تجرى في مكان عام Public place ، ضمن غرض التنبؤ الاستباقي Proactive forecasting بالأشخاص الخطيرين أو أولئك الذين يتوقع منهم ارتكاب جريمة ما.

[1]) فقرة (ج) من المادة (٣٤) من القانون المذكور.

أولا– استخدام تقنية تمييز بصمة الصوت أثناء التحقيق:

أشرنا فيما سبق أن بصمة الصوت ذات صلة قوية ببعض الجرائم، فقد يتم التعرف على الجاني من خلال بصمة صوته المميزة له، كما هو الحال في جرائم السب والقذف والتهديد، وغيرها من الجرائم القولية، حيث تعتبر الألفاظ المنطوقة محل التجريم. كما قد يكون الصوت دليلاً قوياً في إثبات توافر الركن المفترض في بعض الجرائم، من ذلك جرائم الاعتداء على العرض بالإكراه أو بدون رضاء، حيث يكون صوت المجني عليها أو عليه دليلاً قوياً على المقاومة ورفض المواقعة، أو إعلان صريح عن عدم رضائها أو رضائه بفعل المواقعة. كما قد يكون الصوت دليلاً قوياً على المشاركة الإجرامية، لاسيما أفعال التحريض والاتفاق، كما لو نُسب الصوت إلى المتهم بما يثبت بما لا يدع مجالاً للشك في صدور التحريض أو الاتفاق منه([1]).

كما أشرنا إلى تنوع طرق التعرف على بصمة الصوت أو تحديد هوية المتكلم من نبرة صوته، من ذلك: الطريقة التقليدية عن طريق الأذن البشرية، أو من خلال جهاز يحول النبرات الصوتية إلى رسومات أو تخطيط بشكل معين يعبر عن ما يميز صوت شخص ما عن آخر، ثم الطريقة الآلية والتي تتم باستخدام حاسب آلي يقوم بتحليل الصوت، ومطابقته بالأصوات الأخرى المخزنة على ذاكرة الحاسب الآلي، وتعد الطريقة الأخيرة هي الأفضل([2])، إلا أن الممارسات الإجرائية الحديثة في هذا المجال

[1]) حول المزيد من أهمية بصمة الصوت وعلاقتها بالجرائم من الناحية الإجرائية راجع: د/ عمر عبد المجيد مصبح، بصمة الصوت ودورها في الإثبات الجنائي، مرجع سابق، ص٢٥، ٢٦.

[2]) المرجع السابق، ص٢٧، ٢٨.

تقوم على استخدام تقنيات الذكاء الاصطناعي في تحليل الأصوات بشكل يفوق قدرات الجهاز المستخدم في الطريقة الآلية والمرتبط بالحاسب الآلي، حيث يضمن الذكاء الاصطناعي السرعة الفائقة في التحليل، والدقة اللامتناهية في تحديد هوية الشخص، بالإضافة إلى قدرة الذكاء الاصطناعي في التغلب على بعض المعوقات والصعوبات التي تعترض تحليل الصوت، مثل سوء التسجيل أو تداخل الأصوات، أو إحداث المتهم تغييرات في نبرة صوته.

جدير بالذكر أن المشرع المصري قد عالج القيام بإجراء مراقبة وتسجيل المحادثات السلكية واللاسلكية الخاصة بالأفراد بمعرفة النيابة العامة، كإجراء من الإجراءات التحقيق الابتدائي، وذلك بموجب نص الفقرة الثانية من المادة (٢٠٦) من قانون الإجراءات الجنائية بقولها: "ويجوز لها–النيابة العامة– أن تضبط لدى مكاتب البريد جميع الخطابات والرسائل والجرائد والمطبوعات والطرود، ولدى مكاتب البرق جميع البرقيات وأن تراقب المحادثات السلكية واللاسلكية وأن تقوم بتسجيلات لمحادثات جرت في مكان خاص متى كان لذلك فائدة في ظهور الحقيقة في جناية أو في جنحة معاقب عليها بالحبس لمدة تزيد على ثلاثة أشهر.

ويشترط لاتخاذ أي إجراء من الإجراءات السابقة الحصول مقدماً على أمر مسبب بذلك من القاضي الجزئي بعد اطلاعه على الأوراق".

من النص السابق يتبين أن المشرع وضع ضوابط وقيود على تسجيل المحادثات التي تجرى في مكان خاص، وبمفهوم المخالفة يكون التسجيل في الأماكن العامة لا يخضع للتنظيم الوارد بالنص السابق.

ومن الضوابط والقيود التي تطلبها المشرع المصري لمشروعية الإجراء، أن يكون التسجيل من اختصاص النيابة العامة، ومن ثم لا يجوز من مأموري الضبط القضائي، مع حقها في ندب أحد هؤلاء للقيام بالإجراء، وفق نص المادة (٢٠٠) إجراءات جنائية([1]).

أن يكون للإجراء فائدة في ظهور الحقيقة في التحقيق بشأن جناية أو جنحة معاقب عليها بالحبس مدة تزيد على ثلاثة أشهر، وبمفهوم المخالفة، لا يجوز التسجيل إذا كانت الجريمة جنحة معاقب عليها بالحبس أقل من ثلاثة شهور، أو معاقب عليها بالغرامة فقط. هذا بالإضافة إلى شرط قانوني يتعلق بضرورة الحصول على أمر مسبب من القاضي الجزئي، وهو ما يوجب على النيابة العامة أن تقدم الأسباب المبررة لتسجيل المحادثات في المكان الخاص، وأن تكون هذه الأسباب مقنعة للقاضي، وتبرر أن يصدر أمره بإجراء التسجيل.

بينما جاءت معالجة المشرع الإماراتي يشوبها عدم الوضوح في تحديد مكان المحادثات المراد تسجيلها، وفي النص على مبررات الإجراء، بخلاف معالجة المشرع المصري، فقد نصت المادة (٢٧٣/٢) من قانون الإجراءات الجزائية رقم (٣٨) لسنة ٢٠٢٢م على إنه: " ٢– لعضو النيابة العامة بعد موافقة النائب العام مراقبة وتسجيل المحادثات بما في ذلك السلكية واللاسلكية".

[1]) والتي نصت على أنه " لكل من أعضاء النيابة العامة في حالة إجراء التحقيق بنفسه أن يكلف أي مأمور من مأموري الضبط القضائي ببعض الأعمال التي من خصائصه".

وتبدو الإشكالية التي تواجه استخدام تقنية التعرف على بصمة الصوت، كإحدى تقنيات الذكاء الاصطناعي، لأغراض التنبؤ بالجرائم Predicting crimes، أو إقامة الدليل الصوتيVoice guide على بعضها، تلك الإشكالية تتمثل في مدى مشروعية تسجيل والتقاط المحادثات والأحاديث الخاصة التي تجرى بين الأفراد في الأماكن العامة، مثل: أماكن التسوق، والمقاهي وأماكن الترفيه، وغيرها.

نعتقد أن استخدام هذه التقنية في تسجيل المحادثات الخاصة للأفراد بشأن جريمة ارتكبت بمعرفة سلطة التحقيق يخضع لذات الشروط سالفة الذكر، كما أن استخدامها في تحليل الصوت المسجل للمتهم يخضع لذات الشرط المتعلق بضرورة قصر الإجراء على عضو النيابة العامة دون امتداده إلى مأموري الضبط القضائي أو رجال الشرطة. وقد ثم يكون التسجيل الخفي لبصمة الصوت باستخدام تطبيقات الذكاء الاصطناعي للمحادثات والأحاديث التى تجرى في مكان خاص هو أمر مشروع متى تم بإذن من سلطة التحقيق، لغرض كشف الحقيقة أو تحصيل دليل بشأن الجريمة محل التحقيق يصلح للإدانة([1]).

ما تقدم يوضح موقف المشرع المصري بشأن ضوابط وقيود تسجيل المحادثات التي تجرى في مكان خاص، فهل مفاد ذلك أن تسجيل المحادثات التي تجرى في مكان عام لا تسرى عليها هذه الضوابط وتلك القيود؟

[1]) انظر: د/ جميل عبد الباقي الصغير، الحق في الصورة والإثبات الجنائي، مرجع سابق، ص٣٤١.

ثانيا– استخدام الذكاء الاصطناعي في تمييز بصمة الصوت مع جمهور الأفراد:

يدق الأمر بالنسبة لاستخدام تطبيقات الذكاء الاصطناعي في تسجيل بصمة الصوت للأفراد في الأماكن العامة التي تجرى فيها محادثات أو أحاديث خاصة، أوضح مثال على ذلك: استخدام السيارات ذاتية القيادة، أو الطائرات بدون طيار، أو الروبوتات فائقة الذكاء، فلنا أن نتخيل تزويد هذه السيارة بتقنية تسجيل المحادثات التي تتم بين راكبيها من الجمهور، مما يطرح تساؤلا مهما حول مدى مشروعية تسجيل هذه المحادثات ومدى اعتبارها دليلا ذات حجية– لاسيما اذا تضمن التسجيل الاعتراف بارتكاب جريمة، أو التحريض أو الاتفاق على ارتكاب جريمة، أو تضمنت المحادثة التحضير لعمل إرهابي أو ارتكاب جريمة ماسة بأمن الدولة؟

يمكن افتراض حدوث ذلك مع تصور انفراد راكب تلك السيارة فأجرى مكالمة هاتفية أو أجرى محادثة مع راكب آخر، تضمنت ما أشرنا إليه، فما مشروعية تسجيل مضمون هذه المكالمة أو المحادثة بمضمونها السابق؟

يمكن القول: إنه باستقراء آراء الفقه الجنائي في شأن التسجيل الخفي للمحادثات الخاصة للأفراد فقد تباينت فيما بينها حول مدى مشروعية الإجراء، ومدى الاعتداد به كدليل إثبات، سواء بالإدانة أو البراءة؛ حيث اتجه الرأي الأول: إلى القول بأن استعمال جهاز التسجيل الآلي خفية إجراء صحيح لا يشوبه بطلان؛ فمن غير المتصور أن نحرم العدالة الجنائية مما يفرزه العلم من إمكانيات قد تحدث نقلة نوعية

في تحقيق العدالة الناجزة، مع اشتراط اتخاذ الإجراء بصدد جريمة وقعت، وصدور أمر من السلطة المختصة([1]).

بينما اتجه الرأي الثاني: إلى القول ببطلان استخدام أجهزة التسجيل الصوتي خفية لتعارضها مع حق الإنسان في حرمة الحياة الخاصة، وتمتعه بالخصوصية في تفاصيل حياته بحيث تكون بمنأى عن إطلاع الغير.

بينما اتجه رأي ثالث إلى: جواز استخدام تقنيات التسجيل الصوتي خفية في شأن بعض الجرائم الخطيرة، مثل الجرائم الماسة بأمن الدولة، والجريمة المنظمة والاتجار بالمخدرات وغيرها.

و يرى البعض أن استخدام بصمة الصوت في مكان خاص من قبل سلطة التحقيق أمر جائز، مادام في مصلحة التحقيق، بينما يكون باطلا وغير مشروع إذا كان من غير جهة التحقيق، أما إذا تم التسجيل الصوتي في مكان عام مثل تسجيل ندوة أو محاضرة عامة فلا بأس به([2]).

من جانبنا نعتقد أن الأمر ليس بهذه السهولة والوضوح في القطع بجواز أو عدم جواز استخدام تقنية الذكاء الاصطناعي ذات القدرات الفائقة في التعرف على بصمة الصوت لتحديد هوية الشخص؛ حيث يجب التمييز بين فرض التقاط هذه التقنيات

---

[1]) انظر في هذا الرأي: د/ حسن ربيع، حقوق الإنسان ومشروعية استخدام رجال الشرطة للوسائل المستحدثة للتحقيق الجنائي، مجلة الفكر الشرطي، مركز بحوث الشرطة، القيادة العامة لشرطة الشارقة، الإمارات العربية المتحدة، المجلد الأول، العدد ٤، مارس ١٩٩٣م، ص١٤٩، ١٥٠.

[2]) انظر في هذه الآراء: د/ عمر عبد المجيد مصبح، بصمة الصوت ودورها في الإثبات الجنائي، مرجع سابق، ص٣٤.

لأصوات الأفراد في مكان مفتوح لا يضمن أي قدر من الخصوصية أو العزلة للشخص عند التحدث، مثل أماكن التسوق المفتوحة للجمهور أو الحفلات العامة أو الندوات إلى غير ذلك من الأماكن والتجمعات التي تتم فيها محادثات أو أحاديث صوتية بين الأفراد، أو يجري فيها الأشخاص مكالمات هاتفية بصوت مرتفع؛ حيث يؤكد الفقه([1])أن وجود الشخص في مثل هذه الأماكن والتجمعات يخلع عن الحديث أو المحادثة طابع الخصوصية والسرية، ومن ثم يكون التقاط الصوت وتسجيله بواسطة تقنيات الذكاء الاصطناعي لاشك في مشروعيته.

يختلف الحكم بالنسبة للمحادثة غير المباشرة التي تجرى بواسطة الهاتف المحمول، حيث لم يعتد المشرع المصري ونظيره الإماراتي عند تطبيق نص المادة (٣٠٩) مكررا (١) من قانون العقوبات المصري، والمادة (٤٣١) من قانون الجرائم والعقوبات الإماراتي، بمكان إجراء المحادثة الهاتفية، وما إذا كانت قد أجريت في مكان عام أم خاص؛ على اعتبار أن إجراء المحادثة عن طريق الهاتف المحمول يعد قرينة مطلقة على إضفاء الصفة الخاصة عليها([2]) بل تمتد الحماية إلى المحادثة الهاتفية حتى ولو

[1]) حيث يقرر هذا الفقه أنه لا يعد خاصاً الحديث الذي يجرى بالتليفون السلكي من مكان عام وبصوت عال دون تحوط، كما لو أجراه الشخص في مقهى أو محل عام، أو بطريق التليفون المحمول إذا جرت بصوت عال ومسموع للكافة دون استراق السمع.

انظر: د/ محمد زكي أبو عامر، مرجع سابق، ص٨٧. يؤيد ذلك مسلك المشرع الفرنسي حيث نص على مشروعية التسجيل السمعي أو البصري الفيديو في الأماكن العامة أو لمصلحة الشرطة الادارية أو لإثبات بعض الجرائم. انظر في هذا د/ عمر عبد المجيد مصبح، مرجع سابق، ص٣٥.

[2]) د/ محمود نجيب حسني، مرجع سابق، بند ١٠٥٦، ص٧٩٠.

لم تتناول أية موضوعات خاصة بطرفيها؛ حيث يكون الحديث خاصاً إذا جري من خلال الهاتف المحمول، ولو تناول موضوعا عاما لا علاقة له بالحياة الخاصة([1]).

بينما كان المشرع الإماراتي أكثر وضوحا في نص المادة (٢١) من قانون مكافحة الشائعات والجرائم الالكترونية؛ حيث أضاف المشرع لصور الفعل الإجرامي: استراق السمع، أو اعتراض، أو تسجيل، أو نقل، أو بث، أو إفشاء محادثات، أو اتصالات، أو مواد صوتية، أو مرئية، مع عدم اشتراط المشرع الإماراتي المكان الخاص لقيام الجريمة، بمعنى أن ارتكاب صور السلوك الإجرامي المنصوص عليها يكفي لتوفر الركن المادي بغض النظر عن طبيعة المكان، خاصا أم عاما. كما نجده يوسع من نطاق محل الجريمة، فلا يقصره على المكالمات الهاتفية على نحو ما ورد بقانون الجرائم والعقوبات، وإنما يدخل في نطاق التجريم كافة المحادثات والاتصالات، سواء تلك التي يجريها الشخص عن طريق الهاتف أو تلك التي يجريها عن طريق شبكات الإنترنت باستخدام برامج مخصصة لذلك، بل إن المشرع الإماراتي لم يكتف بذلك، وإنما أدخل في نطاق محل الجريمة أية مواد صوتية أو مرئية تخص شخص ما، مفاد ذلك أن المشرع أراد بسط الحماية الجنائية لما قد يقوم به الشخص من إجراء تسجيل صوتي له، يدلي فيه باعترافات أو إقرارات أو ذكريات معينة مع نفسه، أي لا يأخذ شكل الحديث مع طرف آخر([2]).

---

[1]) د/ محمد زكي أبو عامر، الحماية الجنائية للحرية الشخصية، مرجع سابق، ص٨٦.

[2]) د/ محمد نور الدين سيد، الحماية الجنائية للحق في خصوصية المكالمات الهاتفية ، مرجع سابق، ٥٩١

وعليه؛ نجد صعوبة في حسم الأمر حول مدى مشروعية تسجيل الأحاديث أو المحادثات الخاصة بين الأفراد باستخدام تطبيقات الذكاء الاصطناعي والتي تجرى في مكان يوفر لهم العزلة والانفراد في إجراء الحديث أو المحادثة مثل: السيارة ذاتية القيادة، حيث لا ينكر أحد أن هذه السيارة تضفي على المحادثة طابع الخصوصية لاسيما في ظل عدم وجود سائق بشري، كما أنه لا يسمح للغير بدخولها أو الركوب فيها إلا بإذن من الراكب الموجود فيها والمستخدم لها بالفعل، وعليه نجزم أنها تعتبر في حكم المكان الخاص الذي لا يجوز استراق السمع أو تسجيل المحادثات أو الأحاديث الخاصة التي تجرى فيه.

وفي ذات الوقت لا يمكن القطع بعدم مشروعية التسجيل واستبعاده كدليل للإدانة إذا تضمن اعترافا أو تخطيطا أو اتفاقا أو تحريضا على ارتكاب جريمة لاسيما الجرائم الجسيمة مثل تلك الماسة بأمن الدولة، الداخلي أو الخارجي، والجرائم الإرهابية، والاتجار بالمخدرات وغيرها من الجرائم الخطيرة كجرائم الاعتداء على العرض بالإكراه.

لنا أن نتخيل قيام أحد الأشخاص باصطحاب سيدة معه في السيارة ذاتية القيادة، وأثناء تواجدها قام بمحاولة إغتصابها بالقوة أو الإكراه، وقامت السيارة بتقنياتها العالية بتسجيل الواقعة، وما تضمنه من أصوات تؤكد الإكراه الواقع على المجني عليها، ورفضها الاعتداء، فهل يمكن قبول هذا التسجيل كدليل إدانة أمام سلطات التحقيق والمحاكمة، على الرغم من عدم وجود إذن بالتسجيل، وبرغم ما أثير بشأن الحق في الخصوصية؛ لذلك نعتقد في ضرورة تدخل المشرع الجنائي بالنص صراحة على

استخدام تطبيقات الذكاء الاصطناعي في تسجيل المحادثات والأحاديث الخاصة بدون إذن من سلطات التحقيق، ومدى اعتبار هذا التسجيل دليلا مقبولا للإدانة أو البراءة.

المطلب الثاني

مدى مشروعية استخدام الروبوتات فائقة الذكاء

في العمل الشرطي والقضائي.

فكرة الشرطي الروبوت Robot cop انتقلت من عالم الخيال السينمائي إلى واقع ملموس، وانتقل من حلم يراود الإدارات الشرطية إلى حقيقة أثبتت فاعليتها في القيام ببعض المهام والأعمال الشرطية والأمنية بديلاً عن الشرطي البشري، لاسيما تلك التي تنطوي على قدر من المخاطرة، أو تحتاج سرعة فائقة ودقة عالية في أداءها، مثل تفكيك القنابل وإبطال العبوات الناسفة، كما قد يستخدم هذا الروبوت في تأمين الأماكن الحساسة والمؤتمرات الأمنية، وفي أعمال الحراسة([1]).

الفرع الأول

صور استخدام الروبوت فائق الذكاء في العمل

الشرطي والقضائي

إن أعمال الاستدلال والتحري عن الجرائم من الأعمال الشرطية التي برهنت على فاعلية استخدام الروبوتات فائقة الذكاء Super smart robots أو الروبوت الخارق

[1]) مقال بعنوان " الروبوت يبدأ عمله في شرطة دبي" منشور على موقع مؤسسة دبي للمستقبل، مرصد المستقبل، بتاريخ ١٢ يونيو ٢٠١٧، تاريخ زيارة الموقع ٢٠٢٠/١٢/٢٤م:
https://mostaqbal.ae/dubais-newest-addition-police-force-robot/

Super robo، ومن قبل ذلك فاعليتها في التنبؤء الاستباقي بالجريمة من خلال التعرف على الوجه، والتحليل السريع والدقيق للبيانات الخاصة بالأشخاص، لاسيما الخطرين أمنيًا أو من لديه خطورة إجرامية تتحدد من خلال سوابقه الإجرامية أو من خلال فهم سيولوجية الشخص، ومدى إتزان ردود أفعاله تجاه المواقف التي يتعرض لها.

أولاً– استخدام الروبوت فائق الذكاء في التنبؤ بالجريمة:

ذكرنا سابقا أن القيادة العامة لشرطة دبي أعلنت في وقت سابق عن انضمام أول شرطي آلي ذكي إلى صفوف كوادرها الأمنية لتأدية المهام المُوكلة إليه، ولاشك أن مجال التنبؤ بالجريمة من أهم الاستخدامات التي تم الاعتماد فيها على الروبوت، وأداها بشكل أفضل من الشرطي البشري؛ حيث أعلنت شرطة دبي أن باستطاعة الشرطي الألي كشف المشاعر، وفهم حركة الأجسام، والتعرّف على الإيماءات وإشارات اليد عن بعد، كما يمكنه رصد تعابير السعادة، والحزن، والإبتسام على وجوه الناس، كما يستطيع الروبوت إرسال مقاطع فيديو إلى غرف العمليات بإدارات ومراكز الشرطة([1])، كما أن تقنية التعرف على الوجه المزود بها الروبوت تساعده في القيام بتلك المهمة بشكل أسرع وأكثر دقة؛ حيث يمكنه –كما ذكرنا– تحديد هوية الشخص من خلال التعرف على ملامح وجهه.

[1]) الروبوت وتطبيقات الذكاء الاصطناعي، منشور على البوابة الرسمية لحكومة الإمارات العربية المتحدة، تاريخ الزيارة ٢٠٢٠/١٢/٢٤م:
https://u.ae/ar-ae/about-the-uae/digital-uae/robotics-and-ai-applications

ويمكن تغذية تقنيات الذكاء الاصطناعي ببيانات تحتوي على تجارب سابقة لأنشطة غير مشروعة وإجرامية، ثم تبدأ الخوارزميات بالتعلم والتدرب على تلك المدخلات، وصولاً إلى فهمها، وإتقان التعامل معها، ومن ثم تكتسب هذه التقنيات القدرة على التنبؤ بأنماط الأنشطة الإجرامية أو غير المشروعة، والكشف عنها، وضبط مرتكبيها. من قبيل ذلك: التقنيات التي يمكنها التنبؤ بالتوجهات والقناعات الفكرية والايدولوجية الفكرية من خلال مراقبة وسائل التواصل الاجتماعي Social Media ، لاسيما، Twitter ،Facebook.

ومن الجدير بالذكر أن هناك تقنيات للذكاء الاصطناعي تساعد في التنبؤ بموقع وتوقيت ارتكاب الجرائم، كما أن هناك برامج تحلل طريقة وأسلوب مشي الأشخاص المقدمين على ارتكاب جرائم الاعتداء، كما هناك برامج تحلل سلوكيات الأشخاص الذين يرغبون في السرقة والعنف والتحرش. كما يمكن استخدام خوارزميات الذكاء الاصطناعي في جلسات استماع إطلاق السراح المشروط، ومنها: خوارزمية (COMPAS) التي تستخدم لتقرير العودة إلى الإجرام في نظام العدالة الجنائية في جلسات استماع إطلاق السراح؛ حيث تبين أن هذا النظام كان يعطي نتائج متحيزة بشكل منهجي، هذا التحيز أدى إلى تفاوت الأحكام الجنائية التي تستخدم هذه التقنيات([1]).

[1]) Osonde A. Osoba, William Welser IV ,The Risks of Artificial Intelligence to Security and the Future of Work, op. cit. P: 8.

ثانيا– القيام بأعمال الاستدلال والتحري:

جدير بالذكر أن استخدام الروبوت فائق الذكاء في القيام بأعمال الاستدلال والتحري ومنها: القيام بإجراء الاستيقاف([1]) حال وجود شخص محل ريبة وشك طواعية، مما يسمح للشرطي الروبوت بالتدخل لسؤال الشخص عن حالة الريبة والشك التي أوجد نفسه فيها، ومن ثم استيضاح أمره، وهذا عمل مقبول من الشرطي البشري، إلا أن استخدام الشرطي الروبوت في القيام به أثبت جدارة وفاعلية أفضل بكثير من البشري، حيث يستطيع من خلال تقنية التعرف على الوجه التحقق من هوية الشخص، والولوج إلى قاعدة البيانات الخاصة به، بحيث يمكن التعرف على ما إذا كان هذا الشخص مطلوبا أمنياً أو صادراً بشأنه أمراً بالقبض أو من الفارين، أو حتى من المخالفين لقوانين الإقامة داخل البلاد. ولاشك أن هذه التقنيات توفر الكثير من الوقت

[1]) جدير بالذكر أن استخدام الروبوت الذكي في استيقاف المركبات الثقيلة بات أمرا واقعا في إمارة دبي، حيث أعلنت هيئة الطرق والمواصلات بدبي عن مبادرات الرقابة والتفتيش التي تشمل استخدام طائرات من دون طيار في عمليات رصد المركبات الثقيلة المتهربة من التفتيش، والتقاط صور للوحات المقطورات، واستخدامها للتعرف على بروز الحمولة وتوزيعها، وسلامة بدن المركبة، وكذلك استخدام الرجل الآلي في عملية استيقاف المركبات وتوجيهها لنقطة التفتيش ما أسهم في زيادة الأمن والسلامة لأفراد الشرطة والمفتشين، حيث يتم الاستعانة بالروبوت في توقيف المركبات الثقيلة التي تسجل مخالفات لا يمكن ان تسمح لها بالسير مطلقا حفاظا على سلامة المركبة والسائق ومستخدمي الطريق، وإن استخدام الروبوت على هذا النحو يضمن سلامة المفتش الميداني الذي كان سابقا يقوم بهذه المهمة. انظر: هنادي أبو نعمة، روبوت يوقف المركبات الثقيلة في دبي .. وطائرة من دون طيار تكشف مخالفاتها، الإمارات اليوم، منشور بتاريخ ٠٧ أكتوبر ٢٠١٩، على الموقع الرسمي، تاريخ الزيارة ٢٠٢٠/١٢/٢٤م:
https://www.emaratalyoum.com/local-section/other/2019-10-07-1.1259569

وتجنب الشخص المستوقف تعرضه لاصطحابه إلى مركز الشرطة لاستيضاح أمره حال فشله في تفسير حالة الريبة والشك التي وجد فيها، كما يحدث من الشرطي البشري.

إن القدرات الفائقة للشرطي الروبوت في القيام بالاستيقاف قد تسفر عن حقيقة الشخص المستوقف، فقد يتبين صدور أمراً بالقبض عليه، أو أنه من الفارين، أو المخالفين لقوانين الإقامة، وقد يسفر الاستيقاف على حالة تلبس بارتكاب جريمة، كما هو الحال بالنسبة للاستيقاف من الشرطي البشري. هذا ما يطرح تساؤلاً مهما حول مدى إمكانية قيام الشرطي الروبوت بإجراء القبض أو احتجاز الشخص؟ وما الإجراء الأنسب إذا لم يكن من غير المتصور قيامه بهذا الإجراء؟ وهو ما سوف نجيب عليه لاحقاً.

ثالثا- استخدام الروبوت في أعمال التفتيش والمعاينة:

أشار البعض([1]) إلى أن التقدم الهائل في تكنولوجيا نقل الصوت والصورة باستخدام الكاميرات الرقمية التي تتميز بالتصوير بالأشعة تحت الحمراء Infrared Rays سهل إمكانية إجراء المعاينة عن بعد، كما يمكن الاستعانة بطائرة بدون طيار للاستفادة من قدراتها الفائقة في التصوير ونقل الصوت والصورة مباشرة إلى مركز التحكم، ومن ثم يمكن لعضو النيابة العامة متابعة عملية المعاينة مباشرة، ومشاهدة مسرح الجريمة، وما يتضمنه من أدلة ظاهرة، مثل: وضع الجثة، أو حالة مكان

[1]) د/ حليمة حالد المدفع، استخدام تقنية الاتصال عن بعد في التحقيق والمحاكمات الجزائية، كلية الدراسات العليا، جامعة الشارقة، ٢٠٢٠م، ص١٤٣.

ارتكاب الجريمة، حالة الأبواب والنوافذ إلى غير ذلك من الملابسات والأدلة الظاهرة المؤثرة في تكوين رؤية عضو النيابة العامة عن الواقعة محل التحقيق.

وقد ساعد استخدام تقنيات الذكاء الاصطناعي ومنها: الروبوتات فائقة الذكاء على تحليل العديد من المعلومات البصرية والأدوات المبعثرة التي وصل تحليلها إلى الجاني، والكشف عن أسلوب ارتكاب الجريمة والأدلة المتحصلة من مسرح الجريمة من خلال الصور التي يتم التقاطها أثناء المعاينة، كما يضمن استخدام هذه التقنيات في إجراء المعاينة التيسير على عضو النيابة العامة في اتخاذ ما يراه مناسبا من أوامر لمأموري الضبط القضائي بمسرح الجريمة، وكذلك لخبراء الأدلة الجنائية، دون أن يتطلب ذلك انتقاله شخصيا([1]).

من المستقر عليه أن التفتيش سواء أكان واقعاً على الأشخاص أو المنازل بهدف البحث عن أدلة هو من إجراءات التحقيق المخولة للنيابة العامة، وليس من إجراءات الاستدلال والتحري المنوطة بمأموري الضبط القضائي، ومنهم رجال الشرطة، ومع ذلك فهو جائز من رجال الشرطة استثناءً في حالات معينة، أهمها التلبس بالجريمة، والندب من سلطة التحقيق.

وكثيرٌ ما يقع الخطأ في إذن التفتيش خاصة في بيانات الشخص أو المنزل محل التفتيش، كما قد يتراخى الحصول على الإذن مما قد يؤدي إلى تمكن الجناة من إتلاف الشيء محل التفتيش أو إخفائه؛ لذلك كان لتقنيات الذكاء الاصطناعي دوراً في

[1]) د/ حليمة خالد المدفع، المرجع السابق، ص١٤٤.

إجراء التفتيش؛ فقد أشار البعض إلى إذن التفتيش الذكي، الذي يقوم على فكرة الربط الإلكتروني بين إدارات ومراكز الشرطة والنيابة العامة؛ حيث يقدم طلب الإذن إلكترونياً على تطبيق ذكي يتم تحميله على الهواتف والألواح الذكية لرجال الشرطة، يسهل على عضو النيابة العامة الإطلاع عليه وتوقيعه في دقائق معدودة، ثم إرساله إلى رجل الشرطة المعني بالتنفيذ([1]).

رابعا- استخدام الروبوت في التحفظ والقبض على الجناة:

هل يمكن أن نتصور إمكانية استخدام الشرطي الروبوت القوة مع الشخص المتلبس بارتكاب جريمة أو من تبين صدور أمر بالقبض عليه من خلال التعرف على وجه، بداية نُذكر بتجربة شرطة دبي الفريدة في هذا المجال؛ حيث أطلقت أول شرطي روبوت مزود بتقنية التعرف على الوجه، وإرسال مقاطع فيديو ومتابعة جمهور الأفراد في التجمعات وأماكن التسوق حيث باستطاعته قراءة تعابير الوجه والتنبؤ بما قد يقع من الشخص من خلال تحليل تعابير وجهه، وبياناته وسوابقه الإجرامية، مما قد يدفع إلى تدخله؛ لمنع ارتكاب فعلا إجراميا من هذا الشخص، وقد أشارت شرطة دبي أن هذا الروبوت لن يكون في استطاعته اعتقال الأشخاص والقبض عليهم واحتجازهم، وإنما حددت مهامه في مساعدة الأفراد والإجابة على تساؤلاتهم والمساعدة في إنجاز بعض المعاملات السريعة مثل: التبليغ عن الجرائم، وتقديم الشكاوي([2]). في اعتقادنا أن ذلك ليس بالمستبعد ولا بالمستحيل في المستقبل القريب؛ حيث إن صناعة

[1]) المرجع السابق، ص١٥٣، ١٥٤.

[2]) مقال بعنوان " الروبوت يبدأ عمله في شرطة دبي" مصدر سابق.

الروبوتات فائقة الذكاء في تطور مستمر لا حدود ولا سقف لما قد تكون عليه إمكانياتها في المستقبل، فقد تزود هذه الروبوتات بقدرات فائقة في استخدام القوة، وفي حدود معينة تكفي لتنفيذ أمر القبض على الشخص حال تلبسه بارتكاب جريمة، ويمكن حصر ذلك في التلبس بالجرائم الجسيمة، مثل: الجرائم الإرهابية، وتلك الماسة بأمن الدولة، وكذلك الحال بالنسبة للأشخاص شديدي الخطورة الأمنية، وقد يكون تنفيذ ذلك في صورة التهديد باستخدام السلاح أيا كان نوعه، كما لو كان عصاً كهربائية أو ذراعاً إلكترونية تطلق مادة مخدرة أو نبضات كهربائية.

وبعيدا عن الأمر بالقبض وتنفيذه من قبل الشرطي الروبوت قد يكون من المتصور إلى حد كبير منطقا وعقلا أن يصدر الروبوت أمرا بعدم مغادرة المكان إلى الشخص المتلبس بارتكاب جريمة أو كل شخص وجد في مسرح جريمة متلبس بها، مع الاتصال فورا بمركز التحكم بالإدارات الشرطية المعنية لإرسال أفراد شرطة بشريين، وقد يتم ذلك في غضون دقائق معدودة. هذا ما يطرح التساؤل حول قيمة الأمر الصادر من الشرطي الروبوت بعدم مغادرة المكان للأفراد الحاضرين بمسرح الجريمة أو للشخص المتلبس بالجريمة، يرى الباحث: أن هذا الأمر يكتسب ذات قيمة الأمر الصادر من الشرطي البشري؛ حيث يجب على الأفراد الامتثال للأمر بعدم المغادرة، وإلا تعرض من يخالف ذلك إلى عقوبة الغرامة المقررة قانونا؛ حيث يجوز للشرطي البشري وكذلك الشرطي الروبوت تحرير محضرا ورقيا بالنسبة للأول وإلكترونيا بالنسبة للثاني، يوضح فيه المخالفة وبيانات الشخص المخالف.

أما بخصوص الأمر الصادر من الروبوت الشرطي للشخص المتلبس بارتكاب الجريمة فإنه يعد أمرا من قبيل التحفظ على الشخص ويعد مقدمة للقبض عليه، إما بمعرفة رجال شرطة بشريين، وإما من قبل الشرطي الروبوت حال منحه هذه الإمكانية؛ حيث يمكن –كما ذكرنا– منح الروبوت إمكانية استخدام القوة الكافية لتنفيذ القبض على المتلبس بالجريمة، مع تحديد شكل وحدود هذه القوة.

الفرع الثاني

تبرير مشروعية استخدام الروبوتات فائقة الذكاء

في العمل الشرطي والقضائي

نتناول في هذا الفرع سند مشروعية استخدام الروبوت فائق الذكاء في العمل الشرطي كوسيلة للاستدلال أو في العمل القضائي سواء من سلطة التحقيق، أو من مأموري الضبط القضائي استثناءً في حالات التلبس.

أولاً– الروبوت فائق الذكاء مجرد وسيلة تكنولوجية حديثة:

يؤكد بعض الفقه أن استعانة مأموري الضبط القضائي بالطرق الفنية من أجل البحث والتحري عن الجرائم التي يتم إبلاغه عنها، يعد أمراً مشروعاً منتجاً أثره، طالما أن الاجراءات التي قام بها لا تنال من حقوق وحريات الأفراد لاسيما الحق في الخصوصية وحرمة الحياة الخاصة(١). كما أشار البعض الآخر إلى أنه يجوز

(١) د/ جميل عبد الباقي الصغير، الحق في الصورة والإثبات الجنائي، مرجع سابق، ص٣٣٤.

الاستعانة بالوسائل الإلكترونية الحديثة، ومنها وسائل الاتصال عن بعد في جميع مراحل الدعوى الجزائية، لاسيما مرحلة جمع الاستدلالات باعتبارها مرحلة تمهيدية أولية، ومرحلة التحقيق الابتدائي([1]).

من جانبنا نؤكد على مشروعية استخدام روبوتات الذكاء الاصطناعي في إجراءات الاستدلال والتحري عن الجرائم متي تم ذلك بمعرفة أحد رجال الشرطة، وبإشرافه المباشر؛ حيث لا يعدو الروبوت سوى أن يكون وسيلة إلكترونية حديثة يجوز لرجل الشرطة الاستعانة بها، من قبيل الاستعانة بالطرق الفنية، كما لو قام رجال الشرطة باستخدام الروبوت في التعرف على المشبوهين أو فحص بصمة الصوت والعين للمشبوهين فلا يخرج الأمر عن نطاق استخدام التكنولوجيا الحديثة في مكافحة الجريمة والتحري عنها، كما كان الحديث قديماً عن استخدام نظم الحاسب الآلي في الاستدلال والتحري عن الجرائم بمعرفة مأموري الضبط القضائي، وهو ما أضحي من الأمور المسلم بها، واستقرت عليها الممارسات الشرطية، وأقرتها الاتجاهات القضائية على اختلاف أنواعها.

ونعتقد أن الأمر لا يختلف كثيرا بالنسبة لمشروعية الاستعانة بالروبوت فائق الذكاء في القيام ببعض إجراءات التحقيق بمعرفة سلطة التحقيق؛ إذ لاشك في جواز استعانة سلطات التحقيق بوسائل التكنولوجيا الحديثة في سبيل كشف غموض الجريمة، وضبط مرتكبيها، وإقامة الدليل المرجح لإدانتهم، كما يحدث عند استخدام

[1]) د/ حليمة خالد المدفع، استخدام تقنية الاتصال عن بعد في التحقيق والمحاكمات الجزائية، مرجع سابق، ص٢٣.

الروبوت في تحليل البصمات لاسيما بصمة الصوت من خلال التسجيلات المضبوطة؛ حيث أثبتت تقنيات الذكاء الاصطناعي نحاجا وفاعلية في التحقق من هوية الشخص من خلال بصمة الصوت أو بصمة العين بشكل أسرع وأكثر دقة من الاستعانة بالوسائل التقليدية في مختبرات الأدلة الجنائية.

كما أثبت الروبوت فاعلية وجدارة في معاينة ورفع الآثار والبصمات في مسرح الجريمة لاسيما الجرائم الإرهابية، لاسيما في التحقق من هوية الجناة والضحايا في عمليات التفجير من خلال تحليل البصمة الوراثية بواسطة تقنيات الذكاء الاصطناعي في وقت قياسي مقارنة بمختبرات الأدلة الجنائية والطب الشرعي.

لكن يدق الأمر حول الحديث عن مشروعية قيام الروبوت مستقلاً عن التدخل البشري ببعض الإجراءات السابقة سواء في مرحلة الاستدلال والتحري أو في مرحلة التحقيق، كما لو قام باستيقاف شخصاً تبين من خلال تقنية التعرف على الوجه أنه مطلوب أمنياً أو من مخالفي قوانين الإقامة، أو صدر بحقه أمرا بالقبض عليه من النيابة العامة، أو تبين من خلال قراءة تعابير الوجه والجسد، أو من خلال سوابقه الإجرامية وجود احتمال بارتكاب جريمة منه. فما مدى مشروعية هذا الإجراء إذا قام به الروبوت بنفسه دون تدخل البشر؟ وماذا لو احتاج الأمر اصطحاب الشخص المستوقف إلى مركز الشرطة أو التحفظ عليه لحين وصول رجال الشرطة لمباشرة القبض، فما مدى مشروعية إجراءات التحفظ على الشخص؟

بداية نؤكد على أن قانون الإجراءات الجزائية المصري ونظيره الاماراتي خلا من أي نصوص تنظم استخدام الروبوت فائق الذكاء في أعمال الاستدلال والتحقيق، وعليه

نؤكد على أن الأمر يحتاج إلى تدخل المشرع الاجرائي بتنظيم الإجراءات التي يمكن الاستعانة بالروبوت فائق الذكاء في القيام بها مستقلاً عن رجال الشرطة؛ هذا ما يقتضي من المشرع الاجرائي النص على اعتبار هذا الروبوت من مأموري الضبط القضائي ذو طبيعة خاصة.

ثانياً– تبرير مشروعية قيام الروبوت فائق الذكاء بأعمال القبض والاحتجاز:

وأخيرا لو افترضنا تزويد الروبوتات فائقة الذكاء بالقدرة على توقيف الشخص والقبض عليه – وهو أمر حاصل لا محالة في ضوء استشراف مستقبل هذه الروبوتات– لاسيما القبض على من يكون في حالة تلبس بارتكاب جريمة يجوز القبض فيها، فما مدى مشروعية إجراء القبض على الشخص المتلبس بارتكاب جريمة؟

نؤكد على أن هذا الافتراض ليس بالمستحيل، بل ويمكننا القول أن التطلع الأمثل لاستخدامات الشرطي الروبوت ينبيء بتزويده بالقوة اللازمة لتوقيف شخص ما والقبض عليه، هذا من منطلق تخفيف العبء إلى حد كبير عن كاهل رجال الشرطة لاسيما في حالات المطاردات الخطيرة، أو المداهمات لأوكار التشكيلات العصابية أو الجماعات الإجرامية المنظمة أو الخلايا الإرهابية، فمما لاشك فيه أن القبض على هؤلاء ومداهمة أوكارهم يحمل الكثير من الخطورة وتهديد أمن وسلامة رجال الشرطة. وهو ما حدث في الولايات المتحدة الأمريكية؛ حيث أثير الحديث حول استخدام الروبوت في اعتقال المجرمين، لاسيما في الجرائم الخطيرة، كما حدث في واقعة إطلاق نار جماعي في إحدى الولايات والذي انتهى بمقتل مطلق النار بقنبلة ألقاها

روبوت، مما أثار مخاوف بعض القانونين من التطور الجديد في آليات إنفاذ القانون وتأثيره على قرينة البراءة([1]). وبما أن هذا الأمر حاصل لا محالة وجب أن نكون أكثر استعدادا بمنظومة تشريعية إجرائية تناسب هذا التطور، ومن ثم نوجه الدعوة إلى المشرع الجنائي الإجرائي بسرعة التدخل بوضع المعالجة التشريعية لاستخدام الروبوتات فائقة الذكاء في القيام بإجراء القبض مستقلا عن رجال الشرطة.

[1]) Osonde A. Osoba, William Welser IV ,The Risks of Artificial Intelligence to Security and the Future of Work, op. cit. P: 8.

المبحث الثاني

استخدام تطبيقات الذكاء الاصطناعي

في التحقيق الإبتدائي والمحاكمة الجزائية.

تمهيد:

بسبب نتائج الثورة الصناعية الرابعة شهدت كافة المجالات المهنية ومن أهمها المجال القضائي تحولا تكنولوجياً مذهلا في العقود الأخيرة، ويمكن القول أن تقنيات الذكاء الاصطناعي أحد أهم مسرعات هذا التحول، فقد ظهرت في المجال القضائي العديد من البرامج والتقنيات التي قد تؤثر على توظيف العنصر البشري في هذا المجال، من ذلك: ما يعرف بـ(وكيل النيابة الروبوت)، و(القاضي الروبوت)، ومن ثم يعد استخدام تقينات الذكاء الاصطناعي في الحقل القضائي وسيلة مهمة لغايات تحسين كفاءة القضاة، ومعاونيهم من الخبراء والمترجمين، مستغلين في ذلك القدرات الفائقة والمعلومات الهائلة التي تمتلكها هذه التقنيات؛ حيث يمكنها تزويد أعضاء النيابة العامة والقضاة بمعلومات مذهلة عن السوابق الجنائية للمتهم، والأحكام السابقة في الواقعة الإجرامية محل الدعوى الجزائية، كما يمكن أن تعين هذه التقنيات أعضاء النيابة العامة والقضاة في اصدار أوامر التحقيق، والقرارات والأحكام القضائية، لكن هذا الاعتماد المتسارع على تلك التقنيات يحيطها الكثير من التشكك في دقة نتائجها، وموضوعيتها، بالإضافة إلى ما أثير بشأن مشروعية استخدامها.

تقسيم:

نقسم هذا المبحث إلى المطلبين التاليين:

المطلب الأول: استخدام الروبوتات فائقة الذكاء في التحقيق الإبتدائي.

المطلب الثاني: استخدام تقنية التحليلات التنبؤية في إصدار القرارات والأحكام القضائية.

المطلب الأول

استخدام الروبوتات فائقة الذكاء في التحقيق الإبتدائي.

من الثابت أن بعض إجراءات التحقيق الابتدائي ومنها: استجواب المتهم، وسماع الشهود، تحتاج إلى مقومات ومهارات خاصة لدى المحقق الجنائي، منها: الفراسة، وقراءة تعابير الوجه وفهم لغة الجسد، ومهارة توجيه الأسئلة بشكل يعكس حنكة وخبرة عالية لدى المحقق؛ كل هذه المقومات والمهارات تبرز أهميتها في استخلاص الدليل المادي، وما يترتب على ذلك من إجراءات أخرى، مثل: إصدار الأمر بالحبس الإحتياطي.

وفي ظل تسابق الدول في الاستفادة من القدرات الفائقة لتطبيقات الذكاء الاصطناعي، ومنها الروبوتات فائقة الذكاء، فقد كشفت نيابة دبي بدولة الإمارات العربية المتحدة بتاريخ ١٥ فبراير ٢٠١٨م عن دراسة مشروع (وكيل النيابة الروبوت)، الذي يعد أحد صور مبادرة (النيابة العامة الذكية) التي تقوم بأتمتة عمل النيابة العامة، بما يحقق الربط التكنولوجي بينها وبين أجهزة الشرطة والمؤسسات العقابية وغيرهما؛ بحيث تصل أوامرها وقرارتها إلى الجهة المنفذة بشكل فوري، دون مجال لضياع الوقت.

هذا ما يطرح تساؤلات كثيرة حول فاعلية قيام الروبوت فائق الذكاء بإجراءات التحقيق الإبتدائي بديلاً عن المحقق البشري، في بعض الاجراءات الجزائية التي تواجه تحديات كبيرة، وتثير إشكاليات كثيرة، خاصة إستجواب المتهم، والمواجهة، وسماع الشهود، بالنظر إلى اعتماد هذه الاجراءات على مقومات ومهارات شخصية لابد أن تتوافر في المحقق البشري، كما ذكرنا آنفا.

وعليه؛ يتم طرح التساؤل الآتي: ما مدى فاعلية استخدام الروبوت فائق الذكاء في القيام بإستجواب المتهم وسماع الشهود؟ وما هي التحديات التي تواجه هذا الإستخدام؟ وفي سبيل الاجابة على هذه التساؤلات نقسم هذا المطلب إلى الفرعين الآتيين:

الفرع الاول

المهارات التي يعتمد عليها التحقيق الجنائي.

تتنوع المهارات والخصائص الأساسية التي يعتمدها عليها التحقيق الجنائي، منها مهارات شخصية وخصائص نفسية، وذهنية، نعرض فيما يلي لأهم هذه المهارات والسمات والخصائص:

أولاً– السمات والخصائص النفسية:

١– الاتزان الانفعالي:

يراد به "حالة التروي والمرونة النفسية الوجدانية، تجاه المواقف الانفعالية تجعل الأشخاص أكثر سعادة، وهدوءاً، وتفاؤلاً، وثباتاً من الناحية المزاجية، وثقة بالنفس،

بخلاف الأشخاص الذين لا يتمتعون بهذا الاتزان لديهم شعور بالدونية، ومن السهل اثارتهم، وأكثر ميلاً للكآبة، والتشاؤم، ومتقلبي المزاج"([1]). هذا الاتزان يجعل الشخص أكثر مرونة في التعامل مع المشكلات الحياتية التي تواجهه، والاعتدال في اتخاذ القرارات دون تفريط أو إفراط، مما يكسبهم الكفاءة والثقة بالنفس.

٢- قوة الوجدان:

كون المحقق إنسان بشري لابد أن تتوافر فيه قوة الوجدان، بأن يكون قادراً على التفاعل مع الآخرين، بالمشاعر، والعواطف، والأحاسيس، والمحبة، فلا يكون منفصلاً عنهم، متكبرا عليهم، متعالياً في برجه العاجي، بل لابد أن تتوفر فيه القيم الاجتماعية والوجدانية التي تجعله مصدر جذب وتفاعل مع الآخرين([2]).

٣- السيطرة على مجريات التحقيق:

لابد أن تتوافر في المحقق الجنائي القدرة على السيطرة والاستحواذ على مجريات التحقيق، لاسيما عند مباشرة استجواب المتهم أو مواجهته بالمتهمين الآخرين أو الشهود أو المجني عليهم، بحيث يكون قادرا على الإمساك جيدا بإدارة دفة الحديث والسيطرة على مجراه، فلا ينزلق في حديث أو أقوال لا جدوى منها، ولا يقع في متاهات وتفاهات الأقوال والإفادة، ويكون قادرا على السيطرة على جنوح المتهم أو إسهابه في الأقوال دون جدوى. فقد يجلس المحقق مع المتهم يسمعه ساعات طويلة

---

[1]) د. راشد محمد المري، المهارات الفنية لرجل الأمن في التحقيق والبحث الجنائي، مجلة روح القوانين، جامعة طنطا، العدد ٩٢، أكتوبر ٢٠٢٠م، ص٨٣.

[2]) د. عدنان خالد التركماني، المعايير الشرعية والنفسية في التحقيق الجنائي، المركز العربي للدراسات الأمنية والتدريب، الرياض،١٤١٤هـ، ١٩٩٣، ص١٠٩.

ولكن لا يخرج من أقواله أو كلامه بشيء يفيد في التحقيق، بحيث يكون المتهم هو المسيطر على الحديث والتحقيق لا المحقق.

كما يجب أن تتوفر في المحقق القدرة على توجيه الأسئلة بهدوء واتزان، بعيداً على العصبية والانفعال مما قد يصيبه بالتوتر، فقد السيطرة على مجريات الاستجواب أو سماع الشهود، وغيرهما من الاجراءات التي تحتاج مهارة كلامية.

ثانياً– الخصائص والسمات الذهنية والعقلية:

١– الفِراسة والفِطنة:

من أهم سمات وخصائص المحقق الجنائي أن يمتلك الفِراسة ويراد بها اصطلاحاً "مجموعة الدلائل الحسية والشكلية التي يمكن من خلالها وصف مشاعر وانطباعات الشخص الآخر، بالاعتماد على عدد من النظريات والقواعد التي صنفت مجموعة من تعابير الوجه والأحاسيس التي تترجم صفات الشخص ومشاعره في تلك اللحظة، وطباعه العامة". والفِراسة علم يقدم طرحاً مغايراً لفهم طبيعة البشر وطبائعهم، والربط بين الظاهر من مشاعر وحركات جسدية، وبين ما هو متصل بها من صفات وطبائع وقناعات ذاتية([1])، فهي الاستدلال بالأمور الظاهرة على الأمور الخفية.

تعد الفِراسة سمة الحكماء، وصفة دالّة على الفطنة، لاعتمادها على الحدس ودقة الملاحظة، وقد ارتبط علم الفِراسة قديماً بمعرفة الناس الخيّرين وسواهم، كما استخدمت

[1]) يمان هاشم القدور، مقال بعنوان "معنى الفراسة" منشور بتاريخ ١٤ أبريل ٢٠١٩، على الرابط الالكتروني:

https://mawdoo3.com/

للكشف عن بعض الجوانب الشخصية للآخرين([1]). وقيل أن الفِراسة هي: الاستدلال بهيئات الإنسان وأشكاله وألوانه وأقواله على أخلاقه وفضائله ورذائله، أو هي الاستدلال بالخلق على الخُلق، وتنقسم إلى أنواع متعددة، منها: الفِراسة الرياضية، والخلقية، والإيمانية([2]).

الفِطنة لغة تدل على ذكاء وعلم بشيء. والفِطنة كالفَهم، وهي ضِد الغباوة، ومن فوائد الفِطنة: أنها من مقوماتِ الشخصية الناجحة؛ فقد يتمتع الرجل بالقوة والأمانة، ولا يتمتع بالفِطنة، ومن ثم لا يستطيع أن يسير أعماله بالطريقة المطلوبة؛ قيل: "القوة والأمانة لا يكفيان في حصولِ المقصودِ ما لم ينضم إليهما الفِطنة والكِياسة. ومن فوائدها أيضا إكساب الشخص القدرة على التعامل مع مختلف المواقف، واستثمار الأوقات فيما ينفع، والقدرة على استثمار المهارات فيما يناسبها بصورة صحيحة، والرجل الفَطِن لا يُغرر به ولا يخد، مع القدرة على مراعاة أحوال الناس واختلافهم، والتعامل معهم وفق ذلك، وإكساب الشخص القدرة على تمييز الحق من الباطل، وكشف زيف الأمور([3]).

---

[1]) المرجع السابق.

[2]) عبد العزيز عبد الله الراجحي، شرح كتاب الحموية لابن تيمية، منشور على موقع المكتبة الشاملة الالكتروني:

https://shamela.ws/book/37019/1

[3]) الدرر السنية، موسوعة الاخلاق والسلوك، منشورة على الموقع الالكتروني:

https://dorar.net/alakhlaq/2279/

ولاشك أن التحقيق الجنائي يتطلب أن يتمتع المحقق بالفِراسة والفطنة، والاستفادة من فوائدهما في الوصول إلى الحقيقة فيمن ارتكب الجريمة محل التحقيق، وإقامة الدليل ضده، وتقديمه إلى المحاكمة مع قناعة المحقق بكفاية الادلة على إدانته.

٢– الذكاء والقدرة على التذكر:

الذكاء من أهم السمات والخصائص العقلية التي يعتمد عليها التحقيق الجنائي، ويشمل القدرة على التحليل، والتخطيط، وحل المشاكل، وبناء الاستنتاجات، وسرعة التصرف، كما يشمل القدرة على التفكير المجرد، وجمع وتنسيق الأفكار، وسرعة التعلم.

هناك ربط واضح بين الذكاء وقوة الذاكرة، لذلك من السمات الإساسية التي يجب أن يمتلكها المحقق الناجح امتلاكه ذاكرة فائقة، وآليات التخزين السليمة للمعلومة، ومن ثم يحتاج المحقق عقلية قادرة على استدعاء المعلومات على اختلاف أنواعها، خاصة المعلومات والنصوص القانونية والأحكام القضائية، والاستفادة منها في وصف وتكييف الواقعة الجنائية محل التحقيق، هذا بالإضافة إلى قدرته على تذكر ما ورد في محضر الاستدلال وأقوال الشهود والمتهم؛ بحيث تكون ذاكرته حاضرة في المواجهة الفورية والسريعة للمتهم أو الشاهد بما ذكره في محضر الاستدلال، من واقع ذكراته، دون الرجوع إلى المحضر.

٣– القدرة على الفهم الواقعي للوقائع:

كما يجب أن تتوافر في المحقق سمة عقلية متقدمة تتمثل في قدرة المحقق على فهم الوقائع بشكل واقعي، والربط بين ملابساتها ووضع التصور الأقرب للواقع من خلال

أقوال المجني عليهم والشهود والمتهم، ولا يعتمد على التصور الافتراضي الذي يضعه رجل الضبط، فقد يكون غير واقعي أو منقطع الصلة بالواقع.

كما يجب أن تتوفر في المحقق القدرة على الربط الواقعي بين الأدلة القولية، مثل: الاعتراف وشهادة الشهود، وبين الأدلة المادية المستخلصة من المعاينة والتفتيش. فقد يكون اعتراف المتهم أو أقوال الشاهد منبت الصلة بما ورد بالمعاينة وما كشف عنه مسرح الجريمة، باعتباره الدليل الصامت، هذه السمة تمكن المحقق من الوقوف على مدى صدق المتهم في اعترافه أو صدق الشاهد في أقواله.

الفرع الثاني

توظيف قدرات الروبوتات فائقة الذكاء في القيام بإجراءات التحقيق الابتدائي.

عرضنا بايجاز فيما سبق للسمات والخصائص التي ينبغي أن تتوافر في المحقق الجنائي الناجح، وتفترض فكرة توظيف قدرات الروبوتات فائقة الذكاء في القيام بإجراءات التحقيق الجنائي طرح التساؤل الآتي: **فهل تمتلك هذه الروبوتات تلك السمات والخصائص؟**

عرضنا في الفصل التمهيدي للبحث قدرات تقنيات الذكاء الاصطناعي، وكان من أهمها القدرة على التخزين اللامحدود للمعلومات والبيانات، أو ما يعرف بـ (Big Data)، وقدرتها على استرجاعها بسرعة تفوق قدرة البشر، ومن ثم تتميز هذه

التقنيات بالكم الهائل من المعلومات والبيانات الذي يفوق بكثير ما يستوعبه العقل البشري، كما تتميز بالقدرة على الاسترجاع بسرعة تفوق قدرة العقل البشري، ليس ذلك فحسب، بل يمكنها معالجة هذه المعلومات والبيانات وتحليلها على نطاق واسع، بشكل وسرعة تفوق بكثير قدرة العقل البشري.

كما عرضنا لقدرة تلك الروبوتات على استخدام التعلم الذاتي وشبكات التعلم العميق Deep Learning، ما يمنحها القدرة على الاستنتاج وحل المشكلات المعقدة واتخاذ القرارات بشكل ذاتي، واتخاذ رد الفعل على أوضاع لم تبرمج عليها.

ولكن هل تمتلك الروبوتات فائقة الذكاء بعض السمات والخصائص النفسية الوجدانية التي يمتلكها المحقق البشري؟

لا يجادل أحد في امتلاك هذه الروبوتات للقدرات العقلية، سالفة الذكر، في ذات الوقت، لا يجزم أحد في امتلاكها –حتى وقتنا– السمات النفسية الوجدانية التي عرضنا لها في الفرع السابق، خاصة سمة الفِراسة والفِطنة، وقوة الوجدان، والسيطرة والاستحواذ على مجريات الكلام في التحقيق؛ فهذه السمات والخصائص تعتمد بشكل أساسي على مقومات نفسية وجدانية بشرية يفتقدها الروبوت.

ما تقدم يدفعنا إلى طرح التساؤل الآتي: **إلى أي مدى يمكن توظيف قدرات الروبوتات فائقة الذكاء في القيام بإجراءات التحقيق الجنائي؟**

من الثابت أن إجراءات التحقيق الجنائي الابتدائي تتنوع بالنظر إلى القدرات التي تتطلبها إلى: إجراءات تعتمد على قدرات عقلية وذهنية، مثل: الاستجواب وسماع

الشهود. واجراءات روتينية، مثل: إصدار أوامر التحقيق، كالأمر بالقبض والحبس الاحتياطي، والإذن بالتفتيش أو مراقبة المراسلات والمكالمات.

ومن ثم يمكن توظيف قدرات الروبوتات فائقة الذكاء في الاستعانة بها في القيام بإجراءات الاستجواب وسماع الشهود، من ذلك: الاستعانة بقدرات هذه الروبوتات في معالجة المعلومات والبيانات واسترجاعها والاستفادة من قدرتها على التخزين اللامحدود للنصوص القانونية والأحكام القضائية، والسجلات والوثائق، وعليه؛ يمكن للمحقق البشري أن يستعين بهذه القدرات العقلية الفائقة للروبوتات في الوقوف على مدى صدق المتهم في أقواله من خلال استرجاع سجله الاجرامي وسوابقه الجنائية، كذلك الحال بالنسبة للشاهد، يمكن التحقق من صدقه أو كذبه، من خلال استرجاع المعلومات والبيانات المتعلقة بماضيه، وما يتعلق بسجله الاجرامي، خاصة إذا سبق عليه الحكم في جرائم شهادة زور، هذه المعلومات قد لا تتوفر للمحقق البشري أثناء الاستجواب أو سماع أقوال الشاهد.

كما يمكن توظيف القدرات التي يمتلكها الروبوت فائق الذكاء والتقنيات والبرامج المزود بها مثل: تقنية الترجمة الفورية بلغات متعددة، والتي تساعد المحقق البشري في مواصلة التحقيق مع المتهم أو الشهود من مختلف الجنسيات غير العربية، دون الاستعانة بمترجم بشري. كما يمكن الاستعانة بتقنية التعرف على الوجوه المزود بالروبوت الذكي التي تُمكن المحقق البشري من التعرف على الأشخاص المشتبه فيهم من خلال صورهم التي يتم عرضها على الروبوت ومن خلال التقنية يتمكن الروبوت من استرجاع المعلومات والبيانات الخاصة بهؤلاء وتحليلها في وقت قياسي.

هذا بالنسبة للإجراءات التي تتطلب قدرات عقلية أو ذهنية معينة، بيد أن الأمر يبدو أكثر وضوحاً عند استخدام تقنيات الروبوتات فائقة الذكاء في إصدار أوامر التحقيق الابتدائي، خاصة أوامر بالقبض، والتفتيش، ومراقبة المراسلات والمكالمات وتبليغها إلى مأموري الضبط القضائي المكلف بتنفيذها. فليس خفياً على أحد أن الكثير من القضايا يحكم فيها ببراءة المتهمين بسبب بطلان في إجراءات القبض والتفتيش ومراقبة المراسلات والمكالمات، يرجع البطلان في تأخر صدور الإذن أو الأمر بمباشرة هذه الاجراءات، ومن تكون الاستعانة بتقنيات الذكاء الاصطناعي الحل الناجع لضمان صحة وسلامة القيام بتلك الإجراءات.

يثور التساؤل بخصوص الأمر بالحبس الاحتياطي **هل للذكاء الاصطناعي دورا خاصا في إصداره؟** من الثابت أن الأمر بالحبس الاحتياطي من الإجراءات ذات الخصوصية في التحقيق الابتدائي، بالنظر إلى أهميته، وجسامته في سلب الحرية للمتهمين، واحتجارهم مدة ليست بالقليلة، لذلك استقر الفقه والقضاء على ضروة توافر مبررات تجيز الأمر به، من سلطة التحقيق أو المحكمة، من هذه المبررات، الحيلولة دون هروب المتهم أو منعه من التدخل في الأدلة بإفسادها أو إخفائها أو التلاعب والعبث بها، ولاشك يرجع هذا إلى تقدير المحقق أو المحكمة بالنظر إلى ظروف المتهم ومدى خطورته الإجرامية، ومدى امكانياته في التدخل في الأدلة والتلاعب بها، **فما صورة الاستعانة بقدرات الذكاء الاصطناعي في سلامة ومعقولية ومشروعية الأمر بالحبس الاحتياطي؟**

ذكرنا من قبل أن تقنية التحليلات التنبؤية من أهم تقنيات الذكاء الاصطناعي التي يمكن استخدامها في العمل الشرطي والقضائي، سواء في صورة التنبؤ بالجرائم، بغرض الحد منها ومكافحتها، أو في صورة التنبؤ باحتمالية عودة المتهم إلى الاجرام عند إصدر قرار بالإفراج المشروط من قبل المحكمة، وأخيراً في صورة التنبؤ بمدى خطورة المتهم ومحاولته التدخل بالأدلة والعبث بها، أو محاولة الهروب، وعدم المثول أمام المحكمة عند الإفراج عنه من قبل النيابة العامة في مرحلة التحقيق الابتدائي، أو من قبل المحكمة في مرحلة المحاكمة.

مما تقدم، نؤكد على إمكانية الاستعانة بتقنية التحليلات التنبؤية المزودة بها الروبوتات فائقة الذكاء في التنبؤ عند إصدار الأمر بالإفراج المؤقت عن المتهم وإخلاء سبيله من قبل النيابة بمدى خطورة المتهم واحتمالية هروبه أو احتمالية تدخله في الأدلة القائمة ضده، أو العبث بها، ومن قبل تصدر النيابة العامة أمرا بحبسه احتياطياً، إذا كانت نتيجة التنبؤ ايجابية، بينما تصدر أمراً بإخلاء سبيله، إذا كانت نتيجة التنبؤ سلبية.

كما يمكن الاستعانة بها عند النظر في تجديد الأمر بالحبس الاحتياطي؛ حيث تصدر النيابة العامة أمرا بتجديد حبس المتهم احتياطياً إذا كان هناك تنبؤ قوي باحتمالية هروبه أو تدخله في الأدلة والعبث بها، أو تصدر أمراً بعدم التجديد والإفراج المؤقت عنه إذا لم يكن هناك تنبؤ باحتمالية ذلك.

خلاصة ما تقدم، إنه يصعب القول بقيام الروبوتات فائقة الذكاء مستقلاً بالنظر إلى السمات والخصائص النفسية التي يتطلبها التحقيق الجنائي، لاسيما قوة الوجدان،

والاتزان العاطفي، بينما يمكن توظيف قدراتها والاستعانة بها في مساعدة المحقق الجنائي، بالنظر إلى قدراتها العقلية الهائلة التي قد تفوق قدرات العقل البشري، خاصة قدرتها على استيعاب كم هائل من المعلومات والبيانات واسترجاعها في ثوان معدودة، بالإضافة إلى قدرتها على معالجة وتحليل هذه المعلومات والبيانات بسرعة تفوق قدرة المحقق البشري، كذلك قدرتها على الترجمة الفورية بلغات متعددة.

المطلب الثاني

استخدام تقنية التحليلات التنبؤية في تحقيق العدالة الجنائية.

يشير مصطلح تقنية التحليلات التنبؤية إلى استخدام الإحصائيات وتقنيات الذكاء الاصطناعي في استنتاج تنبؤات حول النتائج والأداء المستقبلي للمدانين؛ حيث تغوص هذه التحليلات في حجم البيانات الضخمة الماضية والحالية للتنبؤ بمدى احتمالية تكرار الوقائع الإجرامية منهم مرة أخرى، يتيح ذلك للقضاة توظيف المعلومات والإحصاءات في قراراتهم للاستفادة من الأحداث المستقبلية المحتملة من الأشخاص. وقد أسفر استخدام خوارزميات الذكاء الاصطناعي التنبؤية إلى ظهور مصطلح (العدالة التنبؤية)، الذي يعتمد على توظيف البيانات الضخمة (Big Data) في مجال العدالة من خلال استناد قرارات الإفراج المشروط أو الإفراج المبكر وغيرها على نتائج التحليل التنبؤي للسلوك الإجرامي المستقبلي([1]).

[1]) د. أحمد عبد الواحد العجماني، استخدام تقنيات الذكاء الاصطناعي في الإجراءات الجزائية، دراسة مقارنة، رسالة دكتوراة، جامعة الشارقة، ٢٠٢٣، ص١٣٣-١٣٤.

الفرع الأول

مفهوم العدالة الجنائية التنبؤية

بالنظر إلى أن العدالة لا تخرج عن كونها استخدام مجموعة من المهارات والخبرات القانونية في تحليل وفهم النصوص القانونية والظروف المحيطة بالواقعة وفق مفهوم التحليلات القانونية Legal analytics في إطار تنبؤات قانونية، تشعر القاضي بعدالة ما ينطق به في الحكم. وإن حالة التأثير الملحوظ لتقنيات الذكاء الإصطناعي على العلوم الإنسانية لاسيما القانون، أنتج عدالة إفتراضية استشرافية، تعارف عليها فقهاً بمصطلح "العدالة التنبؤية" Predictive Justice، والتي تمثلت في القدرة على مساعدة القضاء في الوصول إلى عدالة أكثر موثوقية، قائمة على الترابط بين القانون وعلم الرياضيات، ما أثبت أن العدالة لا تقوم على الجانب الإنساني فقط، بل لها جانب رياضي إحصائي([1]).

وقد عبر الفقه عن فكرة العدالة التنبؤية –بإيجاز– بأنها "تثبيت المستقبل برؤية الماضي وفق مفهوم الحاضر" ومن ثم يصبح الحاضر هو المستقبل المكرر للماضي، وسنصبح في حاضر لا ينتهي يمزج بين طياته الماضي والحاضر والمستقبل، وإن

[1]) انظر: د. محمد عرفان الخطيب، العدالة التنبئية والعدالة القضائية الفرص والتحديات، دراسة نقدية معمة في الموقف الانكلوسكسوني واللاتيني، مجلة الحقوق والعلوم الإنسانية، المجلد ١٢، العدد الأول، مايو ٢٠١٩م، ص١٣.

المعادلة الإحصائية سوف تجعل الفارق بين الماضي والمستقبل شبه منعدم، إذ أنها تخبر بصيغة الحاضر ما كان عليه الماضي، وما سيكون عليه المستقبل([1]).

بالرغم من المخاوف الفقهية من شيوع رقمنة العدالة([2]) إلا أن مصطلح "العدالة التنبؤية" أضحى أمراً واقعياً فرض نفسه بقوة في الأوساط الفقهية والقضائية، ويشير هذا المصطلح إلى استخدام تقنيات الذكاء الاصطناعي القائمة على الخورازميات الرياضية، التي ترمي إلى تحليل مجموعة كبيرة من الأحكام والقرارات القضائية من أجل تقييم فرص الفوز في المحاكمة، وتقدير أنواع معينة من الدعاوى القضائية المتخصصة بمبلغ التعويض([3]). بينما تُعرف خوارزميات([4]) التَّحليلات التنبؤية، بأنها "تقنية تعتمد على تحليل البيانات وتستنتج نماذج مختلفة تمثل بشكل فني للفئات والتصنيفات للبيانات المهمة، وتعتمد هذه التَّقنيات على بيانات سابقة يتم استخدامها

[1]) المرجع السابق، ص١٩.

[2]) سوف نعرض لهذه المخاوف في الفرع الثاني من هذا المطلب.

[3]) سينتيا الفليطي، العدالة التنبؤية، الموسوعة السياسية، منشور بتاريخ ١٢ أبريل ٢٠٢٠م، على الرابط الالكتروني:

https://political-encyclopedia.org/dictionary/

[4]) تعرف (الخوارزمية) بأنها "عملية أو مجموعة من العمليات التي يجب اتباعها في حل المشكلات فهي عملية منظمة تتابع في خطوات منطقية". كما تعرف بأنها: "مجموعة من الحلول المتسلسلة المنطقية والرياضية المطلوبة لإيجاد حل لمشكلة معينة".

See: Delacroix.S.(2018).Computer systems fit for the legal profession? Legal Ethics, doi:10.1080/1460728x.2018.1551702, www.lawsociety.org.uk.

للقيام بالتنبؤ"([1]). وهناك من عرفها بأنها: "برمجية حسابية قادرة على البحث في مختلف القرارات القضائية السابقة؛ وذلك لاستخراج ملف من الملفات القضائية أو نص من نصوص القواعد الإجرائية.. ألخ" ([2]).

[1]) Amankwaa, A. & Mccartney, C. (2018). The effectiveness of the current use of forensic DNA in criminal investigations in England and Wales. Wiley Interdisciplinary Reviews: Forensic Science, 3(10).

[2]) فؤاد بنصغير، العدالة الخوارزمية في القانون المغربي، مجلة مغرب القانون، 5(12)، (2018)، 1-34.

الفرع الثاني

المخاوف الفقهية من استخدام خوارزميات العدالة الجنائية التنبؤية

أشار بعض الفقه([1]) إلى أن الاعتماد على خوارزميات العدالة التنبؤية تثير العديد من المخاوف منها: مدى دقة البيانات التي يتم بناء على تحليلها بواسطة هذه الخوارزميات وعدم تحيزها أو اتسامها بالعنصرية، بالنظر إلى أن مدخلي البيانات والمعلومات هم بشر، لهم أفكارهم وميولهم وانتماءاتهم، التي قد تكون معلنة أو غير معلنة، من ذلك: ما يتعلق بالاعتبارات الدينية والعرقية والمنشأ الجغرافي، وكذلك التوجهات الاجتماعية والتطرفات الفكرية؛ هذا ما قد يترتب عليه من أخطاء متوقعة في الأحكام والقرارات القضائية، فضلاً عن الأثر المترتب عليها في تكوين عقيدة القاضي.

كما أشار البعض([2]) إلى أن معارضي العدالة التنبؤية لديهم مخاوف من رقمنة العدالة، بحيث يصبح العمل القضائي ظاهرة رقمية أكثر منه ظاهرة إنسانية فكرية، مما يؤثر سلباً على منظومة العمل القضائي، وتجرده من جوهره. واستطرد هذا الفقه مشيراً إلى أن العدالة التنبؤية هي خلاصة مجموعة من المعطيات التي انتهت إليها المعالجة الرقمية من خلال تحليل مجموعات كبيرة من البيانات والمعلومات القانونية بواسطة خوارزميات الذكاء الاصطناعي، من خلال قراءة وتحليل آلاف الوثائق بشكل

---

[1]) د. محمود سلامة عبد المنعم الشريف، الطبيعة القانونية للتنبؤ بالجريمة بواسطة الذكاء الاصطناعي ومشروعيته، مرجع سابق، ص٣٤٦.

[2]) انظر: د. محمد عرفان الخطيب، مرجع سابق، ص١٩–٢٠.

دقيق، تلك القراءة وذلك التحليل الذي سوف يبني عليه القاضي اقتناعه في الحكم، على الرغم أنه لم يقم بنفسه بقراءة وتحليل هذه الوثائق، مع استحالة أو صعوبة ذلك بالجهد البشري؛ ومن ثم يكمن مصدر القلق والتخوف من رقمنة العدالة أن القاضي بنى عقيدته أو حكمه على ما لم يقرأه بنفسه.

ومن المخاوف التي انتابت بعض الفقهاء ما يتعلق بنمطية العدالة الرقمية بالاعتماد المفرط على الخوارزميات، حيث إنها تحكم على الشخص التقيد بالماضي، وعدم إتاحة الفرصة له في تغيير حياته، ومنحه فرصة ثانية، ما يجعل نتائجها غير منصفة، بالنسبة لبعض المجرمين، الذين قرروا تغيير مسار حياتهم والتخلي عن إجرامهم، وعزموا على عدم العودة إلى الجريمة، بينما نجد الخوارزميات تعطي نتائجها بتحليل البيانات والمعلومات عن ماضيه وسوابقه الإجرامية، ومدى احتمالية عودته إلى الجريمة في ضوء ذلك.

كما أشار البعض([1]) إلى أن الاعتماد على الخوارزميات لا يجعل القضاة هم المتحكمون في العدالة، بل مبرمجي هذه الخوارزميات، ومدخلي البيانات والمعلومات بها، على اختلاف ميولهم وانتماءاتهم وعقائدهم الفكرية، ما يجعل نتائجها –كما أوضحنا سابقاً– متحيزة وغير منصفة، وبالتالي يكون حكم القاضي متأثرا بذلك، مشوباً بالتحيز وعدم الانصاف. كما أن هذه العدالة التنبؤية القائمة على الرقمية تقضي على قدرة الابتكار والإبداع للتفكير لدى القاضي، ويجد الأخير نفسه واقعاً تحت تأثير نتائج تمليها عليه خوارزميات ياضية ومعادلات لوغارتمية، مما يعيق

[1]) المرجع السابق، ص٢١-٢٢.

تطور القانون، ويحد من إبداع القضاء، بحيث يصبح عمل حسابي قائم على الرقمنة، ذو نهج تقليدي وليس إبداعي.

بينما دافع البعض([1]) عن تقنيات العدالة التنبؤية، معلقاً على المخاوف السابقة بأنها مبالغ فيها، مؤكداً أن الجيل القادم من رجال المؤسسة القضائية قادرين على التكيف مع هذه التقنيات، وأن الحلول التي تقدمها تلك التقنيات لن تحرم القاضي من سلطته التقديرية في الأخذ بها، مرجحاً بين تلك الحلول وإبداعه وتفكيره في الموضوع وفق قناعته الشخصية. كما أن هذه العدالة لن تقضي على الاجتهاد القضائي. بل إن تلك العدالة سوف تحسن كفاءة القضاء؛ إذ أنها تعطي مؤشرات ترجيحية تاركة لرجال القانون ومنهم القضاة القدرة على تحليل هذه المؤشرات من خلال خبرتهم المهنية وقدرتهم على فهم النصوص وتحليلها؛ ما يجعل من هذه المؤشرات مجرد عناصر مساعدة للقاضي على الفهم الصحيح والأفضل لموضوع الدعوى.

واستطرد هذا الفقه([2]) مؤكدا – من وجهة نظره– أن تقنيات العدالة التنبؤية لن تحكم، وإنما تقدم مؤشرات تساعد على استشراف الحل، معتبراً تلك التقنيات مجرد خبير رقمي يساعد القاضي على تكوين رأيه في موضوع النزاع، من خلال تحليل مئات الآلاف من الأحكام القضائية؛ مما يدعم الاجتهاد القضائي ويزيد فاعليته، ويضيف قيمة قانونية لقراراته.

---

[1]) المرجع السابق، ص٢٢.

[2]) المرجع السابق، ص٢٣–٢٧.

وقد اختتم هذا الفقه تحليله للمخاوف التي أثارتها العدالة التنبؤية بالتوصية بضرورة اعتبار هذه المخاوف تحديات وليست معوقات، ولا يمكن جعلها مثبطة عن المضي قدما في هذا النهج القضائي الرقمي الجديد، مع السعي نحو الاستفادة من قدرات هذه التقنيات، والعمل على التكيف معها، وتحويلها من تحدٍ إلى فرص للارتقاء بالمنظومة القضائية في مجتمعاتنا العربية([1]).

كما أشار البعض([2]) إلى مخاوف تتعلق بحق المتهم في محاكمة عادلة، وما يرتبط به من الحق في المشاركة الفعالة في إجراءات المحاكمة، ومن أهمها: حق الدفاع في مناقشة الشهود، والحق في تفنيد الأدلة القائمة ضده في جلسة استماع علينة، والحق في مباشرة كافة إجراءات المحاكمة في حضور المتهم. بيد أن الاعتماد على خوارزميات الذكاء الاصطناعي تعد قيدا على حقوق المتهم المرتبطة بحقه في المحاكمة العادلة، وطالب هذا الفقه بضرورة تحقيق توازن عادل بين الحق في مناقشة الشهود والمشاركة في إجراءات المحاكمة وتفنيد الأدلة من جهة، وبين استخدام هذه الخوارزميات في العدالة من جهة أخرى.

---

[1]) د. محمد عرفان الخطيب، مرجع سابق، ص٣٠-٣٢.

[2]) د. عمر عبد المجيد مصبح، توظيف خوارزميات "العدالة التنبؤية" في نظام العدالة الجنائية: الآفاق والتحديات، المجلة الدولية للقانون، كلية القانون، دار نشر جامعة قطر، المجلد١٠، العدد المنتظم الأول، ٢٠٢١م، ص٢٥٨-٢٥٩.

الفرع الثالث

تقييم فاعلية استخدام الخوارزميات التنبؤية

حول تقييم مدى فاعلية استخدام هذه الخوارزميات في مجال التنبؤ بالجريمة، أشار بعض الفقه([1]) إلى أن مخاطر التنبؤ الخوارزمي باحتمالية ارتكاب الجريمة يختلف مقدارها باختلاف المرحلة من مراحل الإجراءات الجزائية التي يتم اللجوء إليه فيها، فإذا وقع خطأ في التنبؤ الخوارزمي في مرحلة جمع الاستدلالات والتحري، فإنها مجرد أعمال استدلال تتخذ في مواجهة الشخص، فإذا تبين عدم توافر الخطورة لديه تم اطلاق سراحه؛ وعليه إذا تبين وجود خطأ في التنبؤ الخوارزمي يمكن تدارك الأمر.

بينما يزداد الأمر صعوبة عند استخدام تلك الخوارزميات من القاضي في مرحلة المحاكمة، فإذا جاء نتائج التنبؤ على غير الحقيقة، بأن المتهم الماثل أمامه تتوافر لديه خطورة إجرامية، ومن المحتمل عودته إلى الجريمة مرة أخرى، ومن ثم يتم الحكم عليه بناء على هذه المعطيات، مما يحرم المتهم من إمكانية الاستفادة من أحكام التخفيف أو تطبيق الافراج المشروط أو الحكم مع وقف التنفيذ.

كما أن استخدام هذه التقنيات لاشك يؤثر على تكوين عقيدة القاضي عند الحكم، والتدليل على ذلك تؤكده الشواهد العملية التي أسفر عنها استخدام تقنية (كومباس) COMPAS في تقييم احتمالية العودة إلى الإجرام في المستقبل، التي تعتمد على

[1]) د. محمود سلامة عبد المنعم الشريف، مرجع سابق، ص٣٤٦.

تحليل البيانات الشخصية، والسوابق الإجرامية، كما تعتمد على إجابات المتهم على عدد من الأسئلة، بناء على هذا التحليل وتلك الإجابات تحدد درجة خطورة المتهم([1]).

وقد شكك البعض([2]) في عدالة خوارزميات الذكاء الاصطناعي المستخدمة في مرحلة المحاكمة، مستشهدا في التدليل على ذلك بنتائج تقنية COMPAS التي تعتبر ملكية خاصة، لا يحق للمتهم الطعن في صحة نتائجها، فقد رفضت المحكمة العليا الأمريكية الطعن المقدم من المتهم Loomis ضد نتائج هذه التقنية التي حددت درجة خطورته بالشديدة، وبناء عليها أصدرت محكمة ولاية Wiscons عام ٢٠١٦ على المتهم بالسجن ٦ سنوات، وقد طعن المتهم على الحكم مستنداً إلى أن استخدام التقنية ينتهك حقه في الدفاع لسببين، الأول: اعتماد التقنية على بيانات غير دقيقة. والثاني: عدم إلمام القاضي بمنهجية التقنية في تحليل البيانات، كما أن اعتماد القاضي على هذه البيانات مشوب بعدم الدستورية؛ لأنها بيانات تتسم بالعنصرية. برغم هذه الأسباب رفضت محكمة الاستئناف الطعن، كما رفضت – أيضاً– المحكمة العليا الأمريكية الطعن عام ٢٠١٧م، مؤكدة أن استخدام التقنية لا يمثل أي انتهاك لحقوق الدفاع.

[1]) Fass, T. L., Heilbrun, K., DeMatteo, D., & Fretz, R. (2008). The LSI-R and the COMPAS: Validation data on two risk-needs tools. Criminal Justice and Behavior, 35(9), 1095-1108.

[2]) انظر: د. محمود سلامة عبد المنعم الشريف، مرجع سابق، ص٣٤٦-٣٤٧. د. عمر عبد المجيد مصبح، مرجع سابق، ص٢٥٩.

كما قررت المحكمة أنه لا يجوز الإفصاح عن منهجية عمل التقنية في تحليل البيانات وإفشاء سريتها، بالنظر إلى أنها تجارية، ذات ملكية خاصة([1]).

كما أشار البعض إلى أن من المخاطر التي تصاحب استخدام خوارزميات العدالة التنبؤية في مرحلة المحاكمة ما يتعلق بنقص المعرفة والخبرة من قبل القضاة والمؤسسات القضائية في التعامل مع هذه الخوارزميات، وفهم خصائصها، واستيعاب درجة مصداقيتها موضوعيتها([2]).

ولما كان من المستقر عليه في العمل القضائي أن القاضي يعتمد على حدسه ووجدانه عند إصدار الأحكام الجزائية، مع فهمه الشخصي للنص الجنائي، وتقديره الوجداني للأدلة القائمة ضد المتهم، وقناعته الشخصية بمدى كفايتها للإدانة أو البراءة، كل هذا قد يؤدي إلى وجود تناقضاً في الأحكام الجزائية بشأن وقائع مشابهة، وقد أشار البعض إلى أن الاعتماد على تقنيات الذكاء الاصطناعي في القيام بدور القاضي لاسيما عند تحليل البيانات، وتصنيف القضايا، ومراجعة كافة التشريعات والقوانين المتعلقة بموضوع الدعوى، والأحكام القضائية الصادرة من مختلف المحاكم في وقائع مشابهة، مما يساعد على التنبؤ واتخاذ القرار بموضوعية، ودون تحيز، وبسرعة فائقة وبدقة تصل إلى ٧٩%([3]).

---

[1]) Criminal Law, Sentencing Guidelines, Wisconsin Supreme Court Requires Warning Before Use of Algorithmic Risk Assessments in Sentencing. (2017, March 10). State v. Loomis, 881 N.W.2d 749 (Wis. 2016). Harvard Law Review, Vol. 130, pp. 1530-1537.

[2]) انظر: د. عمر مصبح، المرجع السابق، ص٢٥٦.

[3]) المرجع السابق، ص٢٦٠، ٢٦١.

ولكن برغم ما ذكره الرأي السابق، من سرعة ودقة الخوارزميات التنبؤية في تحليل البيانات والتعامل مع القوانين والأحكام ذات الصلة بالدعوى المنظورة، إلا أن العمل القضائي من المجالات التي تعتمد بشكل أساسي على الوجدان البشري، لا على العقل والمنطق فقط، فهل تملك هذه الخوارزميات هذا الوجدان؟ وهل يمكن الاضمئنان إلى الأحكام التي تصدر بناء على العقل والمنطق ولو كان صادرا عن ذكاء اصطناعي؟

نعتقد أن هذه هي الإشكالية والتحدي الأكبر الذي يواجه استخدام هذه الخوارزميات في المحاكمة وإصدار الأحكام الجزائية، هذا بالإضافة إلى تحدي قانوني، يتمثل في الفراغ التشريعي في قوانين الاجراءات الجزائية في المنطقة العربية، باستثناء ما قامت به دولة الامارات العربية المتحدة من الاعتماد بشكل كبير على تقنيات الذكاء الاصطناعي والأنظمة الرقمية في العمل الشرطي والقضائي، من ذلك استخدامها في التنبؤ بالجريمة، والقيام ببعض أعمال الاستدلال، من قبل مأموري الضبط القضائي، وفي أعمال التحقيق الابتدائي بمعرفة النيابة العامة. في حين كان المشرع المصري أبعد من الاستفادة من تلك التقنيات والأنظمة، لاسيما في العمل القضائي. ومن ثم نوصي بضرورة وضع التنظيم التشريعي الاجرائي لاستخدام تقنيات الذكاء الاصطناعي في العمل الشرطي لأغراض التأمين، أو منع الجرائم والتنبؤ بارتكابها، أو لأغراض الضبط القضائي، من قبل رجال الشرطة وغيرهم الممنوحين صفة الضبطية القضائية، أو في القضائي، من أعضاء النيابة العامة، أو القضاة.

الخاتمة

تناول البحث موضوع ذات أهمية نظرية وعملية ملموسة، وقسمناه إلى مبحث تمهيدي تناولنا فيه مفهوم الذكاء الاصطناعي والتقنيات المستخدمة في العمل الشرطي والقضائي، عرضنا في المطلب الأول منه التعريفات التي قيل بها، وأنواعه، بالنظر إلى قدرة الذكاء الاصطناعي على التعلم واتخاذ قرارات مستقلة عن البشر، وتناولنا في المطلب الثاني تقنيات الطائرات المسيرة، والسيارات ذاتية القيادة، والروبوتات فائقة الذكاء، كنماذج للتقنيات المستخدمة في العمل الشرطي والقاضي.

كما تناولنا في الفصل الأول من البحث، الاختراق الإلكتروني كأحد أكثر التحديات التي تواجه استخدام التقنيات السابقة، وجاء الفصل بعنوان: مخاطر الاختراق الإلكتروني لتقنيات الذكاء الاصطناعي وصور مواجهته. وقسمنا هذا الفصل إلى ثلاثة مباحث، تناولنا في المبحث الأول: التعريف بالاختراق الإلكتروني وكيفية التصدي تقنياً وتشريعياً. وعرضنا فيه تعريف الإختراق الإلكتروني وأنواعه في المطلب الأول، وتناولنا مراحل الإختراق الإلكتروني وسبل المكافحة التقنية في المطلب الثاني، وفي المطلب الثالث عرضنا لصور المواجهة التشريعية للاختراق الإلكتروني، في القانونين المصري والاماراتي.

ثم عرضنا في المبحث الثاني: مخاطر الاختراق الإلكتروني على الأمن المعلوماتي، وقسمناه إلى ثلاثة مطالب، عرضنا في المطلب الأول منها: تعريف الأمن المعلوماتي وعناصره، ثم التمييز بين مفهوم الأمن المعلوماتي وغيره من المصطلحات المشابهة

في المطلب الثاني، ثم في المطلب الثالث عرضنا مخاطر اختراق تقنيات الذكاء الاصطناعي على الأمن القومي وعلاقتها بالحروب الإلكترونية. وفي المبحث الثالث تناولنا: تحليل التهديدات السيبرانية لأنظمة الذكاء الاصطناعي وصور الاختراقات الواقعة عليها، وقسمناه إلى ثلاثة مطالب، عرضنا في المطلب الأول: تحليل التهديدات السيبرانية والأثار الأمنية لاختراق أنظمة الطائرات المسيرة. وفي المطلب الثاني: تحليل التهديدات السيبرانية والأثار الأمنية لإختراق أنظمة المركبات ذاتية القيادة. وفي المطلب الثالث: صور الاختراق الإلكتروني لأنظمة الطائرات المسيرة ذاتياً والمركبات ذاتية القيادة.

ثم في الفصل الثاني تعرضنا بشيء من التحليل والتعقيب لإشكالية مهمة تتعلق باستخدام تقنيات الذكاء الاصطناعي في العمل الشرطي والقضائي، وتتعلق هذه الإشكالية في مدى مشروعية هذا الاستخدام، وجاء الفصل بعنوان: مشروعية استخدام تطبيقات الذكاء الاصطناعي في العمل الشرطي والقضائي. وقسمناه إلى مبحثين، تناولنا في المبحث الأول: مدى مشروعية استخدام تقنيات الذكاء الاصطناعي من مأموري الضبط القضائي. وعرضنا فيه مطلبين، تناولنا في المطلب الأول: مدى مشروعية استخدام تقنية تمييز بصمة الوجه والصوت. وفي المطلب الثاني: مدى مشروعية استخدام الروبوتات فائقة الذكاء في العمل الشرطي. وأخيراً تناولنا في المبحث الثاني والأخير من البحث: مدى مشروعية استخدام تقنيات الذكاء الاصطناعي في التحقيق الإبتدائي والمحاكمة. وقسمناه إلى مطلبين، تناولنا في

المطلب الأول: استخدام الروبوتات فائقة الذكاء في التحقيق الإبتدائي. وفي المطلب الثاني: استخدام تقنية التحليلات التنبؤية في تحقيق العدالة الجنائية.

وانتهى الباحث من دراسته وتوصل إلى العديد من النتائج، ومنها انتهى الباحث إلى بعض التوصيات، مع الرجاء من الله –تعالى– بأن تلقى هذه التوصيات القبول وترى شمس التطبيق العملي.

أولا– نتائج الدراسة:

١– إن الذكاء الاصطناعي يتمحور في عملية محاكاة الذكاء البشري باستخدام خوارزميات تمنحه قدرات تقارب قدرات الذكاء البشري أو تفوقه، وذلك بحسب قدرتها على التحليل والتفكير، والتعلم العميق، والتصرف الذاتي.

٢– إن تقنية التحليلات التنبؤية تساعد محللي العمليات الأمنية والشرطية على مواجهة التهديدات والهجمات السيبرانية، كما تمكن المحللين من الاستجابة السريعة لهذه التهديدات.

٣– شاع استخدام تقنية الطائرة بدون طيار– خاصة المسيرة ذاتياً– في القيام بأعمال المراقبة الجوية للتجمعات البشرية، والكشف عن البضائع المهربة، وتأمين الحدود، والمسح الكيميائي والبيولوجي والإشعاعي والنووي والكشف عن المتفجرات؛ بيد أن ضعف أنظمتها على صد الهجوم السيبراني يجعلها عرضة للاختراق.

٤– إن إنظمة السيارات ذاتية القيادة تحتاج إلى التحسينات التي تضمن تغلبها على الثغرات الأمنية التي قد تعرضها للهجوم السيبراني.

٥- يعد استخدام الروبوتات فائقة الذكاء تطوراً متقدماً في العمل الشرطي، يمكن الاعتماد عليها في المهام التي تتضمن خطرا على سلامة الشرطيين البشريين، مثل تفكيك العبوات الناسفة، وتأمين الطرق، وفي الأعمال الشرطية المتكررة التي تتطلب دقة عالية وسرعة فائقة أو تلك الأعمال التي قد تصيب الشرطي البشري بالملل والفتور.

٦- برغم ايجابيات استخدام تقنيات الذكاء الاصطناعي خاصة في مجال العمل الشرطي، إلا إنها لا تخلو من السلبيات مثل: قابليتها للاختراق، وتعرضها للتهديدات والهجمات السيبرانية، وتعارضها مع الحق في الخصوصية والحق في الصورة.

٧- إن استخدام خوارزميات الذكاء الاصطناعي في تقييم احتمالية ارتكاب جريمة في المستقبل في مجال العمل القضائي، وفي أعمال الشرطة التنبؤية؛ قد يؤدي إلى نتائج متحيزة وغير منصفة.

٨- إن عقوبة الغرامة المقررة لجريمة الدخول غير المشروع لموقع إلكتروني أو حساب خاص أو نظام معلوماتي في قانون مكافحة جرائم تقنية المعلومات المصري غير متناسبة مع جسامة الفعل، خاصة إذا نتج عنه اتلاف أو محو أو تغيير أو نسخ أو إعادة نشر البيانات والمعلومات المخزنة في تقنيات الذكاء الاصطناعي؛ لما قد يترتب عليه من خطورة أو ضرر لحق ذوي الشأن في الخصوصية وسرية البيانات والمعلومات المتعلقة بهم.

٩- لا ينطبق وصف جريمة الهجوم على طائرة أو سفينة في الفقرة الأولى من المادة (٣٣٨) من قانون الجرائم والعقوبات الاماراتي على فعل الاختطاف الإلكتروني للطائرة المسيرة؛ لإنها لا تعد من قبيل وسائل المواصلات أو النقل العام. كما لا ينطبق وصف جريمة تعريض سفنية أو طائرة أو وسيلة من وسائل النقل العام في المادة (٣٣٩) من القانون السابق، والمادة (١٦٧) من قانون العقوبات المصري.

١٠- ينطبق وصف جريمة السرقة على فعل الاستيلاء على المسيرة باختراق أنظمة تشغيلها، باعتبارها مالا مملوكا للغير، بإلإضافة إلى جريمة الدخول غير المشروع لنظام معلوماتي أو شبكة معلوماتية أو وسيلة تقنية معلومات المنصوص عليها في المادة (٢) من المرسوم بقانون مكافحة جرائم تقنية المعلومات الاتحادي.

١١- إنطباق وصف جريمتي الاعتداء على وسائل المواصلات والنقل المنصوص عليهما في المادتين (٣٣٨)، (٣٣٩) من قانون الجرائم والعقوبات الاماراتي على فعل الاختطاف الإلكتروني للسيارة ذاتية القيادة باعتبارها من وسائل النقل، بالإضافة إلى إنطباق جريمتي السرقة، والدخول غير المشروع لنظام معلوماتي، كذلك إنطباق وصف جريمة اختطاف وسيلة من وسائل النقل لغرض إرهابي، المنصوص عليها في المادة (٥) من قانون مكافحة الجرائم الإرهابية.

١٢- يعد مشروعا استخدام تقنية التعرف على الوجه في الأماكن التي تشترط تحديد الهوية لدخولها استنادا إلى الرضا الصريح أو الضمني. كذلك استخدامها حال استيقاف الأشخاص محل الريبة والشك من قبل رجل الشرطة.

١٣- يعد مشروعاً استخدام الروبوتات فائقة الذكاء في أعمال الاستدلال والتحري عن الجرائم، والتنبؤ بالجريمة، وتحليل البيانات، وفي القيام ببعض إجراءات التحقيق متى كان ذلك بإشراف مباشر لرجل الشرطة أو سلطة التحقيق. بينما يختلف الأمر في فرض استخدام الروبوت مستقلاً عن التدخل البشري.

١٤- يصعب – في الوقت الحالي- القول بقيام الروبوتات فائقة الذكاء باستجواب المتهم أو سماع الشهود مستقلاً؛ بالنظر إلى السمات والخصائص النفسية التي يتطلبها التحقيق الجنائي، بينما يمكن توظيف قدراتها في مساعدة المحقق البشري بالنظر إلى القدرات العقلية الهائلة التي تمتلكها هذه الروبوتات.

١٥- برغم سرعة ودقة الخوارزميات التنبؤية في تحليل البيانات والتعامل مع القوانين والأحكام ذات الصلة بالدعوى المنظورة، إلا أن العمل القضائي من المجالات التي تعتمد بشكل أساسي على الوجدان البشري للقاضي، لا على العقل والمنطق فقط، ولا تملك هذه الخوارزميات هذا الوجدان، ومن ثم لا يمكن الاضمئنان إلى الأحكام التي تصدرها تلك الخوارزميات بناء على العقل والمنطق فقط مجردة من الوجدان.

١٦- خلو قانون الإجراءات الجزائية المصري من أية نصوص صريحة تنظم استخدام الروبوت فائق الذكاء في العمل الشرطي والقضائي، والأمر يحتاج إلى تدخل المشرع الاجرائي عاجل.

ثانيا- التوصيات:

١- قيام المشرع المصري بمعالجة الاختراق الإلكتروني لتقنيات الذكاء الاصطناعي والتلاعب في برمجيتها، وأنظمة تشغيلها بنصوص إجرائية خاصة.

٢- تدخل المشرع المصري بمعالجة تجريم فعل اختطاف الطائرة بدون طيار، لاسيما المسيرة ذاتياً، والسيارات المستقلة ذاتية القيادة بنصوص عقابية خاصة، مع تقرير العقوبة المناسبة لفعل الاختراق الالكتروني لأنظمتها التشغيلية.

٣- وضع الخطط والبرامج لرفع كفاءة رجال الشرطة وأعضاء النيابة العامة في الإلمام بقدرات تقينات الذكاء الاصطناعي لضمان الاستخدام الأمثل، لاسيما عند استخدام الطائرات بدون طيار، خاصة المسيرة ذاتياً، والمركبات ذاتية القيادة، والروبوتات فائقة الذكاء وغيرها من تقنيات الذكاء الاصطناعي.

٤- تدخل المشرع المصري بتنظيم الإجراءات التي يمكن الاستعانة بالروبوت فائق الذكاء في القيام بها مستقلاً عن رجال الشرطة؛ هذا ما يقتضي النص على اعتبار هذا الروبوت من مأموري الضبط القضائي ذو طبيعة خاصة.

٥- وضع التنظيم التشريعي الاجرائي لاستخدام تقنيات الذكاء الاصطناعي عموماً في العمل الشرطي، لمنع ارتكاب الجريمة والتنبؤ بها، أو في العمل القضائي من النيابة العامة في مرحلة التحقيق الابتدائي، أو من المحكمة في مرحلة المحاكمة.

قائمة المراجع والمصادر

أولاً- المراجع والمصادر العربية:

أ) الكتب والمؤلفات:

١- أحمد محمد حسان "نحو نظرية عامة لحماية الحق في الحياة الخاصة في العلاقة بين الدولة والأفراد" دراسة مقارنة، دار النهضة العربية، ٢٠٠١.

٢- أسامة عبد الله قايد "الحماية الجنائية للحياة الخاصة وبنوك المعلومات" الطبعة الثانية، دار النهضة العربية، القاهرة، ١٩٨٩.

٣- حسني الجندي "قانون الاجراءات الجزائية في دولة الامارات العربية المتحدة معلقا عليه بأقوال الفقه وأحكام القضاء" الجزء الأول، الطبعة الاولى، دار النهضة العربية، ٢٠٠٩.

٤- عادل عبد النور: أساسيات الذكاء الاصطناعي، منشورات مواقف، بيروت، ٢٠١٧م.

٥- ـــــــــــــــ مدخل إلى عالم الذكاء الاصطناعي، مدينة الملك عبد العزيز للعلوم والتقنية، المملكة العربية السعودية، ٢٠٠٥م.

٦– عدنان خالد التركماني، المعايير الشرعية والنفسية في التحقيق الجنائي، المركز العربي للدراسات الأمنية والتدريب، الرياض، ١٤١٤هـ، ١٩٩٣م.

٧– عصام أحمد البهجي، حماية الحق في الحياة الخاصة في ضوء حقوق الانسان والمسؤولية المدنية، دار الجامعة الجديدة للنشر، الاسكندرية، ٢٠٠٥.

٨– عمر عبد الله نصيف، استخدام نظم الذكاء الصناعي كأداة للتميز في الجودة والتنافسية، دراسة ميدانية لقطاع المستشفيات الخاصة في محافظة جدة، مجلة الأندلس للعلوم الاجتماعية والتطبيقية، المجلد (٢)، العدد الخامس، فبراير ٢٠١٠م.

٩– ك. إريك دريكسلر، وكريس بيترسون، وجايل برجاميت: استشراف المستقبل "ثورة التكنولوجيا النانوية"، ترجمة وتقديم: رؤوف وصفي، المركز القومي للترجمة، القاهرة، الطبعة الأولى، ٢٠١٦م.

١٠– محمود شاكر سعيد، د/ خالد بن عبد العزيز الحرفش، مفاهيم أمنية، جامعة نايف العربية للعلوم الأمنية، الرياض، الطبعة الأولى، ٢٠١٠م.

١١– محمود عبد الرحمن محمد "نطاق الحق في الحياة الخاصة دراسة في القانون الوضعي والشريعة الاسلامية" دار النهضة العربية، ١٩٩٦.

١٢– ممدوح خليل بحر، حماية الحياة الخاصة في القانون الجنائي، دراسة مقارنة، مكتبة دار الثقافة للنشر والتوزيع، عمان، الاردن، ١٩٩٦م.

ب) البحوث والمؤتمرات والرسائل العلمية:

١- أبو بكر خوالد، د/ خيرالدين بوزرب، فاعلية استخدام تطبيقات الذكاء الاصطناعي الحديثة في مواجهة فيروس كورونا (coved-19): تجربة كوريا الجنوبية نموذجاً، مجلة بحوث الادارة والاقتصاد، جامعة زيان عاشور بالجلفة، الجزائر، مجلد ٢، عدد خاص٢، (٢٠٢٠).

٢- أحمد ابراهيم محمد ابراهيم، المسؤولية الجنائية الناتجة عن أخطاء الذكاء الاصطناعي في التشريع الإماراتي (دراسة مقارنة)، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، ٢٠٢٠م.

٣- أحمد عبد الواحد العجماني، استخدام تقنيات الذكاء الاصطناعي في الإجراءات الجزائية، دراسة مقارنة، رسالة دكتوراة، جامعة الشارقة، ٢٠٢٣م.

٤- أحمد عادل جميل، ود/ عثمان حسين عثمان: إمكانية استخدام تقنيات الذكاء الصناعي في ضبط جودة التدقيق الداخلي "دراسة ميدانية في الشركات المساهمة العامة الأردنية"، بحث مقدم للمؤتمر العلمي السنوي الحادي عشر بعنوان "ذكاء الأعمال واقتصاد المعرفة"، جامعة الزيتونة الأردنية، كلية الاقتصاد والعلوم الإدارية، عمان، الفترة من ٢٣-٢٦ أبريل ٢٠١٢.

٥- أحمد كاظم: الذكاء الصناعي، قسم هندسة البرمجيات، كلية تكنولوجيا المعلومات، جامعة الإمام الصادق، بغداد، ٢٠١٢م.

٦– أسماء على سالم الشامسي، جرائم الاعتداء على حرمة الحياة الخاصة للأشخاص في ظل المرسوم بقانون رقم ٥ لسنة ٢٠١٢م، بشأن مكافحة جرائم تقنية المعلومات، دراسة مقارنة، رسالة ماجستير، جامعة الامارات العربية المتحدة، ٢٠١٨م.

٧– أيمن محمد السيد الأحول، د/ أحمد دسوقي، التحديات الأمنية المعاصرة للظواهر الاجرامية المستحدثة، الفكر الشرطي، القيادة العامة لشرطة الشارقة، مركز بحوث الشرطة، المجلد ٢٢، العدد ٨٦،يوليو ٢٠١٣.

٨– ايهاب خليفة، اقتصاديات الروبوت، تصاعد الاهتمام العالمي بتطبيقات الذكاء الاصطناعي، المنهل، مجلة اتجاهات الأحداث، تحليلات المستقبل، العدد٨، مارس ٢٠١٥م.

٩– جميل عبد الباقي الصغير، الحق في الصورة والاثبات الجنائي، مجلة كلية القانون الكويتية العالمية، العدد ١٠، ٢٠١٤.

١٠– حازم حسن أحمد الجمل، الحماية الجنائية للأمن السيبراني في ضوء رؤية المملكة ٢٠٣٠م، مجلة البحوث الأمنية، كلية الملك فهد الأمنية – مركز الدراسات والبحوث، المجلد ٣٠، العدد ٧٧، أغسطس ٢٠٢٠م، ذوالحجة ١٤٤١هـ.

١١– حسن أحمد المومني، أهمية وأثر الذكاء الاصطناعي في مستقبل العمل الشرطي: البيانات الكبري نموذجاً، ورقة عمل مقدمة للمؤتمر الخامس والعشرين، جمعية المكتبات المتخصصة، فرع الخليج العربي،

إنترنت الأشياء: مستقبل مجتمعات الانترنت المترابطة، أبوظبي، في الفترة من ٥-٧ مارس ٢٠١٩م.

١٢- حسن ربيع، حقوق الانسان ومشروعية استخدام رجال الشرطة للوسائل المستحدثة للتحقيق الجنائي، مجلة الفكر الشرطي، مركز بحوث الشرطة، القيادة العامة لشرطة الشارقة، الامارات العربية المتحدة، المجلد الأول، العدد ٤، مارس ١٩٩٣م.

١٣- حليمة حالد المدفع، استخدام تقنية الاتصال عن بعد في التحقيق والمحاكمات الجزائية، كلية الدراسات العليا، جامعة الشارقة، ٢٠٢٠م.

١٤- راشد محمد المري، المهارات الفنية لرجل الأمن في التحقيق والبحث الجنائي، مجلة روح القوانين، جامعة طنطا، العدد ٩٢، أكتوبر ٢٠٢٠م.

١٥- سعيد عبيدي، خطر الالآت الذكية على الانسان، مجلة الوعي الاسلامي، السنة ٥٥، العدد ٦٣٣، جمادى الأولى، ١٤٣٩هـ، يناير ٢٠١٨م.

١٦- صفوت عبدالحليم علي، توظيف تكنولوجيا التصوير التليفزيوني المعاصر لتسجيل بصمة العين ودورها في الكشف عن الأدلة الجنائية، مجلة علوم وفنون، جامعة حلوان، مصر، المجلد ٢٠ ،ع ١، يناير ٢٠٠٨م.

١٧- صلاح الدين محمد علي الفرجاني، مخاطر إختراق المواقع الإلكترونية، مجلة المصرفي، بنك السودان المركزي، العدد ٨٣، مارس ٢٠١٧م.

١٨- عبد السلام جاكيمي، الحماية التقنية والجنائية للنظم المعلوماتية، المجلة المغربية للقانون الجنائي والعلوم الجنائية، مركز الدراسات والبحوث الانسانية والاجتماعية، المغرب، العدد الثالث، ديسمبر ٢٠١٦م.

١٩- عبد الفتاح الطاهري، الأمن المعلوماتي وعلاقته بالأمن القومي، مجلة الباحث للدراسات القانونية والقضائية، عدد١٠، فبراير ٢٠١٩م.

٢٠- على شائف محمد شعفل، جعفر زين العابدين، التعرف على تعبير الوجه باستخدام خوارزمية PCA، رسالة ماجستير، جامعة الخرطوم، كلية علوم الحاسوب وتقنية المعلومات، السودان، ٢٠١٣.

٢١- عماد عبد الستار طه زيدان، الثغرات الأمنية فى مواقع الويب: دراسة تطبيقية على مواقع أقسام المكتبات والمعلومات المصرية، المجلة الدولية لعلوم المكتبات والمعلومات، الجمعية المصرية للمكتبات والمعلومات والأرشيف، المجلد ٥، العدد ٤، ديسمبر ٢٠١٨م.

٢٢- عمار باسر زهير، دور أنظمة الذكاء الاصطناعي في التنبؤ بالجريمة، مجلة الفكر الشرطي، مركز بحوث الشرطة، القيادة العامة

لشرطة الشارقة، الامارات العربية المتحدة، المجلد ٢٨، العدد ١١٠، يوليو ٢٠١٩م.

٢٣- عمر عبد المجيد مصبح، بصمة الصوت وأثرها في الاثبات الجنائي، مجلة البحوث الأمنية، المملكة العربية السعودية، العدد (٥٢) شعبان ١٤٣٣.

٢٤- ـــــــــــــــــــ، توظيف خوارزميات "العدالة التنبؤية" في نظام العدالة الجنائية: الآفاق والتحديات، المجلة الدولية للقانون، كلية القانون، دار نشر جامعة قطر، المجلد١٠، العدد المنتظم الأول، ٢٠٢١م.

٢٥- عمرو طه بدوي، النظام القانوني للروبوتات الذكية، المزودة بتقنية الذكاء االصطناعي (الإمارات العربية المتحدة كأنموذج) (دراسة تحليلية مقارنة)، مجلة الدراسات القانونية والاقتصادية، جامعة مدينة السادات، المجلد ٧، العدد ٢، ديسمبر ٢٠٢١ (ملحق ديسمبر).

٢٦- عيسى غازي الذيب، د/ بارعة القدسي، دور البصمة الصوتية والبصرية ومدى مشروعيتهما في الاثبات الجزائي، مجلة جامعة البعث، سوريا، المجلد ٣٩، العدد ٥٢، ٢٠١٧.

٢٧- محمود سلامة عبد المنعم الشريف، الطبيعة القانونية للتنبؤ بالجريمة بواسطة الذكاء الاصطناعي ومشروعيته، المجلة العربية لعلوم الأدلة

الجنائية والطب الشرعي، جامعة نايف العربية للعلوم الأمنية، المجلد الثالث، العدد ٢، ٢٠٢١م.

٢٨- محمد عبد الحفيظ المناصير، إشكالية الشخصية الالكترونية القانونية للروبوت، دراسة تأصيلية تحليلية مقارنة في إطار التشريعين المدني العماني والأوروبي، المجلة العربية للعلوم ونشر الأبحاث، المجلد٦ ، العدد١، ٣٠مارس٢٠٢٠م.

٢٩- محمد عرفان الخطيب، العدالة التنبئية والعدالة القضائية الفرص والتحديات، دراسة نقدية معمة في الموقف الانكلوسكسوني واللاتيني، مجلة الحقوق والعلوم الإنسانية، المجلد ١٢، العدد الأول، مايو ٢٠١٩م.

٣٠- محمد فوزي ابراهيم، البنك الوطني للحامض النووي ودوره في كشف غموض الحوادث المجهولة، مجلة الفكر الشرطي، أكاديمية العلوم الشرطية بالشارقة، الامارات العربية المتحدة، المجلد ٢٧، العدد ١٠٤، يناير ٢٠١٨م.

٣١- محمد محمد الألفي، الحماية القانونية لقواعد البيانات في نظم المعلومات، ورقة عمل لندوة أمن المعلومات والتوقيع الإلكتروني، المنظمة العربية للتنمية الإدارية، القاهرة، ٢٠٠٧م.

٣٢- محمد محمد الطوخي، تقنيات الذكاء الاصطناعي والمخاطر الإلكترونية، مجلة الفكر الشرطي، مركز بحوث الشرطة، القيادة العامة لشرطة الشارقة، المجلد٣٠، العدد (١١٦) بناير ٢٠٢١م،

٣٣- محمد نور الدين سيد، الحماية الجنائية للحق في خصوصية المكالمات الهاتفية دراسة في القانونين الكويتي والاماراتي، مجلة كلية القانون الكويتية العالمية، العدد ١٠، ٢٠١٤.

٣٤- هاني مطر أبو سعود، عباسة طاهر، ارتباطات الأمن المعلوماتي بالأمن القومي، مجلة الدراسات الحقوقية، جامعة سعيدة الدكتور مولاي الطاهر، الجزائر، المجلد ٧، العدد٢، جوان ٢٠٢٠م.

٣٥- يحيي ابراهيم دهشان، الحماية الجنائية للبيانات في ظل التحول الرقمي، مجلة الدراسات القانونية والاقتصادية، جامعة مدينة السادات، المجلد ٩، العدد ٣، سبتمبر ٢٠٢٣م.

ت) التقارير والمقالات:

١- أحمد ماجد، الذكاء الاصطناعي في دولة الامارات العربية، وزارة الاقتصاد، إدارة الدراسات والسياسات الاقتصادية، مبادرات الربيع الأول، ٢٠١٨.

٢- أشرف شهاب، مصطفى الدمرداش، ثورة الـ"بلوك تشين" على أعتاب التغيير، مجلة الأهرام للكمبيوتر والانترنت والاتصالات، ملف بعنوان (لغة العصر) العدد ٢١٥، نوفمبر ٢٠١٨م.

٣- ايهاب خليفة، الذكاء الاصطناعي: تأثيرات تزايد دور التقنيات الذكية في الحياة اليومية للبشر،منشور على منصة المنهل، تاريخ الزيارة: ٢٠٢١/١/١١م، على الرابط الالكتروني التالي:

٤– الدرر السنية، موسوعة الاخلاق والسلوك، منشورة على الموقع الالكتروني:

https://dorar.net/alakhlaq/2279/

٥– تي إكس هارمز، الروبوتات المقاتلة: كيف سيغير الذكاء الاصطناعي طبيعة الحروب القادمة؟ منشور على منصة المنهل، على الرابط الالكتروني:

http://platform.almanhal.com.uoseresources.remotexs.xyz/Reader/Article/105668/11/1/2021

٦– جريدة الاتحاد، الامارات العربية المتحدة، عدد ١٨ يناير ٢٠١١م، تاريخ الزيارة ١٣ ديسمبر ٢٠٢٠م.

٧– خلدون غسان سعيد " تقنيات متطورة للتعرف على الوجوه تصمم بنظم الذكاء الصناعي والتعلم العميق وتوظّف في استخدامات أمنية وطبية وتجارية، جريدة الشرق الأوسط، الثلاثاء – ١٧ جمادى الآخرة ١٤٤١ هـ – ١١ فبراير ٢٠٢٠ م، العدد ١٥٠٥٠.

٨– رنا ابراهيم، استراتيجية "البلوك تشين" المستقبل الآمن لتسريع المعاملات الحكومية، مجلة دبي القانونية، صادرة عن النيابة العامة بدبي، عدد (٣٠) يناير، ٢٠١٩م.

٩– الروبوت وتطبيقات الذكاء الاصطناعي، منشور على البوابة الرسمية لحكومة الامارات العربية المتحدة. تاريخ الزيارة ٢٠٢٠/١٢/٢٤م:

https://u.ae/ar-ae/about-the-uae/digital-uae/robotics-and-ai-applications

١٠- سعيد خلفان الظاهري: الذكاء الاصطناعي "القوة التنافسية الجديدة"، مركز استشراف المستقبل ودعم اتخاذ القرار، شرطة دبي، العدد (٢٩٩)، دبي، نشرة شهر فبراير ٢٠١٧م.

١١- شادي عبد الوهاب، وإبراهيم الغيطاني، وسارة يحيى: فرص وتهديدات الذكاء الاصطناعي في السنوات العشر القادمة، تقرير المستقبل، ملحق يصدر مع دورية "اتجاهات الأحداث"، العدد ٢٧، مركز المستقبل للأبحاث والدراسات المتقدمة، أبوظبي، ٢٠١٨م.

١٢- شيرين فاروق، شرطة دبي تُطلق الروبوت «أمل» للتوعية بمخاطر المخدرات، مقال منشور في جريدة البيان بتاريخ ٣١ ديسمبر ٢٠١٧م.

١٣- طه الراوي، مقال بعنوان "الذكاء الاصطناعي وأثره على الاقتصاد" نون بوست، بتاريخ ٢٠٢٠/١٠/٤م، منشور على الرابط الالكتروني التالي، تاريخ الزيارة ٢٠٢١/٣/١٤م:

https://www.noonpost.com/content/38443

١٤- عبد العزيز عبد الله الراجحي، شرح كتاب الحموية لابن تيمية، منشور على موقع المكتبة الشاملة الالكتروني:

https://shamela.ws/book/37019/1

١٥- علي حميد بن خاتم، الكفالة الذكية ضمانة إلكترونية تلغي إجراء حجز جوازات السفر، مجلة دبي القانونية، صادرة عن النيابة العامة بدبي، عدد (٣٠) يناير، ٢٠١٩م.

١٦- لوران بروبست وأخرون، تقرير بعنوان "استشراف مستقبل المعرفة" إعداد مؤسسة محمد بن راشد آل مكتوم للمعرفة، دار الغرير للطباعة والنشر، دبي، الامارات، بدون تاريخ نشر.

١٧- محمد محمد خليفة، الذكاء الاصطناعي في ميزان التشريع، مجلة دبي القانونية، تصدرها النيابة العامة–دبي، العدد ٢٨، مارس ٢٠١٨م.

١٨- مقال بعنوان " الروبوت يبدأ عمله في شرطة دبي" منشور على موقع مؤسسة دبي للمستقبل، مرصد المستقبل، بتاريخ ١٢ يونيو ٢٠١٧.

١٩- مقال بعنوان " تقنية التعرف على الوجه" مجلة العلوم والتكنولوجيا، منشور على الموقع الالكتروني للمجلة. تاريخ الزيارة ٢٠٢٠/١٢/١٤م.
http://www.tqmagazine.net/Details.aspx?id=554

٢٠- مقال بعنوان "٧ أنواع للذكاء الاصطناعي.. تعرف عليها، مجلة الحكومية الرقمية، منشور على الموقع الالكتروني للمجلة بتاريخ ١٨ أغسطس ٢٠١٩م، تاريخ الزيارة ٢٠٢٠/١١/٣م:
https://digitalgov.sa/?p=2330

٢١- مقال بعنوان طرح أول كتاب من تأليف الذكاء الاصطناعي، مجلة الاعمار والاقتصاد، عدد ٣٥٠، السنة ٢٦، ٣١ آيار ٢٠١٩، شركة الأوائل للتوزيع، بيروت، لبنان.

٢٢- نور الصباحي، التعرف على الوجوه باستخدام خوارزمية " تحليل المكونات الأساسية" Principal Component Analysis PCA، منشور بواسطة Schwarz Tigers Weblog ، بتاريخ ٤ يناير ٢٠١٣م.

٢٣- هنادي أبو نعمة، روبوت يوقف المركبات الثقيلة في دبي .. وطائرة من دون طيار تكشف مخالفاتها، الامارات اليوم، منشور بتاريخ ٠٧ أكتوبر ٢٠١٩.

٢٤- يمان هاشم القدور، مقال بعنوان "معنى الفِراسة" منشور بتاريخ ١٤ أبريل ٢٠١٩، على الرابط الالكتروني:

https://mawdoo3.com/

ثانياً- المراجع والمصادر الأجنبية:

1- Amankwaa, A. & Mccartney, C. "The effectiveness of the current use of forensic DNA in criminal investigations in England and Wales" Wiley Interdisciplinary Reviews: Forensic Science, 2018, 3(10).
2- Andrew J. Kerns, and others, "Unmanned Aircraft Capture and Control Via GPS Spoofing," Journal of Field Robotics, Vol. 31., No. 4, July/August 2014

3- Angwin, Julia, Jeff Larson, Surya Mattu, and Lauren Kirchner, “Machine Bias: There’s Software Used Across the Country to Predict Future Criminals. And It’s Biased Against Blacks,” ProPublica, May 23, 2016. As of December 5, 2016.
4- Brown, Brad, Michael Chui, and James Manyika, “Are You Ready for the Era of ‘Big Data’?” McKinsey Quarterly, Vol. 4, No. 1, October 2011.
5- Center for Internet Security, “EI-ISAC Cybersecurity Spotlight— CIA Triad,” webpage, undated. As of April 27, 2020.
6- De Deo, Simon, “Wrong Side of the Tracks: Big Data and Protected Categories,” Ithaca, N.Y.: Cornell University Library, May 28, 2015. As of March 7, 2017.
7- Delacroix.S. (2018).Computer systems fit for the legal profession? Legal Ethics,٢٠١٨, doi:10.1080/1460728x.2018.1551702, www.lawsociety.org.uk.
8- Divya Joshi, “Commercial Unmanned Aerial Vehicle (UAV) Market Analysis – Industry Trends, Companies and What You Should Know,” Business Insider, August 8, 2017.
9- Dwork, Cynthia, Moritz Hardt, Toniann Pitassi, Omer Reingold, and Richard Zemel, “Fairness Through Awareness,” Proceedings of the 3rd Innovations in Theoretical Computer Science Conference, Cambridge, Mass., January 8–10, 2012.

10- Fernando Trujano, Benjamin Chan, Greg Beams, and Reece Rivera, "Security Analysis of DJI Phantom 3 Standard," Massachusetts Institute of Technology, May 11, 2016.

11- James M. Anderson and others, Autonomous Vehicle Technology, A Guide for Policymakers, Published by the RAND Corporation, Santa Monica, Calif., 2016.

12- Jeff Crume, Doug Lhotka, Carma Austin, Security and Artificial Intelligence: FAQ, published by IBM Security.

13- Junia Valente and Alvaro E. Cardenas, "Understanding Security Threats in Consumer Drones Through the Lens of the Discovery Quadcopter Family," Proceedings of the 2017 Workshop on Internet of Things Security and Privacy, Dallas, Tex.: Association for Computing Machinery, 2017.

14- KATHARINA LEY BEST and Others, How to Analyze the Cyber Threat from Drones, Background, Analysis Frameworks, and Analysis Tools, Published by the RAND Corporation, Santa Monica, Calif. 2020.

15- Kerns, Andrew J., Daniel P. Shepard, Jahshan A. Bhatti, and Todd E. Humphreys, "Unmanned Aircraft Capture and Control Via GPS Spoofing," Journal of Field Robotics, Vol. 31, No. 4, July/ August 2014.

16- Larson, Jeff, Surya Mattu, Lauren Kirchner, and Julia Angwin, "How We Analyzed the COMPAS

Recidivism Algorithm," ProPublica, May 23, 2016. As of December 6, 2016.

17- Laura Fraade-Blanar, Nidhi Kalra, Autonomous Vehicles and Federal Safety Standards, published by RAND Corporation, 2017.

18- Lee, Peter, "Learning from Tay's introduction" blog, Microsoft website, March 25, 2016. As of December 5, 2016.

19- Manar Abu Talib and Others, Systematic literature review on Internet-of-Vehicles communication security, International Journal of Distributed Sensor Networks, Vol. 14(12), 2018.

20- MARY LEE and others, The Internet of Bodies, Opportunities, Risks, and Governance, published by The RAND Corporation, 2020.

21- Nick Statt, "Skydio's AI-Powered Autonomous R1 Drone Follows You Around in 4K" The Verge, February 13, 2018.

22- John E. Kelly, Computing, Cognition, and the Future of Knowing: How Humans and Machines are Forging a New Age of Understanding, September 2016, Vol. 28/No.8.

23- Osonde A. Osoba, Keeping Artificial Intelligence Accountable to Humans, August 20, 2018, available on internet.

24- Osonde A. Osoba, William Welser IV ,The Risks of Artificial Intelligence to Security and the Future of Work, RAND, Saint Monica, California, USA, 2017.

25- Osonde A. Osoba, William Welser IV, An Intelligence in Our Image, The Risks of Bias and Errors in Artificial Intelligence, Published by the RAND Corporation, Santa Monica, Calif., 2017.

26- Quain, John R., "These High-Tech Sensors May be the Key to Autonomous Cars," New York Times, September 26, 2019.

27- Randy Rieland, Artificial Intelligence Is Now Used to Predict Crime. But Is It Biased?, MARCH 5, 2018.

28- Sander Walters, "How Can Drones Be Hacked? The Updated List of Vulnerable Drones and Attack Tools," available at: https://medium.com/@swalters/how-can-drones-be-hacked-the-updated-list-of-vulnerable-drones-attack-tools-dd2e006d6809, 1/1/2021.

29- Sandvig, Christian, Kevin Hamilton, Karrie Karahalios, and Cedric Langbort, "Auditing Algorithms: Research Methods for Detecting Discrimination on Internet Platforms," paper presented to the Data and Discrimination: Converting Critical Concerns into Productive Inquiry preconference of the 64th Annual Meeting of the International Communication Association, Seattle, Wash., May 22, 2014.

30- Sean E. Goodison and others, Autonomous Road Vehicles and Law Enforcement, published by RAND Corporation, 2017.

31- Siddiqui, Faiz, “What Self-Driving Cars Can’t Recognize May Be a Matter of Life and Death,” Washington Post, November 11, 2019.