

Using artificial intelligence techniques to search for crime evidence

Tarek El Sayed Mahmoud Yousef

Lecturer at the Faculty of Law Member of the Egyptian Society for Political Economy and Legislation Member of the Egyptian Society for International Law

DOI: <https://doi.org/10.31918/twejer.eli24.13>

Published: 13/20/2024

Abstract

In the field of criminal law, the use of artificial intelligence techniques raises many problems related to criminal liability, the extent of the permissibility of using these techniques in combating crimes, and the extent to which their use affects the freedoms of individuals.

This research comes to shed light on the permissibility of using artificial intelligence techniques by security services in maintaining security, as well as in the field of predicting and combating crime. Through it, we attempt to expose ways of using artificial intelligence techniques in excavating evidence of crime and the extent of the legitimacy of that.

The research also addresses exposure to the risks of the use of artificial intelligence by security services and its impact on protecting the right to privacy, all through the use of a comparative analytical approach.

استخدام تقنيات الذكاء الاصطناعي في التنقيب عن أدلة الجريمة بين الواقع والتحديات (دراسة مقارنة)

د. طارق السيد محمود يوسف

محاضر بكلية الحقوق

عضو الجمعية المصرية للاقتصاد السياسي والتشريع

عضو الجمعية المصرية للقانون الدولي

١. مقدمة

يحتل الذكاء الاصطناعي في الوقت الراهن مكان الصدارة بين موضوعات البحث العلمي على مستوى العالم في محاولة جادة للبحث عن وسائل الاستفادة منه في مختلف النواحي الحياتية، والوقوف كذلك على مدى الخطر الذي يشكله التطور السريع في هذا المجال، ومحاولة البحث عن سبل للوقاية من تلك المخاطر (أبو عقيل، ٢٠٢٣، ص ١)، ونظرًا لما تحقّقه تقنيات الذكاء الاصطناعي من مزايا على المستوى الإقتصادي، فإن مختلف دول العالم تحرص على السعى بكل طاقتها للاستفادة من هذه التقنيات إلى أقصى درجة ممكنة، في سبيل تحقيق التنمية المستدامة، باعتبار أن التقدم في هذا المجال أصبح محورًا رئيسيًا في خطط التنمية المستقبلية.

ليس هذا وحسب، بل أدى التطور التكنولوجي الهائل، والمتسارع إلى غزو تقنيات الذكاء الاصطناعي لكافة المجالات الحيوية، حيث تستخدم في التعليم كالتدريس الآلي، وكذلك في المجالات الطبية كربات الرعاية الصحية (Moritz Goldener, 2015, p.115:117)، فضلاً عن المجالات الاقتصادية والعسكرية، وكذلك في مجال العدالة الجنائية. (الدويش، ٢٠٢٠، ص ٤).

ويستخدم مصطلح الذكاء الاصطناعي للدلالة على التطبيقات التي تؤدي مهام معقدة وتعتمد على الأجهزة الرقمية والإلكترونية، (اليومي، ٢٠٢٣، ص ١٠٣٣)، وهو كما يصفه البعض لا يعتبر شيئاً محسوساً، ولكنه نظام أو برنامج مترابط بعلاقات رياضية بإمكانها معالجة المعلومات، بمعنى أنه ليس آلة فيزيائية، وهو يختلف عن الروبوت المتحرك وإن كان يسكنه مثلما هو الحال بالنسبة للذكاء البشري والدمغ فلكل منهما مفهوم مختلف رغم أن الدماغ هي موطن الذكاء البشري (حلال، ٢٠٢١، ص ١٢).

وقد أدى تشعب مجالات الذكاء الاصطناعي وكذلك تشعب اختصاصات البحث العلمي المتعلقة به إلى تعدد التعريفات والمفاهيم لهذا المصطلح، وعلى صعيد التعاريف الذي قدمها الفقه القانوني، فقد جاءت متفقة في مضمونها، باعتبار الذكاء الاصطناعي مجرد محاكاة للذكاء البشري. (الصادق، ٢٠٢٣، ص ٨٩٥)

وفي رأينا أن التعريفات التي تقوم على اعتبار الذكاء الاصطناعي مجرد محاكاة للذكاء البشري تفتقر إلى الدقة؛ وذلك لعدة أسباب، أهمها أن ذكاء الآلة يجب النظر إليه بمفهوم يختلف تمامًا عن الذكاء البشري كما إن هذا التعريف وإن صدق على تطبيقات الذكاء الاصطناعي البسيطة، فهي لا تصدق على الذكاء الاصطناعي التوليدي وهو الذي يتخطى حدود ذكاء العقل البشري، وفي ضوء ذلك يمكننا تعريف الذكاء الاصطناعي بأنه: "علم قائم على توظيف التكنولوجيا في منح الآلة قدرات تمكنها من التصرف واتخاذ القرار بطريقة محدودة وفقاً لتوجيه العنصر البشري، أو بطريقة غير محدودة وتلقائية دون أي سيطرة بشرية.

ولقد شهد العقد الأخير اتجاه العديد من الدول إلى تبني تقنيات الذكاء الاصطناعي في المجال الجنائي ففي الصين هناك محاكم ذكية يعهد لها بالفصل في القضايا الصغيرة، كما تتم الاستعانة بالذكاء الاصطناعي في

مجال التنبؤ بالجريمة، وظهر كذلك ربوتات تتولى التحقيق في الجرائم، كما تبنت الولايات المتحدة الأمريكية تقنيات الذكاء الاصطناعي في التنبؤ بالجرائم والتنقيب عن الأدلة، وتأتي الإمارات في مقدمة الدول العربية من حيث العناية الخاصة بالذكاء الاصطناعي ومحاولة الاستفادة منه في كافة المجال ومن بينها المجالين الأمني والجنائي.

والحقيقة أن استخدام تقنيات الذكاء الاصطناعي في المجال الجنائي بوجه عام، والإجراءات الجنائية بوجه خاص، يثير العديد من الصعوبات، وهو موضوع لا زال محلاً للنقاش واختلاف وجهات النظر على الصعيدين التشريعي والفقه.

ومن هنا تولدت فكرة هذا البحث في محاولة للتعرف على علاقة الذكاء الاصطناعي بالقانون الجنائي فيما يتعلق بشقه الإجرائي، المتمثل في إجراءات جمع الاستدلالات والتحقيق الجنائي، ويأتي البحث ليلقي الضوء على دور تقنيات الذكاء الاصطناعي في مرحلة ما قبل المحاكمة وما يرتبط بها من إجراءات تتعلق بالاستدلال والتحقيق.

أهمية موضوع البحث:

تتمثل أهمية موضوع البحث في أنه يأتي في وقت تتسارع فيه التطورات التكنولوجية، ومن بينها تقنيات الذكاء الاصطناعي، وكذا اتجاه العديد من الدول للأخذ بهذه التقنيات في مجال التنبؤ بالجريمة وجمع الأدلة، وإجراء التحقيقات الجنائية، في ظل غياب النصوص الصريحة التي تنظم وسائل وسبل اللجوء لهذه التقنية. إشكالية البحث:

تدور مشكلة البحث الرئيسية في محاولة البحث عن إجابة لعدة تساؤلات وهي:

ما هي الاستفادة من الاستعانة بتقنيات الذكاء الاصطناعي في الإجراءات الجنائية؟

ماهي السبل التي يمكن من خلالها الاستعانة بتطبيقات الذكاء الاصطناعي في الاستدلال والتحقيق؟

هل يمكن الاعتماد على تقنيات الذكاء الاصطناعي للقيام بإجراء التحقيق الجنائي؟

هل من تجارب واقعية تفيد باستخدام تقنيات الذكاء الاصطناعي في الاستدلال والتحقيق؟

ما مدى مشروعية استخدام تقنيات الذكاء الاصطناعي في التحقيق الجنائي.

ما هي المخاطر المحتملة من استخدام تقنيات الذكاء الاصطناعي في التحقيقات الجنائية.

منهج البحث:

يستند البحث إلى المنهج الوصفي لوصف مدى انتشار ظاهرة الاستعانة بهذه التقنيات، كما يستخدم المنهج التحليلي، في سبيل التعرف على مسلك الدول في استخدام هذه التطبيقات وحدوده ووسائله ومبرراته، كما تمت الاستعانة بالمنهج المقارن عند عرض الآراء الفقهية لاختيار أقربها إلى الصحة.

خطة البحث:

تم تقسيم البحث إلى مبحثين وأربعة مطالب، على النحو الوارد بالمتن.

٢. استخدام تقنيات الذكاء الاصطناعي في الوقاية من الإجمام ومكافحته

يستهدف الضبط الإداري - في المقام الأول - الحفاظ على النظام العام بعناصره الثلاثة المتمثلة في الأمن العام، السكينة العامة، والصحة العامة، (المسلماني، ٢٠١٧، ص ٧٤) ولا شك أن المحافظة على الأمن العام تتطلب من سلطات الضبط اتخاذ كل ما يلزم من إجراءات للحيلولة دون وقوع الجريمة، وهو ما يعرف بالإجراءات الاحترازية، على عكس الضبط القضائي الذي يستهدف البحث عن مرتكب الجريمة بعد وقوعها

وجمع الأدلة التي تؤكد اثبات الاتهام أو نفيه، وتتزايد أهمية الضبط الإداري في نطاق الدور الوقائي للقانون الجنائي المتمثل في الردع العام. (حسن، ٢٠١٩، ص ٤١٨؛ بهنام، ١٩٨٤، ص ٤٢٩).

ومما لا شك فيه أن التطور الهائل الذي يشهده العالم في المجال التقني والتكنولوجي، قد أدى إلى ظهور العديد من السلوكيات الإجرامية التي لم تكن معهودة من قبل، وهو ما بات يعرف بالجرائم المستحدثة، وهذا النوع من الجرائم يتميز عن الجرائم التقليدية بالعديد من المزايا وأبرزها: سهولة ارتكابها، صعوبة اكتشافها بالإضافة إلى كونها عابرة للحدود، (صقر، ٢٠٢٠، ص ٥١٢)، وهو ما يستلزم بنية تشريعية قوية تكفل التصدي لهذا النوع من الجرائم ومكافحتها، وهو ما لا يمكن تحقيقه إلا بوجود أجهزة أمنية قوية تتضمن عناصر بشرية مدربة، ومؤهلة وتمتلك كافة المهارات التي تكفل قيامها بواجباتها في حفظ الأمن والوقاية من الجريمة.

وفي الآونة الأخيرة تم اللجوء لاستغلال تقنيات الذكاء الاصطناعي لحماية الأمن القومي، ففي الولايات المتحدة الأمريكية تستخدم أنظمة الذكاء الاصطناعي لتحليل البيانات والفيديوهات التي يتم التقاطها من خلال عمليات المراقبة وتنبيه المحللين بالأنشطة المشبوهة، كما طورت ولاية شيكاغو استراتيجية تقوم على استخدام تقنيات الذكاء الاصطناعي في تحليل البيانات وبعض الأنماط السلوكية للتنبؤ بالسلوك الإجرامي (البابلي، ٢٠١٩، ص ٦٢).

وفي سبيل التعرف على سبل استخدام الذكاء الاصطناعي في مكافحة الجريمة سواء من خلال الإجراءات التي تتخذها سلطات الضبط الإداري في الوقاية أو الحيلولة دون وقوع الجريمة، أو من خلال الإجراءات التي تتخذ بعد وقوع الجريمة من قبل سلطات الضبط القضائي المعنية بالتحقيق، سنقسم الدراسة في هذا المبحث إلى مطلبين على النحو التالي:

١, ٢. استخدام تقنيات الذكاء الاصطناعي في التنبؤ والوقاية

تساعد التكنولوجيا كثيرًا في الحيلولة دون وقوع العديد من الجرائم، بل قد أدت بالفعل إلى اختفاء بعض الجرائم أو تراجعها بشكل كبير، فجرائم مثل التحرش لم يعد لها وجود في وسائل المواصلات الحديثة بفضل استخدام كاميرات التصوير الذكية، ولا شك أن اعتماد الأجهزة الأمنية في عملها على استخدام التكنولوجيا من شأنه أن يسهم في تفعيل دورها في حفظ الأمن ومنع الجريمة قبل وقوعها، وهو ما يمثل أهم الانعكاسات الإيجابية للتطور التكنولوجي على الصعيد الأمني، وهو الأمر الذي دفع العديد من الدول إلى الاستفادة إلى أقصى حد من تقنيات الذكاء الاصطناعي في المجال الأمني. (البابلي، ٢٠١٨، ص ١١٥).

ويرى البعض (فريد ويرنر، ٢٠٢٠، ص ١٤، ITU News Magazin, No2) أن الامكانيات الهائلة التي يتمتع بها الذكاء الاصطناعي من شأنها أن تساعد في التصدي لغالبية المشاكل التي تواجه البشرية، إذ يساعد استخدام تقنيات الذكاء الاصطناعي في خفض عدد الوفيات السنوية على الطرق بمقدار ١,٣ مليون شخص، كذلك يسهم الذكاء الاصطناعي في التصدي للجرائم السيبرانية.

وتستطيع أجهزة الأمن من خلال استخدام البرمجيات الذكية في تحليل البيانات المتوافرة لديها عن الجرائم والمجرمين في التعرف على الأوقات والأماكن التي من المتوقع أن تحدث فيها الجريمة، وتحديد المشتبه بهم من خلال تحليل أنماط السلوك الإجرامي، وهو ما يسهم في تحركها بشكل استباقي واعتراض المجرم ومنع وقوع الجريمة. (خليفة، ٢٠١٩، ص ١٣).

ويُفرق الفقه (البابلي، ٢٠١٩، ص ٧٨) بين أربعة أساليب تستخدمها الشرطة التنبؤية وهي: أسلوب التنبؤ بالجرائم، أسلوب التنبؤ بالجناة، أسلوب التنبؤ بهوية المجرمين، وأخيرًا أسلوب التنبؤ بضحايا الجريمة، وقد تم الاستعانة بالذكاء الاصطناعي في التنبؤ بالجريمة من قبل أحد مراكز الشرطة في ولاية لوس أنجلوس

بالولايات المتحدة عام ٢٠١١، ثم عمم هذا الأسلوب في معظم مراكز الشرطة داخل الولاية بحلول عام ٢٠١٤.

كذلك قامت شرطة مدينة نيويورك بإنشاء مركز إدارة الجريمة وهو يحتوى على مستودع معلوماتى عن الجرائم التي حدثت وتحدث في المدينة، ويعمل على استخدام تقنيات تحليل البيانات والتنبؤ التحليلي، للوقوف على المخاطر المحتملة، والتنبؤ بالجرائم المحتملة واتخاذ التدابير اللازمة ومن بينها تحسين زمن الاستجابة السريعة، وتوزيع الدوريات في الأماكن الأكثر عرضة لحدوث الجرائم، والعمل على الحيلولة دون وقوعها. (عوضين، فايق (مارس ٢٠٢٢، ص ١٨)

ومن وجهة نظر البعض فإنه يجب تشجيع الاستفادة من تقنيات الذكاء الاصطناعي في مجال مكافحة الجريمة، والوقاية منها، نظرًا للامكانيات الهائلة المتوفرة في هذه التقنيات، إذ من خلال الخوارزميات يمكن بسهولة اكتشاف الغموض في أى واقعة إجرامية بصورة أكثر دقة، كما أن الاستعانة بهذه التقنيات - وخاصة تقنية التعلم العميق - من شأنه المساعدة في تصنيف المجرمين وبطريقة موضوعية بعيدًا عن الأهواء الشخصية بما يخدم العدالة (Akerkar2019, pp.32:35).

وتسعى العديد من الدول في الوقت الراهن للاستعانة بتقنيات الذكاء الاصطناعي في المجال الأمني، وخصوصًا في تعزيز قدرات الأجهزة الأمنية في مجال مكافحة الجرائم وتأتى الإمارات العربية المتحدة في مقدمة الدول العربية التي وظفت تقنيات الذكاء الاصطناعي في مختلف المجالات، ومن الأليات التي انتهجتها في هذا الصدد، تبنى مشروع نظام تحليل المشاعر على مواقع التواصل الإجتماعى بالتعاون مع مركز أبو ظبي للإحصاء، وفي مجال الأمن تبنّت مشروع قياس مشاعر الحشود من صور الفيديو في سبيل التنبؤ بتصرفات بعض الأشخاص حيال التطبيقات الأمنية. (مبادرات الربع الأول ٢٠١٨، الانترنت).

<file:///C:/Users/dr%20tark/Downloads/AI%20Report%202018.pdf>

وفي عام ٢٠١٥ قامت شرطة دبي باستخدام الطائرات الذكية للمراقبة الجوية، أثناء الأحداث الرياضية والمهرجانات والاحتفالات، ومؤخرًا كشفت القيادة العامة لشرطة دبي عن آلية جديدة ستستخدم في التخطيط الذكي لحوادث السير البسيطة عبر تقنيات الذكاء الاصطناعي، من خلال تحليل الحوادث البسيطة وإصدار التقارير بشكل فوري للسائقين دون تدخل بشري. (المكتب الاعلامى لحكومة دبي على الانترنت، بتاريخ ٢٠٢٣/١٠/١٩).

ويأتى قطاع المرور ضمن القطاعات المستدفة في الاستراتيجية التي تتبناها الدولة بشأن الذكاء الاصطناعي، إذ يتم العمل على تطوير آليات وقائية كالتنبؤ بالحوادث والازدحام المروري، ووضع سياسات مرورية أكثر فاعلية. (استراتيجية الإمارات للذكاء الاصطناعي، البوابة الرسمية للحكومة، <https://u.ae/>).

و تتعدد سبل الاستعانة بتقنيات الذكاء الاصطناعي في العمل الشرطى، فعلى سبيل المثال تستخدم تقنيات الذكاء الاصطناعي في قراءة لوحات السيارات بدقة، الشرطى الآلى، الخوذات الذكية، السيارات الشرطية ذاتية القيادة، مراكز الشرطة الذكية، المراقبة الذكية من خلال تقنية التعرف على الوجوه في المطارات والميادين والشوارع، ومن خلال الكاميرات الذكية يمكن مراقبة الحالة الأمنية ومتابعة حركات المجرمين والمشتبه بهم، وكذلك استغلال الخوارزميات في تحليل البيانات في سبيل التنبؤ بالجرائم، وتحاول حكومة الإمارات الاستفادة من كافة هذه التقنيات في المجال الأمنى(علاى، عمار راشد، ديسمبر ٢٠٢٣، ص ٣٧٢). ونظرًا لتغير استراتيجية عمل الشرطة في مختلف الدول في التعامل مع الجريمة والتركيز على محاولة التصدى لها قبل وقوعها بدلًا من الملاحقة القضائية لمرتكبيها بعد وقوعها، فيما يعرف بالاستراتيجية الوقائية، فقد بدأ التوجه من قبل الأجهزة الأمنية نحو الاستفادة بالتطور التكنولوجى لأقصى حد في مجال

التنبؤ بالجريمة، ومن هنا عرف البعض (البابلي ٢٠١٩، ص ٨١) الشرطة التنبؤية بأنها: "الشرطة التي تعتمد على الاستخبارات في عملية تقييم المخاطر، من خلال جمع المعلومات.

وفي رأينا يمكن تعريف الشرطة التنبؤية بأنها: "آلية تستخدم من قبل الأجهزة الأمنية تقوم على توظيف التكنولوجيا وتقنيات الذكاء الاصطناعي في حفظ الأمن ومكافحة السلوك الإجرامي".

صور الاستعانة بتقنيات الذكاء الاصطناعي في الاستراتيجية الوقائية:

هناك العديد من السبل التي تنتهجها الأجهزة الأمنية في الاستعانة بتقنيات الذكاء الاصطناعي في التصدي للأنشطة الإجرامية، والحيلولة دون وقوع الجريمة، ومن بينها الاستعانة بالكاميرات الذكية الاستعانة بتقنيات التعلم الآلي بالتنبؤ بأعمال الشغب، استخدام تحليل البيانات الضخمة في التصدي للأعمال الإرهابية، الاستعانة بتقنيات الذكاء الاصطناعي في التصدي للهجمات السيبرانية، توظيف البيانات الضخمة لجمع المعلومات من وسائل التواصل الاجتماعي، في سبيل تبني تدابير استباقية للوقاية من الجريمة، استخدام أجهزة محاكاة أبراج الهواتف الخلوية في مجال حفظ الأمن الداخلي. (العجماني، أحمد عبد الواحد، ديسمبر ٢٠٢٣ ص ٦٢٤).

ونظراً لعدد اتساع البحث لعرض الكثير من التفاصيل، سنحاول -في اطلالة سريعة - التعرض لأهم صور استخدام التقنيات الذكية في التنبؤ بالجريمة وذلك على النحو التالي:

أولاً: الاستعانة بتقنيات الذكاء الاصطناعي في مكافحة الإرهاب:

كانت قضية الإرهاب - وما زالت - موضع اهتمام المجتمع الدولي (تعتبر اتفاقية جنيف لعام ١٩٣٧ أول اتفاقية دولية تعنى بمكافحة الإرهاب؛ الاتفاقية الأوروبية لقمع الإرهاب عام ١٩٧٧م، الاتفاقية العربية لمكافحة الإرهاب، ١٩٩٨م، اتفاقية الأمم المتحدة لمكافحة الإرهاب، الاتفاقية الدولية لمنع تمويل الإرهاب لسنة ١٩٩٩م، للاطلاع على الصكوك الدولية في مكافحة الإرهاب، راجع الرابط التالي، الزيارة ٢٠٢٣/١٠/٩).

<https://www.un.org/counterterrorism/ar/international-legal-instruments>

ونظراً لما تسببه الأعمال الإرهابية من خسائر بشرية ومادية، فضلاً عن أنها تشكل أكبر تهديد لأمن واستقرار المجتمعات، لذا حرصت كافة الدول على مستوى العالم على سن تشريعات خاصة في محاولة التصدي له والقضاء عليه (العراق: قانون مكافحة الإرهاب رقم ١٣ لسنة ٢٠٠٥؛ تونس: قانون أساسي عدد ٢٦ لسنة ٢٠١٥؛ مصر القانون ٩٤ لسنة ٢٠١٥ وتعديلاته؛ الإمارات: المرسوم بقانون اتحادي رقم (٢٠) لسنة ٢٠١٨ في شأن مواجهة جرائم غسل الأموال ومكافحة تمويل الإرهاب وتمويل التنظيمات غير المشروعة، ولائحته التنفيذية؛ قانون الإتحادي رقم (٧) لسنة ٢٠١٤ في شأن مكافحة الجرائم الإرهابية). ووفقاً لما ذهب إليه بعض الباحثين فإن الاستعانة بتقنيات الذكاء الاصطناعي من قبل الأجهزة الأمنية يعتبر أحد الوسائل التي تستخدم بالفعل في العديد من الدول، ومن خلال هذه التقنيات تستطيع الأجهزة الأمنية توجيه الموارد بطريقة فعالة للحيلولة دون وقوع الجريمة، فمن خلال تحليل البيانات يمكن الاستدلال على المشتبه بهم، وكذلك تحديد الأماكن المستهدفة لارتكاب الجريمة، ومع ذلك فلا بد من استخدام الذكاء الاصطناعي في ضوء مجموعة من الضوابط والشروط التي تكفل المحافظة على احترام حريات الأفراد وضمان عدم التحيز.

من ناحية أخرى ومن خلال تقنيات التعرف على الوجوه وتحليل الصور والفيديوهات، وتقنيات تحليل الصوت يمكن الكشف عن هوية المشتبه بهم بسهولة، كذلك تستطيع أجهزة الشرطة أن تعمل على تحليل الشبكات الاجتماعية للعصابات الإجرامية، وكذلك تحليل البيانات عبر وسائل التواصل الاجتماعي للكشف

عن المتورطين، كما يمكن الاستعانة بتقنيات الذكاء الاصطناعي في مجابهة المنصات الاعلامية للجماعات الإرهابية. (Galdon Clavell, G2016,P.91:93).

كذلك تستخدم تقنيات النظم الخبيثة (تعرف بأنها تقنية ذكية مصممة للتعامل مع المشكلات وحلها من خلال توظيف المعرفة والاستنتاج، ومن أمثلتها نظام تحديد الموقع GPS، أنظر: Peter J F&other,2014,p3) في مواجهة الأسلحة البيولوجية أو ما يطلق عليه الإرهاب البيولوجي، للتعرف على الأسلحة وصفاتها وطرق تصنيعها، ومكوناتها الكيميائية، وتستطيع النظم الخبيثة توجيه الجهات المعنية إلى سبل المواجهة والاحتواء، والاحتياطات التي يلزم اتباعها.

ثانياً: الاستعانة بتقنيات الذكاء الاصطناعي في التنبؤ بالهجمات السيبرانية:

الحرب السيبرانية عبارة عن هجمات إلكترونية تستهدف الحاسب الآلي، ومن خلالها يمكن شل البنية المعلوماتية، وهو الأمر الذي يؤدي إلى كم هائل من الخسائر بمختلف أنواعها، خاصة حينما تستهدف الهجمات البنية التحتية، وقطع أنظمة الاتصالات، كما قد تؤدي إلى مسح كامل للمعلومات والبيانات، (أبو عقيل ٢٠٢٣، ص ١٣)، وبعض الهجمات السيبرانية قد تؤدي إلى أضرار كارثية، ومن أبرز الأمثلة على ذلك فيروس ستاكسنت الذي طورته الولايات المتحدة بمساعدة إسرائيل لشن هجوم على المواقع النووية في إيران عام ٢٠١٠م.

https://www.bbc.com/arabic/worldnews/2011/01/110116_us_iran_israel_stuxnet_nuke

ومن قبيل الحروب السيبرانية أيضاً قيام الجماعات الإرهابية باستخدام تقنيات برامج الفدية في تدمير الشبكات أو حذف البيانات بالكامل. (Andy Greenberg.Aug. 22, 2018, online).

وفي سبيل مواجهة التصدي لهذه المخاطر؛ تحرص غالبية الدول على دعم الأجهزة الأمنية في اتخاذ كافة التدابير التي تحول دون وقوع أي شكل من أشكال الاعتداءات الإلكترونية، ويعد ذلك أهم الأولويات في السياسة الدفاعية ضد الجرائم الإلكترونية (ياسين، ٢٠٢٢، ص ١٠٤٨ : ١٤٠٩).

ومن الممكن استخدام تقنيات الذكاء الاصطناعي في مواجهة التهديدات السيبرانية من قبل فرق تكنولوجيا المعلومات، وبعض هذه التهديدات يمكن التعامل معها ببساطة من خلال آلية أو خوارزميات التعلم الآلي، في وقت استجابة قصير، كذلك يمكن الاستفادة من تقنيات الذكاء الاصطناعي في تزويد فرق الأمن المختصة بتقارير مبسطة تسهم في سرعة المعالجة واتخاذ القرار المناسب، إذ يعد التعلم الآلي من أهم أدوات الذكاء الاصطناعي وأقواها في مجابهة الجرائم السيبرانية. (محارب، سبتمبر ٢٠٢٣، ص ١٤ : ١٥).

ومن جانبنا نود الإشارة إلى أن استخدام تقنيات الذكاء الاصطناعي في التصدي للهجمات السيبرانية بات ضرورة ملحة – خصوصاً في عالمنا العربي – حيث تسعى مختلف الدول العربية إلى بذل كافة الجهود لمسايرة التقدم التقني، من خلال تبني استراتيجية التحول الرقمي، والحكومة الإلكترونية، ومن شأن الهجمات السيبرانية أن تقوض كل هذه الجهود (ناظم، ٢٠٢٣، ص ٢٤ وما بعدها).

ثالثاً: الاستعانة بالكاميرات الذكية:

من خلال الاستعانة بالكاميرات الذكية يمكن ضبط حركة سير المرور، كما إن استخدام الرادارات الذكية من شأنه الحد من حوادث المركبات، حيث إن مراقبة الطرق بهذه التقنيات من شأنها دفع قائد المركبات إلى الالتزام بسرعات محددة، كما يمكن من خلال المراقبة التنبؤ باحتمال حدوث الاختناقات المرورية والحيلولة دون اصطدام السيارات، وتتجه غالبية الولايات في أمريكا الاستفادة من تقنيات الذكاء الاصطناعي في سبيل الحد من حوادث السيارات ، ففي ولاية نيفادا قامت ثلاث جهات حكومية محلية في الولاية بالعمل على برنامج تجريبي في عام ٢٠٢٠ يعتمد خوارزميات الذكاء الاصطناعي لتحسين حركة المرور في الولاية، وقد شمل هذه البرنامج التعاوني قسم دوريات الطرق السريعة التابع لإدارة السلامة

العامة في الولاية، ولجنة النقل الإقليمية لجنوب نيفادا، وإدارة النقل، ومشاركة من شركة (Waycare) التي تطور حلولاً ذكية لإدارة المرور، ويكمن الهدف الرئيسي من هذا البرنامج في خفض حوادث الاصطدام بنسبة ٥٪ في المواقع الأكثر عرضة للحوادث الخطرة، ومراقبة الأثر الذي تحققه الإجراءات الوقائية على سلوك السائقين وسرعة المركبات. (الذكاء الاصطناعي للحد من حوادث المرور في نيفادا، الرابط التالي <https://ibtekr.org/cases>).

وعلى مستوى العالم العربي تستخدم تقنيات الذكاء الاصطناعي في ضبط حركة المرور في كل من الامارات، والمملكة العربية السعودية، قطر، سلطنة عمان، الأردن، ومصر، كما تستخدم الحكومة المصرية أنظمة الذكاء الاصطناعي في تحليل لقطات كاميرات المراقبة في الأماكن العامة لاكتشاف السلوك المشبوه ومنع الجريمة. (<https://www.marwanosman.net/blog/Artificial-Intelligence-in-Egypt>).

رابعاً: الاستعانة بتقنية التعلم الآلي في تحليل البيانات :

يذهب البعض إلى أن غزو الرقمنة لكافة المجالات الحياتية، استدعى بالضرورة اللجوء لتقنية المعلومات في حسم النزاعات القانونية، وفقاً لما يفرضه المنطق لذا؛ تتعدد مبررات الاستعانة بالتكنولوجيا الرقمية في مجال العدالة الجنائية، وأول هذه المبررات يتمثل في: مساعدة الشرطة التنبؤية في مكافحة الجريمة، وخصوصاً تلك الجرائم التي ترتكب من خلال شبكة الإنترنت. (عبد الكريم، فهيل عبد الباسط، ٢٠٢٢، ص ٩١٠).

فمن خلال الاستعانة بالخوارزميات (يعرفها البعض بأنها مجموعة من الخطوات الرياضية والمنطقية المتسلسلة يتم اتباعها لحل المشكلات، أنظر: مصبح، عمر عبد المجيد ٢٠٢١، ص ٢٣٧) يتم نقل الخبرات الذهنية للبشر إلى الآلات الذكية التي تعمل بسرعة فائقة وفقاً لنظام البرمجة الخاص بها، وتستطيع التنبؤ إلى نتائج في منتهى الدقة، (مهني، ٢٠٢٢ ص ٢١٨) وبشكل أفضل وأسرع، بعيداً عن التدخل البشري والذي غالباً ما يتأثر بالضغط العصبي والنفسي.

وفي رأينا يمكن تعريف خوارزميات العدالة التنبؤية بأنها: " تقنية ذكية تحتوي معادلات رياضية متصلة بتسلسل، وتعتمد على الذكاء الاصطناعي، لها القدرة على التحليل والاستنتاج المنطقي".

واقترح البعض ضرورة السعي للاستفادة من الخوارزميات من قبل دوائر الطبي العدلي في العراق وإقليم كردستان من خلال إنشاء بنك مركزي يتضمن الأحماض النووية والصور الإشعاعية للمجرمين بشكل منفصل، وكذا الاستعانة بالخوارزميات للتعرف على الوجوه وفرزها، والتنبؤ بوجه المشتبه به من خلال القدرة على رسم صورة افتراضية استناداً للبيانات المقدمة من قبل المجنى عليه. (عبد الكريم، فهيل عبد الباسط، ٢٠٢٢، ص ٩١٤).

وتستخدم المملكة المتحدة الخوارزميات في تحليل ودراسة ماضي أصحاب السوابق في سبيل منع وقوع جرائم مشابهة في المستقبل، اعتماداً على دراسة الحالة الاجتماعية والاقتصادية والمنطقة الجغرافية، وتعد تقنية HART أشهر الخوارزميات المستخدمة في التنبؤ بمستوى خطر قيام المشتبه بهم بارتكاب جرائم في المستقبل، وهي تعتمد في تبؤها على مجموعة من القيم تتمثل في تاريخ المشتبه به، وعمره وجنسه ومنطقته الجغرافية. (Oscar H. 2010, p34:36).

وفي الولايات المتحدة الأمريكية تطبق الخوارزميات الذكية على نطاق واسع في مجال العدالة الجنائية – بوجه عام- كما تستخدم كذلك من قبل الجهات الأمنية في التنبؤ بالجريمة، مع اتجاه المشرع في معظم الولايات إلى سن التشريعات التي تكفل تنظيم استخدام هذه التقنيات بما لا يتعارض مع حريات الأشخاص وقد صدر أول قانون بشأن الشفافية في صنع القرار الخوارزمية من قبل مجلس ولاية نيويورك، ويقرر

القانون انشاء فريق عمل يختص بمراقبة عدالة الخوارزميات ومدى صلاحيتها للاستخدام في نطاق الولاية (مصبح ٢٠٢١، ص٢٤٩)، ويقرر العديد من الباحثين بأن الاستفادة من التقنيات الذكية في مجال التنبؤ بالجريمة أثبت فاعليته في المملكة المتحدة، حيث أن دمج التكنولوجيا الحديثة في العمل الشرطي من شأنه الاسهام في تدخلها السريع في التصدي للمجرمين، والحيلولة دون ارتكاب الجريمة. (Lilian Edwards 2016, P.30:31).

كما يقرر البعض بأن التعديلات التي أدخلها المشرع الأمريكي على القوانين المتعلقة بمعالجة الخوارزميات من شأنها كفالة التزام المطورين بالاستخدام المنضبط لهذه التقنيات، كما أن هذه التعديلات تكفل قدرًا من الحماية مع تقرير المسؤولية. (Pfeiffer, 2023, Tech Policy Press) وفي العموم يمكن القول بأن البيانات المنظمة والدقيقة تلعب دورًا بارزًا في عملية اتخاذ القرار، ورسم الخطط والاستراتيجيات، وهي إحدى مميزات التكنولوجيا، فمن خلالها يمكن التنبؤ بالمستقبل، وفي ضوء هذا التنبؤ يمكن تفادي العديد من المشاكل، ومن هنا تعمل الدول على الاستفادة من التقنيات الذكية في مجال تحليل البيانات الضخمة في مختلف المجالات، السياحية والطبية، والأمنية. (على، رزق سعد سبتمبر ٢٠٢٣، ص١٥٧٩).

وعلى الصعيد العراقي يسعى اقليم كردستان العراق نحو الاستفادة من تقنيات الذكاء الاصطناعي، فهناك محاولات تبذل من قبل الحكومة في الإقليم لوضع استراتيجيات تستهدف التطوير التكنولوجي، نأمل أن تكلل بالنجاح، خاصة بعد الاعلان في مايو ٢٠٢٣ عن انشاء مركزين للذكاء الاصطناعي بمشاركة أمريكية، (<https://shafaq.com/ar> الزيارة ٢٠٢٣/٢/٢)، كما تعمل الحكومة في الإقليم على استضافة معارض في مجال تكنولوجيا المعلومات من اجل مواكبة عصر التحول الرقمي (<https://hitex.tech/ar>)

كذلك وكبداية تم تبنى مشروع رووداو لتنمية واستخدام الذكاء الاصطناعي ومن شأنه أن يجعل نشر الأخبار المفبركة عملاً غير يسير، سيهيء الفرص للشباب والخبراء والمبدعين الرقميين في كوردستان والشئات للمشاركة في هذا المشروع الحديث.

(<https://www.rudawarabia.net/arabic/kurdistan/20082023>)

ويثبت الواقع أن هناك رغبة حقيقية من قبل الحكومة العراقية في التطوير، ومواكبة التطور التقني وعلى المشرع العراقي أن يسارع بخطوات إيجابية والعمل على تهيئة البنية التشريعية التي تتناسب مع التقدم التكنولوجي، ومتطلبات الاستفادة من تقنيات الذكاء الاصطناعي في كافة المجالات، ويأتي في مقدمة الخطوات المطلوبة الاسراع في سن التشريع الخاص بجرائم تقنية المعومات، وكذلك قانون حماية البيانات الشخصية.

2.2. استخدام تقنيات الذكاء الاصطناعي في البحث عن الأدلة الجنائية

ينشأ حق الدولة في العقاب بمجرد وقوع الجريمة، وينظم القانون كافة الإجراءات التي تتبع منذ وقوع الجريمة وحتى صدور الحكم على الفاعل، وتعتبر الدعوى الجنائية هي الوسيلة التي من خلالها اتخاذ كافة هذه الإجراءات، (أبو خطوة، ٢٠٢١، ص٢٧٩: ٢٨١)، ومن وجهة نظر الفقه (شمس الدين ٢٠١٧، ص٢١٤: ٢١٥) فإن الدعوى الجنائية تمر بمرحلتين: الأولى مرحلة ما قبل المحاكمة، وفي هذه المرحلة تضطلع السلطات الأمنية متمثلة في أجهزة الشرطة باختصاصها في جمع الأدلة ومحاولة التعرف على الفاعل، ومن ثم إعداد ملف بالأدلة التي حصلت عليها واحالته إلى الجهات المعنية بالتحقيق، التي تقدر مدى كفاية الأدلة لإثبات وقوع الجريمة ونسبتها لشخص بعينه، لتحيلها إلى القضاء للفصل فيها، ومن خلال هذه الإحالة تدخل الدعوى في مرحلتها الثانية وهي مرحلة المحاكمة.

ولمرحلة ما قبل المحاكمة أهمية بالغة، (أبو عقيل، ٢٠١٨) ففي هذه المرحلة يتم جمع الأدلة واتخاذ إجراءات البحث والتحري، وجمع الاستدلالات ثم بعد ذلك يتولى جهاز الإدعاء مهمة التحقيق لتقدير الأدلة، وتتوقف صحة وعدالة المحاكمة على صحة هذه الإجراءات، إذ أن أي إجراء يتخذ بالمخالفة للقانون أثناء جمع الأدلة والتحقيق قد يؤدي لبطلان سائر الإجراءات.

وتتم إجراءات جمع الاستدلالات من قبل سلطات الضبط الإداري، حيث لا تعتبر هذه الإجراءات ضمن إجراءات التحقيق ولكنها تمهد له، بيد أن جمع الاستدلالات لا بد وأن يتم في ضوء مقتضيات الشرعية الجنائية، بمعنى أن أعمال الاستدلال بطبيعتها لا تستهدف سوى جمع المعلومات من خلال أساليب مشروعة لذا؛ يجب أن تكون مجردة من القهر والإجبار، وأن تتم بأساليب مشروعة، وخلال هذه المرحلة لا يتقيد مأمور الضبط في عمله إلا بالشرعية، لتأتي كل أعمال مطابقة لما يفرضه القانون. (حسن، ٢٠١٩، ص ٤٢٩: ٤٣٠).

وقد أظهر التطور التكنولوجي ظهور العديد من صور الجرائم التي تتميز بطابعها الخاص، هذا الطابع المتمثل في استغلال التكنولوجيا والتقنيات الحديثة في ارتكاب الجرائم ومن ذلك القرصنة الإلكترونية، سرقة المعلومات، انتهاك الحق في الخصوصية، الإرهاب الإلكتروني، التجسس، السرقات الإلكترونية، (عبد الكافي، ٢٠٢٠، ص ١٠٩: ١١٢)، وكلها صور لجرائم تقنية المعلومات (البالول، ٢٠٢١، ص ٤٩)، فضلاً عما أفرزته تكنولوجيا الذكاء الاصطناعي من جرائم (دهشان، ٢٠٢٠، ص ١١٤)، أخرى كالتزييف العميق والروبوت القاتل، وجرائم الروبوتات الجراحية، (حسن، ٢٠٢٢، ص ١٨: ٢١) والجرائم المرتكبة بواسطة الطائرات المسييرة، وهي جميعاً تتسم بالخطورة، (سعد، ٢٠٢٢، ص ١٨) التي تستدعي تبني الأسلوب المناسب في التعامل معها (Marcelo Corrales&Other, 2018, p105) من قبل السلطات الأمنية.

ومما يزيد من خطورة تلك النوعية من الجرائم كونها جرائم تتسم بطابعها التقني، وسهولة ارتكابها، فضلاً عن صعوبة اكتشافها وملاحقة مرتكبيها، (سلامة، ٢٠٢٣، ص ٣٩١)، ففي وثيقة عمل أصدرها الانتربول أكد فيها على أن: التكنولوجيات الرقمية أصبحت محركاً للتنامي المطرد للجريمة السيبرانية ونماذج الجرائم الإلكترونية، كما أدى لتعدد أساليب السلوك الإجرامي، وتمكن الجناة من ارتكابها عابرين حدود الولايات القضائية (وثيقة عمل، مركز الابتكار بالانتربول ٢٠٢٢، ص ٩) لذا؛ تتفق الآراء على أن التعامل مع هذه النوعية من الإجرام وملاحقة الجناة يتطلب خبرات خاصة وفي ذات الوقت يفرض ضرورة الاستعانة بالتقنيات الحديثة في محاولة الكشف عنها والتحقيق بشأنها. (البرعي، ص ١٥٩٨).

وفي ذات الصدد يؤكد البعض، (العميري، ٢٠٢٢، ص ٤٦٤) على أن تقنيات الذكاء الاصطناعي لا بد وأن يكون له دور في التحري والتحقيق بشأن الجرائم التي ترتكب من قبل عصابات الجريمة المنظمة التي تعتمد على التقنيات في مباشرة أنشطتها الإجرامية، ومن هنا يجب تطوير تقنيات الذكاء الاصطناعي لغرض الاستعانة بها في حفظ الأمن، وكذا في مرحلتى جمع الاستدلالات والتحقيق الجنائي.

وفي ضوء ما تقدم سنحاول من خلال هذا المطلب أن نعرض بإيجاز لبعض السبل التي يمكن من خلالها الاستعانة بالذكاء الاصطناعي في البحث عن الأدلة الجنائية، ثم نعرض بعد ذلك لمشروعية إجراء التحقيق باستخدام تقنيات الذكاء الاصطناعي:

أولاً: وسائل الاستعانة بالذكاء الاصطناعي في البحث عن الأدلة:

تتعدد سبل الاستفادة من تقنيات الذكاء الاصطناعي في البحث عن الأدلة الجنائية، منها التحليل الجنائي الرقمي، استخدام الروبوتات، والطائرات دون طيار، وكذلك استخدام السيارات ذاتية القيادة، الكاميرات الذكية والتصوير ثلاثي الابعاد لمسرح الجريمة، إلى غير ذلك من الوسائل، وفيما يلي بيان سريع لأهما:

- التحليل الجنائي الرقمي بتقنيات الذكاء الاصطناعي:

التحليل الجنائي الرقمي هو عملية استعادة وتحليل المحتويات الموجودة على الأجهزة الرقمية كأجهزة الكمبيوتر بمختلف أنواعها، والهواتف الذكية، ويعرفها البعض بأنها مجموعة من الإجراءات تبشر من قبل الأجهزة المعنية لجمع البيانات الرقمية وتحليلها، بهدف الكشف عن الجريمة. (Zarza, 2015, p95: 98).

ويعتمد هذا النوع من الإجراءات على الدمج بين المعلومات الجنائية التقليدية وعلوم الحاسب الآلي والشبكات بهدف استخراج الأدلة من الأجهزة الالكترونية وشبكة الإنترنت والشبكات العصبية والوسائط الرقمية، من خلال تحليل كافة البيانات المتاحة، وهذه تقنية تعتمد على تقنيات الذكاء الاصطناعي بشكل أساسي، ويتم توظيف قدرات الذكاء الاصطناعي في تفتيش الأجهزة وجمع وترتيب المعلومات، ومن خلال تقنيات الذكاء الاصطناعي يمكن التوصل إلى الملفات المحزوفة. (البابلي، ٢٠١٩، ص ١٦٨).

- استخدام تقنيات الذكاء الاصطناعي في التعرف على البصمات الوراثية:

نظرًا لوجود الحمض النووي في جميع أجزاء الجسم البشري فإنه يسهل الحصول عليه، ويمكن استخدام الحمض النووي من قبل الطب الشرعي باعتباره بديلاً عن فحص عينات الدم، ومن أهم مزايا الحمض النووي سهولة تخزين الملفات التي تحتويه على أجهزة الكمبيوتر، ومن هنا اتجهت بعض الدول، كالمملكة المتحدة إلى انشاء قاعدة بيانات تضم السمات الوراثية، وهي قاعدة بيانات الحمض النووي للمخبرات الجنائية الوطنية.

(<https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1490298/>)

ويلعب الذكاء الاصطناعي دور بالغ الأهمية في مساعدة الطب الشرعي في هذا الشأن، حيث تساعد العلماء في تسريع عملية الحصول على النتائج، كما تستخدم تقنيات الذكاء الاصطناعي للحد من التناقضات البشرية والوصول إلى نتائج أكثر دقة، (المطروشى، ٢٠٢٣، ص ١٥) وباتت عمليات التعرف بفضل الذكاء الاصطناعي تتم تلقائياً ولذا؛ يؤكد العديد من الباحثين على ضرورة دمج نتائج الحمض النووي في قاعدة بيانات المواطنين، وتبادلها مع الأجهزة الأمنية، لكونه يفيد في حل القضايا، والتعرف على المفقودين ومجهولي الهوية، وكذلك الجناة المحكوم عليهم، ومن خلال ربط تقنيات الذكاء الاصطناعي بقواعد البيانات سيصبح من اليسير اكتشاف الجرائم التي وقعت، وكذا تحقيق نتائج دقيقة بشأن التنبؤ بما يُحتمل ارتكابه من جرائم. (علي، ٢٠٢٣، ص ١٦١٥).

وقد قامت كل من الصين والولايات المتحدة الأمريكية، وفرنسا بتشديد قاعدة بيانات محلية لمواطنيها، ويسمح لسلطات إنفاذ القانون أن تخزن فيها ملفات الحمض النووي للمواطنين، لتتمكن الشرطة فيما بعد من البحث عن الشخص الذي يكون قد ترك في مسرح الجريمة أى أثراً بيولوجياً من خلال مقارنته بما يوجد في قاعدة البيانات، كما ابتكرت الولايات المتحدة ما يعرف بنظام فهرس الحمض النووي المدمج. (Granja, 2020, p.57:60).

- تقنيات ذكية لتصوير مسرح الجريمة:

من بين تقنيات الذكاء الاصطناعي توجد أجهزة ذكية تسمح بحفظ الصورة أو تسجيل الفيديو بدقة متناهية يتم الاستعانة بها في تصوير مسرح الجريمة، دونما حاجة لجهاز كمبيوتر خارجي، وهو ما يسهل على إجراءات المعاينة العودة لمراجعة مسرح الجريمة لمراجعة الأدلة والآثار، ويحتوى الجهاز على كاميرا تعمل بالأشعة تحت الحمراء، بإمكانها تصوير كافة أشكال الأدلة التي من الممكن أن تتواجد في مسرح الجريمة. (اللوغاتي، ٢٠١٨، ص ٧٥: ٧٧)، (العمرين، ص ٤٦٥).

وفي الصين يتم الاستعانة بتقنيات الذكاء الاصطناعي على نطاق واسع في المجال الجنائي، إذ طورت برمجيات المراقبة التي تعمل باستخدام تقنية الخوارزميات، وهكذا يتم مطابقة الصور والأصوات مع أنواع أخرى من البيانات المسجلة مسبقاً في قاعدة البيانات، فضلاً عن استخدام الخوارزميات في مجموعات البيانات الموحدة لتحسين تطبيق القانون، ويقوم برنامج انفاذ القانون بمطابقة الصور ووسائل التواصل الاجتماعي مع Sharp Eyes وهو برنامج نظام سحابي تابع للشرطة الصينية، ومن خلال قاعدة البيانات يمكن للجهات ذات الاختصاص من متابعة الجناة ومخالفي القواعد القانونية المحتملين، وتعتبر الصين من أوائل الدول تقنية برمجيات المراقبة التي تعتمد على "خوارزميات الذكاء الاصطناعي". (عبد المجيد ٢٠٢١ ص ٢٤٩).

- استخدام البصمات الدماغية في التحقيق:

من خلال تقنيات الذكاء الاصطناعي يمكن استخدام البصمات الدماغية وهي عملية مسح للدماغ البشري، تستطيع التقاط تفاعلات دماغ المشتبه به أثناء استجوابه من قبل جهات التحقيق، ومن خلالها يمكن التثبت من علاقته بالجريمة المرتكبة، وهي قليلة التكاليف ولا تحتاج إلى وقت لإجراءها، ووفقاً لما يقرره البعض فإن هذه الوسيلة تختلف تماماً عن جهاز كشف الكذب، وقد استخدمت هذه التقنية بالفعل، ففي الهند تم الحكم على إحدى الطالبات بالسجن المؤبد لتسليمها لخطيبها السابق، حيث ثبت للقاضي خلال المداولات وإجراءات المسح الدماغى بأن المتهمه على دراية تامة بكيفية ارتكاب الجريمة، وتم الاعتماد على بصمة المخ باعتبارها دليلاً مشروعاً ضد المتهمه. (العمرين، ٢٠٢٢، ص ٤٧٠؛ رسلان ٢٠١٣، ص ١١١: ١١٢). كما تم استخدام هذه التقنية في الولايات المتحدة الأمريكية. (طابع، ٢٠١٦، ص ٢٣٢ وما بعدها)

ثانياً: مشروعية إجراء التحقيق من قبل تقنيات الذكاء الاصطناعي:

تشير بعض الدراسات إلى أن العديد من دول العالم تتجه لاستخدام الروبوتات المستقلة في العمل الأمنى، في سبيل الاعتماد على عناصر شرطية غير بشرية ومستقلة تماماً يمكن الاعتماد عليها في المواقف التي تنطوى على مخاطر، كتفكيك العبوات الناسفة، وفي هذا الإطار أعلنت شرطة دبي عام ٢٠١٧ عن اطلاق أول روبوت للتوعية بمخاطر المخدرات بأسلوب مبتكر. (علاى، ٢٠٢٣، ص ٣٩٤).

في يناير ٢٠٢٢ نشرت صحيفة الخليج تقريراً جاء فيه، " طور باحثون من الأكاديمية الصينية للعلوم في الصين روبوتاً يعمل «محققاً جنائياً» يحدد الجرائم، ويوجه التهم ضد المشتبه فيهم بدقة تزيد على ٩٧٪. وقد أمضوا الفترة ٢٠١٥ و ٢٠٢٠ في تدريبه باستخدام أكثر من ١٧ ألف قضية جنائية مختلفة. وبحسب ما ورد، يمكن للذكاء الاصطناعي أن يتهم المشتبه فيهم باستخدام ١٠٠٠ «سمة» مختلفة مشتقة من وثائق حالة وصفها الإنسان. وذكروا إن استخدام برنامج الذكاء الاصطناعي المتقدم في الروبوت يعمل

على بعض الجنايات الأكثر شيوعاً، بما في ذلك الاحتيال والسرقة والقيادة الخطرة، وإعاقة العدالة وإدارة عمليات المقامرة غير القانونية، وفي الوقت المناسب، يأمل الفريق في تحسين الذكاء الاصطناعي، مما يسمح له بإكمال مهام أكثر تعقيداً مثل التعرف على الجرائم غير الشائعة، وتوجيه تهم متعددة ضد مشتبه فيه واحد".

(<https://www.alkhaleej.ae/>)

وفي دولة الامارات الامارات، وفي أواخر أكتوبر ٢٠٢١ تم كشف النقاب عن أول روبوت للتحقيق في جرائم الأطفال، وصرحت القيادة العامة لشرطة أم القيوين إن الروبوت مارس عمله كفترة تجريبية مدة ٣ سنوات، لافتة إلى أنه "حقق نتائج مبهرة في التحقيق في الجرائم الواقعة على الأطفال". وعن طبيعة اللغة التي يتحدث بها "روبوتوك" أثناء التحقيق، قالت شرطة أم القيوين إنه يمكنه التحدث باللغتين العربية والإنجليزية، بجانب استخدامه اللهجة المحلية. وأوضحت أن الروبوت لديه القدرة على الكشف عن حالات الأطفال النفسية، ويمكنه تغيير تعابير وجهه ٣٦٠ مرة، وهو ما يمكنه أن يؤدي إلى طمأنينتهم أثناء التحقيق. وأوضحت أن روبوتوك يمكنه معرفة من قام بالتحقيق معهم، عن طريق "تقنية «تمييز الوجه» وقراءة تعابير، ونطق الأسئلة المكتوبة لتوجيهها للطفل من خلال شاشات التحكم، وعرض صور المشتبه بهم من خلال جهاز آي باد". (<https://gate.ahram.org.eg/News/3002564.aspx>).

وفي الإمارات أيضاً شهد عام ٢٠١٧ الإعلان عن استخدام أول شرطى آلى، (سيد، ٢٠٢١، ص ٨٤) وتم استخدام الروبوت في تلقى البلاغات والشكاوى، وسماع أقوال الشاكي، ومن ثم إرسال البلاغ إلى غرفة العمليات، كما تم استخدام الروبوت في التحفظ على الجناة، واجراء معاينات لمسرح الجريمة، (العجماني، ٢٠٢٣، ص ٦٢٢).

كما استخدمت شرطة دبي طائرات التدخل السريع وهي طائرات دون طيار تضم أحدث الوسائل في نظام بث صفارات واسعة المدى وهي الأولى من نوعها، ووفقاً للقانون ٤ لسنة ٢٠٢٠ بشأن تنظيم الطائرات بدون طيار في دبي، فإن الطائرات دون طيار تستخدم في العديد من المجالات، ومنها: تقديم الخدمات العامة، والرقابة والتفتيش في عدة مجالات، كمراقبة الحركة المرورية، والتأمين الجوى للفاعليات.(بوابة دبي التشريعية).

نستخلص مما تقدم أن الاستعانة بالروبوتات في مجال الإجراءات الجنائية بات أمراً واقعاً، وهو ما يثير التساؤل حول مشروعية تولى الروبوت لعملية التحقيق برمتها وإصدار القرار؟ في معرض الإجابة عن هذا التساؤل ذهب البعض للقول بأن معظم التشريعات قد اعترفت بأنظمة الذكاء الاصطناعي وقدرتها على القيام بأعمال، كإبرام العقود، تحت مسمى الوكيل الإلكتروني، وبالتالي يسهل تطبيق ذلك في القواعد الجنائية خاصة في مرحلتى الاستدلال والتحقيق، وإقرار نصوص في قانون الإجراءات تسمح بإجراء التحقيق من قبل تقنيات الذكاء الاصطناعي، وقيامها بدور المحقق في إدارة الاستجواب، وقياس سرعة اجاباته والتغيرات التي قد تطرأ على ملامحه، مع الاحتفاظ بصلاحيات اتخاذ القرار للعنصر البشرى. (العميريين، ٢٠٢٢، ص ٤٦٣).

ومن جانبنا لا ننفق وهذا الرأي وذلك لعدة أسباب، أولها غياب النص التشريعي الصريح الذي يبيح الاستعانة بهذه التقنيات في إجراء التحقيق، أن هذه التقنيات قد تستغل لأغراض غير مشروعة من قبل الحكومات الاستبدادية، من خلال تغذية الروبوت ببيانات متحيزة، كما أنه في حال الخطأ في إدخال البيانات وإن تم بطريقة غير عمدية فمن شأن ذلك الإخلال بافتراض البراءة، حيث سيؤدي حتماً لنتائج غير دقيقة، كما أن استخدام هذه التقنيات في التحقيق الجنائي يثير العديد من المخاوف لدى كثير من المدافعين عن حقوق الإنسان، لكونها ليست دائماً موثوقة في قراراتها. (عبد الكريم، ٢٠٢٠، ص ٩١٦).

٣. مخاطر استخدام الذكاء الاصطناعي من قبل الأجهزة الأمنية

يثير استخدام تقنيات الذكاء الاصطناعي في مجال العدالة الجنائية بوجه عام والتحقيقات الجنائية بوجه خاص العديد من الصعوبات، فالقاعدة العامة أن كافة الإجراءات الجنائية لابد وأن تتخذ في حدود مبدأ الشرعية هذا المبدأ الذي يقوم في الأساس على مبدأ افتراض البراءة، (سرور ، ١٩٩٩ ، ص ٥٥٣؛ سرور ٢٠٠٢ ص ٣٥).

فالسماح للجهات الأمنية أو السلطات المسؤولة في استخدام البيانات المخزنة لديها في الأغراض الأمنية قد يؤدي للمساس بالحقوق والحريات التي كفلها الدستور، كالحق في الخصوصية، كما أن الخشية من تحيز الخوارزميات الذكية قد ينطوي على إهدار لمبدأ أصل البراءة، ويضيف الفقه إلى ذلك إشكالية أخرى تتعلق بالدليل المستمد من تقنيات الذكاء الاصطناعي ومدى ما يحوزه من حجية، ومشروعية الحصول عليه. (على ٢٠٢٣، ص ١٦١٩).

ويعتبر البعض أن أبرز التحديات التي تواجه استخدام تقنيات الذكاء الاصطناعي في العمل الأمني يتمثل في وجوب قواعد تقرر مشروعية هذا الاستخدام وفقاً لما جرى عليه العمل في قانون الإجراءات الجنائية، كما أن استخدام هذه التقنيات يثير العديد من المخاوف التي تتعلق بحق الخصوصية، فضلاً عما قد يحدثه الاختراق الإلكتروني لبرمجة الذكاء الاصطناعي من مشكلات. (على، ٢٠٢٣، ص ٣٩٧: ٣٩٨).

وفي ضوء ما تقدم نحاول في هذا المبحث الوقوف على حدود وضوابط استخدام تقنيات الذكاء الاصطناعي في الاستدلال والتحقيق، ثم يلي ذلك الحديث عن مخاطر استخدام الذكاء الاصطناعي المتعلقة بالحق في الخصوصية، وذلك في مطلبين على النحو التالي:

٣، ١. حدود وضوابط استخدام تقنيات الذكاء الاصطناعي

في سبيل وضع الضوابط لاستخدام تقنيات الذكاء الاصطناعي في مجال العدالة الجنائية بوجه عام، فقد أصدرت المفوضية الأوروبية لكفاءة العدالة التابعة لمجلس الاتحاد الأوروبي ميثاقاً أخلاقياً تضمن خمسة مبادئ، وهي : احترام حقوق الإنسان الأساسية، عدم التمييز لتجنب تطوير الخوارزميات بشكل متحيز، الجودة وتمثل في الاعتماد على المصادر العلمية لتصميم الخوارزميات، الأمن ويتحقق من خلال الاعتماد على البيانات الأمنية من قبل الخوارزميات، وأخيراً الحياد والشفافية. (عبد الكريم، فهيل عبد الباسط ، ٢٠٢٢، ص ٩١٢).

وعلى مستوى العالم العربي، نجد أن المشرع الإماراتي قد أقر بعض النصوص التي تتعلق باستخدام تقنيات الذكاء الاصطناعي في بعض الجوانب التي تتصل بالشق الجنائي، ومن هذا القبيل ما نصت عليه المادة ٣٤ من القانون ٤ لسنة ٢٠٢٠ بشأن تنظيم الطائرات دون طيار في إمارة دبي، إذ تقرر أنه: " لضبط الأفعال المخالفة بواسطة الطائرات بدون طيار "

أ- لمأموري الضبط القضائي المختصين أن يطلبوا من النيابة العامة إذنًا لاستخدام الطائرات بدون طيار لأغراض البحث والتحري وجمع المعلومات والإيضاحات المتعلقة بالجرائم والمخالفات في الأماكن الخاصة، بناءً على معلومات جديّة.

ب- على مأمور الضبط القضائي أن يُرفق بطلب الإذن بالمراقبة باستخدام الطائرات بدون طيار محضراً يُدوّن فيه كافة المعلومات والتحريات التي دفعته لطلب استخدام الطائرة بدون طيار في الأماكن الخاصة.

ج- يُباشِر مأمور الضبط القضائي أعمال المراقبة باستخدام الطائرات بدون طيار بنفسه، وله في سبيل ذلك الاستعانة بغيره من الفنيين متى اقتضت أعمال المراقبة ذلك".

د- يُستثنى من الحصول على إذن النيابة العامة، حالات الضرورة التي تستدعي السرعة في ضبط آثار الجرائم أو الأدلة التي يُخشى طمسها أو ضبط مُرتكبي الجرائم حال التلبس بها أو حالات تهديد أمن وسلامة الدولة. (<https://dlp.dubai.gov.ae/Legislation>)

أما فيما يتعلق بالتنظيم القانوني لآخلاقيات الذكاء الاصطناعي بوجه عام، فإنه يمكن القول بأن المملكة العربية السعودية، ودولة الإمارات بوصفهما على رأس قائمة الدول العربية التي تولي اهتماماً خاصاً بالذكاء الاصطناعي، وتسعى كلتاهما إلى إحراز نتائج متقدمة في هذا المجال، فقد وضعتا مجموعة من الضوابط الأخلاقية، حيث أصدرت الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا) وثيقة مبادئ وأخلاقيات الذكاء الاصطناعي في سبتمبر من العام ٢٠٢٣م. وقد أكد المبدأ الخامس على ضرورة الالتزام بمعايير الموثوقية والسلامة، حيث يلزم أن يكون النظام موثقاً وأمناً من خلال عدم تعريض المجتمع للخطر، ويجب أن تكون لديه آليات مدمجة لمنع وقوع الضرر، لذا يرتبط إطار الحد من المخاطر ارتباطاً وثيقاً بهذا المبدأ، وينبغي على مسؤولي نظام الذكاء الاصطناعي العمل على تقليل المخاطر المحتملة والأضرار غير المقصودة إلى أدنى حد ممكن.

كما تضمن المبدأ السابع إرشادات المساءلة والمسؤولية، ويؤكد كذلك على ضرورة خضوع نظام الذكاء الاصطناعي للرقابة والإشراف البشري، (<https://sdaia.gov.sa/ar/default.aspx>) وهو ذات النهج الذي اتبعته الإمارات.

ويمكن القول أنه حتى الآن لا تتضمن التشريعات أي معالجة شاملة للجوانب المختلفة لتكنولوجيا الذكاء الاصطناعي، سواء فيما يتعلق بنطاق استخدامها في المجال الجنائي ومشروعيتها، أو فيما يتعلق بالمسؤولية الجنائية الناشئة عن استخدام هذه التقنيات؛ إذ إن معظم التشريعات اعتبرت أعمال البرامج امتداداً لمستخدميها الذين يسألون بشكل مطلق عن نتائج أعمالها، كما لو كانت صادرة مباشرة عنهم، لتساوي التشريعات في الحكم بين البرامج الأخرى التي تفتقد لخصائص الذكاء والاستقلالية والحركة.

وفيما يتعلق بأراء الفقه بشأن استخدام تقنيات الذكاء الاصطناعي فقد جاءت على النحو التالي: يرى الفريق الأول: أن التطور المتسارع لتقنيات الذكاء الاصطناعي يحتم على الجهات المعنية السعي لإعداد تشريعات قانونية تضبط استخدامها، وتحدد المسؤوليات في نتائج الممارسات والأعمال، لخلق بيئة استثمارية متطورة ورائدة في التقنيات التكنولوجية المرتبطة بالذكاء الاصطناعي. (علاوي ٢٠٢٢، ص ٤٠٠)

وقد ذهب فريق آخر إلى القول بأن استعانة مأموري الضبط القضائي بتقنيات الذكاء الاصطناعي في مرحلة الاستدلال، أو للتنبؤ بالجريمة من شأنه أن يمكن مأموري الضبط من اتخاذ الإجراءات التحفظية على وجه السرعة في حال وقوع الجريمة، أو الحيلولة دون وقوعها في حال كانت المعلومات تشير إلى قرب وقوعها (الشريف، ٢٠٢١، ص ٣٤٨).

بيد أن رأى آخر يعارض هذا التوجه، على اعتبار أن استخدام تقنيات الذكاء الاصطناعي في أعمال البحث والتحري أو التنبؤ بها سيؤدي بالضرورة للمساس بالحرريات، كما يمس بحرمة الحياة الخاصة، وهو ما يستدعي ضرورة حظر القيام بها من قبل مأموري الضبط؛ إلا بإشراف من الجهات المختصة بالتحقيق، أو بأمرها. (علي، ٢٠٢٣، ص ١٦٣٨).

وفي رأينا أن الاستعانة بتقنيات الذكاء الاصطناعي في مجال القانون الجنائي لا بد وأن يستند على تشريع قائم بضبط الممارسات ويوضح الإجراءات بشكل دقيق من أجل كفالة إحترام مبدأ الشرعية الجنائية وحفاظاً على الحقوق والحرريات.

وفي رأينا أيضاً أنه في ظل غياب النصوص التي تنظم حدود استخدام تقنيات الذكاء الاصناعي في مجال التحري عن الجرائم وجمع الأدلة والتحقيق فيها، فإن كل إجراء ينطوي على استخدام هذه التقنيات لا يستند إلى نص يعتبر إجراءً مخالفاً للقانون ويترتب عليه البطلان ووفقاً لما هو سائد في التشريعات اللاتينية، كما يحق للمتهم أن يطالب باستبعاد الدليل المتحصل بطرق غير مشروعة وفقاً للمتعارف عليه في النظام الأنجلو أمريكي. (الصلابي، ٢٠٢٠، ص ٢٤٢ ومابعداها).

2.3. مخاطر تقنيات الذكاء الاصطناعي وحماية الحق في الخصوصية

مفهوم الخصوصية:

في أول قانون صدر بالولايات المتحدة بشأن الخصوصية، عرف لويس براندز مصطلح الخصوصية بأنها: "حق الفرد في الحفاظ على معلوماته الشخصية وحياته الخاصة بشكل اختياري وحر" (مهنى، ص ٢٢٤). أى قدرة الشخص على حماية كافة ما يتعلق به من معلومات من الاطلاع عليها من قبل الآخرين وخصوصاً المنظمات والمؤسسات.

مخاطر التكنولوجيا المتعلقة بالخصوصية:

في ظل الثورة التكنولوجية التي يشهدها العالم، ومع الزيادة الكبيرة في استخدام الحواسيب والإنترنت، وتزايد الخدمات التي تقدمها هذه التكنولوجيا وتوسع إمكانياتها بشكل هائل. وما يحققه هذا التطور من مزايا عديدة، إلا أنه في المقابل، قد يشكل خطراً أمنياً جسيماً على الحق في الخصوصية. (محمد، سبتمبر ٢٠٢٣، ص ١٥٢)

وهذه المخاطر تتزايد وتتعاظم بمرور الوقت نتيجة التطورات المتلاحقة في المجالات التقنية، فمنذ ظهور التقنيات التي يطلق عليها "إنترنت الأشياء"، وهي عبارة عن شبكة من الأشياء التي تحتوي على تقنية مضمنة تسمح بالاتصال بالإنترنت، كما تشير إلى الاتصال الذي يحدث بين هذه الأشياء والأجهزة والأنظمة الأخرى التي تدعم الإنترنت، ويمكن أن تكون هذه الأشياء آلات أو مكونات مادية أو حيوانات أو حتى أشخاصاً. يسمح إنترنت الأشياء (IoT) بالاتصال بالإنترنت بما يتجاوز الأجهزة التقليدية، مثل أجهزة الحاسوب والهواتف الذكية، ويمتد إلى مجموعة متنوعة من الأشياء اليومية.

(<https://www.mcit.gov.sa/ar/iot>)

وكما يرى البعض فإن اتساع استخدام هذه التقنيات من شأنه أن تجعل كل ما يحيط بالإنسان متصلاً بالإنترنت، وهو ما ينتج عنه كم ضخم من البيانات الشخصية في كل لحظة تستخدم فيها هذه الأجهزة الذكية، كالصور، مقاطع الفيديو، والرسائل الإلكترونية، وسجلات المكالمات، وبيانات الخرائط، وهو ما سيؤدي بالضرورة إلى تحديد موقع الشخص، هواياته، اهتماماته، وكذا توجهاته الفكرية. (البرعى، ٢٠٢٢، ص ٥٠). ويتعاظم حجم التخوف بشأن انتهاك حقوق الإنسان عن طريق التشهير والتمييز والعنف والعنصرية حال التساهل في الحفاظ على البيانات الشخصية للأفراد، ونشر المعلومات والهويات بغير ضوابط من شأنه أن يؤدي لمشاكل كبيرة، (الصادق، ٢٠٢٣، ص) فقد اعتبر تقرير صادر عن الهيئة الهولندية لحماية البيانات

تعليقاً على انتبغ أثناء التصدى لجائحة كوفيد ١٩، أن استعمال تطبيقات تتبع الاتصال يشكّل انتهاكاً طويلاً الأمد للحق الأساسى فى الخصوصية، خاصة حتل معالجة معطيات لها علاقة بصحة المرضى، والتي تدخل ضمن المعلومات الحساسة. (تقرير ايسيسكو، الرابط التالى).

<https://www.bna.bh/.aspx?cms=q8FmFJgiscL2fwIzON1%2BDoxGYVcOLIDNr5z7fUg8U1E%3D>

يتفق الحق فى حماية البيانات الشخصية بالحق فى الخصوصية الرقمية وهو (التسليم بحق الأفراد فى التمتع بفسحة للتنمية الذاتية تقوم على مبدأ التفاعل والحرية أو حقهم فى مجال خاص يتسع لهم فيه التفاعل أو عدم التفاعل مع الآخرين دون الخضوع لتدخل الدولة أو تدخل زائد يمارسه أفراد آخرون بلا دعوة. أوجه الحماية لحق الخصوصية:

نظراً لأن المعالجة التشريعية للأمن المعلوماتى تقتضى وجود تشريعات تتعامل مع الجرائم الإلكترونية من ناحية، وتشريعات أخرى تضمن اقرار الحماية للبيانات الشخصية وتداولها، بما يسهم فى ضبط الأمن المعلوماتى فى الدولة. (رجب ٢٠٢٢، ص ١٢١: ١٢٢) فقد اتجهت كافة التشريعات إلى تبنى نصوص خاصة تكفل الحماية للبيانات الشخصية. ولا جدال فى أن الشريعة الإسلامية الغراء كان لها فضل السبق على كافة النظم الوضعية فى التأكيد على حماية الخصوصية بكافة ابعادها. (الحازمى، ٢٠٢٢، ص ٢٤٦٥) **موقف الاتحاد الأوروبى:**

يحمى الاتحاد الأوروبى البيانات الشخصية للأفراد التى تستخدمها سلطات إنفاذ القانون لمنع الجرائم الجنائية، أو التحقيق فيها، أو اكتشافها أو مقاضاة مرتكبيها، إذ تم اعتماد التوجيه الخاص بحماية البيانات الشخصية التى تتم معالجتها لأغراض منع الجرائم الجنائية عام ١٠١٦ ودخل حيز التنفيذ عام ٢٠١٨ (<https://www.consilium.europa.eu/en/policies/data-protection/data-protection-law-enforcement>)

ويهدف التوجيه بالأساس إلى حماية البيانات الشخصية للأفراد المشاركين فى الإجراءات الجنائية سواء كانوا شهوداً أو ضحايا أو مشتبه بهم. من خلال وضع إطاراً شاملاً لضمان مستوى عال من حماية البيانات، مع الأخذ فى الاعتبار الطبيعة المحددة لمجال الشرطة والعدالة الجنائية. وهو يساهم فى زيادة الثقة ويسهل التعاون فى مكافحة الجريمة فى أوروبا، من خلال تنسيق حماية البيانات الشخصية من قبل سلطات إنفاذ القانون فى الدول الأعضاء فى الاتحاد الأوروبى دول شنغن، ويعد التوجيه جزءاً من إصلاح حماية البيانات فى الاتحاد الأوروبى، إلى جانب اللائحة العامة لحماية البيانات (GDPR)، وتلتزم كافة الهيئات والمؤسسات والمكاتب التابعة للاتحاد الأوروبى بضمان تطبيق ما ورد باللائحة من نصوص، مع الأخذ فى الاعتبار أن اللائحة تطبيق لحماية البيانات الخاصة بالأشخاص الطبيعيين دون غيرهم، كما تنطبق على المعالجة بكل أشكالها ووسائلها.

(<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1725>)

وتضمنت اللائحة نصاً صريحاً يقرر تحمي هذه اللائحة الحقوق والحريات الأساسية للأشخاص الطبيعيين، ولا سيما حقهم فى حماية البيانات الشخصية (Art1, Subject matter and objectives) وتؤكد المادة ٥ من اللائحة على أن المعالجة لا تكون مشروعة إلا إذا كانت ضرورية لتحقيق الصالح العام أو تمت فى سياق ممارسة رسمية من قبل سلطة مختصة، أوجاءت المعالجة امتثالاً للالتزام قانوني، كما تقرر اللائحة أن المعالجة تكون مشروعة متى تمت بموافقة صريحة من صاحب البيانات. (Art.7).

ويمكن القول بأن غالبية الدول تتبنى تشريعات تقرر الحماية للبيانات الشخصية، (اللمعى، ٢٠٢٢، ص ١٤)، وكانت السويد من أولى الدول التى تبنت تشريعاً لحماية البيانات الشخصية (الفزعة، ٢٠٢٣، ص ١٦٠٤).

ثم تلتها باقى الدول الأوروبية، في حين فضلت الولايات المتحدة حماية البيانات الشخصية بطريقة تختلف عن النهج الذي اتبعته دول الاتحاد الأوروبي حيث تتعدد القوانين التي تتناول حماية البيانات في الولايات المتحدة بحسب المجال الذي تتعلق به البيانات

<https://www.unodc.org/e4j/ar/cybercrime/module-10/key-issues/data-protection-legislation.html>

والقاعدة العامة في القانون السويدي تقضى بأن البيانات الشخصية المتعلقة بالجرائم أو الإدانات الجنائية المشار إليها في المادة ١٠ من اللائحة الأوروبية العامة لحماية البيانات لا يمكن معالجتها إلا من قبل السلطات العامة، ووفقاً للقانون السويدي فإن قيام كاميرات المراقبة المثبتة في أحد المحلات بعرض تسلسل الأحداث على نحو أفضى إلى اكتشاف جريمة سرقة لا يعد خروجاً على القواعد المنظمة لحماية البيانات. (البيان التنظيمي الصادر عن الهيئة السويدية لحماية الخصوصية، ٢٠٢١).

<https://www.imy.se/globalassets/dokument/rattsligt-stallningstagande/imyrs-2021-1-lagovertradelser.pdf>

على الصعيد العربى:

اتجهت غالبية الدول العربية إلى تبني تشريعات خاصة لحماية البيانات الشخصية، وكانت تونس والمغرب من أوائل الدول التي سنت تشريعات خاصة لحماية البيانات الشخصية، وبعد صدور اللائحة الأوروبية لحماية البيانات اتجهت، السعودية، مصر، الإمارات، إلى إصدار تشريعات خاصة لحماية البيانات الشخصية، وقد تأثرت جميعها باللائحة الأوروبية إلى حد بعيد.

فقد أصدر المنظم السعودي نظام حماية البيانات الشخصية متضمناً أربعين مادة وقد خصص المادة الأولى لإيراد التعاريف وتحديد مفهوم المصطلحات لغرض تطبيق النظام^(١)، وفي ضوء هذه المادة عرف البيانات الشخصية بأنها: " كل بيان -مهما كان مصدره أو شكله- من شأنه أن يؤدي إلى معرفة الفرد على وجه التحديد، أو يجعل التعرف عليه ممكناً بصفة مباشرة أو غير مباشرة، ومن ذلك: الاسم، ورقم الهوية الشخصية، والعناوين وأرقام التواصل، وأرقام الرخص والسجلات والممتلكات الشخصية، وأرقام الحسابات البنكية والبطاقات الائتمانية، وصور الفرد الثابتة أو المتحركة، وغير ذلك من البيانات ذات الطابع الشخصي.

وتعليقاً على هذا النص اتجه رأى في الفقه^(٢) إلى أن النظام السعودي حينما ذكر عبارة " كل بيان أيًا كان مصدره أو شكله" في بداية التعريف قد قصد بذلك أن يمد مظلة الحماية على البيانات الشخصية بغض النظر عن طبيعة الدعاية المدونة عليها، بمعنى أن التعريف يشمل أيضاً حماية البيانات المدونة ورقياً، على عكس نهج المشرع المصرى في قصر الحماية على البيانات الشخصية المعالجة آلياً. (القانون ١٥١/٢٠٢٠). ويمكن القول بتفوق التشريع المغربى على معظم التشريعات العربية التي صدرت حديثاً، حيث منح المشرع بموجب قانون حماية المعطيات الشخصية رقم ٠٩٠٨ لسنة ٢٠٠٩ للأشخاص امكانية رفض القرارات القضائية الخوارزمية من ناحية، ومنحهم كذلك الحق في معرفة المنطق الذي يحكم كل معالجة آلية للمعطيات

(١) مجموعة الأنظمة السعودية المجلد الأول أنظمة الأمن الداخلي والأحوال المدنية والأنظمة الجنائية، نظام حماية البيانات الشخصية، مرسوم ملكي رقم (م/١٩) وتاريخ ١٤٤٣/٢/٩ هـ، منشور على الرابط التالي

<https://laws.boe.gov.sa/boelaws/laws/lawdetails/b7cfae89-828e-4994-b167-adaa00e37188/1>

(٢) د. ميادة مصطفى أحمد المحروقي، الحماية الجنائية لبيانات الأفراد الشخصية المعالجة إلكترونياً دراسة فى ضوء التشريعات الجنائية المقارنة واللائحة التنظيمية الصادرة عن البرلمان الأوروبي، المجلة القانونية، المجلد ١٦، العدد ٧، كلية الحقوق، جامعة القاهرة، فرع الخرطوم، مايو ٢٠٢٣، ص ١٤٨٨.

الشخصية التي تخصه. (<https://www.dgssi.gov.ma/ar/yhdf-hdha-alqanwn-aly-wd->)
(alatar-alqanwny-almnzm-lqta-albryd-walatsalat-alslkyt)

وإمعاناً في حماية الأفراد في مواجهة الآثار القانونية المترتبة على القرارات الخوارزمية، منح المشرع المغربي بنص المادة ٧/ج من ذات القانون، لأصحاب البيانات الحق في معرفة الآلية التي تحكم كل معالجة مؤتمنة للبيانات ذات الطابع الذاتي المتعلق به إذ جاء في هذه المادة علي أنه: "يحق للشخص المعني بعد الادلاء بها إثبات هويته أن يحصل من المسؤول عن المعالجة في فترات معقولة وعلي الفور ودون عوض علي ما يلي: ج- معرفة المنطق الذي يحكم كل معالجة الية للمعطيات ذات الطابع الشخصي المتعلقة به".

أما فيما يخص التشريع العراقي، فقد كان من المقرر إصدار تشريع خاص يقر بالحماية للبيانات، إلا أنه لم يصدر حتى الآن، بيد أن ذلك لا يعني أن التشريع العراقي لا يحمي البيانات الشخصية، إذ هناك العديد من النصوص التي تكفل الحماية، فقد أشار إليها الدستور العراقي ضمناً بموجب المادة ١٧ والتي تقرر كفالة الحق في الخصوصية، وكذلك في المادة ٤٠ التي تحظر التنصت على الاتصالات، أما النصوص التي تكفلت بحماية البيانات الشخصية في العراق، فمنها الماد ٧ من قانون الأحوال المدنية. إلا أن الفقه يجمع على أن صدور قانون خاص يكفل حماية البيانات الشخصية في العراق قد بات ضرورة حتمية. (راضى، ٢٠٢٢ ص ١٦٦).

ونؤيد ما ذهب إليه البعض من أن ما أقره المشرع المغربي من نصوص جدير بالثناء، وهي خطوة مهمة يرجى أن تراعى من قبل المشرع في كافة الدول العربية. (عبد المجيد ٢٠٢١ ص ٢٤٦).

وفي الختام نود الإشارة إلى أنه وعلى الرغم من تبني التشريعات العربية لتشريعات خاصة تحمي البيانات الشخصية إلا ما أقرته من استثناءات قد فرغها من مضمونها إلى حد بعيد، كما أن الجزاءات الجنائية المقررة كجزاء للإخلال بالنصوص التي تكفل حماية البيانات لا ترقى لتحقيق الردع العام أو الخاص، على عكس نهج المشرع الفرنسي الذي أورد نصوصاً جزائية رادعة تحقق الردع وتكفل احترام النصوص التي قررت الحماية، فضلاً عن أنه أورد الجزاءات ضمن نصوص قانون العقوبات الفرنسي.

الخاتمة:

على الرغم من المزايا العديدة التي حققها التطور التكنولوجي الهائل في العقدين الأخيرين إلا أن هذا التطور كان محفوقاً بالعديد من المخاطر، حيث نجم عنه ظهور العديد من أنماط السلوك الإجرامي، الذي يهدد أمن المجتمعات واستقرار الدول، كما أنه لا يتقيد بالحدود الجغرافية، ونظراً لاعتماده على التقنيات الحديثة فإن مكافحته تتطلب اجراءات خاصة تختلف تماماً عن الإجراءات المتبعة لمجابهة الإجرام التقليدي.

كما أن هذا النوع المستحدث من الإجرام يفرض العديد من التحديات على سلطات تنفيذ القانون، إذ تتطلب أن يكونا على أتم الجاهزية والاستعداد لمواجهة تلك الجرائم بكل ما هو متاح، فضلاً عن كونه يفرض عليهم عبئاً جديداً يتخطى الحدود الوطنية، ويتطلب يقظة متناهية ومهارات من نوع خاص.

وإذا كانت الجماعات الإجرامية تستغل التكنولوجيا في ارتكاب جرائمها، فليس من المعقول أن يحظر على القائمين بحفظ الأمن ومكافحة الجريمة الاستفادة من ذات التقنيات في محاولة للتصدي لهؤلاء المجرمين، بيد أن ذلك يثير إشكالية أخرى تتعلق بحقوق وحريات الأفراد، لذا؛ فلا بد أن تستند لمبدأ المشروعية.

ومن خلال هذا البحث حاولنا مناقشة كل ما سبق من اشكاليات ومخاطر، في محاولة لرسم تصور عام عن تقنيات الذكاء الاصطناعي ودورها في مكافحة الجريمة والوقاية منها.

حيث تعرضنا لسبل استخدام الذكاء الاصطناعي في مرحلة جمع الاستدلالات وبيننا بعض موقف الدول في تطبيقها والعمل بها، ثم موقف الفقه من مشروعيتها.

ثم تلى ذلك البحث في نطاق الاستعانة بتقنيات الذكاء الاصطناعي في مرحلة التحقيق ومدى مشروعيتها، ثم انتهينا لبيان المخاطر التي يثيرها استخدام تقنيات الذكاء الاصطناعي في الاستدلال والتحقيق على الحق في الخصوصية، ومساعي الدول للحد من هذه المخاطر.

وفي ختام هذا البحث قد توصلنا لمجموعة من النتائج والتوصيات نلخصها على النحو التالي:

4. النتائج:

- أصبح الذكاء الاصطناعي واقعًا وحقيقة وهو ما دفع العديد من الدول إلى الاستفادة منه في كافة مجالات الحياة.
- على الرغم من كل المنافع التي يقدمها الذكاء الاصطناعي إلا أن تطوره المتسارع قد كشف عن كم من المخاطر على الدول العربية أن تتيقظ لمجابهتها.
- أن الاستفادة الحقيقية من تقنيات الذكاء الاصطناعي ومواجهة ما يصاحبها من المخاطر لن تتحقق إلا من خلال بنية تشريعية قوية تتناسب وهذه التقنيات.
- هناك العديد من تقنيات الذكاء الاصطناعي يمكن الاستفادة منها في ملاحقة الجرائم ومرتكبيها بيد أنها في حاجة لغطاء قانوني.
- لا يوجد حتى الآن تشريعاً شاملاً ينظم استخدامات الذكاء الاصطناعي في مجال الإجراءات الجنائية.
- أن استخدام تقنيات الذكاء الاصطناعي في التحقيق وجمع الاستدلالات دون وجود نص يقر ذلك يشكل اختلاً لمبدأ الشرعية وإهداراً لمبدأ أصل البراءة.
- هناك العديد من المخاطر التي ينطوي عليها استخدام الذكاء الاصطناعي في التحقيق الجنائي.
- جاءت قرانين حماية البيانات الشخصية في معظم الدول العربية - باستثناء المغرب - متجاهلة لدور الذكاء الاصطناعي في معالجة البيانات.
- الحماية المقررة للبيانات الشخصية في التشريعات العربية تعد حماية ظاهرية، وقد تبنت جزاءات لا تحقق الردع ولا تكفل حماية فعالة.
- تأخر المشرع العراقي كثيراً في إصدار مجموعة من التشريعات باتت تفرضها الضرورة خاصة في ظل سعيه نحو التنمية والاستفادة من التكنولوجيا.

التوصيات:

- على الدول العربية التي تولى اهتماماً بالذكاء الاصطناعي الاسراع بسن التشريعات اللازمة التي تنظم استخداماته بموجب نصوص ملزمة، وعدم الاكتفاء بالمبادئ التوجيهية.
- ضرورة العمل على تعديل التشريعات المرتبطة بالبيانات الشخصية لتكفل حماية حقيقية وتبث الطمأنينة في نفوس المواطنين.
- أن احترام مبدأ الشرعية وافتراض البراءة يفرضان على المشرع ضرورة التدخل الفوري ووضع النصوص التي ترسم حدود الاستعانة بالذكاء الاصطناعي في التحقيقات الجنائية على نحو دقيق.

- يجب حظر الاستعانة بتقنيات الذكاء الاصطناعي من قبل الشرطة إلا بعد صدور قرار قضائي يمنحها هذا الحق حفاظاً على الحقوق والحريات.
- على المشرع أن يبذل جهداً في وضع نصوص تكفل التوازن بين حماية حقوق الخصوصية وبين حق الدولة في اتخاذ كافة الإجراءات لحفظ أمنها القومي، مع ضرورة تبني مفهوم واضح ودقيق للخصوصية يتناسب مع التطور التكنولوجي وعدم التقيد بالمفهوم التقليدي.
- يقترح أن يضع المشرع نصاً صريحاً يتضمن مجموعة من التقنيات التي يحظر استخدامها تماماً في التحقيق الجنائي نظراً لتعارضها مع مبدأ أصل البراءة.
- على القضاء في كافة الدول العربي إلى حين تدخل المشرع أن يؤكد على احترام مبدأ الشرعية الجنائية، من خلال استبعاده لكافة الأدلة المتحصلة نتيجة استخدام الذكاء الاصطناعي.

قائمة المصادر

- أبو خطوة، أحمد شوقي عمر (٢٠٢١)، المبادئ العامة في قانون الإجراءات الجنائية، دار النهضة العربية القاهرة.
- أبو عقيل، طارق السيد محمود (٢٠١٨) مرحلة ما قبل المحاكمة في الدعوى الجنائية الدولية، رسالة دكتوراه كلية الحقوق، جامعة بنها.
- أبو عقيل، طارق السيد محمود (٢٠٢٣) تقنيات الذكاء الاصطناعي ودورها في تسهيل الإرهاب الإلكتروني بحث مقدم لمؤتمر الذكاء الاصطناعي والقانون، كلية الحقوق، جامعة الزيتونة، الأردن، نوفمبر.
- البابلي، عمار ياسر محمد زهير (٢٠١٩) دور أنظمة الذكاء الاصطناعي في التنبؤ بالجريمة، مجلة الفكر الشرطي، المجلد ٢٨، العدد ١١٠، مركز بحوث الشرطة، أكاديمية شرطة الشارقة، الامارات.
- البابلي، عمار ياسر محمد زهير، (٢٠١٨)، الآليات الحديثة لحماية وتأمين نظم المعلومات وآثارها على المنظومة الأمنية، رسالة دكتوراه، كلية الدراسات العليا، أكاديمية الشرطة، القاهرة.
- البالول، نور سليمان يوسف يعقوب، (٢٠٢١)، الأحكام الموضوعية لجرائم المعلوماتية، دراسة مقارنة، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس.
- البرعى، أحمد سعد على (٢٠٢٢) تطبيقات الذكاء الاصطناعي والروبوت من منظور الفقه الإسلامى، مجلة دار الإفتاء المصرية، المجلد ١٨، العدد ٤٨، القاهرة.
- البيومى، رضا إبراهيم عبد الله (٢٠٢٣)، الحماية القانونية من مخاطر الذكاء الاصطناعي، دراسة تحليلية مقارنة، المجلة القانونية، المجلد ١٨، العدد ٣، كلية الحقوق، جامعة القاهرة، (فرع الخرطوم، مصر).
- الدويش، لولوه بنت محمد (٢٠٢٠)، العقوبات البديلة في التشريعات المقارنة والنظام الجزائي السعودي، المجلة الإلكترونية الشاملة متعددة التخصصات، العدد ٢٣.

الحازمي، حنان بنت عيسى بن علي (٢٠٢١) الحماية الجزائية لحرمة الحياة الخاصة في ظل التطور الرقمي في الشريعة الإسلامية والنظام السعودي، مجلة كلية الشريعة والقانون بتفهما الأشراف، العدد ٢٣ الاصدار الثاني ، الجزء الثالث، الدقهلية، مصر .

الصادق، عمرو رجب السيد، (٢٠٢٣)، أثر الذكاء الاصطناعي على القيم وحقوق الإنسان "الحق في حماية البيانات الشخصية"، مجلة بنها للعلوم الانسانية، العدد ٢، جزء ٤، مصر.

بهنام ، رمسيس، (١٩٨٤) الإجراءات الجنائية تأصيلاً وتحليلاً، منشأة المعارف، الإسكندرية. تحليل لاستشراف مستقبل العمل الشرطي، وثيقة عمل من إعداد مركز الابتكار بمنظمة الانترنتبول، النسخة ١، مارس ٢٠٢٢، على الرابط التالي:

حسن، محمد جبريل ابراهيم، (٢٠٢٢) المسؤولية الجنائية الناشئة عن مضار استخدام الذكاء الاصطناعي في المجال الطبي، مجلة الدراسات القانونية، مجلد ٨ ، عدد خاص، كلية الحقوق، جامعة السادات، مصر. حسنى، محمود نجيب، (٢٠١٩) شرح قانون الإجراءات الجنائية، الطبعة السادسة، تنقيح د. فوزية عبد الستار دار النهضة العربية، القاهرة .

حلال ،دونا (٢٠٢١) حلال، الذكاء الاصطناعي، رسالة ماجستير، كلية الحقوق والعلوم السياسية والادارية، الجامعة اللبنانية،

خليفة، ايهاب (٢٠١٩)، تأثير الثورة الصناعية الرابعة على الأمن القومي، مركز المستقبل للابحاث والدراسات المتقدمة، الطبعة الأولى، القاهرة.

دهشان، يحيى إبراهيم (٢٠٢٠)، المسؤولية الجنائية عن جرائم الذكاء الاصطناعي، مجلة الشريعة والقانون، المجلد ٣٤، العدد ٨٢، جامعة الامارات العربية المتحدة.

رجب، ياسر محمد عبد السلام (٢٠٢٢)، التطورات التشريعية المستحدثة في مجال الأمن المعلوماتي- دراسة مقارنة، المجلة العربية للمعلوماتية وأمن المعلومات، المجلد ٣، العدد ٦، المؤسسة العربية للتربية والعلوم والآداب.

سرور، أحمد فتحى، (١٩٩٩)، الحماية الدستورية للحقوق والحريات، دار الشروق، القاهرة.

سرور، أحمد فتحى، (٢٠٠٢)، القانون الجنائي الدستوري، الطبعة الثانية، دار الشروق، القاهرة.

سعد، وليد سعد الدين محمد (٢٠٢٢) المسؤولية الجنائية الناشئة عن تطبيقات الذكاء الاصطناعي، مجلة العلوم القانونية والاقتصادية، المجلد ٦٤، عدد ٢، كلية الحقوق، جامعة عين شمس.

سلامة، نسرين سيد (٢٠٢٣) الجرائم الالكترونية واثرها على المجتمع، مجلة القاهرة للخدمة الاجتماعية، المجلد ٣٩، العدد ٢، أبريل، القاهرة

سيد، محمد نور الدين، (٢٠٢١) التحديات الأمنية لاستخدام الذكاء الاصطناعي والأنظمة الرقمية في العمل الأمنى، وسبل المواجهة، مجلة العلوم الشرطية، القيادة العامة لشرطة الشارقة

الشريف، محمود سلامة عبد المنعم (٢٠٢١)، الطبعة القانونية للتنبؤ بالجريمة بواسطة الذكاء الاصطناعي ومشروعيته، المجلة العربية لعلوم الأدلة الجنائية، والطب الشرعي، المجلد ٢، العدد ٣، جامعة نايف، الرياض.

شمس الدين، أشرف توفيق، (٢٠٢٠) شرح قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة.
 صقر، فوزى محمد (أكتوبر ٢٠٢٠)، تدابير الضبط الإداري لمكافحة جرائم وسائل التواصل الاجتماعي، مجلة مصر المعاصرة، العدد ٥٤٠، الجمعية المصرية للاقتصاد السياسى والتشريع والإحصاء، القاهرة.
 الصلابي، سارة على (٢٠٢٠)، قاعدة استبعاد الأدلة غير المشروعة في الإجراءات الجنائية: دراسة تحليلي طابع، الهانى (٢٠١٦)، تقنية بصمة المخ في المجال الجنائي، دار النهضة العربية، القاهرة.
 عبد الكافي، اسماعيل عبد الفتاح (٢٠٢٠) الثورة الرقمية والذكاء الاصطناعي في القرن الحادي والعشرين، الدار الثقافية للنشر، القاهرة.

عبد الكريم، فهيل عبد الباسط، (٢٠٢٢)، دور التكنولوجيا الرقمية في تحقيق العدالة الجنائية: الفرص والتحديات مجلة جامعة دهوك، المجلد ٢٥، العدد ٢ (العلوم الانسانية والاجتماعية)
 العجماني، أحمد عبد الواحد (ديسمبر ٢٠٢٣) مدى مشروعية استخدام تقنيات الذكاء الاصطناعي في أعمال الاستدلال والتحرى عن الجرائم، مجلة جامعة الشارقة للعلوم القانونية، المجلد ٢٠، العدد ٤.
 علاى، عمار راشد، وآخر (ديسمبر ٢٠٢٣) استخدام تطبيقات الذكاء الاصطناعي في مجال التنبؤ بالجريمة والوقاية منها، مجلة جامعة الشارقة للعلوم القانونية، المجلد ٢٠، العدد ٤، الامارات العربية المتحدة.
 على، رزق سعد (سبتمبر ٢٠٢٣) استخدام تقنيات الذكاء الاصطناعي وتحليل البيانات في الكشف عن الجرائم مجلة الدراسات القانونية والاقتصادية، المجلد ٩، العدد ٣، كلية الحقوق، جامعة السادات، مصر.
 العميريين، وجيه محمد سليمان، (٢٠٢٢)، الذكاء الاصطناعي في التحرى والتحقيق عن الجريمة، دراسة مقارنة، مجلة الميزان للدراسات الإسلامية والقانونية، جامعة العلوم الإسلامية والقانونية، المجلد ٩، عدد ٣ جامعة العلوم الإسلامية العالمية، عمادة البحث العلمى.

عوضين، فايق (مارس ٢٠٢٢) استخدامات تقنيات الذكاء الاصطناعي بين المشروعية وعدم المشروعية الجزء الأول، ماهية الذكاء الاصطناعي ومجالات استخداماته الأمنية، المجلة الجنائية القومية، المجلد ٦٥ العدد ١، المركز القومى للبحوث الاجتماعية والجنائية، القاهرة.

فريد ويرنر، (٢٠٢٠)، الذكاء الاصطناعي من أجل تحقيق الصالح العام- خان الوقت من أجل التغيير، ITU News Magazin, No2، الرابط التالي على الانترنت
 في الاجتهاد القضائي للمحكمة الأوروبية لحقوق الإنسان، المجلة الدولية للقانون، المجلد ٩، العدد ٢، كلية القانون، دار نشر جامعة قطر.

محارب، عبد العزيز قاسم (سبتمبر ٢٠٢٣)، الذكاء الاصطناعي والأمن السيبراني، مجلة المال والتجارة العدد ٦٥٣، نادى التجارة، القاهرة.

محمد، هالة محمد امام (٢٠٢٣)، خصوصية البيانات في عصر البيانات الضخمة، نظرة قانونية، المجلة الأمريكية الدولية للعلوم الانسانية والاجتماعية، العدد ١٧، الجزء ٢.

القرعة، محمد السعيد، (٢٠٢٣)، المواجهة الجنائية للمعالجة والاستغلال غير المشروع للبيانات الشخصية على ضوء القانون ١٥١ لسنة ٢٠٢٠، المجلة القانونية، المجلد ١٨، العدد ٣، كلية الحقوق، جامعة القاهرة، فرع الخرطوم.

المعنى، ياسر محمد (٢٠٢٢)، السياسة الجنائية المعاصرة في حماية خصوصية البيانات الشخصية الإلكترونية مجلة وح القوانين، العدد ٩٧، كلية لحقوق، جامعة طنطا، مصر.

المسلماني، محمد أحمد ابراهيم (٢٠١٧) النطاق القانوني لسلطة الضبط الإداري في الظروف العادية والاستثنائية، دراسة مقارنة، دار الفكر الجامعي، الاسكندرية.

مصبح، عمر عبد المجيد (٢٠٢١) توظيف خوارزميات العدالة التنبؤية في نظام العدالة الجنائية: الآفاق والتحديات، المجلة الدولية للقانون، مجلد ١٠، العدد ١، كلية القانون، جامعة قطر.

المطروشي، سعيد سالم محمد، (٢٠٢٣)، دور الذكاء الاصطناعي في تحديد البصمة الإجرامية، مجلة العلوم الشرطية، المجلد ١٥، العدد ١، أكاديمية شرطة الشارقة. الامارات

مهني، محمود محمد محمد (٢٠٢٢) استخدام التسويق الإلكتروني لتطبيقات تكنولوجيا الذكاء الاصطناعي وتحليل البيانات الضخمة وتأثيره على الخصوصية في العصر الرقمي، مجلة مستقبل العلوم الاجتماعية الجمعية العربية للتنمية البشرية، مجلد ٨، العدد ٣.

ناظم، الزهيري طلال (مارس ٢٠٢٣)، مبادرات الحوكمة الإلكترونية في العراق و عوامل نجاحها، مجلة الحوكمة، المسؤولية الاجتماعية والتنمية المستدامة، المجلد ٥، العدد ١، جامعة غليزان، الجزائر.

ياسين، صباح رمضان، (شباط ٢٠٢٢)، تداعي وظيفة الردع إزاء المجرم المعلوماتي، مجلة الباحث، المجلد ٣، جامعة سوران، كردستان، العراق.

المراجع الأجنبية:

Akerkar Rajendra.(2019), Artificial Intelligence for Business, Springer Nature.

Andy Greenberg. (Aug. 22, 2018). The Untold Story of NotPetya, the Most Devastating Cyberattack in History, At: <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>

Galdon Clavell, G. (2016), ‘Policing, Big Data and the Commodification of Security’, in van der Sloot, B., Broeders, D. and Schrijvers, E. (eds) 2016 Exploring the Boundaries of Big Data, Netherlands Scientific Council for Government Policy (WRR) Report, Amsterdam: Amsterdam University Press.

<https://view.ckcest.cn/AllFiles/ZKBG/Pages/875/2019-08-07-AICounterterrorism.pdf>

Kathleen McKendrick,(2019) International Security Department, Research Paper, August, Chatham House,At:

Lilian Edwards, (2016), Privacy in Public Spaces: What Expectations of Privacy Do We Have in Social Media Intelligence? International Journal of Law and Information Technology.Vol, 24(3)

Machado.H &Granja R.2020, Forensic Genetics in the Governance of Crime, Palgrave Macmillan,

Av,

at:

<https://library.oapen.org/bitstream/handle/20.500.12657/23264/1006892.pdf?sequence=1&isAllowed=y>

MARC PFEIFFER , (SEP 21, 2023), First, Do No Harm: Algorithms, AI, and Digital Product Liability, At: <https://www.techpolicy.press/first-do-no-harm-algorithms-ai-and-digital-product-liability/>

Marcelo Corrales • Mark Fenwick Nikolaus Forgó (2018), Robotics, AI and the Future of Law, Springer Nature Singapore Pte Ltd

Moritz Goldener, Cornelius Herstatt, Frank Tlietze,(March 2015) “The emergence of care robotics – A patent and publication analysis”, Technological Forecasting and Social Change, Vol. 92,

Oscar H. Gandy Jr.(2010) Engaging rational discrimination: exploring reasons for placing regulatory constraints on decision support systems.

Peter J.F. Lucas & Linda C. van der Gaag(2014), Principles of Expert Systems, Peter Lucas, January, 2014

مواقع الانترنت:

<https://www.bna.bh/.aspx?cms=q8FmFJgiscL2fwIzON1%2BDoXGYVcOLIDNr5z7fUg8UIE%3D>

<file:///C:/Users/dr%20tark/Downloads/AI%20Report%202018.pdf>

<https://u.ae/>

<https://www.un.org/counterterrorism/ar/international-legal-instruments>

[https://www.bbc.com/arabic/worldnews/2011/01/110116_us_iran_israel_stuxnet_nuke\)](https://www.bbc.com/arabic/worldnews/2011/01/110116_us_iran_israel_stuxnet_nuke)

<https://ibtekr.org/cases>

<https://www.marwanosman.net/blog/Artificial-Intelligence-in-Egypt>

<https://shafaq.com/a>

<https://hitex.tech/ar>

<https://www.rudawarabia.net/arabic/kurdistan/20082023>

<https://www.ncbi.nlm.nih.gov/pmc/articles/PMC149029>

<https://www.alkhaleej.ae>

<https://gate.ahram.org.eg/News/3002564.aspx>

<https://dlp.dubai.gov.ae/Legislation>

<https://sdaia.gov.sa/ar/default.aspx>

<https://www.mcit.gov.sa/ar/iot>

<https://www.consilium.europa.eu/en/policies/data-protection/data-protection-law-enforcement/>

<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1725>

<https://www.imy.se/globalassets/dokument/rattsligt-stallningstagande/imyrs-2021-1-lagovertradelser.pdf>

<https://www.dgssi.gov.ma/ar/yhdf-hdha-alqanwn-aly-wd-alatar-alqanwny-almnzm-lqta-albryd-walatsalat-alslkyt>

<https://www.unodc.org/e4j/ar/cybercrime/module-10/key-issues/data-protection-legislation.html>

Utiliser des techniques d'intelligence artificielle pour rechercher des preuves de crimes

Dr. Tarek El Sayed Mahmoud Yousef

Abstrait:

Dans le domaine du droit pénal, le recours aux techniques d'intelligence artificielle soulève de nombreux problèmes liés à la responsabilité pénale, à l'étendue de l'admissibilité de l'utilisation de ces techniques dans la lutte contre la criminalité et à la mesure dans laquelle leur utilisation affecte les libertés des individus.

Cette recherche vient mettre en lumière la licéité de l'utilisation des techniques d'intelligence artificielle par les services de sécurité pour maintenir la sécurité, ainsi que dans le domaine de la prévision et de la lutte contre la criminalité. À travers ce document, nous tentons d'exposer les manières d'utiliser les techniques d'intelligence artificielle pour extraire des preuves de crimes et l'étendue de leur légitimité.

La recherche aborde également l'exposition aux risques liés à l'utilisation de l'intelligence artificielle par les services de sécurité et son impact sur la protection du droit à la vie privée, tout en utilisant une approche analytique comparative.