جامعة نايف العربية للعلوم الأمنية
NAIF ARAB UNIVERSITY FOR SECURITY SCIENCES
تأسست ١٩٧٨ Est. 1978

Naif Arab University for Security Sciences
Arab Journal of Forensic Sciences & Forensic Medicine
المجلة العربية لعلوم الأدلة الجنائية والطب الشرعي
https://journals.nauss.edu.sa/index.php/AJFSFM

الجمعية العربية لعلوم الأدلة الجنائية والطب الشرعي
Arab Society for Forensic Sciences and Forensic Medicine

The Legal Nature and Legality of Crime Prediction by Artificial Intelligence

الطبيعة القانونية للتنبؤ بالجريمة بواسطة الذكاء الاصطناعي ومشروعيته

محمود سلامة عبد المنعم الشريف*

قسم القانون الجنائي، كلية الحقوق، جامعة الإسكندرية، مصر

Mahmoud Salama Abdelmoneim Elsherif*

Department of Criminal Law, College of Law, Alexandria University, Egypt

Received 4 Jun. 2021; Accepted 29 Sep. 2021; Available Online 30 Dec. 2021

Abstract

Predicting a crime before it occurs is not considered unseen, but rather a probable prediction, it may even be probable, concerned with analyzing a large amount of data according to algorithms prepared in advance for this purpose, that modern technology produced by artificial intelligence has had a great impact in aborting crime early. The fight against criminality is a necessary and vital matter that is renewed and developed according to the reality of its society, and the curtain does not fall - at the same time - on the jurisprudential theories that have always lurked with the criminal, sometimes analyzing him psychologically, sometimes socially, and sometimes biologically, in order to assess his criminal seriousness, and apply appropriate measures to prevent his return to crime. Once again, the algorithms - which are the backbone of AI - are taking on the task more precisely, faster, and cost less. However, the novelty of this method has added a kind of ambiguity in determining its legal nature and legality. With regard to the legal nature, we find that they are no more than security measures that are included in the duties of the arresting officers, because the prediction of a crime precedes its commission of course, and therefore

Keywords: Artificial Intelligence, Algorithms, Big Data, Crime Prediction, Predictive Police, Security Nature, Administrative Control, Inference.

المستخلص

التنبؤ بالجريمة قبل حدوثها، لا يُعد علمًا بالغيب، وإنما هو توقّع مُحتمل، بل قد يكون راجحًا، مناطه تحليل كم كبير من البيانات بموجب خوارزميات أُعدّت سلفًا لهذا الغرض، تلك التكنولوجيا الحديثة التي أنتجها الذكاء الاصطناعي، أصبح لها الأثر البالغ في إجهاض الجريمة مبكرًا. فمكافحة الإجرام أمر ضروري وحيوي يتجدد ويتطور بما يُناسب واقع مُجتمعه، ولا يُسدل الستار - في ذات الوقت - على النظريات الفقهية التي لطالما تربصّت بالمجرم، فتارة تُحللّه نفسيًا، وتارة اجتماعيًا، وتارة بيولوجيًا، حتى تُقيّم خطورته الإجرامية، وتُنزل عليه التدابير المناسبة لدرء عودته للإجرام مرة أخرى، فأصبحت الخوارزميات - التي تعد قوام الذكاء الاصطناعي - تضطلع بتلك المهمة بصورة أدق وأسرع، وتكلفة أقل. إلا أن حداثة تلك الوسيلة أضفت نوعًا من الضبابية في تحديد طبيعتها القانونية ومشروعيتها. فبالنسبة للطبيعة القانونية نجد أنها لا تتعدى كونها تدابير أمنية تدخل في صلب واجبات مأموري الضبط لأن التنبؤ بجريمة ما، سابقًا على ارتكابها بطبيعة الحال، ومن ثم لا يمكن أن يتخذ بصددها

الكلمات المفتاحية: الذكاء الاصطناعي، الخوارزميات، البيانات الضخمة، التنبؤ بالجريمة، الشرطة التنبؤية، الطبيعة الأمنية، الضبط الإداري، الاستدلال.

* Corresponding Author: Mahmoud Salama Abdelmoneim Elsherif
Email: elsherif.m.salama@gmail.com

doi: 10.26735/NGSO4969

إجراءات استدلال أو تحقيق أيًّا كان نوعها. أما فيما يتعلق بمشروعية استخدام الذكاء الاصطناعي في التنبؤ بالجريمة رغم أخطاره التي تمس الحق الدستوري في حماية البيانات الشخصية، فإن تلك الأخطار سرعان ما تتبدد في الحالة التي يضطلع فيها المشرع بسن حماية جنائية لتلك البيانات، فضلًا عن منح مأموري الضبط السلطة المقيدة المناسبة للتمكّن من تفعيل هذه التقنية الحديثة بغية الحد من الجرائم في المستقبل القريب.

no inference or investigation procedures of any kind can be taken regarding it. As for the legality of using artificial intelligence to predict the crime despite its risks affecting the constitutional right to protect personal data, however, those risks are quickly dispelled in the case in which the legislator is involved in enacting criminal protection for that data, as well as granting law enforcement officers the appropriate restrictive authority to be able to activate This new technology aims to reduce crime in the near future.

1. مقدمة

لا غروَ أننا نعيش اليوم عصرًا رقميًا، تلتقي فيه الرياضيات وعلوم الحاسب بطرق مُستحدثة [1] عدُ نواة تكنولوجيا الجيل السادس [2]، التي ربما تُؤثر على سلوك الفرد والجماعة من حيث تطور الجريمة، بذات القدر التي تُؤثر فيه على سُبل مُكافحتها.

ثمّة دراسات مُكثفة تتجه نحو كيفية تجميع البيانات الضخمة واستغلالها لمصلحة منظومة العدالة الجنائية، ولتجنُب مخاطر الأمن القومي، لاسيما مخاطر جرائم الإرهاب والجرائم المنظمة وغيرها [3]، الأمر الذي انعكس بدوره على عمل إدارات الشرطة لتكون أكثر تطورًا في استخداماتها للبيانات الحيوية، وبرامج التعرّف على الوجه، من خلال كاميرات المرور، وكاميرات السيارات، وقارئات لوحات الترخيص، ونظام تحديد المواقع العالمي [GPS]، تلك الوسائل التي تُنتج بيانات رقمية يُمكن دمجها وتحليلها ومعالجتها، لتحديد وتتبع الأفراد بُغية منع وقوع الجريمة [4]، وتحقيق السلامة والأمان [5].

تنعكس التكنولوجيا على القانون تأثرًا وتأثيرًا؛ الأمر الذي يتطلب أن يكون القانون مواكبًا لحركة التكنولوجيا الآنية، حتى يُحقق أعلى قدر من سُبل الحماية للمصلحة العامة، وتطوير منظومة العدالة الجنائية.

المقصود بتنبؤ الجريمة بواسطة الذكاء الاصطناعي

يُقصد بتنبؤ الجريمة، توقع حدوثها مُستقبلًا، بُغية الحيلولة دونها، وإذا كان المشرع المصري قد سنّ من الوسائل التقليدية ما يُحقق ذلك الهدف [6]، لا سيما التدابير الاحترازية التي تعد أوضح مثال للوسائل التقليدية في إجهاض الجريمة قبل ارتكابها بالنسبة للأشخاص ذوي الخطورة الإجرامية، كالإيداع في المصحات العقلية والمؤسسات العلاجية ومؤسسات الرعاية الاجتماعية، كذلك وضع الشخص تحت المراقبة، أو حظر إقامته في مكان معين، أو حظر ارتياد أماكن معينة وهكذا، كما سنّت بعض التشريعات العربية والمقارنة نظام وقف تنفيذ العقوبة بشروط معينة، ونظام الإفراج الشرطي، كذلك نظام الاختبار القضائي للمتهم - أو كما يُطلق عليه في فرنسا إرجاء النطق بالعقاب مع الوضع تحت الاختبار (l'ajournement avec mise à l'épreuve) - ذلك النظام الذي يحول قدر المستطاع بين المتهم وبين الإخلال بأحد الالتزامات التي أوجبتها عليه المحكمة في فترة الاختبار، ومن باب أولى عدم ارتكاب جريمة جديدة [7]، الأمر الذي يحدّ من خطورته الإجرامية بالنسبة للمستقبل [8].

بيد أن التكنولوجيا المُعاصرة قد اختزلت كل تلك الوسائل في تطبيقات ذكاء اصطناعي يُمكن من خلالها الكشف عن جرائم مُتوقع حدوثها في المُستقبل، وبمدة كافية تُمكّن السلطة المُختصّة من منعها، وترجع فكرة التنبؤ الخوارزمي للجرائم إلى الروائي الأمريكي «Philip K. Dick»، وقد اتسمت معظم أعماله بالخيال العلمي، لعلّ أهمها رواية «The Minority Report» التي نُشرت عام 1956 في مجلة "Fantastic Universe"، وتروي القصة قدرة ثلاثة أشخاص على التنبؤ بالجريمة قبل حدوثها، وأطلق عليهم الشرطة التنبئية [9] «Precrime».

وجدير بالذكر أن فكرة التنبؤ بالجريمة لم تأتِ محض الصدفة، أو بمجرد ظهور تقنية الذكاء الاصطناعي، وإنما كانت هناك محاولات جادّة من خبراء مُحترفين لتحديد مقدار أو درجة الخطورة التي يُمكن أن يُسببها بعض الأشخاص للمجتمع، من خلال تقييم مدى ميول الأشخاص للقيام بأعمال عدوانية - آنية أو مستقبلية - أو احتمالية استمرار خطورتهم على المجتمع بعد إطلاق سراحهم [10].

ومن ثم فالتنبؤ بالجريمة بصفة عامة، هو عملية الوقوف على سلوك مُستقبلي ينطوي على خطورة إجرامية لدى بعض الأفراد [11]، ويُتطلب أن يتم التنبؤ بحذر ودقة شديدين لأن التقييم الخاطئ قد يؤدي لإطلاق حرية متهم في الحالة التي يجب فيها الاحتراز منه، والعكس صحيح، فيجب التحقق والتثبت من المعلومات الشخصية الخاصة به [12]. وإذا كان هذا الأمر يتطلب في السابق مُحللين نفسيين وخبراء في علم الاجتماع الجنائي، فاليوم لا يحتاج سوى تطبيق من تطبيقات الذكاء الاصطناعي ليؤدي ذات المهمة بكفاءة ودقة أعلى، ووقت وتكلفة أقل.

إذًا السؤال المطروح هو، ما هي تطبيقات الذكاء الاصطناعي؟ وكيف تضطلع بتنبؤ الجريمة؟ بصيغة أخرى: ما مُتطلبات تطبيقات الذكاء الاصطناعي لتستشعر قرب ارتكاب جريمة ما مُزمع حدوثها في المستقبل؟

الذكاء الاصطناعي Artificial Intelligence (A. I.) ما هو إلا مُحاكاة لذكاء البشر، من خلال تطوير تقنيات تكنولوجية، قادرة على أداء العطاءات البشرية بشكل ذكي عن طريق استخدام احتمالات المنطق استنادًا إلى البيانات المزودة بها [13].

وُيشير البعض إلى أن الذكاء الاصطناعي، هو قدرة التقنيات التكنولوجية الحوسبية على إعطاء نتائج من خلال مُعالجتها التي تتسم فيها بذكاء الإنسان الطبيعي [14، 15]، ورغم أن هذه التقنية مصنوعة، فإنها تتمتع بقدرة على وضع الحلول للمشكلات بشكل منطقي صائب وسريع [16].

إذن علم الذكاء الاصطناعي يهدف إلى فهم طبيعة الذكاء الإنساني، عن طريق إنشاء تطبيقات مُخصصة [17]، قادرة على محاكاة السلوك الإنساني المتّسم بالذكاء [18]، فتلك التقنيات تُفكر، وتستنتج وتُعطي الحلول، بل وتتنبأ بالمستقبل أيضًا [19].

المكونات التقنية لتطبيقات الذكاء الاصطناعي

وحتى تضطلع تطبيقات الذكاء الاصطناعي بدورها في تنبؤ ارتكاب جريمة ما، يتطلب الأمر عِدّة مكونات تقنية، وهي:

أولًا _ الخوارزميات Algorithms

الخوارزميات هي قوام الذكاء الاصطناعي وأهم أركانه، وتعني مجموعة من المسارات والخطوات الرياضية المُتتابعة المتتالية اللازمة لحل مُشكلة ما، والمُعدّة برمجيًا لكي تُعطي نتيجة مُعينة اعتمادًا على مُعطيات ومُدخلات غُذيت بها [20]. وكلمة خوارزمية مُستقاة من اسم عالم الرياضيات الفارسي «محمد بن موسى الخوارزمي» في القرن التاسع، وهي باللغة اللاتينية «Algoritmi»، وتعني التسلسل الدقيق للخطوات المطلوبة للوصول لشيء معين، والتي يكمن استخدامها للفرز، والتصنيف، والتحليل، والتنبؤ[21].

جدير بالذكر أنه لا يُمكن لأنظمة الذكاء الاصطناعي التنبؤ بدون خوارزميات مُتخصّصة ومُعدّة لذلك، ويُمكن وصف تنبؤ الجريمة بواسطة برامج الذكاء الاصطناعي بـ[التنبؤ الخوارزمي للجريمة][22]. فالخوارزميات هي الأداة التي تستخدمها آلات الذكاء الاصطناعي في التنبؤ بالجريمة، من خلال مفاهيم الإحصاء، واكتشاف الأنماط، وتحليل البيانات الضخمة، وربط بعضها ببعض، وإعطاء النتائج [23].

ثانيًا _ البيانات الضخمة Big data

البيانات الضخمة، هي حجم هائل من البيانات يتم تغذية تطبيقات الذكاء الاصطناعي بها [24]، فالعلاقة طردية بين حجم البيانات من ناحية وإمكان توقع جرائم مستقبلية من ناحية أخرى [25]، فكلما تضخّمت البيانات سهُل التوقّع، وهي ذات الفرضية بالنسبة لذكاء الإنسان الطبيعي، فكلما ازدادت معلوماته أصبح بالقطع أكثر إدراكًا، وأكثر قُدرة على اتخاذ القرار الملائم.

ويوجد العديد من مصادر البيانات الضخمة، منها المصادر الناشئة عن إدارة أحد البرامج: سواء أكان برنامجًا حكوميًا أو غير حكومي، كالسجلات الطبية الإلكترونية وزيارات المستشفيات وسجلات التأمين والسجلات المصرفية وبنوك المعلومات وغيرها. كذلك المصادر التجارية: أو ذات الصلة بالمعاملات تعد مصدرًا آخر كالبيانات الناشئة عن معاملات بين كيانين، على سبيل المثال معاملات البطاقات الائتمانية والمعاملات التي تجرى عن طريق الإنترنت بوسائل منها الأجهزة المحمولة. والمصادر الأمنية: كسجلات المتهمين وكافة الإجراءات المتخذة قبلهم من محاضر وتحقيقات وأحكام سابقة. كما أن هناك مصادر تقنية معتمدة على شبكات أجهزة الاستشعار وأجهزة التتبع، كالتصوير بالأقمار الاصطناعية، وأجهزة استشعار الطرق، وأجهزة استشعار المناخ وتتبع البيانات المستمدة من الهواتف المحمولة والنظام العالمي لتحديد المواقع وغيرها. وهناك نوع آخر من المصادر وهو المتعلق بسلوك المجرم مثل مرات البحث على الإنترنت عن منتج أو خدمة ما أو أي نوع آخر من المعلومات، ومرات مشاهدة إحدى الصفحات المشبوهة على الإنترنت. وأخيرًا، مصادر البيانات المتعلقة بالآراء مثل التعليقات المجرم على وسائط التواصل الاجتماعي، مثل فيسبوك وتويتر وغيرها.

ومن الناحية التقنية يُمكن تصنيف البيانات الخام [Data clas-sification] التي يتم تزويد برامج الذكاء الاصطناعي بها إلى ثلاثة أنواع:

- بيانات مُهيكلة Structured Data: وهي البيانات المنظمة في جداول أو قواعد بيانات (Data Base).
- بيانات غير مهيكلة Unstructured Data: وتُمثل النسبة الأكبر من البيانات، وهي البيانات التي يتم الحصول عليها يوميًا من كتابات نصية وصور وفيديو ورسائل ونقرات على مواقع الإنترنت.
- بيانات شبه مهيكلة Semi-structured data: وتُعد نوعًا من البيانات المهيكلة إلا أن تلك البيانات لا تكون في صورة جداول أو قواعد بيانات [26].

ومن ثم تعد البيانات الضخمة هي الوقود بالنسبة للخوارزميات [27]، وهذا النوع من البيانات شديد الأهمية ليس لذاته، وإنما للغاية منه، إذ يُعد هو الوسيلة التي يتم استخدامها بواسطة الخوارزميات، لمسح وتصفية وفهم وتحليل وفرز ومعالجة البيانات [28]، فإذا اتسع نطاق البيانات بالنسبة لمجرم معين أصبح من اليسير تنبؤ ارتكابه للجريمة، ويدخل في مفهوم البيانات الضخمة كل ما يتعلق بنظريات علم الإجرام، والدراسات النفسية للمجرم، والجرائم التي ارتكبها من قبل، وأقواله من خلال المحاضر والتحقيقات، وبياناته الشخصية، والصحية، والاجتماعية والمالية، ونشاطه على وسائل التواصل الاجتماعي، ومحل سكنه، وبيانات عمله، وغيرها من بيانات كما سيتبين لاحقًا.

ثالثًا _ التعلّم العميق Deep learning

يُقصد بالتعلم العميق، هو قدرة الآلة أو التطبيق أو البرنامج على التعلم الذاتي والتلقائي من خلال البيئة المحيطة والتجارب السابقة [29]، ولعلّ التعلّم العميق هو مُستقبل تطبيقات الذكاء الاصطناعي لأنها تتطور ذاتيًا بدون تدخل برمجي، ويتكون لها منطقها الخاص في التحليل والتنبؤ [30].

إذن التعلم العميق، هو تقنية يُفرد لها الخوارزميات الخاصة بها، وتُزود بمجموعة ضخمة من البيانات، تكون قادرة على تحليلها إحصائيًا، وإعطاء نتائج مؤسّسة على منطق مُستساغ من تلقاء نفسها [31].

نخلُص مما سبق إلى أن الذكاء الاصطناعي هو الإناء الذي يحمل بداخله خوارزميات مُعدّة سلفًا لتحليل كم هائل من المعلومات، تلك الخوارزميات يتطور منطقها ذاتيًا مُزامنةً مع تراكم وتضخم البيانات للمجرمين أو المتهمين، عن طريق خاصية التعلّم الذاتي، لتعطي نتائج مُستقبلية دقيقة بتنبؤ إمكانية وقوع جريمة ما في المستقبل من عدمه.

بيد أن تطبيقات الذكاء الاصطناعي المعنية بالتنبؤ بالجريمة باتت واقعًا ملموسًا نظرًا لنجاعتها، فمن حيث الإحصاءات الجنائية التي سُجلت في المدن، قبل وبعد استخدامها لهذه التطبيقات التقنية، نجد أن العنف في شوارع مُقاطعة كينت "Kent" البريطانية مثلًا انخفض بنسبة 6% بعد تجربة برنامج "Predpol" لأربعة أشهر فقط [32]. كذلك انخفضت جرائم السطو المسلح بنسبة 19% في مدينة سنتا كروز "Santa Cruz" بولاية كاليفورنيا الأمريكية، وانخفضت جرائم السرقة بنسبة 4% في ستة أشهر فقط [33]، كما انخفض معدل الجريمة في المدن التي تحتضن تقنيات التنبؤ الخوارزمي للجريمة بنسبة 35% عن المدن التي لم تُفعّل تلك التقنية في الولايات المتحدة الأمريكية [34].

وانعكست فاعلية التطبيقات سالفة الذكر بطبيعة الحال على تضخم عدد أقسام الشرطة التنبؤية، ففي الولايات المتحدة الأمريكية - على سبيل المثال- أصبحت تلك الأقسام حتى عام 2016 خمسون قسمًا [35]. وأغلب دول أمريكا الشمالية، ستعتمد بشكل أساسي في المستقبل القريب على تطبيقات الذكاء الاصطناعي في تنبؤ الجرائم [36]، لا سيما لكشف جرائم ذوي الياقات البيضاء التي تفشّت فيها، كجرائم النصب من خلال بطاقات الدفع الإلكتروني [37]. فقد أصبح هذا التضخم في تبنّي أجهزة الشرطة لتطبيقات الذكاء الاصطناعي لتنبؤ الجريمة ظاهرة في البلدان المُتقدمة، الأمر الذي يعكس بالتبعية مدى أهمية وضع تلك التطبيقات بالنسبة لعلم الإجرام والجزاء من ناحية، والقانون الجنائي من ناحية أخرى.

وتتبدّى فاعلية التنبؤ الخوارزمي بالجريمة كذلك، في القدرة على الحدّ من الهدر في الوقت والمجهود في التنقيب والبحث، فتطبيقات الذكاء الاصطناعي تحتوي على خوارزميات لمطابقة الوجوه، والأصوات، والتعرّف بدقة على التصرفات الشاذّة التي تُنبئ عن احتمال وقوع جريمة ما، تلك التطبيقات تجعل الكاميرات المُثبتة في الطرقات العامة أكثر نجاعة [38] إذ يستحيل عملًا توفير القوة العاملة لتفريغ ورصد هذا الكم الهائل من الفيديوهات للتعرف على شخص المُجرم، كذلك توفيرًا للوقت، الذي يُعد العامل الحاسم في تفادى وقوع الجريمة قبل أوانها [39]. ويتم عرض التنبؤات على الخريطة الكترونية باستخدام مربعات مُرمّزة لونيًا على المناطق الأشد خطورة لحثّ مأموري الضبط على التواجد في تلك الأماكن [40].

أهمية البحث

تتبدّى أهمية البحث بالنظر إلى الطبيعة القانونية لاستخدام تطبيقات الذكاء الاصطناعي التي تضطلع بالتنبؤ بالجريمة، ومدى مشروعيتها من ناحية، وأثرها على الحماية الجنائية لبيانات الأشخاص التي يتم تحليلها ومعالجتها من خلال تلك التطبيقات من ناحية أخرى.

ومن ثم فللبحث أهمية نظرية تتجسّد في حدود وضع تلك التطبيقات في علم الإجرام والجزاء، وقانون الإجراءات الجنائية من ناحية. وأهمية عملية تكمُن في تعزيز الأداء الأمني من خلال التنبؤ الخوارزمي بالجريمة بُغية منعها قبل حدوثها [41]، وبخاصّة الجرائم شديدة الخطورة كالجرائم المنظمة وجرائم الإرهاب، فضلًا عن قلة التكلفة ودقّة النتائج من ناحية أخرى. وأخيرًا الحد من التوسع في الاشتباه الذي قد يطول أشخاصًا بُرآء لا علاقة لهم بالجريمة لمجرد الظن بهم [42، 43].

نطاق البحث

يدور نطاق البحث حول تحديد الطبيعة القانونية لتطبيقات الذكاء الاصطناعي المتُعلقة بالتنبؤ الخوارزمي للجريمة، فضلًا عن مدى مشروعية استعمال تلك الوسائل من قبل مأموري الضبط، والحماية الجنائية التي شمل المشروع بها تلك البيانات محل تطبيقات الذكاء الاصطناعي المتعلقة بالتنبؤ بالجريمة، من ثم يخرج عن نطاق البحث المسائل التقنية البحتة، كآلية تجميع ومُعالجة البيانات، وكيفية إنشاء الخوارزمية، وغيرها.

تساؤلات البحث

يُثير البحث عدّة تساؤلات، لعلّ أهمّها إشكالية كُنه التنبؤ الخوارزمي للجريمة، فهل يُمكن تأصيله إلى النظام القانوني للتدابير الاحترازية أو ينتمي إلى الإجراءات الاستدلالية، أو له طبيعة قانونية أخرى؟ وهل يرتبط تنبؤ الجريمة بواسطة تطبيقات الذكاء الاصطناعي بالصفة الإدارية أو القضائية لمأموري الضبط؟ وما مدى مشروعية استخدام تطبيقات الذكاء الاصطناعي للتنبؤ بالجريمة؟ وهل يتعارض استخدام تلك التقنية الحديثة من حيث تجميع وفرز ومعالجة البيانات مع الحماية الجنائية للبيانات الشخصية أم لا؟

وهل تؤثر مخرجات وتقارير تطبيقات التنبؤ الخوارزمي للجريمة على السلطة التقديرية للقاضي الجنائي في تحديد موقف المتهم، سواء بالإدانة أو البراءة أو التخفيف أو التشديد؟ وهل أحاط المشرع الجنائي المصري البيانات الشخصية التي تعد وقودًا ومحلًا لتطبيقات الذكاء الاصطناعي التي تضطلع بالتنبؤ بالجريمة بالحماية الجنائية اللازمة لعدم اختراقها أو إفشاء سريتها؟

هدف البحث

يستهدف البحث توجيه الأنظار نحو قادمٍ جديد - وهو تطبيقات الذكاء الاصطناعي وأثرها في تنبؤ الجريمة - يتطلب استجلاء وتحديد طبيعته القانونية، كذلك مُعالجة الإشكاليات الناشئة إثر تبنّي تلك التقنية الحديثة، فضلًا عن وضعها في علم الإجرام، ومدى الحاجة إلى استصدار تشريع جديد لينظمها من عدمه، وأخيرًا تحديد مدى مشروعية استخدام تلك التقنية الحديثة في العمل الشرطي.

2. منهج البحث وخطته

عمد البحث نحو تأصيل فكرة التنبؤ بالجريمة بواسطة تطبيقات الذكاء الاصطناعي من زاوية علم الإجرام والجزاء، والقانون الجنائي من خلال مُعالجة إشكالية الطبيعة القانونية لهذه التقنية الحديثة.

كذلك بيان مدى مشروعية التنبؤ الخوارزمي بالجريمة. ومن ثم قُسّمت الدراسة إلى مبحثين على النحو التالي: المبحث الأول: الطبيعة القانونية للتنبؤ الخوارزمي بالجريمة. والمبحث الثاني: مشروعية التنبؤ الخوارزمي بالجريمة.

3. المبحث الأول: الطبيعة القانونية للتنبؤ الخوارزمي بالجريمة

الطبيعة القانونية للتنبؤ الخوارزمي بالجريمة تقتضي التطرق إلى ثلاثة أنماط من الإجراءات حتى يمكن الكشف وبحق عن تلك الطبيعة القانونية لهذه التقنية الحديثة، وهم أولًا: التدابير الاحترازية، وإجراءات الاستدلال، ثم الإجراءات الأمنية المتعلقة بالضبط الإداري، في ثلاثة مطالب على النحو التالي:

3. 1. المطلب الأول: الطبيعة الاحترازية للتنبؤ الخوارزمي بالجريمة

انخرط الفقه في حقبة تاريخية طويلة إلى إيلام المجرمين والانتقام منهم نظير إجرامهم، فكان العقاب هو الوسيلة الوحيدة لتحقيق هذا الهدف، إلا أن ذلك لم يمنع من انتشار الجريمة ومعاودة ارتكابها، الأمر الذي نحا بالفقه [44] إلى ضرورة البحث عن كيفية تأهيل وإصلاح المجرم وإدماجه في المجتمع مرة أخرى، ويرجع الفضل في ذلك إلى المدرسة الوضعية التي وجهت أنظار الباحثين إلى دراسة شخصية المجرم [45]، وفي سبيل ذلك سُنّت مجموعة من التدابير الاحترازية التي تهدف إلى الحدّ من الخطورة الإجرامية لهؤلاء المجرمين، بحيث تكون حائلًا بينهم وبين ارتكاب الجريمة في المستقبل.

ويُقصد بالتدابير الاحترازية: «مجموعة الإجراءات التي تواجه الخطورة الإجرامية الكامنة في شخص مُرتكب الجريمة، والهادفة إلى حماية المجتمع عن طريق منع المجرم من العودة إلى ارتكاب جرائم جديدة» [46، 47].

والتساؤل المطروح في هذا السياق هو: ماذا لو استعانت أجهزة الشرطة بتطبيقات الذكاء الاصطناعي للتنبؤ الخوارزمي بالجريمة؟ هل يُمكننا إسقاط الطبيعة القانونية للتدابير الاحترازية عليها أم لا؟

للوهلة الأولى نجد ثمّة تماثُلًا كبيرًا بين الغاية التي تُحققها التدابير الاحترازية، وبين الغاية التي تُحققها تطبيقات الذكاء الاصطناعي، حيث إن كليهما يستهدف منع وقوع الجريمة بالنسبة إلى المستقبل [48]، بالإضافة إلى كونهما غير مُحددي المدّة بصفة عامة، حيث لا يُمكن بحال معرفة متى ستنقضي الخطورة الإجرامية للمحكوم عليه

حتى تنقضي بالتبعية التدابير المتُخذة ضدّه [49]، أو أن يتم مسح بياناته من على تطبيق الذكاء الاصطناعي لعدم جدواها وقتئذ.

كما تتسم كلتا الوسيلتين بطابع الإكراه والقسر [6, p. 405]، وعلى الرغم من أن العديد من صور التدابير الاحترازية تتمثل في تدابير علاجية أو الإيداع في مؤسسات للرعاية الاجتماعية، فإن توقيعها لا يتوقف على رضا الشخص المعني فهي تُطبق في مواجهته بصرف النظر عن قبوله أو رفضه، فهناك ضرورة تقضي بإنزال تلك التدابير على المحكوم عليه، ولعلّ معيار الضرورة المتُمثل في الحد من الخطورة الإجرامية، هو أيضًا الذي يُجبر مأموري الضبط القضائي على الالتجاء إلى التنبؤ الخوارزمي للجريمة، فلا أهمية تذكر لرضا الشخص الظنين، أو بالأحرى علمه.

القاسم المشترك بين التدابير الاحترازية، والتنبؤ الخوارزمي بالجريمة، يظهر كذلك في فكرة الاحتمالية، فالخطورة الإجرامية تستوجب الاستناد إلى علامات ظاهرة تجعل وقوع الجريمة التالية أقرب من عدم وقوعها، أي تجعل وقوع الجريمة التالية راجحًا، وعدم وقوعها مرجوحًا [50]، فالاحتمال يتحقق إذا أمكن الإحاطة بالكثير من العوامل الدافعة إلى ارتكاب الجريمة [51]، وأمكن التثبت أن هذه العوامل تقود عادة ووفقًا للمجرى العادي للأمور إلى إحداث الجريمة.

جدير بالذكر أن تقييم الخطورة الإجرامية للمتهم، واحتمالية ارتكابه لجريمة تالية يتحقق أيضًا من خلال خوارزميات التنبؤ بالجريمة، وتعطي - اعتمادًا على بيانات معينة - مؤشرًا إلى مدى الخطورة الإجرامية لشخص ما، بل ويُعتد بهذا التقييم في مراحل الإجراءات الجنائية المختلفة، ولعلّ تطبيق كومباس "COMPAS"، من أهم التطبيقات التي تحدد موقع الشخص من الخطورة الإجرامية. الذي يضطلع بقياس وتقييم درجة الخطورة الإجرامية لشخص ما اعتمادًا على خوارزميات تقنية تقوم بتحليل بياناته الشخصية [52].

بيد أن الاعتماد على تطبيق ذكاء اصطناعي لتحديد مدى الخطورة الإجرامية لشخص ما قد يثير مخاوف عدّة من بينها، مدى دقة تلك البيانات وعدم تحيزها أو اتسامها بالعنصرية، والأثر المترتب على الخطأ الوارد فيها في كل مرحلة من مراحل الإجراءات الجنائية، فضلًا عن دورها في بناء عقيدة القاضي الجنائي.

يُجاب عن الشكوك المثارة، بأن مقدار مخاطر التنبؤ الخوارزمي بالجريمة يختلف باختلاف المرحلة التي يُلجأ إليه فيها، عبر مراحل الإجراءات الجنائية، فإذا قدّرت تلك الخوارزميات أن شخصًا ما لديه خطورة إجرامية في مرحلة الاستدلال على غير الحقيقة، فإن تبعات هذا الخطأ لا تخرج عن كونها مجموعة إجراءات استدلال وتحريات تُتخذ في مواجهته، ثم يُطلق صراحه بعد ذلك إذا انتفت لديه الخطورة الإجرامية واقعيًا بعد سماع أقواله. أو حتى بعد التحقيق معه واستجلاء موقفه. إلا أن الوضع يزداد سوءًا في حالة ما إذا استعان القاضي الجنائي في مرحلة المحاكمة بخوارزميات تؤكد - على غير الحقيقة - أن المتهم الماثل أمامها يتوافر لديه خطورة إجرامية، ومن اليسير ضلوعه في مُعاودة ارتكاب الجريمة مرة أخرى، ويتم الحكم عليه جنائيًا بموجب تلك المعطيات، الأمر الذي قد يفوت على المتهم مزية تخفيف الحكم عليه، حتى وإن سلّمنا في نهاية المطاف بضمانة المتهم في استئناف الحكم الصادر في مواجهته.

وعلى الرغم من أن البعض قد لا يتصور أن تطبيقات الذكاء الاصطناعي تؤثر على عقيدة القاضي الجنائي في بناء حكمه، فإن الواقع يثبت لنا العكس، ولعلّ أوضح مثال على ذلك، ما حدث في ولاية ويسكونسن الأمريكية "Wisconsin"، ففي فبراير 2013، اتُهم شخص يُدعى إريك لوميس "Loomis"، بالمساهمة في جريمة إطلاق نار نفّذت من سيارة كان يقودها وقتئذ، وأسند إلى "لوميس" خمس تهم، ولكنه اعترف بالتهمتين الأخف وطأة، وهما جريمة الفرار من أحد ضباط المرور، والقيادة بدون ترخيص، وأثناء سماع أقواله استعان مأمور الضبط القضائي حينئذ بتطبيق كومباس "COM-PAS". الذي يضطلع بتقييم الخطورة الإجرامية للمتهم، وتقييم مدى فرصة عودته لارتكاب الجريمة في المستقبل، من خلال خوارزميات تعتمد على تحليل بياناته الشخصية، وأقواله في الإجابة عن 21 سؤالًا وجّه إليه، وقد صنّف هذا التطبيق بأن المتهم شديد الخطورة. وأرفق مأمور الضبط القضائي هذا التقييم بأوراق القضية، وأحيلت برمتها إلى المحكمة المختصّة، وحكمت المحكمة على المتهم في عام 2016 بالسجن لمدة ستِ سنوات مؤسِسّة حكمها على نتائج تقرير التطبيق الخوارزمي"COMPAS". طعن المتهم على الحكم واستند إلى أن استخدام المحكمة وبناء حكمها على هذا التطبيق الخوارزمي ينتهك حقه لسببين: أولهما: اعتماد هذا التطبيق على بيانات غير دقيقة من ناحية، ولا تعطي للمتهم الحق في الطعن عليها أو التظلم منها من ناحية أخرى، وثانيهما: أن القاضي لا يعلم منهجية تحليل هذا التطبيق للبيانات التي انتهت إلى تقييم خطورته الإجرامية بالنسبة للمستقبل، فضلًا عن كون اعتماد القاضي في حكمه على هذا التطبيق يعد أمرًا غير دستوري لأن بياناته المزود بها هذا التطبيق بيانات تتسم بالعنصرية. رفضت المحكمة الابتدائية طعن المتهم، وكذلك صدّقت محكمة الاستئناف على رفض الطعن، إلى أن وصلت الإجراءات إلى المحكمة العليا، وقضت في حكمها الصادر بتاريخ 26 يونيو 2017، برفض طعن المتهم، وتأكيد الحكم بحبسه، وعلّلت ذلك بأن ليس هناك أيّ انتهاك لحقوق المتهم في إجراءات الدعوى، ولا يجوز إفشاء

السرية التجارية المتعلقة بمنهجية تطبيق"COMPAS" في تحليل البيانات وتقييم الخطورة الإجرامية، كما أن التقييم اعتمد بشكل مباشر على السجل الجنائي للمتهم وصحيفة الحالة الجنائية الخاصة به وبأقواله [53].

رُبما من المهم أن نطرح التساؤل إذًا: هل تضطلع تلك القواسم المشتركة لإضفاء الطبيعة القانونية التي تتسم بها التدابير الاحترازية على وسيلة التنبؤ الخوارزمي بالجريمة؟

يُجاب عن ذلك التساؤل: بأنه على الرغم من الاعتراف بهذا التماثل، فإنه لا يرقى لحد التطابق، فالتدابير الاحترازية لها من السمات التي تُميزها عن تطبيقات الذكاء الاصطناعي في التنبؤ بالجريمة. ولعلّ من المناسب أن نرصد مظاهر الاختلاف بينهما على النحو التالي:

أولًا _ من حيث الخضوع لمبدأ الشرعية

فالثابت أنه لا تدبير إلا بالنص [51, p. 22] ، والعلّة من شرعية التدابير هو صون حريات الأفراد، ومن ثم لا يجوز البتّة توقيع تدابير غير منصوص عليها مهما كانت شخصية الفرد موحية بخطورته الإجرامية، كما أنه لا يجوز للقاضي الجنائي خلق تدابير جديدة لم يُشر إليها القانون [6, p. 406]. أما بالنسبة للجوء إلى تطبيقات الذكاء الاصطناعي فنظرًا لحداثته لم يتدخل المشرع المصري لتنظيمه قانونيًا، الأمر الذي يخرج به عن الطبيعة القانونية للتدابير الاحترازية إذ إن الحاكم في هذه المسألة هو مبدأ شرعية التدابير. وعلى الرغم من اتحاد العلّة بين كلتا الوسيلتين، فالتنبؤ الخوارزمي بالجريمة يمُس - بما لا يدع مجالًا للشك - بحقوق المحكوم عليه وحرياته الفردية. الأمر الذي يدفع إلى القول بخروج تطبيقات الذكاء الاصطناعي من عباءة الطبيعة القانونية للتدابير الاحترازية، ولا يقدح في ذلك اتحاد العلة لأن مبدأ شرعية التدابير يظل حائلًا لإعمال القياس بينهما.

ثانيًا _ من حيث الصبغة القضائية

إنزال التدابير الاحترازية على المحكوم عليه لا يكون إلا من جهة قضائية، فهو حق استئثاري للقضاء متى توافرت شروطه، من ثم لا يجوز لأي جهة إدارية أن تحكم على الشخص بتدبير احترازي مهما كشفت شخصيته عن خطورة كامنة [6, p. 406]. على العكس من ذلك فإن الجهة الإدارية - المُتمثلة في مأموري الضبط- هي التي تضطلع باستخدام تطبيقات الذكاء الاصطناعي في التنبؤ بالجريمة، في مرحلة سابقة وأولية بغرض تنبؤ الجريمة والحيلولة دونها قدر المستطاع، ثم استكمال إجراءات التحريات، ثم مرحلة التحقيق، وأخيرًا مرحلة المحاكمة. من ثم لا تصدق عليها الطبيعة القانونية التي تتسم بها التدابير الاحترازية، ولا تخضع لنظامه القانوني.

وقد يُرى للخروج من هذا المأزق، وبخاصة في الوضع الراهن الذي يفتقد لوجود نصوص قانونية تنظم عمل الشرطة التنبؤية في مصر، ولغرض إسقاط الطبيعة القانونية للتدابير الاحترازية عليها فتستظل بأحكامها وقواعدها، أن يمتد تفسير نص المادة 28 من قانون العقوبات المصري ليشمل تلك الوسيلة التقنية الجديدة، تلك المادة التي تنص على أن "كل من يُحكم عليه بالسجن المؤبد أو المشدد أو السجن لجناية مخلة بأمن الحكومة أو تزييف نقود أو سرقة أو قتل في الأحوال المبينة في الفقرة الثانية من المادة 234 من هذا القانون أو لجناية من المنصوص عليها في المواد 356 و368 يجب وضعه بعد انقضاء مدة عقوبته تحت مراقبة البوليس مدة مساوية لمدة عقوبته بدون أن تزيد مدة المراقبة على خمس سنين.

ومع ذلك يجوز للقاضي أن يخفض مدة المراقبة أو أن يقضي بعدمها جملة".

وعلى الرغم من أن نظام تنبؤ الجريمة بواسطة تطبيقات الذكاء الاصطناعي يتشابه مع نظام مراقبة البوليس، فإن هذا التشابه ظاهري، ولعلّ ذلك يرجع إلى أن هذا التدبير على وجه الخصوص يُعد بمثابة عقوبة في حد ذاته [54، 55]، وهو يتعارض مع كنه التنبؤ الخوارزمي للجريمة، فالأخير لا يُعد عقوبة بقدر ما يُعد وسيلة لمنع الجريمة في المستقبل. كما أن نظام مراقبة البوليس نطاقه أضيق من وسيلة التنبؤ الخوارزمي للجريمة إذ إن الحكم به محصورًا فقط في الجرائم الواردة بنص المادة آنف الذكر، فلا يمتد لجرائم أخرى حتى ولو كانت أشد خطورة. الأمر الذي يجزم بأن وسيلة التنبؤ الخوارزمي للجريمة أكثر مرونة وأوسع نطاقًا، وربما أكثر فاعلية ونجاعة.

أخيرًا من شروط إنزال التدابير الاحترازية، أن يرتكب الظنين جريمة سابقة [50, p. 106]، ويتأهب المجتمع للاحتراز منه حتى لا يرتكب جريمة تالية، أما تطبيقات الذكاء الاصطناعي فلا يتوافر بها ذات الشرط، فقد ينصب تنبؤها على شخص المجرم، أو على مكان الجريمة [البؤر الساخنة] [56]، أو على نوع الجريمة ذاتها، فهي أوسع في النطاق الموضوعي والشخصي.

نخلُص مما سبق إلى أنه من الصعوبة بمكان أن نُسقط الطبيعة القانونية للتدابير الاحترازية على وسيلة التنبؤ الخوارزمي بالجريمة، لعدة أسباب، أهمها عدم توافر ركن الشرعية بالنسبة لتلك التقنية الحديثة، كذلك لافتقاد الصبغة القضائية في الحكم بها، فضلًا عن أن نظام التدابير الاحترازية يعد أحد دروب الجزاء الجنائي، على خلاف التنبؤ الخوارزمي للجريمة. الأمر الذي يدفعنا إلى البحث عن طبيعة قانونية أخري ربما تتسق مع تلك التقنية الحديثة من حيث سماتها وخصوصيتها.

3. 2. المطلب الثاني: الطبيعة الاستدلالية للتنبؤ الخوارزمي بالجريمة

همّت مُعظم أجهزة الشرطة في البلدان المُتقدمة، بتبني فكرة تطبيقات الذكاء الاصطناعي لتنبؤ الجرائم المستقبلية، ولايزال الباحثون قابعون على تطوير تلك التطبيقات التي سيكون لها الأثر البالغ في الحد من الجرائم بأنواعها، ولعلّ أهم تلكُم التطبيقات وأشهرها هو تطبيق [Predpol] 4, p. 1001 ، الذي يستشعر أماكن الخطر - الأماكن الساخنة - التي يُزمع ارتكاب الجرائم فيها، كذلك التنبؤ بمرتكبيها من خلال تحليل كم هائل من البيانات والصور والفيديوهات، وغيرها - مثل المعلومات المتعلقة بوسائل التواصل الاجتماعي للشخص الظنين، وتاريخ الائتمان، ونشاط الإنترنت، والحالة الصحية، ومعلومات الحي الذي يقطن به، والصحيفة الجنائية. إذ تمثل تلك البيانات الأداة التي تمكّن التطبيق من إعطاء المؤشرات التي ترنو إلى تحديد نسبة احتمال ارتكابه جريمة معينة- بل ويُرسل إلى الدوريات الشرطية خرائط التنبؤ بواسطة الهواتف اللّوحية، كما يُعطي تلميحات وإشعارات بنِسب توقّع ارتكاب الجريمة كمًّا وكيفًا [57].

وإذا كنا قد انتهينا - في المطلب الأول - إلى صعوبة إلباس تقنية التنبؤ الخوارزمي للجريمة ثوب التدابير الاحترازية، فالسؤال المطروح هنا، هل تندرج تلك التقنية تحت عباءة الإجراءات الاستدلالية، من ثم تأخذ حكم أعمال الاستدلال والتحري التي يضطلع بها مأمور الضبط القضائي أم لا؟

من المسلم به أن الاستدلال يهدف إلى جمع عناصر الإثبات اللازمة لتحضير التحقيق الابتدائي [58]، وبالنظر إلى إجراءات الاستدلال على حدة نجد أنها ربما تستغرق وسيلة التنبؤ الخوارزمي بالجريمة بين طياتها، وتُعطي الحق لمأمور الضبط القضائي في مُباشرتها.

ففي إجراء التحريات على سبيل المثال، أجازت محكمة النقض المصرية لمأموري الضبط القضائي أن تجرى التحريات عن الوقائع التي يعلمون بها بأي كيفية كانت [59]، وتطبيقات الذكاء الاصطناعي المخصصة للتنبؤ بالجريمة، لا شك أنها إحدى الوسائل التي تبصر مأمور الضبط، وتحيط علمه بجريمة أوشكت أن تقع.

فضلًا عن ذلك فمن حق مأمور الضبط القضائي بصدد إجراء التحريات، الاستعانة بمعاونيه من رجال السلطة العامة والمرشدين السريين [p. 703 ,60]، فما الضير إذن من اللجوء إلى وسائل تقنية حديثة تقوم بذات العمل الذي يقوم به هؤلاء الأفراد؟ بل إن استخدام وسيلة التنبؤ الخوارزمي للجريمة تُجنب مأمور الضبط القضائي مغبّة الوقوع في الاستجواب متجاوزًا سلطته، حال حصوله على الإيضاحات اللازمة من جميع الأشخاص المتصلين بالواقعة ممن لديهم معلومات عنها لأن حدود سلطته تقف عند السؤال لا الاستجواب، وغايته هي معرفة المعلومات، وهي ذات الغاية التي تُقدمها تطبيقات الذكاء الاصطناعي [p. 24 ,54]، فالقياس هنا لاتحاد العلّة له محل من الإعراب.

وتتبدّى أهمية تطبيقات الذكاء الاصطناعي باعتبارها إحدى الوسائل المهمة ذات الطبيعة الاستدلالية، في إجراءات التحفظ على الأشخاص حيث نصت المادة 35 إجراءات جنائية مُعدلة بالقانون 35 لسنة 1973 على أنه في غير حالات التلبس إذا وجدت دلائل كافية على اتهام شخص بارتكاب جناية أو جنحة سرقة أو نصب أو تعدٍ شديد أو مقاومة لرجال السلطة العامة بالقوة أو بالعنف، جاز لمأمور الضبط القضائي أن يتخذ الإجراءات التحفظية المناسبة.

ولا غبار أن اعتبار مؤشرات تطبيقات الذكاء الاصطناعي في التنبؤ بارتكاب جريمة ما، أحد الدلائل التي تحمل على الاعتقاد بوقوع الجريمة ونسبتها إلى المتهم، فعلى سبيل المثال حينما يُعطي البرنامج إشعارًا بأن شخصًا معينًا يُتوقع ارتكابه جريمة سرقة في مكان معين، ويهمّ مأمور الضبط القضائي للتواجد في هذا المكان ويجد الشخص المذكور في حالة ارتباك واضطراب عندما يرى أمامه مأمور الضبط القضائي أو ينادي عليه، فيجوز للأخير التحفظ على هذا الشخص، واستكمال باقي الإجراءات الجنائية في مواجهته.

وطبقًا للمادة 29 من قانون الإجراءات الجنائية المصري، فإن لمأمور الضبط القضائي أثناء جمع الاستدلالات أن يسمع إلى من يكون لديهم معلومات عن الوقائع ومرتكبيها، وأن يستعينوا بأهل الخبرة ويطلبوا رأيهم شفهيًا أو بالكتابة، وإذا كان الاستعانة بالخبرة أمرًا مطلوبًا بل ومحمودًا في الإجراءات الجنائية، فليس هناك ما يمنع من الاستعانة بالوسائل التكنولوجية الحديثة لاسيما تطبيقات التنبؤ الخوارزمي بالجريمة لتحقيق ذات الغرض مثله مثل الاستعانة بالخبراء.

أخيرًا في حقيقة الأمر فإن استخدام وسيلة تطبيقات التنبؤ بالجريمة لا يُعد مساسًا بحريات الأشخاص أو بحقوقهم على خلاف التدابير الاحترازية، التي تقيد حرية المحكوم عليه بها، الأمر الذي يُقرّب الطبيعة القانونية لتلك التقنية الحديثة مع الطبيعة القانونية لإجراءات الاستدلال.

بناء على الحجج السابقة، فإن لجوء مأمور الضبط القضائي لاستعمال تطبيقات الذكاء الاصطناعي في التنبؤ بالجريمة لا يعدو كونه ذا طبيعة استدلالية، يُصدق عليه نظامها القانوني من حيث الضوابط الإجرائية والموضوعية حال استخدامها.

وعلى الرغم من محاولة تأصيل الطبيعة القانونية لتقنيات التنبؤ الخوارزمي للجريمة بواسطة تطبيقات الذكاء الاصطناعي، وردّها إلى النظام القانوني لإجراءات الاستدلال، فإن هناك منظورًا آخر قد يُفنّد تلك الحجج، ويرفع الصفة الاستدلالية من على تلك التطبيقات.

فبالنسبة للحجة الأولى التي استُند فيها إلى قضاء النقض، بقولها: إنه يجوز لمأموري الضبط القضائي أن تُجرى التحريات عن الوقائع التي يعلمون بها بأي كيفية كانت، ومن هذه الكيفية استعمال تطبيقات الذكاء الاصطناعي. يُعد إسقاطًا في غير محله، وذلك لأن كافة إجراءات الاستدلال تبدأ بعد ارتكاب جريمة ما وليس قبلها، وهو ما أكدته المادة 21 من قانون الإجراءات الجنائية المصري بنصها على أنه "يقوم مأمور الضبط القضائي بالبحث عن الجرائم ومرتكبيها، وجمع الاستدلالات التي تلزم للتحقيق والدعوى" الأمر الذي يتعارض مع تقنية التنبؤ الخوارزمي للجريمة. فإجراءات الاستدلالات قبل ذلك تكون واقعة على غير محل، مما يُفسد هذا المنطق ويعيبه. والقول بعكس ذلك يُعد افتئاتًا على مبدأ شرعية الإجراءات الجنائية الذي يرتكز على ثلاثة مبادئ: أولها: أن الأصل في الإنسان البراءة، ثانيًا: الضمان القضائي في الإجراءات الجنائية، أما ثالثًا: وهو الذي يعنينا في هذا المقام، فإن القانون مصدر لقواعد الإجراءات الجنائية. وباعتبار أن الاستدلال أحد الإجراءات الجنائية وأولها، فهو يبدأ بتزامن لارتكاب جريمة ما، أي في حالة التلبس، أو لاحق على ارتكاب جريمة معينة وفقًا للقواعد العامة [60]. ومن ثم يكون الاعتراف بالصفة الاستدلالية في استعمال تطبيقات الذكاء الاصطناعي من قبل مأمور الضبط القضائي متعارضًا مع مبدأ الشرعية الإجرائية. كما أن مقصد محكمة النقض في هذا المقام هو علم مأمور الضبط القضائي بجريمة ما بأي وسيلة من وسائل العلم كالإبلاغ أو من خلال مخبرين سريين، وليس اعتمادًا على برامج الذكاء الاصطناعي التي لم تكن في ذهن المشرع ولا محكمة النقض آنذاك.

أما الحجة الثانية التي استندت إلى أن تلك التقنية الحديثة يكون لها دور حال حصول مأمور الضبط القضائي على الإيضاحات في عدم الانزلاق إلى الاستجواب، أيضًا استنتاج معيب إذ إن الحصول على الإيضاحات يتطلب وقوع جريمة أولًا من ناحية، كما أنه إجراء قائم في كل الحالات من ناحية أخرى، وعلى فرض استخدام تقنية التنبؤ بالجريمة فإن ذلك لا يحول دون الحصول على الإجراءات حال وقوع الجريمة، والقول بعكس ذلك يعني أنه يُمكن الاستغناء عن إجراء الحصول على الإيضاحات باستخدام التطبيق الخوارزمي كبديل له، وهو غير مُستساغ عقلًا. وذات المنطق يُمكن إعماله بالنسبة لاستعانة مأموري الضبط القضائي بالخبراء حال التقصي عن جريمة معينة، فاستخدام تطبيقات الذكاء الاصطناعي لا يحول أيضًا دون اللجوء لسماع الخبراء.

أما الحجة الثالثة والمتعلقة بالتحفظ على الأشخاص استنادًا إلى نتائج برامج التنبؤ الخوارزمي للجريمة باعتبار الأخيرة من الدلائل الكافية، فهو تزيّد في غير محله حيث إن القول بذلك يعني أن المؤشر الذي يعطيه هذا التطبيق لا مجال للخطأ فيه، سواء على مستوى الخوارزميات، أو على مستوى البيانات، وهو أمر يتخلله صعوبة بالغة، بل وقد يتعارض مع الواقع، فعلى الرغم من أن الخوارزميات باتت تنتشر بشكل واسع جدًا [61]، فإنها ليست منزهة عن الخطأ؛ وأدل على ذلك بما ذُكر في تقرير راند"RAND" عن "مخاطر الذكاء الاصطناعي على الأمن ومستقبل العمل" [62]. الذي ذُكر فيه أن ضَعف البيانات المغذية لخوارزميات الذكاء الاصطناعي وتحيّزها مؤشر خطير ينعكس على النتائج لا مناص.

وفي الولايات المتحدة الأمريكية على سبيل المثال، اكتشف العلماء تحيُّزًا عنصريًا مُمنهجًا في تقدير الخطورة الإجرامية للأشخاص ذوي البشرة السوداء، بالرغم من أن الجرائم الأشد خطورة يرتكبها البيض. وتكشف الإحصاءات الجنائية أن المتهمين السود أكثر عُرضة لسوء التصنيف من المتهمين البيض بمقدار الضِّعف فيما يتعلق بالعود إلى الجريمة، على الرغم أيضًا من أن البيض الذين عادوا لارتكاب الجريمة مرة أخرى نسبتهم أعلى من السود بمقدار 63.2% [63].

كما أن تطبيقات الذكاء الاصطناعي التي تتنبأ بالخطورة الإجرامية لدى شخص ما، لا تعدو كونها شبهات ظنّية [22, pp. 5-6]، لا ترقى إلى حد الدلائل الكافية المعقولة التي تحمل على الاعتقاد بوقوع الجريمة ونسبتها إلى المتهم، ومن ثم تتعارض مع سلطة مأمور الضبط القضائي في التحفظ على الأشخاص.

أخيرًا القول بتطابق طبيعة إجراءات الاستدلال وطبيعة التنبؤ الخوارزمي بالجريمة، في أن كليهما لا يمسّ حريات الفرد -على خلاف التدابير الاحترازية التي تمس وتقيد حريات الأفراد- فيه مُغالطة كبيرة، فأعمال الاستدلال باعتبارها جزءًا من الإجراءات الجنائية تمس- بما لا يدع مجالًا للشك - الحرية الشخصية وغيرها من الحقوق والحريات عند مباشرتها قبل المتهم[64]، لذا لا يُسمح لمأمور الضبط القضائي باتخاذ أي إجراء يمس حقوق وحريات متهم إلا بعد إذن النيابة العامة [المادة 40 إجراءات جنائية والمادة 54 من الدستور المصري 2014]، باستثناء ما ورد في القانون بنص خاص، أو ما يدخل في نطاق سلطة الضبط القضائي وفقًا للقانون كما هو منصوص عليه في المادة 34 إجراءات جنائية مصري.

نخلُص مما سبق إلى أن التنبؤ بالجريمة من خلال تطبيقات الذكاء

الاصطناعي يخرج عن كنه الإجراءات الاستدلالية لأن ثمة تعارضًا زمنيًا بينهما. حيث إن كافة إجراءات الاستدلال لاحقة على وقوع الجريمة لا قبلها، فالتنبؤ بالجريمة بواسطة الخوارزميات سابق على كافة الإجراءات الاستدلالية، الأمر الذي يدفعنا للبحث عن طبيعة قانونية أخرى تتطابق مع فكرة التنبؤ الخوارزمي بالجريمة.

3. 3. المطلب الثالث: الطبيعة الأمنية للتنبؤ الخوارزمي بالجريمة

لمّا كانت وسيلة التنبؤ الخوارزمي بالجريمة بواسطة تطبيقات الذكاء الاصطناعي تخرج عن كونها ذات طبيعة احترازية من جهة، أو ذات طبيعة استدلالية من جهة أخرى، فليس معناه أنها تخرج عن الإطار القانوني، وإنما تميل إلى التمتّع بصفة إدارية [أمنية]، تدخل في صلب عمل هيئة الشرطة بموجب وظيفتها في الضبط الإداري حيث نصت المادة 3 من قانون هيئة الشرطة المصري المستبدلة بالقانون رقم 25 لسنة 2012 على أن "تختص هيئة الشرطة بالمحافظة على نظام الأمن العام والآداب، وبحماية الأرواح والأعراض والأموال، وعلى الأخص منع الجرائم وضبطها، كما تختص بكفالة الطمأنينة والأمن للمواطنين في كافة المجالات، وتنفيذ ما تفرضه عليها القوانين واللوائح من واجبات".

وتعهد الدول إلى سلطتها التنفيذية - المُتمثلة في هيئة الشرطة - بتنظيم المجتمع تنظيمًا وقائيًا، بحيث تضطلع بكفالة أمن المُجتمع واستباب النظام فيه [60, p. 65]، من خلال تدارك ومنع الأخطاء التي قد يرتكبها أحد الأفراد قبل وقوعها والتي يكون من شأنها الإخلال بالنظام العام في المجتمع [65].

ويُمارس الضبط من قِبل السلطة العامة بواسطة نوعين من الأنشطة، هما وظيفة الضبط الإداري، ووظيفة الضبط القضائي، فحيث تدور الوظيفة الأولى حول وقاية المجتمع من الجريمة وإجهاضها في مرحلة مُبكرة باتخاذ التدابير الأمنية اللازمة، تتجه الوظيفة الثانية إلى تعقّب الجريمة ومُرتكبيها بعد وقوعها بُغية تجميع أدلتها تمهيدًا للتحقيق فيها واستكمال إجراءات الدعوى الجنائية [66].

بناء عليه تدخل تدابير التنبؤ بالجريمة من خلال تطبيقات الذكاء الاصطناعي، ضمن الإطار المُحدد للضبط الإداري للشرطة، باعتبار أن كليهما يتغيّا مُهمة وقائية [60, p. 65]، تنحصر في المحافظة على النظام العام والحيلولة دون وقوع الجرائم، حيث يتوجه مأموريالضبط القضائي من خلال تلميحات وإشعارات تطبيق الذكاء الاصطناعي بالتواجد في البؤر الإجرامية لمنع وقوع الجريمة [67].

غني عن البيان، أن الضبط الإداري وظيفته تتلخّص في منع وقوع الجريمة باتخاذ كافة التدابير الوقائية والاحتياطات اللازمة لحماية الأفراد والمجتمع من خلال سلطات الضبط الإداري [68]، التي تتمثل في الأمن العام والصحة العامة والسكينة العامة [69]، ويرتئي الباحث أن الدور الوقائي للضبطية الإدارية يتعاظم في ظل السياسة الجنائية المعاصرة التي تضع الوقاية من الجريمة في المقام الأول من اهتماماتها، ولعلّ وسيلة تطبيقات الذكاء الاصطناعي التي تضطلع بالتنبؤ بالجريمة قبل حدوثها إحدى أهم الوسائل الفعّالة في إطار الضبط الإداري [, p.4869].

ولتأكيد الطبيعة الإدارية (الأمنية) لاستعمال تطبيقات الذكاء الاصطناعي لتنبؤ الجريمة يُمكن الرجوع لعدّة معايير، أولها: المعيار الشكلي، ويتجسد هذا المعيار في القائم بالعمل، فمن يضطلع بإعمال تلك التطبيقات هم مأموري الضبط القضائي بصفتهم الإدارية، وليست القضائية [70]. ثانيًا: المعيار الغائي، ومفاده أن الهدف من استعمال تلك التقنية الحديثة هو إجهاض الجريمة قبل وقوعها، أما إذا وقعت بالفعل فيدخل العمل في الضبطية القضائية وليست الإدارية [71]. ثالثًا: المعيار الوظيفي: فاللجوء إلى تطبيقات الذكاء الاصطناعي للتنبؤ بالجريمة مُتعلق بحفظ النظام العام فهو إجراء إداري وقائي، لا يهدف إلى البحث عن جريمة ارتكبت بالفعل [72].

ونظرًا لأهمية استعمال الوسائل التقنية الحديثة في إجهاض الجريمة من منبعها، لا سيما تطبيقات الذكاء الاصطناعي الآنف ذكرها، تتجه أنظار الدول لاقتنائها، لما تُقدمه من خدمة هائلة في التنبؤ بالجريمة، الأمر الذي ينعكس بالضرورة على الحدّ من الجرائم الخطيرة كالجرائم الإرهابية، والجرائم المنظمة وغيرها.

بيد أن دورة التنبؤ بالجريمة من خلال تطبيقات الذكاء الاصطناعي، تتطلّب في البداية تزويد قسم الشرطة ببيانات كبيرة "Big data"، متعلقة بأماكن الجريمة، أو متعلقة بالمجرم ذاته، حتى يتم تقييم خطورته الإجرامية، تعطي تلك البيانات مؤشر تقييم الخطورة الإجرامية لشخص ما من ناحية، كما يتم معالجتها من خلال خوارزميات معدّة للتنبؤ بالجريمة من ناحية أخرى، ولعل أهم تلك البيانات التي يتم تزويد تطبيق الذكاء الاصطناعي بها هي، الصحيفة الجنائية لشخص ما، والجريمة المرتكبة ودلالاتها الرمزية وجسامتها، وردود أفعال المذنب أو أهليته للانحراف والتي تكشف عنها بواعث الفعل الإجرامي وصفات الجاني، وسلوكه السابق والمعاصر واللاحق للجريمة، والبيئة الخاصة بالجاني وظروفه العائلية والاجتماعية. أي إن هناك أمارات مادية ترتبط بالفعل الإجرامي المرتكب وجسامته وأمارات شخصية تتعلق بشخص الجاني وبكل الظروف والعوامل المحيطة بهذا المجرم. فضلًا عن ذلك ما تم تجميعه

من صور وفيديوهات ونشاط المجرم عبر وسائل التواصل الاجتماعي، وعلاقة المجرم بأقرانه وأصدقائه في المحيط الاجتماعي ومحيط العمل، وبياناته الصحية، وموقفه المالي والائتماني، وغيرها من البيانات. ثم مُعالجة تلك البيانات بواسطة خوارزميات الذكاء الاصطناعي لتنتج في نهاية المقام معلومة مفادها مدى ضلوع هذا الشخص بارتكاب جريمة في المستقبل، وتحديد مكان البؤر الإجرامية المتوقع ارتكاب الجريمة فيها. بناء عليه يأخذ رجال الشرطة دورهم الاستباقي من خلال تواجدهم في تلك الأماكن لإجهاض الجريمة قبل وقوعها.

نخلُص مما سبق إلى أن الشرطة التنبؤية التي تعتمد على تقنيات الذكاء الاصطناعي، ما هي إلا أحد دروب الضبطية الإدارية التي تضطلع بتنبؤ الجريمة بفترة زمنية كافية لإجهاضها قبل حدوثها.

4. المبحث الثاني: مشروعية التنبؤ الخوارزمي بالجريمة

قد يثور التساؤل حول مدى مشروعية التنبؤ الخوارزمي بالجريمة الذي يتطلب تجميع البيانات الشخصية لأشخاص مُعينين واستخدامها - لاسيما وإن كانت هذه البيانات حساسة - بغرض تحليلها إحصائيًّا ومعالجتها آليًا لمعرفة ما إذا كان بإمكان هذا الشخص ارتكاب جريمة في المستقبل من عدمه؟ وهل قرر المشرع المصري حماية جنائية لتلك البيانات محل تطبيقات الذكاء الاصطناعي أم لا؟ لذا نعرض في مطلبين متتاليين الأساس القانوني لمشروعية التنبؤ الخوارزمي بالجريمة، ثم الحماية الجنائية للبيانات داخل تطبيقات الذكاء الاصطناعي المستخدمة للتنبؤ بالجريمة. على النحو التالي:

4. 1. المطلب الأول: الأساس القانوني لمشروعية التنبؤ الخوارزمي بالجريمة

وفقًا للسياق السابق فوظيفة الضبط الإداري التي يضطلع بها مأموري الضبط في مصر تخول لهم رخصة التنبؤ بالجريمة من خلال وسائط الذكاء الاصطناعي المستحدثة، وهو في ذاته يُعد أساسًا قانونيًا لمشروعية التنبؤ الخوارزمي بالجريمة، ولمّا كانت البيانات الشخصية وقودًا لتلك البرامج التقنية، فاللجوء إلى جمعها ومعالجتها ثم القيام بتحليلها للتنبؤ بوقوع جريمة مستقبلية من عدمه، فيه - بالقطع - مساس بالحماية المقررة لتلك البيانات إذ إن معالجة تلك البيانات يقصد به أي عملية إلكترونية أو تقنية لكتابة البيانات الشخصية، أو تجميعها، أو تسجيلها، أو حفظها، أو تخزينها، أو دمجها، أو عرضها، أو إرسالها، أو استقبالها، أو تداولها، أو نشرها، أو محوها، أو تغييرها، أو تعديلها، أو استرجاعها أو تحليلها؛ وذلك باستخدام أي وسيط من الوسائط أو الأجهزة الإلكترونية أو التقنية، سواء تم ذلك جزئيًا أو كليًا وفقًا لما نصت عليه المادة الأولى من قانون حماية البيانات الشخصية المصري رقم 151 لعام 2020.

ومن ثم يثور التساؤل حول مدى التعارض بين مهمة مأموري الضبط في استخدام تطبيقات الذكاء الاصطناعي للتنبؤ بالجريمة، والحماية الجنائية المكرّسة لبيانات هؤلاء الأشخاص محل تلك التطبيقات؟

حمى المشرع المصري البيانات الشخصية بموجب قانونين حديثين، الأول: هو قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018 [73]، والثاني: قانون حماية البيانات الشخصية لعام 2020 [74].

أما بالنسبة للأول: فقد عرّف البيانات الشخصية في المادة الأولي منه على أنها "أي بيانات متعلقة بشخص طبيعي محدد أو يُمكن تحديده، بشكل مباشر أو غير مباشر عن طريق الربط بينها وبين بيانات أخرى". ويضطلع هذا القانون بتجريم الاعتداء على البيانات والمعلومات المعالجة والمواقع الإلكترونية، وبرامج الحاسب الآلي، وتحديد المسؤولية الجنائية لمقدمي الخدمة والمستخدمين [75]. فضلًا عن ذلك جرّم ذات القانون الاعتداء على حرمة الحياة الخاصة والمحتوى المعلوماتي غير المشروع في الفصل الثالث بالمواد 25 و26 منه.

ولدرء شبهة عدم مشروعية استعمال تطبيقات التنبؤ بالجريمة من قِبل مأموري الضبط فإن القانون ذاته استثنى جهات الأمن القومي من تلك الجرائم، وقد نُصَّ في الباب الأول الموسوم بـ«التعريفات»، على ماهية الأمن القومي باعتباره «كل ما يتصل باستقلال واستقرار وأمن الوطن ووحدته وسلامة أراضيه، وما يتعلق بشئون رئاسة الجمهورية ومجلس الدفاع الوطني ومجلس الأمن القومي، ووزارة الدفاع والإنتاج الحربي، ووزارة الداخلية، والمخابرات العامة، وهيئة الرقابة الإدارية، والأجهزة التابعة لتلك الجهات»، أما جهات الأمن القومي، فقد عددها المشرع على النحو التالي «رئاسة الجمهورية، ووزارة الدفاع، ووزارة الداخلية، والمخابرات العامة، وهيئة الرقابة الإدارية». من ثم لا يسري على رجال الشرطة تلك الجرائم، أثناء البحث وتجميع بيانات شخص المجرم من خلال المواقع الإلكترونية ووسائل التواصل الاجتماعي لمعالجتها وتحليلها وتوظيفها في تطبيق الذكاء الاصطناعي الذي يضطلع بالتنبؤ بالجرائم.

أما بالنسبة للثاني، وهو قانون حماية البيانات الشخصية المصري لعام 2020 فقد كان أكثر تحديدًا في مفهوم البيانات الشخصية، وعرفها بأنها «أي بيانات متعلقة بشخص طبيعي محدد أو يمكن تحديده بشكل مباشر أو غير مباشر عن طريق الربط بينها وبين بيانات أخرى، ومنها على سبيل المثال الاسم أو الصوت، أو الصورة أو رقم تعريفي أو محدد للهوية على الإنترنت، أو أي بيانات تحدد

الهوية النفسية أو الصحية أو الاقتصادية أو الثقافية أو الاجتماعية».

وقد ميّز القانون بين البيانات الشخصية الحساسة وغير الحساسة، حتى يكون للأولى حماية جنائية أوسع نطاقًا من الثانية، وعرفها بأنها «بيانات الصحة النفسية أو العقلية أو البدنية أو الجينية أو بيانات القياسات الحيوية «البيومترية» أو البيانات المالية أو المعتقدات الدينية أو الآراء السياسية أو الحالة الأمنية، وفي جميع الأحوال تُعد بيانات الأطفال من البيانات الشخصية الحساسة».

ويُجرم هذا القانون جمع البيانات الشخصية أو معالجتها أو الإفصاح عنها بأية وسيلة من الوسائل إلا بموافقة صريحة من الشخص صاحب البيانات أو في الأحوال المُصرح بها قانونًا، ويكون لصاحب البيانات عدد من الحقوق في مقدمتها العلم والاطلاع والوصول والحصول على البيانات الشخصية الخاصة به الموجودة لدى أي حائز أو متحكم أو معالج، والعدول عن الموافقة السابقة على الاحتفاظ أو معالجة بياناته الشخصية، والاعتراض على معالجة البيانات الشخصية أو نتائجها متى تعارضت مع الحقوق والحريات الأساسية للشخص المعنى بالبيانات.

وقد نصت المادة 37 من قانون حماية البيانات الشخصية 2020 على أن «يعاقب بغرامة لا تقل عن مائة ألف جنيه ولا تجاوز مليون جنيه كل حائز أو متحكم أو معالج جمع أو عالج أو أفشى أو أتاح أو تداول بيانات شخصية معالجة إلكترونيًا بأي وسيلة من الوسائل في غير الأحوال المصرح بها قانونًا أو بدون موافقة الشخص المعني بالبيانات».

وتكون العقوبة الحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن مائتي ألف جنيه، ولا تجاوز مليوني جنيه أو بإحدى هاتين العقوبتين إذا ارتكب ذلك مقابل الحصول على منفعة مادية أو أدبية، أو إذا ترتب على ذلك تعريض الشخص المعني بالبيانات للخطر أو الضرر».

ولعلّ تلك البيانات الواردة تفصيلًا في هذا القانون، هي جزء لا يتجزأ من البيانات التي يتم تغذية تطبيقات الذكاء الاصطناعي بها في الحالة التي يراد فيها التنبؤ بالجريمة أو بالأحرى مُرتكبها، الأمر الذي قد يقدح في مشروعية استعمال تلك التقنية الحديثة، إلا أنه سرعان ما يتبدد هذا الظن بمطالعة المادة الثانية من مواد الإصدار في ذات القانون حيث استثنت جهات الأمن القومي من أحكامه، ونصت على أنه «لا تسري أحكام القانون المرافق على ما يأتي: ... -4 البيانات الشخصية المتعلقة بمحاضر الضبط القضائي والتحقيقات والدعاوى. -5 البيانات الشخصية لدى جهات الأمن القومي وما تقدره لاعتبارات أخرى. وعلى المركز، بناءً على طلب جهات الأمن القومي، إخطار المتحكم أو المعالج بتعديل أو محو أو عدم إظهار أو إتاحة أو تداول البيانات الشخصية، خلال مدة زمنية محددة وفقًا لاعتبارات الأمن القومي، ويلتزم المتحكم أو المعالج بتنفيذ ما ورد بالإخطار خلال المدة الزمنية المحددة به».

وتلك المادة تعد الأساس القانوني الصريح لمشروعية مأموري الضبط في استخدام تطبيقات الذكاء الاصطناعي في التنبؤ الخوارزمي بالجريمة.

والعلّة من هذا الاستثناء واضحة، تتجلّى في حماية الأمن القومي، الذي يُعد إجهاض الجريمة قبل وقوعها من أهم ركائزه، ومن ثم فهذا الاستثناء يُعزز موقف الشرطة التنبؤية في اقتناء وجمع ومُعالجة البيانات الشخصية، وتغذية تطبيقات الذكاء الاصطناعي بها حتى تؤتي ثمارها، غير أن الباحث يرى أنه يُشترط أن يقتصر استعمال تلك التقنية على الأشخاص الذين سبق لهم ارتكاب جريمة تزيد عقوبتها عن سنة، وإلا أصبحت كافّة البيانات الشخصية لاسيما الحساسة، مُستباحة لدى جهات الأمن وهو ما يتعارض مع حرمة الحياة الخاصة كحق دستوري له حماية جنائية، فمن المستساغ عقلًا ألا تكون سلطة الشرطة مُطلقة على البيانات الشخصية للأفراد، وإنما مُحددة في إطار تشريعي معين يضمن في ذات الوقت التوازن بين المصالح المتعارضة.

ويستند الباحث في تحديد مدة السنة إلى اعتبارات معينة، وهي:

أولًا _ أن الجرائم التي تكون مدة عقوباتها أقل من سنة هي جرائم ضئيلة الجسامة لا تستأهل أن تُستغل بمناسبتها كافة البيانات الشخصية للمجرم.

ثانيًا _ أن مُدة السنة مُستقاة من قانون العقوبات نفسه حيث استعملها المشرع صراحة في المادة 55 منه التي تمنح القاضي سلطة إيقاف تنفيذ عقوبة الحبس الذي لا تزيد مدته على سنة، فهي مدة مألوفة لدى المشرع الجنائي المصري.

ثالثًا _ تلك المدة اتفق أغلب الفقه [76]، على أنها تمثل مفهوم الحبس قصير المدة [77]، وما زاد عنها يمثل حبسًا طويل المدة بمفهوم المخالفة.

رابعًا _ نظام التنبؤ بالجريمة كان هدفه بحسب الأصل - في الدول التي اعتنقته - هو الحد من الجرائم شديدة الخطورة التي تمس أمن الدولة من الداخل أو من الخارج كجرائم الإرهاب والجرائم المنظمة العابرة للوطنية وغيرها، وهي تلك الضرورة التي تبيح لإدارات الشرطة أن تعالج البيانات الشخصية، وتقوم بتحليلها لهؤلاء المجرمين، ولم تكن سبيلًا لمكافحة الجرائم البسيطة، ولا ضير في استعمال تلك التقنيات الحديثة في كافة الجرائم، وإنما التخوف من استباحة كافة البيانات الشخصية لأفراد المجتمع تذرعًا بمكافحة تلك الجرائم.

نخلص مما سبق إلى أنه رغم سنّ حماية جنائية للبيانات الشخصية، فإن المشرع المصري استثنى جهات الضبط الإداري لتسهيل أداء وظيفتها، ومن ثم فهناك أرض خِصبة لإعمال تطبيقات الذكاء الاصطناعي في التنبؤ بالجريمة ومواكبة التكنولوجية الحديثة التي تفرض نفسها بقوة في كافة المجالات لاسيما المجال الأمني والجنائي، وهو ما يعد أساسًا قانونيًا صريحًا وفق ما نصت عليه المادة الثانية من مواد الإصدار في قانون حماية البيانات الشخصية المصري رقم 151 لسنة 2020.

4. 2. المطلب الثاني: الحماية الجنائية لبيانات تطبيقات الذكاء الاصطناعي

تخضع بيانات المجرمين أو المتهمين الخطرين محل تطبيقات الذكاء الاصطناعي التي تضطلع بكشف الجرائم قبل ارتكابها للحماية الجنائية الموضوعية المنصوص عليها في قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018، فلا يجوز أولًا: الدخول غير المشروع لكافة تطبيقات التنبؤ بالجريمة أو اعتراضها، ثانيًا: الاعتداء علي سلامة البيانات أو المعلومات أو برامج الذكاء الاصطناعي ذاتها.

حيث نصت المادة 20 من القانون ذاته، والموسومة بـ«جريمة الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة»، في فقرتها الأولى على أنه «يعاقب بالحبس مدة لا تقل عن سنتين، وبغرامة لا تقل عن خمسين ألف جنيه، ولا تجاوز مائتي ألف جنيه، أو بإحدى هاتين العقوبتين، كل من دخل عمدًا، أو بخطأ غير عمدي وبقي دون وجه حق، أو تجاوز حدود الحق المخول له من حيث الزمان أو مستوى الدخول أو اخترق موقعًا أو بريدًا إلكترونيًا أو حسابًا خاصًا أو نظامًا معلوماتيًا يُدار بمعرفه أو لحساب الدولة أو أحد الأشخاص الاعتبارية العامة، أو مملوكًا لها، أو يخصها».

وفي فقرتها الثالثة نصت على أنه «وفي جميع الأحوال، إذا ترتب على أي من الأفعال السابقة إتلاف تلك البيانات أو المعلومات أو ذلك الموقع أو الحساب الخاص أو النظام المعلوماتي أو البريد الإلكتروني، أو تدميرها أو تشويهها أو تغييرها أو تغيير تصاميمها أو نسخها أو تسجيلها أو تعديل مسارها أو إعادة نشرها، أو إلغائها كليًا أو جزئيًا، بأي وسيلة كانت، تكون العقوبة السجن، والغرامة التي لا تقل عن مليون جنيه ولا تجاوز خمسة ملايين جنيه».

وتفترض هذه الجريمة وجود نظام معلوماتي مملوك للدولة أو يُدار بواسطتها والمتمثل في برامج الذكاء الاصطناعي المعنية بالتنبؤ بالجريمة الذي تضطلع به الشرطة التنبؤية في حالة تطبيقه الفعلي من قبل الجهات المختصة إذ إن هذا البرنامج هو محل الاعتداء في صور السلوك المكون للركن المادي المتمثل في اختراق هذا البرنامج بالدخول غير المصرح به عمدًا أو خطأً، أو تجاوز البقاء المصرح به المدة الزمنية المحددة له، أو تعدّى مستوى الدخول المسموح به أو التعدي على البيانات بداخله.

وفيما يتعلق بجريمة الدخول غير المشروع، لم يحدد المشرع وسائل هذا الدخول، فقد يستخدم الجاني أجهزة تُمكنه من كسر شفرة قواعد بيانات تطبيقات الذكاء الاصطناعي المُعدّة للتنبؤ بالجريمة، أو قد يستخدم شفرة صحيحة، ولكنها مملوكة لشخص آخر مصرح له بالدخول، كما يمكن اختراق البرنامج من خلال استخدام فيروسات معينة أو قرصنة إلكترونية. ويستوي أن يتم الدخول بطريق مباشر أو غير مباشر، أي أن يتم الدخول عن بعد، سواء استخدم شبكات اتصال عالمية كانت أو محلية [pp. 113-114 ,78].

بيد أن جريمة الدخول غير المشروع لتطبيقات الذكاء الاصطناعي المعنية بالتنبؤ بالجريمة من جرائم الخطر، وليس من جرائم الضرر أي تتحقق بمجرد إتيان السلوك إذ لا يُشترط أن تترتب أي نتيجة على الدخول المجرد، فهي جريمة تامة في ذاتها [78].

أما جريمة تجاوز حدود التصريح، فيُفترض فيها أن الجاني يملك إذنًا سابقًا للدخول إلى برنامج الذكاء الاصطناعي المُعدّ للتنبؤ بالجريمة، ولكنه تجاوز حدود هذا الإذن من حيث مُدته أو نطاق المعلومات المُصرّح له بالاطلاع عليها، كما لو قام بالدخول في غير المواعيد المحددّة في التصريح أو تجاوز المدّة المحددّة له.

أما فيما يتعلق بجريمة البقاء غير المشروع، فتفترض أن الجاني وَلِجَ بطريقة غير مشروعة لبرنامج الذكاء الاصطناعي المعدّ للتنبؤ بالجريمة عن طريق الصدفة، وظلَّ بداخله دون تصريح أو إذن ممّن يملُك السيطرة عليه من مأموري الضبط المعنيين.

أما من حيث الركن المعنوي، فوفقًا لصريح نص المادة 20 من قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018، فتقع الجريمة سواء أكان عن عمد أم عن خطأ؛ حيث نصت على أنه «... كل من دخل عمدًا، أو بخطأ غير عمدي .....»، إلا أن الباحث يرى أن جريمة الدخول غير المشروع جريمة عمدية لابد أن يتحقق فيها علم الجاني بعدم مشروعية دخوله إلى البرنامج، وينتفي القصد الجنائي لدى الفاعل إذا كان الدخول قد تم بطريق الخطأ أو إذا ثبت أنه دخل للبرنامج بمحض الصدفة ثم خرج منه.

ويُلاحظ أن المشرع أعطى سلطة تقديرية للقاضي في اختيار العقوبة الأنسب بين العقوبات المحددة وفقًا لنص المادة 20 وهي الحبس مدة لا تقل عن سنتين، وبغرامة لا تقل عن خمسين ألف جنيه، ولا تجاوز مائتي ألف جنيه، أو بإحدى هاتين العقوبتين، فجعل العقوبة

تخييرية بين حد أدنى وحد أقصى. ومع ذلك وضع ظرفًا مشددًا في حالات معينة تتعلق جميعها بانتهاك البيانات المدرجة داخل برنامج الذكاء الاصطناعي، وجعل العقوبة هي السجن، والغرامة التي لا تقل عن مليون جنيه ولا تجاوز خمسة ملايين جنيه. وقد عدد المشرع تلك الحالات على سبيل الحصر، وهي إتلاف تلك البيانات أو المعلومات أو النظام المعلوماتي، أو تدميرها أو تشويهها أو تغييرها أو تغيير تصاميمها أو نسخها أو تسجيلها أو تعديل مسارها أو إعادة نشرها، أو إلغاؤها كليًا أو جزئيًا، بأي وسيلة كانت. ووفقًا لقواعد التفسير المضيق للنصوص الجنائية لا يجوز أن تمتد تلك الحالات إلى غيرها ولا يقاس عليها من باب أولى، كما لو كان الدخول إلى برنامج الذكاء الاصطناعي بغرض التهديد أو الابتزاز.

وربما يثور التساؤل حول الحالة التي يدخل فيها الجاني بطريقة غير مشروعة لبرنامج الذكاء الاصطناعي المعدّ للتنبؤ بالجريمة، الذي يُدار بواسطة الدولة، بغرض فضّ سرية بيانات أحد الأشخاص المتهمين وإفشاء صحيفته الجنائية؟ بصيغة أخرى هل يُعد فعل إفشاء سرية البيانات محل تطبيقات الذكاء الاصطناعي ظرفًا مشددًا أم لا؟

بالنظر إلى المادة 20 من قانون مكافحة جرائم تقنية المعلومات في فقرتها الثالثة، نجد أن المشرع لم ينص صراحة على تلك الحالة، الأمر الذي لا يكون فيه فعل الإفشاء ظرفًا مشددًا للجريمة، ولا يقدح في ذلك ما ذكرته نص المادة بـ«إعادة نشرها»، أي إعادة نشر البيانات مرة أخرى بأي وسيلة من الوسائل إذ إن تلك الحالة تفترض أن البيانات كانت قد نشرت من قبل وحذفت، ثم أعيد نشرها مرة أخرى، فبيانات الصحف الجنائية لا يتم نشرها بأي صورة من الصور، كذلك بعض البيانات الفردية والاجتماعية والصحية للمتهمين أو المجرمين. فهذه الحالة تناقش البيانات السرية ابتداءً التي استخدمت في برنامج معدّ للتنبؤ الخوارزمي بالجريمة لذا كان حريًا على المشرع أن يضيف كلمة «النشر» أو «الإفشاء» كأحد أوجه التعدي على البيانات الشخصية محل برنامج الذكاء الاصطناعي حتى يدخل في ثناياها فعل إفشاء سرية تلك البيانات كظرف مشدد، وهو ما اعتنقه بعض المشرعين، فعلى سبيل المثال نص المشرع العماني في المادة 3 من قانون مكافحة جرائم تقنية المعلومات الصادر بالمرسوم السلطان رقم 12/2011، على أنه «... فإذا ترتب على ما ذكر في الفقرة الأولى إلغاء أو تغيير أو تعديل أو تشويه أو إتلاف أو نسخ أو تدمير أو نشر أو إعادة نشر بيانات أو معلومات إلكترونية مخزنة في النظام المعلوماتي...». كذلك المشرع الكويتي في المادة 2 من قانون مكافحة جرائم تقنية المعلومات رقم 63 لسنة 2015 لديه، نص على أنه «... فإذا ترتب على هذا الدخول إلغاء أو حذف أو إتلاف أو تدمير أو إفشاء أو تغيير أو إعادة نشر بيانات أو معلومات، فتكون العقوبة...». كذلك المشرع الإماراتي الذي نص في المادة 2 من قانون مكافحة جرائم تقنية المعلومات الصادر بالمرسوم بقانون رقم 5 لسنة 2012 على «... إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو نسخ أو نشر أو إعادة نشر أي بيانات أو معلومات».

ويمكن تفريد البيانات الشخصية التي قد يتم إفشاء سريتها من خلال اختراق برامج الذكاء الاصطناعي المعدّة للتنبؤ بالجريمة، ولا يعد إفشاؤها ظرفًا مشددًا وفق صريح نص المادة 20 من قانون قانون مكافحة جرائم تقنية المعلومات المصري في فقرتها الثالثة، على النحو التالي:

أولًا _ البيانات الفردية

وهي تلك البيانات التي من شأنها تحديد شخصية الشخص الطبيعي بشكل ينفي جهالة شخصيته تحت أي شكل كان [79]، سواء المتعلقة باسم الشخص وصورته، وجنسيته، وفصيلة دمه، وديانته وسكنه أو أية صفة يعين بها كوظيفته، أو مهنته، أو مؤهله، أو صفات شخصيته كالبصمة المميزة له عن الآخرين [80].

ثانيًا _ بيانات الوقائع المدنية والصحيفة الجنائية

وتحدد تلك البيانات حركة الفرد في المجتمع [81]، فبيانات الوقائع المدنية هي عناصر الحالة المدنية للفرد وهي: الميلاد، والزواج، والطلاق، والجنسية، والإقامة، والوفاة، كما تشمل الرقم القومي، وعنوان المسكن، وعنوان البريد، والخدمة العسكرية، وتاريخ دخول ومغادرة الأجنبي والتأشيرة التي يحصل عليها لهذا الغرض، فهذه الوقائع غالبًا ما تنظمها الدوائر الحكومية، أما صحيفة الحالة الجنائية فهي تشمل الجرائم التي ارتكبها من قبل من حيث الزمان والمكان، ونوعها والمدة التي سُلبت فيها حريته، وما إذا كان خاضعًا للمراقبة أم لا.

ثالثًا _ البيانات الاجتماعية والصحية

وهي تلك المعلومات التي تتصل بسيرة الفرد الاجتماعية وتكوينه والمخاطر التي يعيش بجوارها، وكل ما يتعلق بمكانة الفرد الاجتماعية والعائلية والأوساط التي يتعامل معها [83, p. 186]، ويدخل في هذا النطاق الأمور المتعلقة بالحياة الزوجية كالطلاق وظروفه، وإبرام زواج جديد وغيرها. كذلك بياناته الصحية كما لو كان يتم علاجه من مرض مزمن، أو كان له سوابق صحية ذات سمعة غير طيبة كالإدمان على المواد المخدرة مثلًا.

جدير بالذكر أن المشرع المصري عاقب أيضًا بالحبس مدة لا

تقل عن سنتين، وبغرامة لا تقل عن ثلاثمائة ألف جنيه، ولا تجاوز خمسمائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من حاز أو أحرز أو جلب أو باع أو أتاح أو صنع أو أنتج أو استورد أو صدَّر أو تداول بأي صورة من صور التداول، أي أجهزة أو معدات أو أدوات أو برامج مصممة أو مطورة أو محورة أو أكواد مرور أو شفرات أو رموز، أو أي بيانات مماثلة، بدون تصريح من الجهاز أو مسوغ من الواقع أو القانون، وثبت أن ذلك السلوك كان بغرض استخدام أي منها في ارتكاب أو تسهيل ارتكاب أي جريمة من الجرائم المنصوص عليها في هذا القانون، أو إخفاء آثارها أو أدلتها أو ثبت ذلك الاستخدام أو التسهيل أو الإخفاء، وفقًا للمادة 22 من قانون مكافحة جرائم تقنية المعلومات لعام 2018.

نخلص مما سبق إلى أن المشرع المصري أضفى حماية جنائية على البيانات الشخصية التي يتم تغذية برامج الذكاء الاصطناعي بها، والتي بدونها لا يمكن بحال توقع حدوث جريمة في المستقبل إذ إن تلك البيانات هي التي يتم تحليلها من خلال الخوارزميات المعدة لذلك للتنبؤ بالجريمة في المستقبل.

5. الخاتمة

لمّا كانت خاتمة البحث هي مغزاه، فمغزى هذا البحث هو تبصير المشرع المصري نحو قادمٍ جديد ربما يكون له الأثر البالغ في إجهاض الجريمة مبكرًا، فتولد ميتة، ألا وهو تنبؤ الجريمة بواسطة الذكاء الاصطناعي، الذي ينعكس أثره على دحض الجرائم الخطيرة التي تهدد الأمن القومي لاسيما جرائم الإرهاب والجرائم المنظمة وغيرها.

جدير بالذكر أن البحث تناول إشكاليتين الأولى: تحديد الطبيعة القانونية لتطبيقات الذكاء الاصطناعي التي تضطلع بتنبؤ الجريمة، حتى تنجلي خصوصيته، ويسهل على المشرع وضعه في القانون الجنائي بصفة عامة. أما الثانية فتتعلق بمدى مشروعية استخدام تلك التطبيقات المستحدثة.

5. 1. النتائج

من خلال البحث يُمكن استنتاج الآتي:

- أن الطبيعة القانونية لوسيلة التنبؤ الخوارزمي بالجريمة هي طبيعة أمنية إدارية، مقصدها تحقيق الضبط الإداري، وهي مرحلة سابقة على الإجراءات الجنائية، ومن ثم تخرج عن كونها ذات طبيعة احترازية أو طبيعة استدلالية.
- أن الإجرام انخفض بنسب متفاوتة، في المدن التي استخدمت مراكز شرطتها، تطبيقات الذكاء الاصطناعي التي تضطلع بتنبؤ الجريمة مما يؤكد أهمية استخدام تلك التقنية.
- أن مؤشرات تطبيقات الذكاء الاصطناعي في تقييم الخطورة الإجرامية لشخص المجرم، قد تؤثر على عقيدة القاضي الجنائي في نطاق الإدانة، سواء بتخفيف العقوبة أو تغليظها أو حتى مقدارها حسب السياسة التشريعية التي ينظمها قانونه.
- أن البيانات الضخمة المطلوب تزويد خوارزميات الذكاء الاصطناعي بها، لا تتعارض مع حق الشخص في سرية بيانات الشخصية، وبخاصة مع الاستثناءات التي أوردها المشرع المصري في كل من قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018، وقانون حماية البيانات الشخصية لعام 2020. مما يضفي المشروعية اللازمة لاستخدام تلك التقنية الحديثة.

5. 2. التوصيات

ومن خلال ما تم التوصل إليه من نتائج يوصي البحث بما يلي:

- ضرورة التدخل التشريعي لتنظيم الاستعانة بوسيلة التنبؤ الخوارزمي بالجريمة، وتحديد كافة أطره القانونية، لاسيما مدى جواز إعماله بأثر رجعي، وكذلك شروط اللجوء إليه، ومدى جواز وقف العمل به بالنسبة لشخص معين، والمدد المحددة لاستخدام تلك التقنية الحديثة من قِبل مأموري الضبط، وأثر زوال حكم الإدانة على التحليل الخوارزمي لبيانات المحكوم عليه أيًا كان سبب زوال الحكم، سواء بالعفو الشامل، أو رد الاعتبار، أو غيرها.
- ضرورة التدخل التشريعي لتحديد نطاق الشرطة التنبؤية من حيث جمع البيانات الشخصية الحساسة وغير الحساسة، وقصرها على الأشخاص ضليعي الإجرام، أو من سبق لهم ارتكاب جرائم خطيرة دون غيرهم.
- كذلك ضرورة حظر جمع البيانات الشخصية بنوعيها بالنسبة للأشخاص الذين يرتكبون جرائم تقل عقوبتها عن مدة سنة، حيث إن تلك الجرائم عادة ما ترتكب خطأً، الأمر الذي ينفي وجود خطورة إجرامية لدى فاعلها.
- العمل على تطوير مرفق الشرطة وميكنته، وإنشاء أقسام خاصة بداخلها يُطلق عليها "الشرطة التنبؤية"، تضطلع بمباشرة عملها بالاستعانة بالمتخصصين في نظم المعلومات والبرمجيات.
- ضرورة تدريس "علم الإجرام الخوارزمي" كجزء من مقررات

علم الإجرام والجزاء في كليات الحقوق، حتى يكون على الدارسين المعرفة البينية بين علم الإجرام وتطبيقات الذكاء الاصطناعي وأثر كل منهما على الآخر.

المصادر والمراجع

1. Danaher, J., Hogan, M. J., Noone, C., Kennedy, R., Behan, A., De Paor, A., ... & Shankar, K. (2017). Algorithmic governance: Developing a research agenda through the power of collective intelligence. Big Data & Society, 4(2), 2053951717726554.

2. حجازي، مصطفى. (2020، 04 مارس). التاريخ للمستقبل.. 2027 البداية. صحيفة المصري اليوم، السنة 16، العدد 5742، https://bit.ly/2NXPoEJ.

3. Lyon, D. (2014). Surveillance, Snowden, and big data: Capacities, consequences, critique. Big data & society, 1(2), 2053951714541861.

4. Smith, G. J., & O'Malley, P. (2017). Driving politics: Data-driven governance and resistance. The British Journal of Criminology, 57(2), 275-298.

5. Brayne, S. (2017). Big data surveillance: The case of policing. American Sociological Review, 82(5), 977-1008.

6. عبد المنعم، سليمان. (2015). أصول علم الإجرام والجزاء، دار المطبوعات الجامعية، ص. 410.

7. Pradel, J. (2015). Droit Pénal Général Cujas, 21 éd, p. 632.

8. محمد، أمين مصطفى. (2015). نظام الامتناع عن النطق بالعقاب في القانون الكويتي، دراسة مقارنة بنظام الاختبار القضائي في القانون المصري والفرنسي، دار المطبوعات الجامعية، ص. 6.

9. Dick, P., K. (n. d.). The Minority Report. Retrieved March 4, 2020, from https://bit.ly/36vaaBQ.

10. Farrington, D. P. (1985). Criminological Prediction-An Introduction (From Prediction in Criminology, P 2-33, 1985, David P Farrington and Roger Tarling, ed.-See NCJ-99006).

11. الألفي، رمضان السيد. (1998). نظرية الخطورة الإجرامية، دار النهضة العربية، ص. 203.

12. Pies, R. W. (1994). Clinical manual of psychiatric diagnosis and treatment: A biopsychosocial approach. American Psychiatric Pub.

13. Lasry, B., & Kobayashi, H. (2018). Human Decisions Thoughts on AI. The united nations educational, Scientific and cultural organization. pp. 20-21.

14. Bughin, J., Hazan, E., Ramaswamy, S., Chui, M., Allas, T., Dahlstrom, P., ... & Trench, M. (2017). Artificial intelligence: The next digital frontier?. p. 6.

15. Rich, E., & Knight, K. (1991). Artificial intelligence. pp. 105-192.

16. الشرقاوي، محمد علي. (1996). الذكاء الاصطناعي والشبكات العصبية، سلسلة علوم وتكنولوجيا حاسبات المستقبل، مركز الذكاء الاصطناعي للحسابات، مطابع المكتب المصري الحديث، ص. 14.

17. بونيه، الآن. (إبريل، 1993). الذكاء الاصطناعي واقعه ومستقبله، عالم المعرفة ترجمة: على صبري فرغلي، الكويت، العدد 172، ص. 10.

18. أسعد، عبير. (2017). الذكاء الاصطناعي، دار البداية، الطبعة الأولى، ص. 3 وما يليها.

19. Winograd, T. (2006). Thinking Machines: Can There Be? Are We? The Foundations of Artificial Intelligence. Derek Partridge & Yorick Wilks eds., p. 167.

20. Osoba, O. A., & Welser IV, W. (2017). An intelligence in our image: The risks of bias and errors in artificial intelligence. Rand Corporation. p. 4.

21. موسي، عبد الله.، بلال، أحمد حبيب. (2019). الذكاء الاصطناعي، ثورة في تقنيات العصر، المجموعة العربية للتدريب والنشر، الطبعة الأولى، ص. 98.

22. Berk, R. (2013). Algorithmic criminology. Security Informatics, 2(1), 1-14.

23. Hannah-Moffat, K. (2019). Algorithmic risk governance: Big data analytics, race and informa-

tion activism in criminal justice debates. Theoretical Criminology, 23(4), 453-470.

24. Manyika, J., Chui, M., Brown, B., Bughin, J., Dobbs, R., Roxburgh, C., & Hung Byers, A. (2011). Big data: The next frontier for innovation, competition, and productivity. McKinsey Global Institute.

25. Chan, J., & Bennett Moses, L. (2016). Is big data challenging criminology?. Theoretical criminology, 20(1), 21-39.

26. البار، عدنان مصطفى.، المرحبي، خالد علي. (2018، 03 ديسمبر). البيانات الضخمة ومجالات تطبيقها. https://bit.ly/36vELPJ.

27. Balkin, J. M. (2017). 2016 Sidley Austin Distinguished Lecture on Big Data Law and Policy: The Three Laws of Robotics in the Age of Big Data. Ohio St. LJ, 78, 1217.

28. لطابي، مريم. (2018). البيانات الضخمة وصناعة المعلومات، مجلة الحكمة للدراسات الإعلامية والاتصالية، المجلد 6، العدد 4، ص. 61.

29. Hao, J., & Ho, T. K. (2019). Machine learning made easy: A review of scikit-learn package in Python programming language. Journal of Educational and Behavioral Statistics, 44(3), 348-361.

30. Brennan, T., & Oliver, W. L. (2013). Emergence of machine learning techniques in criminology: implications of complexity in our data and in research questions. Criminology & Pub. Pol'y, 12, 551.

31. Goodfellow, I., Bengio, Y., Courville, A., & Bengio, Y. (2016). Deep learning (Vol. 1, No. 2). Cambridge: MIT press.

32. Soliman, O. (2018, Nov. 27). Kent police cancel 'predictive policing' software. Retrieved 03 March, 2020, from https://bit.ly/3cy2sL1.

33. Friend, Z. (2013, April 9). Predictive Policing: Using Technology to Reduce Crime. Retrieved 12 March, 2020 from https://bit.ly/3re6vjB.

34. Hunt, P., Hollywood, J. S., & Saunders, J. M. (2014). Evaluation of the Shreveport predictive policing experiment. Santa Monica: Rand Corporation.

35. Robinson, D., & Koepke, L. (2016). Stuck in a Pattern: Early Evidence on 'Predictive Policing'and Civil Rights. Washington, DC: Upturn.

36. Artificial Intelligence and Life In 2030. (2016, Septmper). One Hundred Year Study on Artificial Intelligence, Report of the 2015 Study Panelartificial. Retrieved 12 March, 2020, from March 4, from https://ai100.stanford.edu/sites/g/files/sbiybj9861/f/ai_100_report_0831fnl.pdf.

37. Pearson, J. (2015, February 4). Artificial Intelligence Could Help Reduce HIV Among Homeless Youths, Team core, University of Southern California. Retrieved March 4, 2020, from https://stanford.io/2Lb9ABU.

38. The Opinion Page. (2013, April 22). Big Op-Ed: Shifting Opinions On Surveillance Cameras. Retrieved March 4, 2020, from https://n.pr/3pILIVm.

39. Arikuma, T., & Mochizuki, Y. (2016). Intelligent multimedia surveillance system for safer cities. APSIPA Transactions on Signal and Information Processing, 5.

40. إي إم آي تي تكنولوجي ريفيو العربية. (2018، 19 نوفمبر). هل يمكننا التنبؤ بالزمان والمكان الذي ستحدث فيه جريمة ما؟. https://bit.ly/3j4EGaN.

41. البحيري، عمرو سيد جمال. (2019). أثر تطبيقات الذكاء الاصطناعي على رفع كفاءة الأداء الأمني بالتطبيق على تأمين الطرق، رسالة دكتوراه، كلية الدراسات العليا، أكاديمية الشرطة، ص. 13.

42. المحكمة الدستورية المصرية. (1993، 2 يناير). عدم دستورية نص المادة الخامسة من المرسوم بقانون رقم 98 لسنة 1945 بشأن المتشردين والمشتبه فيهم، وسقوط أحكام المواد المرتبطة بها وهي (13، 6، 15) منه. حكم المحكمة الدستورية الصادر بتاريخ 2 يناير 1993، مجموعة المكتب الفني، ج. 5، ق. 10، ص. 103.

43. القهوجي، علي عبد القادر. (1996). قانون الاشتباه: دراسة

تحليلية انتقادية، دار الجامعة الجديدة، ص. 25.

44. الصيفي، عبد الفتاح. (1972). الجزاء الجنائي، دار النهضة للطباعة والنشر، ص. 9.

45. محمودي، نور الهدى. (2011). التدابير الاحترازية وتأثيرها على الظاهرة الإجرامية، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر باتنة، الجزائر، ص. 20.

46. بهنام، رمسيس. (1986). علم الوقاية والتقويم، منشأة المعارف، ص. 100.

47. أنور، يسر. (1971). النظرية العامة للتدابير والخطورة الإجرامية، دراسة في الدفاع الاجتماعي ضد الجريمة، مجلة العلوم القانونية والاقتصادية، العدد الأول، ص. 1.

48. حسني، محمود نجيب. (1976). النظرية العامة للتدابير الاحترازية، مجلة إدارة قضايا الحكومة، س11، ص. 3.

49. حسني، محمود نجيب. (2016). شرح قانون العقوبات القسم العام، النظرية العامة للجريمة، النظرية العامة للعقوبة والتدبير الاحترازي، دار النهضة العربية، الطبعة الثامنة، ص.1044.

50. حسني، محمود نجيب. (1988). النظرية العامة للقصد الجرمي، دار النهضة العربية، ص. 175 وما بعدها.

51. ثروت، جلال. (2002). نظرية الجريمة المتعدية القصد، منشورات الحلبي الحقوقية، ص. 218 وما بعدها.

52. 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.

53. 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.

54. عبد الملك، جندي. (1976). الموسوعة الجنائية، الجزء الخامس، دار إحياء التراث العربي، ص144. وما بعدها.

55. نقض جنائي، الطعن رقم 18344 لسنة 83 قضائية، بتاريخ جلسة 8/11/2014، حكم غير منشور، جمهورية مصر العربية.

56. عبد المطلب، ممدوح عبد الحميد. (2019). الشرطة الاستخباراتية، العمل الشرطي القائم على الذكاء الاصطناعي وتحليل المعلومات، دار النهضة العربية، الطبعة الأولى، ص. 33.

57. Mohler, G., O. (2017, Oct. 31). Event forecasting system, US 9, 805, 311 B1, pp. 14-15. Retrieved March 5, 2020, from https://bit.ly/3ctnlXL.

58. سرور، أحمد فتحي. (2016). الوسيط في قانون الإجراءات الجنائية، الكتاب الأول، دار النهضة العربية، ص. 699.

59. نقض جنائي، الطعن رقم 38273 لسنة 74 قضائية، الصادر بجلسة 4/12/2010، مكتب فني 61 - قاعدة 87 - صفحة 682. جمهورية مصر العربية.

60. حسني، محمود نجيب. (2019). شرح قانون الإجراءات الجنائية وفقًا لأحد التعديلات التشريعية، دار النهضة العربية، الطبعة السادسة، المجلد الأول، ص. 22، 23 وما بعدها.

61. Andreessen, M. (2011, Aug. 20). Why Software Is Eating the World. The Wall Street Journal. Retrieved March 10, 2020, from https://on.wsj.com/3raTrvv.

62. Osoba, O. A., & Welser, W. (2017). The risks of artificial intelligence to security and the future of work. RAND. https://bit.ly/2YvX56K.

63. Larson, J., Mattu, S., Kirchner, L., & Julia, A. (2016, May 23. How We Analyzed the COMPAS Recidivism Algorithm. ProPublica. Retrieved March 13, 2020, from https://bit.ly/3tcHirL.

64. الحمادي، خالد محمد علي. (2015). حقوق وضمانات المتهم في مرحلة ما قبل المحاكمة، دار النهضة العربية، الطبعة الثانية، ص. 119 وما بعدها.

65. الشهاوي، قدري عبد الفتاح. (1999). ضوابط السلطة الشرطية في التشريع الإجرائي المصري والمقارن، منشأة المعارف، ص. 19.

66. السبكي، ممدوح إبراهيم. (1998). حدود سلطات مأمور الضبط القضائي، في التحقيق، دار النهضة العربية، ص. 4.

67. Weisburd, D. (2016). Does hot spots policing inevitably lead to unfair and abusive police practices, or can we maximize both fairness and effectiveness in the new proactive policing. U. Chi. Legal F., 661.

68. أبو الخير، عادل. (1995). الضبط الإداري وحدوده، الهيئة المصرية العامة للكتاب، ص. 82 وما بعدها.

69. إسماعيل، عادل إبراهيم. (2001). سلطات مأمور الضبط القضائي بين الفعالية وضمان الحريات والحقوق الفردية، رسالة دكتوراه، كلية الدراسات العليا، أكاديمية الشرطة، ص. 48.

70. طنطاوي، إبراهيم حامد. (1991). سلطات مأمور الضبط القضائي، مطبعة دار التأليف، ص. 75 وما بعدها.
71. عبد العزيز، مدحت محمد. (2001). الأمر الجنائي، دراسة مقارنة بين التشريعين المصري والفرنسي، الطبعة الأولى، دار النهضة العربية، ص. 106.
72. علي، شمس مرغني. (1974، ديسمبر). المعيار الوظيفي كمعيار للتمييز بين العمل الإداري والعمل القضائي، مجلة العلوم الإدارية، السنة 16، العدد 3، ص. 114.
73. الجريدة الرسمية، العدد 32 مكرر (ج)، بتاريخ 14 أغسطس سنة 2018م، جمهورية مصر العربية.
74. الجريدة الرسمية، العدد 28 مكرر (هـ) بتاريخ 15 يوليو سنة 2020م، جمهورية مصر العربية.
75. موسى، حوراء. (2017). الجرائم المرتكبة عبر وسائل التواصل الاجتماعي، دراسة مقارنة، رسالة دكتوراه، كلية الحقوق، جامعة الإسكندرية، ص. 36 وما بعدها.
76. محمد، أمين مصطفى. (2010). النظرية العامة لقانون العقوبات الإداري (ظاهرة الحد من العقاب)، دار المطبوعات الجامعية، ص.97.
77. عبيد، حسنين إبراهيم. (1970). نظرية الظروف المخففة، دراسة مقارنة، دار النهضة العربية، ص. 334 وما بعدها.
78. إبراهيم، خالد ممدوح. (2009). الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى، ص. 242.
79. مغبغب، نعيم. (2008). مخاطر المعلوماتية والإنترنت، منشورات الحلبي الحقوقية، الطبعة الثانية، ص. 185.
80. المقاطع، محمد عبد المحسن. (بدون سنة نشر). حماية الحياة الخاصة للأفراد وضماناتها في مواجهة استخدام الحاسب الآلي، ذات السلاسل للطباعة والنشر، ص. 75.
81. حسبو، عمر أحمد. (2000). حماية الحريات في مواجهة نظم المعلومات، دار النهضة العربية، ص. 156.