مشروعية استخدام البيانات الشخصية في مرحلة الشُرطة التنبؤِية "في ضوء قانون الذكاء الاصطناعي الأوروبي لعام 2024"

The Legality of Using Personal Data in Predictive Policing in Light of the European Artificial Intelligence Act 2024

د. محمود سلامة الشريف

(مصر)

mahmoudsalamaelsherif@gmail.com

DOI: https://doi.org/10.70411/MJLS.3.2.2025228

تاريخ الاستلام، 07-04-2025 تاريخ المراجعة، 08-04-2025 تاريخ القبول، 08-04-2025

الملخص:

البيانات الشخصية هي جوهر الحق في الخصوصية الرقمية الذي يُعد أحد أهم الحقوق الأساسية في ما نعيشه اليوم من عصر اتسم بالرقمنة، ويهدف هذا الحق إلى حماية الأفراد من جمع واستخدام وتحليل ومعالجة بياناتهم الشخصية دون موافقتهم. بيد أن ظهور الشرطة التنبؤية أثار مخاوف كثيرة حول انتهاك تلك الحقوق إذ إن خوارزميات الشرطة التنبؤية تضطلع بالتنقيب في البيانات والمعلومات وبخاصة الشخصية لاستشراف وتوقع الجرائم المستقبلية أو تتبع مرتكبيها أو ضحاياها، وقد اضطلع القانون الأوروبي للذكاء الاصطناعي المستحدث الصادر في أيار/مايو 2024، بوضع ضوابط وضمانات صارمة لحماية الحق في الخصوصية الرقمية أثناء عمل الشرطة التنبؤية.

الكلمات المفتاحية: الشرطة التنبؤية، الخصوصية الرقمية، تحليل البيانات، الخوارزميات، الذكاء الاصطناعي، البيانات الشخصية.

Abstract:

Personal data is the core of the right to digital privacy, which is one of the most basic rights in the era we live in today, characterised by digitalisation. This right aims to protect individuals from the collection, use, analysis, and processing of their personal data without their consent. However, the emergence of predictive policing has raised many concerns about the violation of these rights, as predictive policing algorithms undertake exploration of data and information, especially personal data, to anticipate future crimes or track their perpetrators or victims. The newly introduced European Artificial Intelligence Law, issued in May 2024 has undertaken the establishment of strict controls and guarantees to protectthe right to digital privacy during predictive policing.

Keywords: predictive policing, digital privacy, data analysis, algorithms, artificial intelligence, personal data.

المقدمة

يُقصد بالشرطة التنبؤية (Predictive Policing)[1] ، هو ذلك النمط الشرطي الذي يضطلع باستخدام خوارزميات (Algorithms) مُحددة[2]، لتحليل كميّات هائلة من المعلومات والبيانات المرتبطة بالمجرمين من

---

[1]. يرى بعض الفقه أن التنبؤ بالجريمة هو "توقع حدوثها مُستقبلًا، بُغية الحيلولة دونها". محمود سلامة الشريف: الطبيعة القانونية للتنبؤ بالجريمة بواسطة الذكاء الاصطناعي ومشروعيته، المجلة العربية لعلوم الأدلة الجنائية والطب الشرعي، العدد 3، المجلد2، 2021، ص342. كذلك؛

Meijer, Albert, and Martijn Wessels. 2019. Predictive Policing; Review of Benefits and drawbacks. International Journal of Public Administration 42: 1031–39.

Pearsall, Beth. 2010. Predictive policing: The Future of Law Enforcement. National Institute of Justice Journal 266: 16–19

Beth Pearsall; Predictive Policing: The Future of Law Enforcement? NIJ Journal / Issue No. 266. P16. On the following link: https://www.ojp.gov/pdffiles1/nij/230414.pdf

ويرى البعض الآخر أنها "عملية الوقوف على سلوك مُستقبلي ينطوي على خطورة إجرامية لدى بعض الأفراد". رمضان السيد الألفي: نظرية الخطورة الإجرامية، دار النهضة العربية، 1998، ص203. كذلك؛

Beck, C., and C. McCue, "Predictive Policing: What Can We Learn From Wal-Mart and Amazon About Fighting Crime in a Recession?" The Police Chief 76, 11, November 2009. On the following link: https://www.policechiefmagazine.org/predictive-policing-what-can-we-learn-from-wal-mart-and-amazon-about-fighting-crime-in-a-recession/

ويُطلِق عليها البعض الآخر مصطلح (الشرطة الاستخباراتية) التي تضطلع بجمع المعلومات المرتبطة بالمخاطر المحتملة وتوظيفها لمنع تهديد محتمل. شادي عبد الوهاب منصور: الشرطة التنبؤية: اعتماد متزايد لأجهزة الأمن الغربية على أساليب الاستخبارات، مجلة أوراق أكاديمية، مركز المستقبل للدراسات والأبحاث المتقدمة، العدد 4، أكتوبر 2018، ص2.

ولعلّ مِن أوائل مَن اضطلع بتعريف "الشرطة التنبؤية–Predictive Policing" هو المعهد الوطني للعدالة بالولايات المتحدة الأمريكية (NIJ-National Institute of Justice)، وهو ذراع البحث والتطوير لدى وزارة العدل الأمريكية، والذي عقد ندوتين لمناقشة الشرطة التنبؤية وأثرها على الجريمة والعدالة في 2009 و2010، ركزت الندوة الأولى على مفهوم الشرطة التنبؤية، وقد قدمت الندوة تعريفاً عملياً للشرطة التنبؤية على أنها: "أي إستراتيجية أو تكتيك للشرطة يطور ويستخدم المعلومات والتحليلات المتقدمة للوقاية من الجريمة بشكل استباقي– Any policing strategy or tactic that develops and uses information and advanced analysis to inform forward-thinking crime prevention".

وركزت الندوة الثانية على كيفية جعل الشرطة التنبؤية متاحة لجميع وكالات إنفاذ القانون. يرجع في ذلك إلى تقرير الندوتين على الرابط الآتي ، بتاريخ دخول 1–6–2024:https://www.ojp.gov/pdffiles1/nij/242222and248891.pdf

[2]. الخوارزميات تعني مجموعة من المسارات والخطوات الرياضية المُتتابعة المتتالية اللازمة لحل مُشكلة ما، والمُعدّة برمجيًا لكي تُعطي نتيجة مُعينة اعتمادًا على مُعطيات ومُدخلات غُذيت بها، يرجع في ذلك إلى؛

مصادر مختلفة، بهدف الاستشراف بالجرائم المستقبلية المحتملة والمساعدة في منعها[1]. وبالتالي تُعد البيانات والمعلومات الرقمية الضخمة (Big Data)[2]، هي وقود تلك الخوارزميات التي تتم هيكلتها لتضطلع بالتحليل الكمّي والكيفي والتنبؤ[3]، ولا شك أن من بين تلك المعلومات والبيانات التي يتم التنقيب عنها أو جمعها أو معالجتها هي البيانات الشخصية المشمولة بحماية قانونية مُكرسّة دستورياً[4]، الأمر الذي يثير تخوّفًا نحو انتهاك خصوصية تلك البيانات حال التنبؤ الشرطي.

أضحت الشرطة التنبؤية ظاهرة سريعة التنامي عالمياً، على سبيل المثال تستخدم أكثر من 50% من أقسام الشرطة في الولايات المتحدة الأمريكية أحد أشكال تكنولوجيا الذكاء الاصطناعي لتحليل الجرائم وتصنيف مرتكبيها[5]، ومن بينها خوارزميات التنبؤ بالجريمة[6]، كما يستخدم حوالي 60% من المدّعين

Uspenski, V. A.. "To the Definition of Algorithms." ,1993. On the following link: https://api.semanticscholar.org/CorpusID:117434268

[1] Safat W, Asghar S, Gillani SA. Empirical analysis for crime prediction and forecasting using machine learning and deep learning techniques, IEEE Access 9 ,2021, pp. 70080-70094. On the following link: https://api.semanticscholar.org/CorpusID:234499744

[2] De Mauro, Andrea et al. "A formal definition of Big Data based on its essential features." Library Review 65 ,2016, pp. 122-126.

[3] Samah Samir; Detecting and Predicting Crimes using Data Mining Techniques: Comparative Study, Proceedings of 1st International Conference on Computers and Information, ICCI 2021, p.57. On the following link: https://ijci.journals.ekb.eg/article_207749_6851eb18a1c11190f9444519b5fba5a0.pdf

[4] حيث نصت المادة 57 من دستور مصر لعام 2014 والمعدل في 2019 على أنه "للحياة الخاصة حرمة، وهي مصونة لا تمس. وللمراسلات البريدية، والبرقية، والإلكترونية، والمحادثات الهاتفية، وغيرها من وسائل الاتصال حرمة، وسريتها مكفولة، ولا تجوز مصادرتها، أو الاطلاع عليها، أو رقابتها إلا بأمر قضائي مسبب، ولمدة محددة، وفي الأحوال التي يبينها القانون. تقابلها المادة 36 من النظام الأساسي لسلطنة عُمان الصادر بالمرسوم سلطاني رقم 6/ 2021، والتي نصت على أنه "للحياة الخاصة حرمة، وهي مصونة لا تمس. وللمراسلات الإلكترونية بأنواعها كافة، والمراسلات الهاتفية، والبرقية، والبريدية، وغيرها من وسائل الاتصال حرمة، وسريتها مكفولة، فلا يجوز مراقبتها، أو تفتيشها، أو الاطلاع عليها، أو إفشاء سريتها، أو تأخيرها، أو مصادرتها، إلا في الأحوال التي يبينها القانون، ووفقًا للإجراءات المحددة فيه".

[5]. Jannik Lindner, Ai In Law Enforcement Statistics, WORLDMETRICS REPORT 2024, June 17, 2024. On the following link: https://worldmetrics.org/ai-in-law-enforcement-statistics/

[6] ولعلّ برنامج "Operation LASER" من أشهر برامج التنبؤ بالجريمة والذي اضطلعت باستخدامة شرطة لوس انجلوس منذ عام 2011، كذلك برنامج "COMPAS" المعمول به في ولاية ويسكونسن الأمريكية "Wisconsin" منذ

العامين في الولايات المتحدة حاليًا خوارزميات للمساعدة في التنبؤ بمعدلات العودة إلى الجريمة[1]. كما أن هنالك 14 قسم شرطة في المملكة المتحدة يستخدم خوارزميات التنبؤ بالجريمة حتى عام 2019[2].

شاع كذلك استخدام الشرطة التنبؤية في كل من أستراليا[3] واليابان[4] وكندا[5]. أما على المستوى العربي بدأت شرطة دبي في اعتناق نظم الشرطة التنبؤية منذ عام 2016[6].

شباط/فبراير 2013، وبرنامج "PredPol" الذي استخدم من قبل شرطة نيويورك والذي يعمل من خلال النظر إلى منطقة جغرافية محددة، حيث يتم تقسيم خريطة الدائرة إلى "مربعات" تبلغ مساحتها 500 قدم مربع، كل منها بحجم كتلة سكنية. ويصبح المربع الذي يُعتقد أنه من المرجح أن يكون مركزاً للجريمة، بسبب تاريخه وموقعه والنشاط الحالي وغير ذلك من العوامل ـ "مربعاً ساخناً–hot box".. يرجع في ذلك إلى؛

David Black, Predictive Policing Is Here Now, The Dallas Morning News, February 26th, 2016, On the following link: https://manhattan.institute/article/predictive-policing-is-here-now

وقد قارنت إدارة شرطة سانتا كروز إحصاءات الجريمة من الأشهر الستة الأولى من عام 2012، بالإطار الزمني نفسه في عام 2011، عندما لم يتم استخدام التحليلات المتقدمة وتكنولوجيا التنبؤ مع الحد من إضافة المزيد من الضباط إلى الشوارع أو تغيير الدورات وأوقات المناوبة، كانت النتائج انخفاضًا بنسبة 19% في سرقة الممتلكات. يرجع في ذلك إلى؛

Miriam Jones, Predictive Policing a Success in Santa Cruz, Calif, Government Technology, October 08, 2012, On the following link: https://www.govtech.com/public-safety/predictive-policing-a-success-in-santa-cruz-calif.html

[1] ·Jannik Lindner, Ai In Law Enforcement Statistics, WORLDMETRICS REPORT 2024, June 17, 2024. On the following link: https://worldmetrics.org/ai-in-law-enforcement-statistics/

[2] ·Leo Kelion; Crime prediction software 'adopted by 14 UK police forces', BBC, 4 February 2019. On the following link: https://www.bbc.com/news/technology-47118229

[3] ·Rick Sarre, Ben Livings; Artificial Intelligence and the Administration of Criminal Justice: Predictive Policing and Predictive Justice. Australia Report. University of South Australia. May 2023. On the following link: https://www.penal.org/sites/default/files/files/A-13-2023_0.pdf

[4] ·KYODO, Kanagawa police to launch AI-based predictive policing system before Olympics, the Japan times, Jan 29, 2018. On the following link: https://www.japantimes.co.jp/news/2018/01/29/national/crime-legal/kanagawa-police-launch-ai-based-predictive-policing-system-olympics/

[5] ·Harvin Bhathal, Canada’s Predictive Policing Tech Is Poorly Regulated Under AI Policy, TRUTHOUT, June 13, 2022, On the following link:https://truthout.org/articles/canadas-predictive-policing-tech-is-poorly-regulated-under-ai-policy

[6] " أن شرطة دبي طورت برمجيات خاصة للتنبؤ بالجريمة، Space Imaging Middle East" SIME· أعلنت شركة حيث يتم تحليل أنماط من قواعد بيانات الشرطة في محاولة لاكتشاف متى وأين من المرجح حدوث الجريمة. مقال بعنوان: شرطة دبي تستخدم الذكاء الاصطناعي للتنبؤ بالجريمة قبل وقوعها، 2016، على الرابط الآتي بتاريخ دخول :2024/6/10https://shorturl.at/T9N0h

وقد بلغ تقدير حجم سوق الشرطة التنبؤية عالمياً، نحو 5.17 مليار دولار أمريكي في عام 2023، ومن المتوقع أن يصل إلى 5.96 مليار دولار أمريكي بنهاية عام 2024 ، بمعدل نمو سنوي مركب قدره 16.23٪ ليصل إلى 14.82 مليار دولار أمريكي بحلول عام 2030[1].

مظاهر أهمية البحث:

تتبدى أهمية البحث من الناحية النظرية، في المخاطر الناجمة عن شيوع وانتشار استخدام التنبؤ الشرطي رغم مميزاته[2]، وبالأخص تأثيره على الحق في الخصوصية الرقمية، إذ أضحى الإنسان مجموعة من البيانات بالتزامن مع ما نعيشه اليوم من عصر رقمي، ولعلّ غموض آلية عمل خوارزميات الشرطة التنبؤية وضحالة الشفافية بها، يزيد من مخاوف انتهاك خصوصية البيانات وبالأخص الشخصية منها،

---

[1] Predictive Policing Market by Technology (Crime Analysis, Facial Recognition Technology, Geo-Location Technology), End-Use (Detective Agencies, Law Enforcement Organization, Military & Defense) - Global Forecast 2024-2030.

[2] ولعلّ من أهم ميزات التنبؤ الشرطي هو الحد من ارتكاب الجرائم الذي انخفض على سبيل المثال بنسبة 19% في جرائم السرقة في مدينة سانتا كروز – Santa Cruz في كاليفورنيا–California الأمريكية، كذلك انخفض معدل الجرائم بنسبة 12% في ولاية لوس أنجلوس– Los Angeles، وفي ولاية نيوجيرسي تقلصت جرائم القتل بنسبة 41٪، وانخفض معدل جميع الجرائم في المدينة بنسبة 26٪، يرجع في ذلك إلى؛

Alice Norga, 4 Benefits And 4 Drawbacks Of Predictive Policing, TECH & RIGHTS, July 12, 2021, On the following link: https://www.liberties.eu/en/stories/predictive-policing/43679

أما دبي، ففي غضون أشهر من اعتماد خوارزميات التنبؤ بالجريمة، تمكنت إدارة الشرطة من الحد من بعض الجرائم بنسبة 25٪ مقارنة بالعام السابق ومن خلال تحليل بيانات الجريمة، تمكنت الإدارة الشرطية في دبي من تحديد المناطق والأطر الزمنية ذات الاحتمالية العالية لجرائم الممتلكات مثل السرقة وسرقة المركبات ومن خلال إعطاء الأولوية للدوريات والمشاركة المجتمعية في هذه المناطق، انخفضت معدلات الجرائم الكبرى والصغرى، يرجع في ذلك إلى:

Predictive Policing: Using Data to Target Crime, Not Communities, Case Studies, On the following link: https://ignesa.com/insights/predictive-policing/

يضاف لميزة درء الجرائم قبل وقوعها، ميزة أخرى تكمن في اتخاذ القرارات المستنيرة لمأموري الضبط القضائي في أقسام الشرطة التنبؤية الأمر الذي يجنبهم إصدار قرارات اعتقال أو ضبط تعسفية أو مبنية على معلومات وأدلة سطحية، فالخوارزميات قادرة على مساعدة مأموري الضبط على التنبؤ بالمخاطر بشكل أفضل، وتحديد هوية الجناة، وتحديد الأماكن الأكثر عرضة لارتكاب الجرائم، وذلك من خلال تحليل كم هائل من البيانات يتأبّى على الأشخاص العاديين تحليله مما يقلص معه وقت اتخاذ التدابير اللازمة وقلة التكلفة كذلك. محمود سلامة الشريف: الطبيعة القانونية للتنبؤ بالجريمة بواسطة الذكاء الاصطناعي ومشروعيته، المرجع السابق، ص342.

والتي يتم تجميعها من خلال كاميرات المراقبة ونظم التعرّف على الوجه، والتتبع الجغرافي ووسائل التواصل الاجتماعي وتطبيقات الهاتف المحمول وملفات التعريف وغيرها من مصادر مرتبطة بالبيئة الرقمية والإنترنت[1]، ولا شك أن تلك المخاطر تتضاعف حال تسريب تلك البيانات الشخصية سواء عمداً أو عن طريق الخطأ[2]. من الجدير بالذكر أن تلك المخاوف قادت الاتحاد الأوروبي لحظر عمل الشرطة التنبؤية جزئياً[3]، بموجب قانون الذكاء الاصطناعي الجديد – Artificial Intelligence Act الصادر في أيار/مايو 2024[4]، والتي صدرت لائحته رقم (1689/2024) ونشرت في الجريدة الرسمية في

---

1. ولا يقتصر حصر وجمع البيانات الشخصية من تلك الوسائل فقط، وإنما أيضا من خلال الإقامة في المدن الذكية التي تعتمد بشكل أساسي على بيانات قاطنيها وبيانات جوانب مختلفة من حياة المدينة، مثل حركة المرور والصحة والطقس وإدارة النفايات، وكاميرات المرور، وغيرها، والمتوقع أنه سيعيش في تلك المدن 68% من سكان العالم بحلول عام 2050، بحسب الأمم المتحدة، وتعتمد المدن الذكية على تقنيات إنترنت الأشياء (IoT) وشبكة استشعار موزع (Distributed Sensing)، والذكاء الاصطناعي لجمع البيانات الضخمة (Big Data)، وبرامج تحليلية ترتكز على الذكاء الاصطناعي والتعلم العميق (Deep Learning)، وقوة حاسوبية (Computing Power) توفر معالجة آنية سريعة لعدد كبير من المتغيرات، وتقنية سلسلة الكتل (blockchain) ، يرجع في ذلك إلى:

Alyse Burnside, IT Security Challenges Emerge in Smart Cities, January 19, 2023, On the following link: https://www.itprotoday.com/vulnerabilities-threats/it-security-challenges-emerge-in-smart-cities

2 .Alice Norga, 4 Benefits And 4 Drawbacks Of Predictive Policing, TECH & RIGHTS, July 12, 2021, On the following link: https://www.liberties.eu/en/stories/predictive-policing/43679

3. دعت منظمة "المحاكمات العادلة- Automating Injustice" لأول مرة إلى حظر أنظمة "التنبؤ" والتصنيف في الشرطة والعدالة الجنائية في عام 2021، وقادت المنظمة حملة من أجل إقرار هذا الحظر إلى جانب منظمة الحقوق الرقمية الأوروبية (EDRi) وأكثر من 50 منظمة من منظمات المجتمع المدني الأخرى. وبعد تجاذب الآراء والمفاوضات التي استمرت لثلاثة أيام عمل، صوتَ أعضاء البرلمان الأوروبي لصالح الحظر بأغلبية 523 صوتًا و46 صوتًا رفضه و49 امتنع عن التصويت، والذي من شأنه حظر استخدام أنظمة الذكاء الاصطناعي "لإجراء تقييمات مخاطر الأشخاص الطبيعيين أو المجموعات" سواء المتعلقة "بتقييم خطر تعرض شخص طبيعي لارتكاب جريمة أو إعادة ارتكاب جريمة"، وكذلك "التنبؤ بحدوث أو تكرار جريمة جنائية فعلية أو محتملة". وتجدر الإشارة إلى أن هذا الحظر هو الأول من نوعه في أوروبا، والعالم. يرجع في ذلك إلى؛

Fair Trials, Partial ban on ‘predictive’ policing and crime prediction systems included in final EU AI Act, 11 December 2023, On the following link: https://www.fairtrials.org/articles/news/partial-ban-on-predictive-policing-included-in-final-eu-ai-act/

4. Artificial Intelligence Act

حزيران/يونيو 2024[1]، والذي تحظر قواعده الجديدة بعض تطبيقات الذكاء الاصطناعي التي تهدد حقوق المواطنين، بما في ذلك أنظمة تصنيف البيانات الحيوية (البيومترية)[2]، القائمة على السمات البشرية الحساسة والاستخراج غير المجدي لصور الوجه من الإنترنت أو لقطات كاميرات المراقبة لإنشاء قواعد بيانات التعرّف على الوجه دون مبرر، كما حظر القانون المستحدث التعرف على المشاعر والسلوك في مكان العمل والمدارس، والتقييم الاجتماعي[3].

أما من الناحية العملية، تكمن أهمية البحث في بيان آلية توظيف البيانات الشخصية في تطبيقات وبرامج الشرطة التنبؤية، ومراحل جمع ومعالجة وتحليل البيانات الشخصية، وتحديد البيانات الأكثر عرضة للانتهاك، فضلًا عن بيان الضمانات القانونية التي أضفتها التشريعات على تلك البيانات حال التنبؤ بالجريمة، وبخاصة القانون الأوروبي الجديد للذكاء الاصطناعي الصادر في عام 2024.

---

[1] REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)

[2] البيانات الحيوية البيومترية هي تلك "البيانات الشخصية الناتجة عن المعالجة باستخدام تقنية محددة تتعلق بالخصائص الجسدية أو الفسيولوجية أو السلوكية لصاحب البيانات والتي تسمح بتحديد أو تؤكد التحديد الفريد لصاحب البيانات مثل صورة الوجه أو بيانات البصمة". يرجع في ذلك إلى:

The data divide: Overcoming an increasing practitioner-academic gap, Larissa Fast, 2 November 2017, On the following link: https://blogs.icrc.org/law-and-policy/2017/11/02/the-data-divide-overcoming-an-increasing-practitioner-academic-gap/

[3] نظام التقييم الاجتماعي، أو الدرجة الاجتماعية، هو نظام يُستخدم لقياس سلوك الأفراد وموثوقيتهم في مجتمع ما، وذلك من خلال جمع وتحليل البيانات عنهم من مصادر مختلفة، مثل السجلات المالية: مثل سجلات الائتمان، وسجلات المدفوعات، وسجلات القروض. والسلوكيات على الإنترنت: مثل نشاطهم على مواقع التواصل الاجتماعي، ومواقع التسوق الإلكتروني، ومحركات البحث. والسلوك المدني: مثل احترام القوانين، ودفع الضرائب، والتطوع في المجتمع. ولا شك أن جمع وتحليل كميات هائلة من تلك البيانات الشخصية يُشكل تهديدًا كبيرًا للخصوصية.

Artificial Intelligence Act: MEPs adopt landmark law, Press Releases, On the following link: https://www.europarl.europa.eu/news/en/press-room/20240308IPR19015/artificial-intelligence-act-meps-adopt-landmark-law

نطاق البحث:

يشمل نطاق البحث تحديد البيانات الشخصية التي تستخدم في خوارزميات الشرطة التنبؤية، والأساس القانوني لحمايتها، ونطاق هذه الحماية، وموقف القانون الأوروبي للذكاء الاصطناعي المستحدث في 2024 منها، والضمانات التي أضافها القانون الأخير على البيانات الشخصية، بالمقارنة مع وضع كلًا من المشرع المصري والعُماني، وبالتالي يخرج عن نطاق البحث المسائل التقنية المتعلقة بإنشاء خوارزميات التنبؤ ذاتها أو تأثيرها على العدالة التنبؤية في مرحلتي التحقيق والمحاكمة الجنائية.

مشكلة البحث وتساؤلاته:

مشكلة البحث الرئيسية هي ماهية أوجه حماية الحق في الخصوصية الرقمية في مرحلة الشرطة التنبؤية، ويتفرع عن هذه الإشكالية عدة تساؤلات يجاب عليها خلال البحث لعل أهمها،

1. ما المقصود بالشرطة التنبؤية، وما هي آلية عمل خوارزمياتها، وما هي الأساليب والمسارات التي تضطلع بها لدحض الجريمة قبل وقوعها؟
2. ما هي البيانات التي تجسد مفهوم الحق في الخصوصية في البيئة الرقمية؟ وهل يكتفى بتغذية خوارزميات التنبؤ بالبيانات الشخصية وثيقة الصلة بالجرائم فقط أم تمتد لغيرها؟
3. ما هو الأساس القانوني لحماية البيانات الشخصية باعتبارها وقود خوارزميات التنبؤ بالجريمة في التشريعات الوطنية والمقارنة؟
4. ما هي الضمانات والاستثناءات التي أوردها قانون الذكاء الاصطناعي الأوروبي الجديد الصادر في 2024، بشأن استخدام البيانات الشخصية للتنبؤ بالجريمة؟

مناهج البحث:

اعتمدت هذه الورقة استخدام المنهج الوصفي والتحليلي والمقارن وذلك لوصف وتحليل النصوص التي أوردها المشرع الأوروبي في قانون الذكاء الاصطناعي الجديد لديه بشأن الضمانات التي أوردها لحماية البيانات الشخصية الرقمية حال عمل الشرطة التنبؤية، ومقارنته مع كل من المشرعين المصري والعُماني.

خطة البحث:

يُقسم البحث إلى مبحثين على النحو الآتي ؛ المبحث الأول يتناول البيانات الشخصية المستخدمة في خوارزميات التنبؤ الشُرطي. أما المبحث الثاني فيتناول نطاق حماية البيانات الشخصية محل خوارزميات التنبؤ الشرطي.

المبحث الأول

البيانات الشخصية المستخدمة في خوارزميات التنبؤ الشُرطي

تمهيد

ترتبط البيانات الشخصية ارتباطًا وثيقًا بالخصوصية الرقمية، فكلما زادت كمية البيانات الشخصية التي يتم جمعها أو معالجتها عن الفرد، زاد احتمال تعرض خصوصيته للخطر، وتُعد البيانات الشخصية[1]وقود برامج وتطبيقات الشرطة التنبؤية، وتتم تغذية البيانات التي تجمعها أقسام الشرطة التنبؤية

[1]. جاء تعريف البيانات الشخصية في المادة 4/1 من اللائحة الأوروبية العامة لحماية البيانات (GDPR) لعام 2016؛ حيث نصت على أن البيانات الشخصية هي المعلومات التي ترتبط بشخص طبيعي معروف الهوية أو يمكن معرفة هويته (موضوع البيانات - Data subject)، والشخص الطبيعي الذي يمكن معرفة هويته هو شخص يمكن التعرف عليه بشكل مباشر أو غير مباشر، على وجه الخصوص بالرجوع إلى معرفٍ مثل الاسم، رقم الهوية، بيانات الموقع، عرف إلكتروني أو إلى عامل أو أكثر من العوامل الخاصة بالهوية الجسمانية، الفسيولوجية، الجينية، العقلية، الاقتصادية، الثقافية أو الاجتماعية لذلك الشخص الطبيعي.

Article 4/1: 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

وعرَّف قانون مكافحة جرائم تقنية المعلومات أو جرائم الإنترنت المصري رقم (175) لسنة 2018، البيانات الشخصية بأنها "أي بيانات متعلقة بشخص طبيعي محدد أو يمكن تحديده، بشكل مباشر أو غير مباشر عن طريق الربط بينها وبين بيانات أخرى". أما قانون حماية البيانات الشخصية المصري الجديد رقم (151) لعام 2020، عرَّف البيانات الشخصية، بأنها أي معلومات عن الفرد التي تكون هويته محددة أو يمكن تحديدها بصورة معقولة سواء من خلال البيانات أو عن طريق الجمع بينها وبين آية بيانات أخرى بما في ذلك الصوت والصورة، كما عرَّف معالجة البيانات الشخصية بأنها كل عملية أو مجموعة عمليات تجري على البيانات الشخصية.

وقد فرَّق بين البيانات الشخصية العادية، والبيانات الشخصية الحساسة، فقد عرفت المادة (أ) من الباب الأول الموسوم بتعريفات، البيانات الشخصية العادية بأي بيانات متعلقة بشخص طبيعي محدد أو يمكن تحديده بشكل مباشر أو غير مباشر عن طريق الربط بينها وبين بيانات أخرى كالاسم أو الصوت أو الصورة، أو رقم تعريفي أو محدد للهوية عبر الإنترنت أو أي بيانات تحدد الهوية النفسية أو الصحية أو الاقتصادية أو الثقافية أو الاجتماعية.

أو تستعين بها حول نوع وموقع وتاريخ ووقت الجرائم السابقة وتحليلها بواسطة خوارزميات الذكاء الاصطناعي؛ لتوليد توقعات حول متى وأين وما هي أنواع الجرائم الأكثر احتمالاً لحدوثها، بغية تحديد البؤر الإجرامية أو تحديد مرتكبيها أو ضحاياها المحتملين، الأمر الذي يمنح لمأموري الضبط القضائي مزية دحض الجريمة استباقياً، والتي يُمكن تصنيفها إلى ثلاث فئات رئيسية؛ هي، بيانات شخصية وثيقة الصلة بالجرائم، وبيانات شخصية عامة، وبيانات بيومترية، ونتناول هذه الفئات في الآتي؛

المطلب الأول

بيانات شخصية وثيقة الصلة بالجرائم

تتضمن هذه البيانات معلومات حول الأشخاص الذين تم القبض عليهم أو اتهامهم بارتكاب جرائم، مثل تاريخ القبض، وسببه، والتهم الموجهة إليهم، ونوع الجريمة التي ارتكبوها ما إذا كانت من قبيل جرائم الأموال العامة أم الخاصة أو الاعتداء على الأشخاص أو غيرها، ومدى جسامتها ما إذا كانت بسيطة أم شديدة الخطورة[1]. يدخل أيضًا في إطار البيانات ذات الصلة الوثيقة بالجرائم، بيانات السجلات الجنائية وتشمل الصحيفة الجنائية معلومات حول الأشخاص الذين أدينوا بارتكاب جرائم سابقة، والعقوبات التي حُكم بها عليهم، والمحكمة التي امتثلوا أمامها، وكنه الجريمة وملابساتها والظروف التي دفعتهم لارتكابها، ومدة العقوبة، ومكان ارتكابها[2].

أما البيانات الشخصية الحساسة، فقد عرَّفتها المادة ذاتها بأنها؛ البيانات التي تفصح عن 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.

أما المُشرع العُماني فقد عرَّف البيانات الشخصية بالمرسوم السلطاني رقم 6 / 2022 في المادة الأولى بأنها "البيانات التي تجعل شخصًا طبيعيًا مُعرفًا، أو قابلًا للتعريف بطريقة مباشرة، أو غير مباشرة، وذلك بالرجوع إلى معرفٍ أو أكثر، كالاسم أو الرقم المدني أو بيانات المعرفات الإلكترونية أو البيانات المكانية، أو بالرجوع إلى عامل أو أكثر خاص بالهوية الجينية أو الجسدية أو العقلية أو النفسية أو الاجتماعية أو الثقافية أو الاقتصادية".

[1] Portland State University (PSU). 2012. Predictive Policing: A Review of Literature. Criminology and Criminal Justice Senior Capstone Project, Paper 5. On the following link: http://pdxscholar.library.pdx.edu/ccj_capstone/5

[2] محمود سلامة الشريف: الطبيعة القانونية للتنبؤ بالجريمة بواسطة الذكاء الاصطناعي ومشروعيته، المرجع السابق، ص347.

يشمل هذا النوع من البيانات كذلك كل الإجراءات الجنائية التي اتُخذت ضد الأشخاص ذات الصلة بالجرائم كبيانات محاضر الاستدلال والتحقيقات كافة التي اتُخذت ضدهم لا سيما بيانات استجوابهم وبيانات أوامر الحبس الاحتياطي الصادرة في مواجهتهم من حيث المدة والسبب، وغيرها من الإجراءات القضائية الأخرى. يضاف إلى ذلك بيانات الإحصاءات الجنائية، والتي تتضمن معلومات حول معدلات الجريمة في مناطق مختلفة، وأنواع الجرائم الأكثر شيوعًا، والخصائص الديموغرافية للجناة.

درجت كذلك أقسام الشرطة التنبؤية على تدشين قواعد بيانات شخصية –database تتم تغذية خوارزميات التنبؤ بها للمساعدة في التنبؤ ودرء الجرائم قبل وقوعها، وتسمى بـ "قواعد بيانات قبل الجريمة– Pre-crime database" ولعل من أشهر أمثلتها نظام "E–CAF" الذي يتنبأ بمن يميل من الصغار أو القُصَر إلى ارتكاب الجرائم، والتدخل قبل حدوث ذلك، ويعمل هذا النظام على أساس البيانات الشخصية وثيقة الصلة بالجرائم وعوامل الخطورة نحو الانحراف[1].

تجدر الإشارة إلى أن البيانات الشخصية وثيقة الصلة بالجرائم لا تضطلع منفردة بإتمام عمل الخورازميات بتنبؤ جريمة ما، إذ يتطلب الأمر إدخال بيانات أخرى عامة تساعد في تحسين مخرجات تلك الخوارزميات في عملية التنبؤ، فعلى سبيل المثال يُشترط إدخال البيانات الجغرافية لمنطقة معينة، وعدد سكانها، ومواقيت الاكتظاظ، وعدد المركبات، وأماكن الأعمال، والمجمعات السكنية والتجارية، وغيرها من البيانات لغرض تحديد البؤر الأكثر عرضه لارتكاب جرائم معينة.

المطلب الثاني

بيانات شخصية عامة

تتضمن هذه البيانات مجموعة من المعلومات الديموغرافية عن السكان بشكل عام لا سيما حول العمر، والجنس، والعرق، والمكان، والحالة الاجتماعية، ومستوى التعليم، والوضع المالي، يُضاف إلى تلك البيانات تتبع سلوكيات المواطنين عبر وسائل التواصل الاجتماعي ونشاطاتهم لا سيما المنشورات، والتعليقات، والصور، والرسائل، وغيرها[2].

---

1. Rosamunde Van Brakel and Paul De Hert,"Policing, surveillance and law in a pre-crime society: Understanding the consequences of technology based strategies", in Technology-led policing, eds, Piet Deelman, et al Antwerpen, Belgium: Maklu Publishers, 2011). 174.

2. Browning, Christopher R., Reginald A. Byron, Catherine A. Calder, Lauren J. Krivo, Mei-Po Kwan, Jae-Yong Lee, and Ruth D. Peterson. 2010. Commercial density, residential

يتم دمج هذه البيانات جنبًا إلى جنب مع البيانات العامة الأخرى مثل بيانات كاميرات المراقبة التي تتضمن صورًا وفيديوهات للأشخاص في الأماكن العامة، مثل الشوارع، والمناطق التجارية، ووسائل النقل العام. كذلك بيانات أنظمة التعرف على الوجه التي تتضمن ملامح الوجه للأشخاص، ويتم استخدامها لمطابقة الأشخاص مع الصور والفيديوهات. ومن البيانات المهمة كذلك في التنبؤ بالجريمة بيانات أنظمة تحديد المواقع الجغرافية (GPS) والتي تتضمن معلومات حول مكان تواجد الأشخاص في الوقت الفعلي[1].

ومن الأساليب التي تعتمد على البيانات الشخصية العامة أيضًا ما يُعرف "باستخبارات المصادر المفتوحة" Open source intelligence (OSINT)، والتي تقوم على تجميع البيانات من المصادر المفتوحة المتاحة للجمهور[2]، كوسائل الإعلام المرئية أو المسموعة أو المقروءة، والإنترنت، كالشبكات الاجتماعية وغيرها، وكل مصادر المعلومات الأخرى المتاحة، وهذا عكس أسلوب استخبارات المصادر السرية أو المغلقة Covert sources، أي غير المتاحة للجمهور[3].

ومن تطبيقات تتبع البيانات الشخصية العامة لتوظيفها في التنبؤ بالجريمة، نظام مراقبة الحدود Borders control والمثال الأبرز على ذلك "نظام سجل اسم المسافر– Passenger name (PNR)" الذي يعتمد على البيانات الشخصية في تقييم "خطورة المسافرين" من خلال تحليل البيانات المخزنة داخله

concentration, and crime: Land use patterns and violence in neighbourhood context. Journal of Research in Crime and Delinquency 47: 329–57.

حوراء موسى، الجرائم المرتكبة عبر وسائل التواصل الاجتماعي، دراسة مقارنة، دار النهضة العربية، 2018، ص93.

أشرف جابر سيد، الجوانب القانونية لمواقع التواصل الاجتماعي، دار النهضة العربية، 2013، ص5.

[1]. تامر صالح: التتبع الجغرافي للمتهم بواسطة تقنية (GPS) والحق في الخصوصية، مجلة البحوث القانونية والاقتصادية، عدد خاص بالمؤتمر الدولي السنوي العشرون، كلية الحقوق، جامعة المنصورة، 23–24 أيار/مايو 2021، ص718.

[2]. هيثم السيد أحمد عيسى: التشخيص الرقمي لحالة الإنسان في عصر التنقيب في البيانات عبر تقنيات الذكاء الإصطناعي وفقاً للائحة الأوروبية العامة لحماية البيانات لعام 2016، دار النهضة العربية، 2019، ص36.

3. Heather J. Williams and Ilana Blum, Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise (California ,US: RAND Corporation, 2018), 8

بواسطة عملية "التنقيب في البيانات– Data Mining DM[1]، وذلك بغية اتخاذ الإجراء المناسب حيال المسافرين الأكثر خطورة عند وصولهم إلى موانئ الدولة أو منعهم من السفر[2].

المطلب الثالث

بيانات شخصية بيومترية

عرّفت المادة (15) من مواد إصدار اللائحة الأوروبية رقم (1689/2024) بشأن قانون الذكاء الاصطناعي الجديد لعام 2024، الهوية البيومترية بأنها "التعرف الآلي على السمات البشرية الجسدية كشكل الوجه وحركة العين وشكل الجسم والصوت وفصيلة الدم ومعدل نبض القلب وغيرها من البيانات الفسيولوجية والسلوكية، كطريقة المشي وبصمات الأصابع ومسح شبكية العين"[3]، والتصنيف البيومتري للأشخاص هو "تحديدهم وفرزهم لفئات بحسب بياناتهم البيومترية اعتمادًا على الجنس أو العمر أو لون الشعر أو لون العين أو الوشم أو السمات السلوكية أو اللغة أو الدين أو العرق، أو التوجه الجنسي أو السياسي"[4].

---

[1]. سيف الدين عثمان فتوح والشفيع جعفر محمود، "التنقيب في البيانات واتخاذ القرارات"، مجلة النيل الأبيض للدراسات والبحوث، كلية النيل الأبيض للعلوم والتكنولوجيا، جامعة النيل الأبيض، العدد الثالث، 2014، ص3–4.

[2]. Els de Busser, Data Protection in EU and US Criminal Cooperation: A Substantive Law Approach to the EU Internal and Transatlantic Cooperation in Criminal Matters Between Judicial and Law Enforcement Authorities (Antwerpen Belgium: Maklu Publishers, 2009), 359-360; U.S. Department of Homeland Security, U.S. Customs and Border Protection, Washington, DC 20229, "U.S. Customs and Border Protection Passenger Name Record (PNR) Privacy Policy, (June 21, 2013). p. 1-8.
https://www.cbp.gov/sites/default/files/documents/pnr privacy_3.pdf. 5/2/2019

3.(15) The notion of 'biometric identification' referred to in this Regulation should be defined as the automated recognition of physical, physiological and behavioural human features such as the face, eye movement, body shape, voice, prosody, gait, posture, heart rate, blood identity by comparing biometric data of that individual to stored biometric data of individuals in a reference database, irrespective of whether the individual has given its consent or not. This excludes AI systems intended to be used for biometric verification ,which includes authentication, whose sole purpose is to confirm that a specific natural person is the person he or she claims to be and to confirm the identity of a natural person for the sole purpose of having access to a service, unlocking a device or having security access to premises.

4 (16) .The notion of 'biometric categorisation' referred to in this Regulation should be defined as assigning natural persons to specific categories on the basis of their biometric data. Such specific categories can relate to aspects such as sex, age, hair colour, eye colour, tattoos behavioural or personality traits, language, religion, membership of a national minority sexual

ترتبط البيانات البيومترية بالجسد البشري وخصائصه الفريدة، مما يجعلها شديدة الخصوصية، ويُثير ذلك مخاوف بخصوص جمع ومعالجة هذه البيانات وتخزينها واستخدامها في خوارزميات الشرطة التنبؤية باعتبارها جزءًا من البيانات الشخصية الحساسة[1]، التي أضفى المُشرع حماية خاصة لها من بينها ضرورة الحصول على موافقة كتابية وصريحة من الشخص المعني حال التعامل فيها[2]. ومن الأمثلة على ذلك قاعدة البيانات البيومترية biometric database التي يستخدمها مكتب التحقيقات الفيدرالي الأمريكي

---

or political orientation. This does not include biometric categorisation systems that are a purely ancillary feature intrinsically linked to another commercial service, meaning that the feature cannot, for objective technical reasons, be used without the principal service, and the integration of that feature or functionality is not a means to circumvent the applicability of the rules of this Regulation. For example, filters categorising facial or body features used on online marketplaces could constitute such an ancillary feature as they can be used only in relation to the principal service

[1]. نصت المادة الأولى من قانون رقم (151) لسنة 2020،بشأن إصدار قانون حماية البيانات الشخصية المصري على أن "البيانات الشخصية الحساسة: البيانات التي تفصح عن 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". يلاحظ من نص المادة أن البيانات البيومترية جزءًا من البيانات الشخصية الحساسة، ولم يضطلع المُشرع المصري بوضع تعريف لها كما فعل المُشرع الأوروبي في قانون الذكاء الاصطناعي لعام 2024. وكذلك المشرع العُماني الذي عرَّفها في أكثر من بند في المادة الأولى من مرسوم سلطاني رقم (6/ 2022) بأن "البيانات الجينية: البيانات الشخصية المتعلقة بالخصائص الموروثة، أو المكتسبة جينيًا، والتي تنتج عن تحليل العينة البيولوجية. البيانات الحيوية: البيانات الشخصية التي تنتج عن معالجة فنية محددة تتعلق بالخصائص الجسدية أو النفسية أو السلوكية كصورة الوجه، أو بيانات البصمة الوراثية. البيانات الصحية: البيانات الشخصية المتعلقة بالصحة الجسدية، والعقلية، والنفسية.

[2]. المادة (12) من قانون رقم (151 لسنة 2020) بشأن إصدار قانون حماية البيانات الشخصية المصري نصت على "يحظر على المتحكم أو المعالج سواء كان شخصًا طبيعيًا أو اعتباريًا جمع بيانات شخصية حساسة أو نقلها أو تخزينها أو حفظها أو معالجتها أو إتاحتها إلا بترخيص من المركز. وفيما عدا الأحوال المصرح بها قانونًا، يلزم الحصول على موافقة كتابية وصريحة من الشخص المعني. وفي حالة إجراء أي عملية مما ذكر تتعلق ببيانات الأطفال، يلزم موافقة ولي الأمر. يقابلها المادة (5) من المرسوم السلطاني رقم (2022/6) بشأن إصدار قانون حماية البيانات الشخصية "تحظر معالجة البيانات الشخصية التي تتعلق بالبيانات الجينية أو البيانات الحيوية أو البيانات الصحية أو الأصول العرقية أو الحياة الجنسية أو الآراء السياسية أو الدينية أو المعتقدات أو الإدانة الجزائية أو المتعلقة بتدابير أمنية إلا بعد الحصول على تصريح بذلك من الوزارة، وفقًا للضوابط والإجراءات التي تحددها اللائحة".

FBI في مكافحة الجرائم التي تحتوي على معلومات ترتبط بملايين الأفراد، وتقوم على تحليل البيانات الشخصية الرقمية لهم[1].

تتضافر كل تلك البيانات سواء وثيقة الصلة بالجريمة أو البيانات الشخصية العامة والبيانات البيومترية لغرض واحد فقط وهو التنبؤ الشرطي، وهذا الأخير له أربعة أساليب مختلفة هي، إما التنبؤ بالجرائم، أو التنبؤ بالمجرمين، أو التنبؤ بالبؤر الإجرامية، أو التنبؤ بضحايا الجريمة[2].

وقَدَمَ بعض الفقه[3] منهجية مغايرة للتنبؤ الشرطي تعتمد على ثلاثة أساليب، هي تحليل المكان، وتحليل الوقت، وتحليل الشبكات الاجتماعية. يركز تحليل المكان بشكل أكبر على تحديد البؤر الإجرامية المعروفة بالنقاط الساخنة[4]، بينما يركز تحليل الوقت على اكتشاف المواقع التي من المرجح أن تحدث فيها الأنشطة الإجرامية بناءً على تحليل البيانات التاريخية للجرائم في بقعة مكانية محددة، والغرض الرئيسي من هاتين الفئتين هو استهداف الجريمة مكانيًا وزمانيًا[5]، ويُستخدم الأسلوب الثالث وهو تحليل الشبكات الاجتماعية إلى حدٍ كبيرٍ في الكشف عن الأشخاص محل التحليل سواء المجرمين أو الضحايا[6].

تَمُر البيانات الشخصية السابق ذكرها بمجموعة من المراحل المتتالية حتى تتمكن الخوارزمية المعدة للتنبؤ بإعطاء مخرجات دقيقة، ويمكن حصر تلك المراحل في الآتي،

---

1. Ferraris et al., "Defining Profiling", 22.

2 ·Perry, Walter L., Brian McInnis, Carter C. Price, Susan Smith, and John S. Hollywood, Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations. Santa Monica, CA: RAND Corporation, 2013. https://www.rand.org/pubs/research_reports/RR233.html

Lopes, Giza, Marvin D. Krohn, Alan J. Lizotte, Nicole M. Schmidt, Bob E. Vasquez, and Jon G. Bernburg. 2012. Labelling and cumulative disadvantage: The impact of formal police Intervention on life chances and crime during emerging adulthood. Crime & Delinquency 58: 456–88.

3 ·Bachner, Jennifer. 2013. Predictive Policing: Preventing Crime with Data and Analytics. Washington, DC: IBM, Centre for the Business of Government, pp. 86–90.

4 ·Lee, YonJei, John Eck, O SooHyn, and Natalie Martinez. 2017. How concentrated is crime at places? A systematic review from 1970 to 2015. Crime Science 6: 1–16.

5 ·Eck, John E., YongJei Lee, O. SooHyun, and Natalie Martinez. 2017. Compared to what? Estimating the relative concentration of crime at places using systematic and other reviews. Crime Science 6: 1–17.

6 ·Weisburd, David. 2015. The law of crime concentration and the criminology of place. Criminology 53: 133–57.

Ferguson, Andrew. 2017. Policing predictive policing. Washington University Law Review 94: 1109–88.

أولًا: جمع البيانات الشخصية (Collection of personal data)، وهي الخطوة الأولى التي تتطلبها خوارزميات الشرطة التنبؤية المدعمة بالتعلم الآلي، ولا شك أنه كلما زادت البيانات، زادت دقة التنبؤات.

ثانيًا: معالجة البيانات الشخصية (Processing of personal data)[1]، قبل أن يمكن استخدام البيانات لتدريب خوارزميات التنبؤ، يجب معالجتها مسبقًا، ويتطلب ذلك تنظيف البيانات وملء القيم المفقودة وتحويل البيانات لجعلها مناسبة للتحليل وإعادة تنميطها وهيكلتها[2]، وتُعد معالجة البيانات مسبقًا أمرًا مهمًا لضمان دقة البيانات وتناسقها، مما يؤدي إلى تحسين دقة التنبؤات.

ثالثًا: التنقيب في البيانات الشخصية (Personal data mining)، وقد كان لتضخم البيانات الشخصية تزايدًا في استخدام تقنيات التنقيب في البيانات DM في بناء ملفات شخصية للأفراد من أجل تحديد ملامح الحالة الشخصية لهم، سواء كانت الحالة الاقتصادية أو الاجتماعية أو الصحية أو النفسية أو المالية أو مدى الثقة المتوفرة فيهم أو قدرتهم على أداء عمل معين أو ميولهم وغير ذلك من الجوانب المختلفة التي تشكل الحالة الشخصية العامة للأفراد[3]. وتعمل خوارزميات الشرطة التنبؤية بالتنقيب في

---

[1]. وعملية المعالجة بوجه عام، وفقا للمادة (4/ 2) من اللائحة الأوروبية العامة لحماية البيانات GDPR هي أي عملية أو مجموعة من العمليات يتم إجراؤها على مجموعة من البيانات الشخصية، سواء بوسائل آلية أم لا، مثال ذلك الجمع، التسجيل، التنظيم، الهيكلة، التخزين، المواءمة، التغيير، الاسترجاع، الاستخدام، الإفصاح عن طريق النقل، النشر، المحو أو غير ذلك.

Article 4/2: 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or therwise making available, alignment or combination, restriction, erasure or destruction. See also: European union agency for fundamental rights and council of Europe, Handbook on European data protection law (Luxemburg: ublications office of the European Union, 2018, 97-98.

[2]. سامح عبد الواحد التهامي: الحماية القانونية للبيانات الشخصية: دراسة في القانون الفرنسي، مجلة الحقوق، كلية الحقوق جامعة الكويت 35، عدد 3، 2011، ص414.

[3]. إيهاب عثمان وعبد الرحمن عثمان: التنبؤات الانتخابية باستخدام تنقيب البيانات، الانتخابات الأمريكية كدراسة حالة، سبتمبر 2016، ص2-4.

https://www.researchgate.net/profile/Abdelrahman_Osman3/publication/307925413_altnbwat_alantkhabyt_bastkhdam_tngyb_albyanat/links/57dle2f708ae0c0081e057b1.pdf

أنمار عرابي: استخدام أدوات التنقيب في البيانات في دراسة تأثير صفات الزبائن على قرار الشراء: دراسة إحصائية لبيانات الزبائن، مجلة العلوم الإدارية والاقتصادية، كلية الاقتصاد والعلوم الإدارية جامعة عدن، عدد5، 2010 ، ص97-113.

البيانات المرتبطة بأفراد عينة لبناء الملفات الشخصية لهم من أجل الكشف عن مدى الخطورة الإجرامية لديهم والتنبؤ بالجرائم قبل وقوعها ومنعها[1].

رابعًا، تدريب الخوارزمية على التنبؤ، بمجرد معالجة البيانات الشخصية وإدراجها في خوارزميات الشرطة التنبؤية، يتم تدريب الخوارزمية باستخدام بيانات مُسمَّاة، حيث تكون المخرجات الصحيحة معروفة أثناء التدريب، يتم ضبط الخوارزمية بغرض تقليل الخطأ بين مخرجاتها المتوقعة والمخرجات الفعلية، وتعتمد دقة الخوارزمية على جودة وكمية البيانات الشخصية المستخدمة للتدريب[2].

خامسًا، تقييم خوارزية التنبؤ الشرطي، بعد تدريب الخوارزمية، يجب تقييمها لتحديد مدى دقتها وفعاليتها. يتم تقييم الخوارزمية على مجموعة منفصلة من البيانات لاختبار قدرتها على تقديم تنبؤات دقيقة على بيانات جديدة[3].

المبحث الثاني

حماية البيانات الشخصية محل خوارزميات التنبؤ الشرطي

تمهيد

نظرًا لأن البيانات الشخصية المستخدمة في خوارزميات الشرطة لتنبؤية تتباين من حيث درجة الخصوصية، فإن التساؤل المطروح الآن هو؛ ما هو الأساس القانوني لحماية تلك البيانات، وما هي الضمانات التي منحها المشرع الأوروبي وبخاصة في قانون الذكاء الاصطناعي المستحدث لها؟

---

[1] هيثم السيد أحمد عيسى: التشخيص الرقمي لحالة الإنسان في عصر التنقيب في البيانات عبر تقنيات الذكاء الإصطناعي وفقاً للائحة الأوروبية العامة لحماية البيانات لعام 2016، المرجع السابق، ص4 و5.

[2] KATARÍNA HIĽOVSKÁ and PETER KONCZ, "Application of Artificial Intelligence and Data Mining Techniques to Financial Markets", Acta všfs 6, (2012): 63. https://pdfs.semanticscholar.org/dl 1 a/4b5f8d7ff01ba8ca25d15423fbc11bf7a56 0.pdf

[3] Model evaluation: After the model has been trained, it must be evaluated to determine its accuracy and effectiveness. The model is evaluated on a separate set of data to test its ability to make accurate predictions on new and unseen data. Model evaluation is important to ensure that the model is not overfitting to the training data, which can reduce its effectiveness in making accurate predictions. Studies have shown that predictive policing using machine learning can be effective in reducing crime rates.
Predictive Policing using Machine Learning, Cogent Infotech, On the following link: https://www.cogentinfo.com/resources/predictive-policing-using-machine-learning-with-examples

المطلب الأول

الأساس القانوني لحماية البيانات الشخصية الرقمية

أضفى المشرع الأوروبي حماية قانونية للبيانات الشخصية بموجب اللائحة الأوروبية العامة لحماية البيانات[1] The general data protection regulation 2016/676 (GDPR)، التي صدرت عن الاتحاد الأوروبي في تاريخ 14 نيسان/بريل عام 2016م، ودخلت إلى حيز النفاذ في تاريخ 25 أيار/مايو 2018م. ووضعت اللائحة معيارًا موضوعيًا للتفرقة بين البيانات الشخصية المشمولة بالحماية وغيرها[2]،

[1] تحقق هذه اللائحة الوحدة التشريعية فيما يتعلق بحماية البيانات الشخصية بين دول الاتحاد الأوروبي؛ ذلك أنها نافذة بذاتها داخل دول الاتحاد دون حاجة إلى إصدار تشريعات وطنية من جانب هذه الدول لتطبيق قواعدها، وهذا هو ما يميز اللوائح الأوروبية EU Regulations عن التوجيهات الأوروبية EU Directives التي تحتاج إلى إصدار تشريعات داخلية في الدول الأعضاء لتطبيق قواعدها.

[2] نص البند (26) من اللائحة على "أنه يؤخذ في الحسبان عند تحديد القابلية للتعرف على الشخص الطبيعي، جميع الوسائل التي من المرجح على نحو معقول استخدامها عند تحديد قابلية الشخص للتعرف، ويرجع إلى العوامل الموضوعية كافة كمقدار الوقت المطلوب لتحديد الهوية وتكاليف ذلك والتكنولوجيا المتاحة وقت المعالجة، وكذلك التطورات التكنولوجية".

Recital No.26: "...To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments..."

وهذا المعيار السابق استُخدم من جانب محكمة العدل الأوروبية The European Court of Justice (ECJ) في قضية Patrick Breyer Bundersrepublick Deutschland التي أثارها مواطن ألماني ضد الحكومية الألمانية نتيجة قيام بعض المواقع التي تديرها مؤسسات تابعة لها، بتخزين عنوان برتوكول الإنترنت الخاص به IP address. بالإضافة إلى مصطلحات البحث وتاريخ الوصول وكمية البيانات، وقد احتجت الحكومة الألمانية بأن عنوان برتوكول الإنترنت (IP)، في هذه القضية كان برتوكولًا متغيرًا Dynamic IP ولا يُعد من البيانات الشخصية؛ ذلك أنه لا يمكن أن يتم التعرف به على هوية المستخدم، وقضت المحكمة في تاريخ 16 أيار/مايو 2016، بأن عنوان برتوكول الإنترنت يُعد من البيانات الشخصية؛ لأنه يمكن من خلاله التعرف على هوية المستخدم مع بيانات أخرى ترتبط به، تستطيع الجهات الحكومية المختصة في ألمانيا طلبها من مزود خدمات الإنترنت Internet service provider (ISP). وأضافت أيضًا المحكمة

وفيما يتعلق باستخدام البيانات الشخصية في خوارزميات الشرطة التنبؤية، ففرقت اللائحة في نطاق الحماية القانونية لتلك البيانات بحسب ما إذا كانت تلك البيانات عامة أو بيانات حساسة[1]. واشترطت لاستخدام البيانات الشخصية العامة للمعالجة بصفة عامة والتنبؤ بصفة خاصة الحصول على رضا الشخص موضوع البيانات[2]، على معالجة بياناته الشخصية لغرض واحد أو أكثر من الأغراض المحددة

بأنه ممكن ألا يكون عنوان برتوكول الإنترنت (IP) من البيانات الشخصية إذا كان تحديد الهوية عن طريقه يحتاج إلى جهد غير متناسب مع الوقت، التكلفة والقوى العاملة.

Patrick Breyer v Bundesrepublik Deutschland.EJC. C-582/14.16/5/2016 ECLI:EU:C:2016:779.https://eurlex.europa.eu/legalcontent/EN/TXT/?uri=CELEX%3A62014CJ 0582.2/2/2019

[1]. ووفقًا للمادة (1/9) من اللائحة يمكن تعريف البيانات الحساسة بأنها البيانات التي تكشف عن الأصل العرقي أو الإثني أو الآراء السياسية أو المعتقدات الدينية والفلسفية أو عضوية النقابات العمالية، وكذلك تشمل البيانات البيومترية والجينية والبيانات المتعلقة بالصحة والحياة الجنسية للفرد.

MIN WANG and ZUOSU JIANG, "The Defining Approaches and Practical Paradox of Sensitive Data: An Investigation of Data Protection Laws in 92 Countries and Regions and 200 Data Breaches in the World", International Journal of Communication 11(2017). https://ijoc.org/index.php/ijoc/article/download/68922111

Bryce Goodman and Seth Flaxman, European Union regulations on algorithmic decision-making and a "right to explanation", Al Magazine 38, No 3(2017): 34. https://arxiv.org/pdf/1606.08813.pdf. 20/3/2019;

والجدير بالإشارة أن البيانات البيومترية التي وردت في التعريف، والتي تُعد نوعًا من البيانات الحساسة، تعني، وفقًا للمادة 4/ 14 من اللائحة، البيانات الشخصية الناتجة من معالجة تقنية معينة ترتبط بالخصائص الفيزيائية أو الفسيولوجية أو السلوكية لشخص طبيعي، والتي تسمح أوتؤكد الهوية الفريدة لذلك الشخص، مثل صور الوجه أو بيانات البصمات كما عرفت أيضا الفقرة الثالثة عشر من الرابعة من اللائحة، البيانات الجينية بانها البيانات الشخصية المتعلقة بالخصائص الجينية الموروثة أو المكتسبة لشخص الشخص، والتي تنجم على وجه الخصوص، عن تحليل عينة بيولوجية من الشخص الطبيعي المعني

[2]. وقد عرّفت اللائحة في المادة (11/4)، الرضا بأنه "أي إشارة حرة، محددة، مستنيرة وليس هناك لَبِس فيها لرغبات الشخص موضوع البيانات، بواسطة تصريح أو فعل إيجابي، يُعَبر بها عن الموافقة على معالجة البيانات الشخصية المرتبطة به".

[2]. Article 4/11: 'consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".

[1]، وأن يكون استخدام البيانات الشخصية للتنبؤ ضروريًا لتنفيذ التزام قانوني. ولا شك أن هذا الشرط يعطي الضوء الأخضر للشرطة التنبؤية لاستخدام تلك البيانات في خوارزميات التنبؤ بالجريمة[2]. ويُشترط أخيرًا أن يكون هنالك ضرورة لاستخدام البيانات الشخصية في التنبؤ وذلك لتحقيق مصلحة سواء للشخص محل البيانات أو مصلحة عامة[3].

وإذا كانت تلك هي المبادئ القانونية التي تحكم استخدام البيانات الشخصية الرقمية العامة لأي غرض ما، إلا أن المُشرع الأوروبي أحاط البيانات الشخصية الحساسة ومن بينها البيانات البيومترية، والبيانات الجنائية ذات الصلة بالجرائم لرقابة أشد، حيث نصت المادة (10) من اللائحة[4]، على أنه لا تتم معالجة البيانات الشخصية المرتبطة بالإدانات أو الجرائم الجنائية أو التدابير الأمنية على أساس المادة (6/1)، وهي الخاصة بمعالجة البيانات العادية كما وضحنا في السابق، إلا تحت رقابة السلطة الرسمية أو عندما يسمح بذلك القانون الأوروبي الاتحادي أو قانون الدول الأعضاء، كما لا يُحتفظ بأي سجل شامل للإدانات الجنائية إلا تحت رقابة السلطة الرسمية[5]. ولعل هذا مفاده أن خوارزميات الشرطة التنبؤية لا يمكن أن تضطلع باتخاذ قرار آلي مباشر دون خضوعه للإشرف والرقابة للسلطة الرسمية وهو ما أكده القانون الأوروبي للذكاء الاصطناعي– Artificial Intelligence Act لعام 2024، إذ نص في المادة (14) على وجوب الإشراف البشري على تقنيات الذكاء الاصطناعي، ويهدف الإشراف البشري إلى منع أو تقليل المخاطر على الصحة أو السلامة أو الحقوق الأساسية التي قد تنشأ عند استخدام نظام الذكاء الاصطناعي عالي المخاطر وفقًا للغرض المقصود منه أو في ظل ظروف إساءة الاستخدام المتوقعة

---

1. Benjamin Docquir, GENERAL DATA PROTECTION REGULATION 2016, Quelles obligations prévoit le projet de règlement européen sur les données personnelles (GDPR) ?(Belgique, Bruxelles: Simont Braun, 2016,p. 20-21.
http://www.simontbraun.eu/images/GDPR_Note_Generale_SimontBraun_Janv_2016.pdf.

2. WP29, "Guidelines on Automated individual decision-making and Profiling", 13.

3. Ibid, 14.

4. Article 10: Processing of personal data relating to criminal convictions and offences: Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority;

5 Kazemi, General Data Protection Regulation, 29

بشكل معقول، خاصةً عندما تستمر هذه المخاطر على الرغم من تطبيق المتطلبات الأخرى المنصوص عليها[1].

أما بخصوص البيانات الشخصية الحساسة ومن بينها البيانات البيومترية فقد حظر القانون الأوروبي للذكاء الاصطناعي الجديد – Artificial Intelligence Act لعام 2024، تقنية "التعرف البيومتري عن بُعد"، مثل أنظمة التعرف على الوجه[2]، في الأماكن العامة، فضلاً عن أنظمة التعرف على المشاعر والمسح الجماعي لقواعد البيانات البيومترية وفقًا لما نصت عليه المادة 5 منه[3]. كما حظرت المادة ذاتها استخدام نظام الذكاء الاصطناعي لإجراء تقييمات مخاطر الأشخاص الطبيعيين من أجل تقييم أو التنبؤ بخطر ارتكاب شخص طبيعي لجريمة جنائية، بناءً على تحديد ملف تعريف الشخص الطبيعي أو تقييم سمات شخصيته وخصائصه فقط[4]؛ غير أن المُشرع الأوروبي وضع استثناءً لهذا الحظر

---

1 .Article 14, Human oversight; 2 .Human oversight shall aim to prevent or minimise the risks to health, safety or fundamental rights that may emerge when a high-risk AI system is used in accordance with its intended purpose or under conditions of reasonably foreseeable misuse, in particular where such risks persist despite the application of other requirements set out in this Section.

2. حظرت المادة (43) من مواد إصدار اللائحة الأوروبية لقانون الذكاء الاصطناعي لعام 2024، استخدام أنظمة الذكاء الاصطناعي التي تنشئ أو توسع قواعد بيانات التعرف على الوجه من خلال جمعها دون مبرر من الإنترنت وكاميرات المراقبة، وهو ما يتعارض مع حقوق الإنسان الأساسية والحق في الخصوصية على وجه الخصوص. يرجع في ذلك إلى النص الآتي؛

(43) The placing on the market, the putting into service for that specific purpose, or the use of AI systems that create or expand facial recognition databases through the untargeted scraping of facial images from the internet or CCTV footage, should be prohibited because that practice adds to the feeling of mass surveillance and can lead to gross violations of fundamental rights, including the right to privacy

3 .Article 5 of the Act, which comprises of a list of 'prohibited practices:' 1 .The following AI practices shall be prohibited....."

4 .EU Parliament approves landmark AI law, The Right to a Fair Trial, including:
Prohibit remote biometric identification (such as face recognition surveillance);
Require public transparency of 'high-risk' AI systems on a public register;
Give people the right to an explanation of an AI system decision;
Give people meaningful ability to challenge AI systems and obtain effective remedies;
Ensure that predictive AI systems in migration are considered high risk;

وأجاز التقييم البشري لتورط شخص ما في نشاط إجرامي، ولكن بشرط أن يستند بالفعل إلى حقائق موضوعية وقابلة للتحقق مرتبطة مباشرة بنشاط إجرامي ما.

ونصت المادة (94) من مواد إصدار اللائحة الأوروبية لقانون الذكاء الاصطناعي لعام 2024، على أنه يحظر معالجة البيانات البيومترية لغرض ما إلا للضرورة القصوى مع الامتثال للمبادئ التي تحكم التعامل في هذا النوع من البيانات التي حددتها اللائحة الأوروبية العامة لحماية البيانات لعام 2016، والتي أهمها الشفافية والنزاهة والتقيد بالغرض[1].

أظهر قانون الذكاء الاصطناعي الأوروبي الجديد – Artificial Intelligence Act لعام 2024، تحدياً كبيرًا في مواجهة إساءة استخدام أدوات الذكاء الاصطناعي، وحظر كل سلوك يتعارض مع قيم الاتحاد المتعلقة باحترام كرامة الإنسان والحرية والمساواة والديمقراطية وسيادة القانون والحقوق الأساسية المنصوص عليها في الميثاق، بما في ذلك الحق في عدم التمييز وحماية البيانات والخصوصية وحقوق الطفل وفقًا لما نصت عليه المادة (28) من مواد إصدار القانون المستحدث[2].

تجدر الإشارة إلى أن المُشرع المصري ونظيره العُماني لم يضطلعا بسن قوانين لتنظيم تقنيات الذكاء الاصطناعي كما فعل المُشرع الأوروبي، كما أن كلا المُشرعان لم يُشرعا تنظيمًا قانونيًا متعلقًا بنشاط الشرطة التنبؤية صراحةً، إلا أنه من خلال نصوص التشريعات الأخرى يمكن أن نستشف قدر الحماية الممنوحة للبيانات الشخصية، فعى سبيل المثال نصت المادة الثانية من مواد إصدار قانون حماية

Ensure that 'high-risk' systems have accessibility requirements for people with disabilities; and widen the definition of AI to cover the full range of AI systems which have been proven to impact fundamental rights. On the following link:
https://www.fairtrials.org/articles/news/eu-parliament-approves-landmark-ai-law/

[1] (94) Any processing of biometric data involved in the use of AI systems for biometric identification for the purpose of law enforcement needs to comply with Article 10 of Directive (EU) 2016/680, that allows such processing only where strictly necessary, subject to appropriate safeguards for the rights and freedoms of the data subject, and where authorised by Union or Member State law. Such use, when authorised, also needs to respect the principles laid down in Article 4 (1) of Directive (EU) 2016/680 including lawfulness, fairness and transparency, purpose limitation, accuracy and storage limitation.

[2] (28) Aside from the many beneficial uses of AI, it can also be misused and provide novel and powerful tools for manipulative, exploitative and social control practices. Such practices are particularly harmful and abusive and should be prohibited because they contradict Union values of respect for human dignity, freedom, equality, democracy and the rule of law and fundamental rights enshrined in the Charter, including the right to non-discrimination, to data protection and to privacy and the rights of the child.

البيانات الشخصية المصري لعام 2020؛ 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.....".

وتلك المادة تقلص بشكل صريح من الحماية الممنوحة للبيانات الشخصية وبخاصة الحساسة تذرعًا بحماية الأمن القومي، وكان حري على المُشرع المصري أن يضع ضوابط لحماية تلك البيانات الشخصية حال استعمالها في التنبؤ الشرطي لا سيما ضرورة الربط بين استخدام البيانات الشخصية وجريمة ارتُكبت بالفعل أو هنالك دلائل قوية على ارتكابها، أو اقتصار إباحة استخدام البيانات الشخصية في خوارزميات الشرطة التنبؤية على الجرائم شديدة الخطورة فقط كالمتعلقة بأمن الدولة الداخلي أو الخارجي[1].

والمُشرع العماني كذلك لم يضع ضوابط صارمة للحد من استخدام البيانات الشخصية في خوارزميات الشرطة التنبؤية، ولم يكن نهجه مختلفًا عما سلكه المُشرع المصري، واستثنى التعامل المطلق في البيانات الشخصية سواء كانت عادية أو حساسة لحماية الأمن الوطني أو الكشف عن الجرائم، حيث نص في المادة (3) من المرسوم السلطاني رقم (2022/6) بشأن إصدار قانون حماية البيانات الشخصية على أنه "لا تسري أحكام هذا القانون على معالجة البيانات الشخصية التي تتم في الأحوال الآتية،

أ- حماية الأمن الوطني، أو المصلحة العامة (...).

و- "كشف أو منع أية جريمة جزائية بناءً على طلب رسمي مكتوب من جهات التحقيق".

وبالتالي يكون المُشرع العُماني كذلك مدعواً لتقليص السلطة المطلقة للجهات الشرطية حال استخدامها للبيانات الشخصية وبخاصة في التنبؤ بالجرائم.

المطلب الثاني

ضمانات حماية البيانات الشخصية في مرحلة الشرطة التنبؤية

نصّت المادة (5) من الباب الثاني من اللائحة رقم (1689/2024) المتعلقة بقانون الذكاء الاصطناعي الأوروبي الجديد لعام 2024، والموسوم بـ "ممارسات الذكاء الاصطناعي المحظورة" على ضمانتين مهمتين لحماية البيانات الشخصية في مرحلة الشرطة التنبؤية وضمان خصوصيتها الرقمية، ونعرض لهاتين الضمانتين على النحو الآتي،

[1]. محمود سلامة الشريف، الطبيعة القانونية للتنبؤ بالجريمة بواسطة الذكاء الاصطناعي ومشروعيته، المرجع السابق، ص347.

أولًا: الارتباط بنشاط إجرامي

حظرت المادة (5) فقرة (1) بند (د) من اللائحة المذكورة أعلاه، تقييم أو تحديد سمات الأشخاص بناءً على بياناتهم الشخصية العادية أو الحساسة أو البيومترية للتنبؤ بالجرائم، وأوردت المادة استثناءً لهذ الحظر العام مفاده جواز هذا النوع من التقييم أو التحديد في حالة تورط شخص ما في نشاط إجرامي بناءً على حقائق موضوعية تربط هذا الشخص ارتباطًا مباشراً بالنشاط الإجرامي[1]. وهنالك ملاحظتين على هذه المادة، الأولى تتعلق بمفهوم عملية التقييم، والثانية تتعلق بمضمون الحظر وهو الارتباط بنشاط إجرامي.

المسألة الأولى: والمتعلقة بالفرق بين مصطلحين أوردتهما المادة، وهما "تقييم السمات الشخصية–assessing" أو "تحديد السمات الشخصية–profiling"، وإن كان يرى البعض[2]، أن كلتاهما بمعنى واحد وأن عملية تقييم السمات الشخصية تستوجب بطبيعة الحال تحديدها، فالتحديد سابق على التقييم، وكان حرّي على المُشرع الأوروبي أن يدمج بينهما. غير أن الفقه الآخر[3] يرى ثمة اختلاف جوهري بين المصطلحين، وهو أن تحديد السمات البشرية هي عملية آلية بالكامل دون تدخل بشري (entirely automated process)، أما عملية تقييم السمات البشرية يكون العامل البشري فيها محل اعتبار، ونظراً لخطورة التنبؤ بالجريمة فيتعين ألا تخضع تلك البيانات الشخصية لقرار آلي محض، وهو ما قد يولد

---

[1] ·Article 5 of the Act, which comprises of a list of 'prohibited practices:'

"(d) the placing on the market, putting into service or use of an AI system for making risk assessments of natural persons or groups thereof in order to assess the risk of a natural person for offending or reoffending or for predicting the occurrence or reoccurrence of an actual or potential criminal offence based on profiling of a natural person or on assessing personality traits and characteristics, including the person's location, or past criminal behaviour of natural persons or groups of natural persons";

[2] ·Sunde, Inger Marie. "AI-Based Law Enforcement Online: The Impact of the European Artificial Intelligence Act (AIA)". Bergen Journal of Criminal Law & Criminal Justice, vol. 10, no. 2, Dec. 2022, pp. 29-50, doi:10.15845/bjclcj.v10i2.3844.

[3] · A difference between "profiling" and "assessing" may lie in the degree of human involvement. While profiling implies an (almost) entirely automated process with no meaningful human intervention, there is no clear indication on the level of human involvement required for "assessing". Jessie Levano, Predictive Policing in the AI Act: meaningful ban or paper tiger? 5 JULY 2024, EUROPEAN LAW BLOG,. On the following link:https://europeanlawblog.eu/2024/07/05/predictive-policing-in-the-ai-act-meaningful-ban-or-paper-tiger/

تناقضًا بين لائحة قانون الذكاء الاصطناعي الجديد لعام 2024، واللائحة الأوروبية لحماية البيانات الشخصية لعام 2016، والتي نصت في المادة (22) منها على الحق في عدم الخضوع للقرار الآلي- "The right not to be subject to automated decision making"[1]، يُضاف إلى ذلك أن لائحة قانون الذكاء الاصطناعي الجديد اشترطت التدخل البشري والإشراف والرقابة على التطبيقات عالية الخطورة للذكاء الاصطناعي لا سيما تطبيقات التنبؤ بالجريمة وفقًا للمادة (14) منها[2]، وذلك لضمان استخدامها الآمن، غير أن المعنى الدقيق لـ "الإشراف البشري" غير واضح في القانون الجديد[3]، وكان حري بالمُشرع أن يحدد درجة التدخل حتى لا يكون هذا الالتزام حبرًا على ورق، إذ إن التدخل البشري قد يقف عند مجرد الضغط على زر نتائج القرار الآلي فقط.

المسألة الثانية: تتعلق بمضمون الحظر وهو ارتباط الشخص المعني بتقييم بياناته الشخصية بنشاط إجرامي، ولكن لم يحدد كذلك المُشرع الأوروبي درجة هذا الارتباط أو حتى معايير يمكن الاستدلال بها على هذا الارتباط، ويكون معيار الارتباط واضحًا إذا ثبت لدى جهاز الشرطة التنبؤية أن الشخص

---

1. راعى المُشرع الأوروبي أن مركز الفرد موضوع البيانات قد يتأثر نتيجة إصدار قرار آلي في مواجهته دون تدخل بشري على أساس المعالجة الآلية لبياناته الشخصية، ومن بين صور هذه المعالجة التشخيص الرقمي بطبيعة الحال، فأقر في المادة (22) من اللائحة بأحقيته في عدم الخضوع لذلك القرار، حيث نصت الفقرة الأولى من المادة المشار إليها على أنه "ينبغي أن يكون للفرد موضوع البيانات الحق في عدم الخضوع لقرار يستند فقط على المعالجة الآلية، بما في ذلك التشخيص، من شأنه أن ينتج آثارًا قانونية تتعلق به أو يؤثر بشكل كبير على نحو مشابه عليه، يرجع في ذلك إلى؛

Article 22: Automated individual decision-making, including profiling:ne data subject shall have the right not to be subject to a decision d solely on automated processing, including profiling, which (148) Article 22: A1 produces legal effects concerning him or her or similarly significantly affects him or her.

Isaka Mendoza and Lee A.B ygrave, "The right not to be subject to automated decisions based on profiling", in EU Internet Law regulation and enforcement, ed, Tatiana Eleni Synodinou,ct.al.(Berlin, Germany: springer, 2017),85-86; Antoni Roig, "SAFEGUARDS FOR THE RIGHT NOT TO BE SUBJECT TO A DECISION BASED SOLELY ON AUTOMATED PROCESSING (ARTICLE 22 GDPR)", European Journal of Law and Technology 8, no.3(2017): 2. http://ejlt.org/article/view/570

2. Article 14; Human oversight High-risk AI systems shall be designed and developed in such a way, including with appropriate human-machine interface tools, that they can be effectively overseen by natural persons during the period in which they are in use……."

3. Laux, J. Institutionalised distrust and human oversight of artificial intelligence: towards a democratic design of AI governance under the European Union AI Act. *AI & Soc* (2023). https://doi.org/10.1007/s00146-023-01777-z

المعني هو من ارتكب الجريمة، في المقابل يكون الارتباط في أضعف حالاته إذا كان للشخص مجرد خطورة إجرامية، الأمر الذي يجعل بياناته عُرضة للاستخدام في خوارزميات التنبؤ بالجريمة، كذلك من اضطلع بالشروع في جريمة ثم عدل عنها اختياريًا، من ثم لم يطلب المشرع الأوروبي سوى أن يكون هنالك دلائل كافية تدل على أن الشخص المعني قد شرع بارتكاب أو ارتكب سلوكًا ماديًا مكونًا لجريمة ما أو كان مساهمًا فيها، وكان حريّ بالمشرع الأوروبي أن يحدد جرائم معينة وهي الجرائم الخطيرة أو شديدة الخطورة التي يُسمح فيها للشرطة التنبؤية باستخدام البيانات الشخصية، وليكن في الجرائم التي تزيد العقوبة فيها عن سنتين، وبالتالي يحظر استخدام البيانات الشخصية في المخالفات كافة، والجُنح البسيطة التي تقل العقوبة فيها عن سنتين.

ثانيًا: الضرورة في تحديد الهوية البيومترية

قد تضطلع أقسام الشرطة التنبؤية بالاعتماد على تحديد الهوية البيومترية عن بُعد بشكل آني "real-time remote biometric identification system"، على سبيل المثال حال المساعدة في تحديد هوية المشتبه بهم في مسرح الجريمة أو لتتبع تحركات الأشخاص المشتبه بهم، أو لمنع دخول الأشخاص المطلوبين للعدالة إلى أماكن معينة لا سيما المطارات أو المناطق الحدودية، الأمر الذي يتطلب تحديد الهوية عن بُعد باستخدام البيانات البيومترية كالبصمة أو الوجه ثم مقارنتهما مع بصمات أصابعهم أو وجوههم بقاعدة بيانات بشكل فوري[1].

والقاعدة العامة أن المشرع الأوروبي حظر استخدام خوارزميات تحديد الهوية البيومترية الآنية عن بُعد في الأماكن العامة وفقًا لما نصت عليه الفقرة (8) من المادة (5) من لائحة قانون الذكاء الاصطناعي الجديد، ومع ذلك استثنت إعمال هذه التقنية في حالات الضرورة وهي؛ أولًا، في حالة البحث عن مختطفين أو ضحايا الاتجار بالبشر أو ضحايا الاستغلال الجنسي، والأشخاص المفقودين. ثانيًا، في حالة منع تهديد محدق ووشيك لحياة الأشخاص الطبيعيين أو سلامتهم البدنية أو تهديد حقيقي متوقع

[1]. Article 3, Definitions (42) 'real-time remote biometric identification system' means a remote biometric identification system, whereby the capturing of biometric data, the comparison and the identification all occur without a significant delay, comprising not only instant identification, but also limited short delays in order to avoid circumvention;

بوقوع هجوم إرهابي. ثالثًا، في حالة تحديد مكان أو تحديد هوية شخص يشتبه في ارتكابه جريمة جنائية، بغرض إجراء تحقيق جنائي أو مقاضاة جنائية أو تنفيذ عقوبة جنائية على جرائم معينة[1].

من ثم إذا توافرت إحدى الحالات الثلاث السابقة ولا يشترط أن يكونوا مجتمعين، يجوز للشرطة التنبؤية أن تضطلع بإعمال تقنية تحديد الهوية البيومترية عن بُعد بشكل آني أو لحظي، وما دون تلك الحالات لا تتوفر حالة من حالات الضرورة[2]، وحسنًا فعل المُشرع الأوروبي لتحديده حالات معينة لبيان مفهوم الضرورة المطلوبة لاستخدام تلك التقنية، ولعل ما يؤكد ذلك ما نصت عليه المادة (34) من مواد إصدار القانون، والتي نصت على أنَّ استخدام نظم تحديد الهوية البيومترية اللحظي عن بُعد في الأماكن المتاحة للجمهور لأغراض إنفاذ القانون ينبغي ألا يتم إلا لتأكيد هوية الفرد المستهدف على وجه التحديد، وينبغي أن يقتصر على ما هو ضروري للغاية، وبيان خطورة وحجم الضرر الذي سيحدث إذا لم يتم

---

1. Article 5,(h) the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purposes of law enforcement, unless and in so far as such use is strictly necessary for one of the following objectives: (i) the targeted search for specific victims of abduction, trafficking in human beings or sexual exploitation of human beings, as well as the search for missing persons;
(ii) the prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or a genuine and present or genuine and foreseeable threat of a terrorist attack;
(iii) the localisation or identification of a person suspected of having committed a criminal offence, for the purpose of conducting a criminal investigation or prosecution or executing a criminal penalty for offences referred to in Annex II and punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least four years.

2. (33) The use of those systems for the purpose of law enforcement should therefore be prohibited, except in exhaustively listed and narrowly defined situations, where the use is strictly necessary to achieve a substantial public interest, the importance of which outweighs the risks. Those situations involve the search for certain victims of crime including missing persons; certain threats to the life or to the physical safety of natural persons or of a terrorist attack; and the localisation or identification of perpetrators or suspects of the criminal offences listed in an annex to this Regulation, where those criminal offences are punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least four years and as they are defined in the law of that Member State. Such a threshold for the custodial sentence or detention order in accordance with national law contributes to ensuring that the offence should be serious enough to potentially justify the use of 'real-time' remote biometric identification systems.

استخدام التقنية، ويتعين لإعمال تلك التقنية تحديد الفترة الزمنية، والنطاق الجغرافي والشخصي، مع إيلاء اعتبار خاص للأدلة المتعلقة بالتهديدات، أو الضحايا أو الجناة[1].

ولعل هنالك ضمانة أخرى نص عليها القانون، هي أنه لا تُمنح السلطة المختصة كـ (السلطة القضائية، أو السلطة الوطنية لحماية البيانات) الإذن إلا إذا اقتنعت بالأدلة المقدمة إليها، وأن معيار الضرورة تحقق لاستخدام تقنية تحديد الهوية البيومترية عن بُعد بشكل آني[2].

بقي أن نشير أخيراً إلى أن المُشرع الأوروبي قرر استثناءً عامًا لاستخدام أي نظام من أنظمة الذكاء الاصطناعي لا سيما الشرطة التنبؤية وسمح به في أغراض الأمن القومي كافة، ولم يُقدم القانون تعريفًا محددًا للأمن القومي[3]، مما يترك مجالًا واسعًا للتفسير من قبل الدول الأعضاء. وقد يؤدي ذلك إلى عدم

---

[1] (34) In order to ensure that those systems are used in a responsible and proportionate manner, it is also important to establish that, in each of those exhaustively listed and narrowly defined situations, certain elements should be taken into account, in particular as regards the nature of the situation giving rise to the request and the consequences of the use for the rights and freedoms of all persons concerned and the safeguards and conditions provided for with the use. In addition, the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement should be deployed only to confirm the specifically targeted individual's identity and should be limited to what is strictly necessary concerning the period of time, as well as the geographic and personal scope, having regard in particular to the evidence or indications regarding the threats, the victims or perpetrator. The use of the real-time remote biometric identification system in publicly accessible spaces should be authorised only if the relevant law enforcement authority has completed a fundamental rights impact assessment and, unless provided otherwise in this Regulation, has registered the system in the database as set out in this Regulation. The reference database of persons should be appropriate for each use case in each of the situations mentioned above.

[2] The competent judicial authority or an independent administrative authority whose decision is binding shall grant the authorisation only where it is satisfied, on the basis of objective evidence or clear indications presented to it, that the use of the 'real-time' remote biometric identification system concerned is necessary for, and proportionate to, achieving one of the objectives specified in paragraph 1, first subparagraph, point (h), as identified in the request and, in particular, remains limited to what is strictly necessary concerning the period of time as well as the geographic and personal scope. In deciding on the request, that authority shall take into account the elements referred to in paragraph 2. No decision that produces an adverse legal effect on a person may be taken based solely on the output of the 'real-time' remote biometric identification system.

[3]. بموجب معاهدة الاتحاد الأوروبي (المادة 2/4) ، تتحمل الدول الأعضاء مسؤولية ضمان أمنها القومي بشكل أساسي، لذلك لا يملك الاتحاد الأوروبي سلطة مباشرة على استخدامات الذكاء الاصطناعي في هذا المجال.

اتساق في كيفية تطبيق هذا الاستثناء. لذا كان حري بالمُشرع الأوروبي العمل على تحديد معايير مشتركة لتقييم مخاطر أنظمة الذكاء الاصطناعي التي تضر بالأمن القومي، حتى لا تقوِض فكرة الأمن القومي حظر التعامل في البيانات الشخصية المستخدمة في خوارزميات الشرطة التنبؤية وتسمح بمزيد من الانتهاكات للحق في الخصوصية الرقمية.

الخاتمة

سعى المُشرع الأوروبي نحو ترسيخ حماية قانونية للخصوصية الرقمية من خلال الحد من استخدام البيانات الشخصية بأنواعها في خوارزميات التنبؤ بالجريمة، بموجب قانون الذكاء الاصطناعي الجديد الذي صدر مؤخرًا ، في المقابل أجاز التعامل في البيانات الشخصية بحذر ووضع مجموعة من الضوابط أهمها أن تكون هنالك ضرورة قصوى ألجأت الشرطة لاستخدام أدوات الذكاء الاصطناعي للتنبؤ بجرائم معينة أو بمرتكبيها أو ضحاياها، كذلك أن يكون هنالك ارتباط وثيق بين من تضطلع باستخدام بياناته الشخصية والجريمة المرتكبة، فضلًا عن حتمية الرقابة البشرية على خوارزميات التنبؤ ونتائجها. غير أن المُشرع الأوروبي استثنى كل ما يتعلق بالأمن القومي وأجاز تذرعًا به أن تقوم الشرطة التنبؤية بكل صلاحياتها دون قيد أو شرط الأمر الذي يجعل هذا الاستثناء يقوِض الحظر الذي نص عليه القانون الأوروبي الجديد. وتوصل الباحث إلى مجموعة من النتائج والتوصيات نعرضها على النحو الآتي،

أولاً: النتائج

1. ترتبط البيانات الشخصية ارتباطًا وثيقًا بالخصوصية الرقمية، فكلما زادت كمية البيانات الشخصية التي يتم جمعها أو معالجتها عن الفرد، زاد احتمال تعرض خصوصيته للخطر.
2. البيانت الشخصية الرقمية هي جوهر الحق في الخصوصية الرقمية، وهي وقود خوارزميات الشرطة التنبؤية، وتتنوع بين بيانات شخصية عامة، وبيانات شخصية وثيقة الصلة بالجرائم، وبيانات شخصية بيومترية.
3. مخاوف انتهاك الحق في الخصوصية الرقمية قاد الاتحاد الأوروربي لسن قانون الذكاء الاصطناعي الجديد لعام 2024، الذي يحد جزئيًا من نطاق عمل الشرطة التنبؤية.
4. حَظَر قانون الذكاء الاصطناعي الأوروربي الجديد بعض التطبيقات التي تهدد حقوق المواطنين، بما في ذلك أنظمة تصنيف البيانات الحيوية (البيومترية) القائمة على السمات البشرية الحساسة والاستخراج غير المجدي لصور الوجه من الإنترنت أو لقطات كاميرات المراقبة؛ لإنشاء قواعد بيانات التعرّف على الوجه دون مبرر.

5. درجت كذلك أقسام الشرطة التنبؤية على تدشين قواعد بيانات شخصية –database تتم تغذية خوارزميات التنبؤ بها للمساعدة في التنبؤ ودرء الجرائم قبل وقوعها، وتسمى بـ "قواعد بيانات قبل الجريمة–Pre-crime database".
6. من الأساليب التي تعتمد على البيانات الشخصية العامة أيضًا ما يُعرف "باستخبارات المصادر المفتوحة" Open source intelligence (OSINT) وتقوم على تجميع البيانات من المصادر المفتوحة المتاحة للجمهور، كوسائل الإعلام المرئية أو المسموعة أو المقروءة، والإنترنت، كالشبكات الاجتماعية وغيرها، وكل مصادر المعلومات الأخرى المتاحة.
7. ترتبط البيانات البيومترية بالجسد البشري وخصائصه الفريدة، مما يجعلها شديدة الخصوصية، ويُثير ذلك مخاوف بخصوص جمع ومعالجة هذه البيانات وتخزينها واستخدامها في خوارزميات الشرطة التنبؤية باعتبارها جزءًا من البيانات الشخصية الحساسة.
8. التنبؤ الشرطي يتم من خلال أربعة أساليب مختلفة هي، إما التنبؤ بالجرائم، أو التنبؤ بالمجرمين، أو التنبؤ بالبؤر الإجرامية، أو التنبؤ بضحايا الجريمة.
9. تَمُر البيانات الشخصية بمجموعة من المراحل المتتالية حتى تتمكن الخوارزمية المعدة للتنبؤ من إعطاء مخرجات دقيقة، وهي؛ أولًا، جمع البيانات الشخصية، ثانيًا، معالجة البيانات الشخصية، ثالثًا، التنقيب في البيانات الشخصية، رابعًا، تدريب الخوارزمية على التنبؤ، خامسًا، تقييم خوارزية التنبؤ الشرطي.
10. وفقًا للائحة الأوروبية العامة لحماية البيانات فإن استخدام البيانات الشخصية للتنبؤ ضروريًا لتنفيذ التزام قانوني أو لتحقيق مصلحة سواء للشخص محل البيانات أو مصلحة عامة.
11. لا تتم معالجة البيانات الشخصية المرتبطة بالإدانات أو الجرائم الجنائية أو التدابير الأمنية باعتبارها بيانات شخصية عادية، وإنما تتم تحت رقابة السلطة الرسمية أو عندما يسمح بذلك القانون الأوروبي الاتحادي أو قانون الدول الأعضاء، كما لا يُحتفظ بأي سجل شامل للإدانات الجنائية إلا تحت رقابة السلطة الرسمية.
12. خوارزميات الشرطة التنبؤية لا يمكن أن تضطلع باتخاذ قرار آلي مباشر دون خضوعه للإشرف والرقابة من السلطة الرسمية، وهو ما أكده القانون الأوروبي للذكاء الاصطناعي– ArtificialIntelligence Act لعام 2024، إذ نص في المادة (14) على وجوب الإشراف البشري على تقنيات الذكاء الاصطناعي.

13. حظر القانون الأوروبي للذكاء الاصطناعي الجديد – Artificial Intelligence Act لعام 2024، تقنية "التعرف البيومتري عن بُعد"، مثل أنظمة التعرف على الوجه في الأماكن العامة، فضلاً عن حظر أنظمة التعرف على المشاعر والمسح الجماعي لقواعد البيانات البيومترية وفقًا لما نصت عليه المادة (5) منه.
14. حظر القانون الأوروبي للذكاء الاصطناعي الجديد – Artificial Intelligence Act لعام 2024، تقييم أو التنبؤ بخطر ارتكاب شخص طبيعي لجريمة جنائية، بناءً على تحديد ملف تعريف الشخص الطبيعي أو تقييم سمات شخصيته وخصائصه فقط؛ وإنما إذا تورط شخص ما في نشاط إجرامي، بشرط أن يستند بالفعل إلى حقائق موضوعية وقابلة للتحقق مرتبطة مباشرة بنشاط إجرامي ما.
15. لم يحدد كذلك المُشرع الأوروبي درجة الارتباط أو حتى معايير يمكن الاستدلال بها على كل من النشاط الإجرامي والشخص المعني باستخدام بياناته في خوارزميات التنبؤ بالجريمة.
16. لا تُمنح السلطة المختصة كـ(السلطة القضائية، أو السلطة الوطنية لحماية البيانات) الإذن باستخدام أنظمة الذكاء الاصطناعي إلا إذا اقتنعت بالأدلة المقدمة إليها، وإن معيار الضرورة تحقق لاستخدام تقنية تحديد الهوية البيومترية عن بُعد بشكل آني.
17. المُشرع المصري ونظيره العُماني لم يضطلعا بسن قوانين لتنظيم تقنيات الذكاء الاصطناعي كما فعل المُشرع الأوروبي، كما أن كلا المشرعان لم يشرعا تنظيمًا قانونيًا متعلقًا بنشاط الشرطة التنبؤية صراحةً.

ثانياً: التوصيات

1. من المناسب أن يحذو المُشرعان المصري والعُماني حذو المشرع الأوروبي بأن يضعا ضوابط لحماية تلك البيانات الشخصية حال استعمالها في التنبؤ الشرطي، لا سيما ضرورة الربط بين استخدام البيانات الشخصية وجريمة ارتكبت بالفعل أو هنالك دلائل قوية على ارتكابها.
2. من المناسب أن يضطلع المُشرع الأوروبي بقصر إباحة استخدام البيانات الشخصية في خوارزميات الشرطة التنبؤية على الجرائم شديدة الخطورة فقط كالمتعلقة بأمن الدولة الداخلي أو الخارجي، دون ان تمتد للجرائم كافة بما فيها المخالفات والجُنح البسيطة.

3. حري بالمشرع الأوروبي أن يحدد درجة التدخل البشري المطلوبة في عملية تحليل البيانات الشخصية بغرض التنبؤ بالجريمة؛ حتى لا يكون هذا الالتزام حبرًا على ورق إذ إن التدخل البشري قد يقف عند مجرد الضغط على زر نتائج القرار الآلي فقط.
4. حري بالمُشرع الأوروبي العمل على تحديد معايير مشتركة لتقييم مخاطر أنظمة الذكاء الاصطناعي التي تضر بالأمن القومي، حتى لا تقوِض فكرة الأمن القومي حظر التعامل في البيانات الشخصية المستخدمة في خوارزميات الشرطة التنبؤية وتسمح بمزيد من انتهاكات الحق في الخصوصية الرقمية.
5. استخدام خوارزميات ومصادر بيانات شفافة، ويجب أن تكون النماذج والبيانات المستخدمة مفتوحة للتدقيق العام لضمان العدالة.
6. من الضروري مراجعة الخوارزميات بشكل منتظم بحثًا عن أية أخطاء قد تعتريها تؤثر في عملية التنبؤ، ويفضل مراجعتها دورياً من قبل خبراء مستقلين لتحديد وتصحيح أية أخطاء.
7. ضرورة اقتصار عمل الشرطة التنبؤية على الأماكن فقط دون الأشخاص، لتجنب التنبؤ بميل الأفراد إلى ارتكاب الجرائم وانتهاك حرمة البيانات الشخصية.
8. ضرورة الحظر الكلي لعمليات الشرطة التنبؤية الآلية، وبيان قدر التدخل البشري في عملية التنبؤ بالجريمة، إذ إن الاعتماد الكلي على تحليل البيانات الشخصية المضمنة لتقنية التعلم الآلي والتعلم العميق قد تكون غير سليمة لأسباب كثيرة يرجع بعضها لجودة البيانات والبعض الآخر لتركيبة وتكوين الخوارزمية ذاتها.
9. قصر استخدام الشرطة التنبؤية على غرض توجيه الدوريات ومأموري الضبط القضائي للبؤر الإجرامية فقط دون استخدامها في الاعتقالات أو تقييم الخطورة الإجرامية أو إصدار الأحكام الجنائية.

بيان تضارب المصالح

يقر جميع المؤلفين أنه ليس لديهم أي تضارب في المصالح.

قائمة المراجع:

أولًا: المراجع القانونية

1. أشرف جابر سيد، الجوانب القانونية لمواقع التواصل الاجتماعي، دار النهضة العربية، 2013.
2. حوراء موسى، الجرائم المرتكبة عبر وسائل التواصل الاجتماعي، دراسة مقارنة، دار النهضة العربية، 2018.
3. رمضان السيد الألفي، نظرية الخطورة الإجرامية، دار النهضة العربية، 1998.
4. هيثم السيد أحمد عيسى، التشخيص الرقمي لحالة الإنسان في عصر التنقيب في البيانات عبر تقنيات الذكاء الاصطناعي وفقاً للائحة الأوروبية العامة لحماية البيانات لعام 2016، دار النهضة العربية، 2019.

ثانيًا: المجلات والمقالات والمنشورات

1. أنمار عرابي، استخدام أدوات التنقيب في البيانات في دراسة تأثير صفات الزبائن على قرار الشراء، دراسة إحصائية لبيانات الزبائن، مجلة العلوم الإدارية والاقتصادية، كلية الاقتصاد والعلوم الإدارية جامعة عدن، عدد5، 2010.
2. إيهاب عثمان وعبد الرحمن عثمان، التنبؤات الانتخابية باستخدام تنقيب البيانات، الانتخابات الأمريكية كدراسة حالة، سبتمبر 2016.
3. تامر صالح، التتبع الجغرافي للمتهم بواسطة تقنية "GPS" والحق في الخصوصية، مجلة البحوث القانونية والاقتصادية، عدد خاص بالمؤتمر الدولي السنوي العشرون، كلية الحقوق، جامعة المنصورة، 23-24 مايو 2021.
4. سامح عبد الواحد التهامي، الحماية القانونية للبيانات الشخصية، دراسة في القانون الفرنسي، مجلة الحقوق، كلية الحقوق جامعة الكويت 35، عدد 3، 2011.
5. سيف الدين عثمان فتوح والشفيع جعفر محمود، التنقيب في البيانات واتخاذ القرارات، مجلة النيل الأبيض للدراسات والبحوث، كلية العلوم والتكنولوجيا، جامعة النيل الأبيض، العدد 3 ، 2014.
6. شادي عبد الوهاب منصور، الشرطة التنبؤية، اعتماد متزايد لأجهزة الأمن الغربية على أساليب الاستخبارات، مجلة أوراق أكاديمية، مركز المستقبل للدراسات والأبحاث المتقدمة، العدد 4، أكتوبر 2018.

7. محمود سلامة الشريف، الطبيعة القانونية للتنبؤ بالجريمة بواسطة الذكاء الاصطناعي ومشروعيته، المجلة العربية لعلوم الأدلة الجنائية والطب الشرعي، العدد 3، المجلد 2، 2021.

ثالثًا: المواقع الإلكترونية

1. الموقع الإلكتروني لوزارة العدل الأمريكية على الرابط الآتي،، بتاريخ دخول 1-6-2024، https‹ //www.ojp.gov/pdffiles1/nij/242222and248891.pdf
2. الموقع الإلكتروني لمقال بعنوان "شرطة دبي تستخدم الذكاء الاصطناعي للتنبؤ بالجريمة قبل وقوعها، 2016، على الرابط الآتي، بتاريخ دخول 2024/6/10، https‹ //shorturl.at/T9N0h

رابعًا: المراجع الأجنبية

1. Alice Norga, 4 Benefits And 4 Drawbacks Of Predictive Policing, TECH & RIGHTS, July 12, 2021
2. Alyse Burnside, IT Security Challenges Emerge in Smart Cities, January 19, 2023,
3. Antoni Roig, "SAFEGUARDS FOR THE RIGHT NOT TO BE SUBJECT TO A DECISION BASED SOLELY ON AUTOMATED PROCESSING (ARTICLE 22 GDPR)", European Journal of Law and Technology 8, no.3, 2017
4. Artificial Intelligence Act‹ MEPs adopt landmark law, Press Releases
5. Bachner, Jennifer. 2013. Predictive Policing‹ Preventing Crime with Data and Analytics. Washington, DC‹ IBM, Centre for the Business of Government
6. Beck, C., and C. McCue, “Predictive Policing‹ What Can We Learn From Wal-Mart and Amazon About Fighting Crime in a Recession?” The Police Chief 76, 11, November 2009
7. Benjamin Docquir, GENERAL DATA PROTECTION REGULATION 2016,Quelles obligations prévoit le projet de règlement européen sur les données personnelles (GDPR) ?(Belgique, Bruxelles‹ Simont Braun, 2016.
8. Beth Pearsall; Predictive Policing‹ The Future of Law Enforcement? NIJ Journal / Issue No. 266.
9. Browning, Christopher R., Reginald A. Byron, Catherine A. Calder, Lauren J. Krivo, Mei-Po Kwan, Jae-Yong Lee, and Ruth D. Peterson. 2010. Commercial density, residential concentration, and crime‹ Land use patterns and violence in neighbourhood context. Journal of Research in Crime and Delinquency 47‹ 329–57.
10. Bryce Goodman and Seth Flaxman, European Union regulations on algorithmic decision-making and a "right to explanation", Al Magazine 38, No 3, 2017
11. David Black, Predictive Policing Is Here Now, The Dallas Morning News, February 26th, 2016
12. De Mauro, Andrea et al. “A formal definition of Big Data based on its essential features.” Library Review 65 ,2016.

13. Eck, John E., YongJei Lee, O. SooHyun, and Natalie Martinez. 2017. Compared to what? Estimating the relative concentration of crime at places using systematic and other reviews. Crime Science 6، 1–17.
14. Els de Busser, Data Protection in EU and US Criminal Cooperation، A Substantive Law Approach to the EU Internal and Transatlantic Cooperation in Criminal Matters Between Judicial and Law Enforcement Authorities (Antwerpen Belgium، Maklu Publishers, 2009
15. ensure that 'high-risk' systems have accessibility requirements for people with disabilities; and widen the definition of AI to cover the full range of AI systems which have been proven to impact fundamental rights.
16. Fair Trials, Partial ban on 'predictive' policing and crime prediction systems included in final EU AI Act, 11 December 2023
17. Ferguson, Andrew. 2017. Policing predictive policing. Washington University Law Review 94.
18. Harvin Bhathal, Canada's Predictive Policing Tech Is Poorly Regulated Under AI Policy, TRUTHOUT, June 13, 2022
19. Heather J. Williams and Ilana Blum, Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise, California ,US، RAND Corporation, 2018
20. Isaka Mendoza and Lee A.B ygrave, "The right not to be subject to automated decisions based on profiling", in EU Internet Law regulation and enforcement, ed, Tatiana Eleni Synodinou,ct.al. Berlin, Germany، springer, 2017
21. Jannik Lindner, Ai In Law Enforcement Statistics, WORLDMETRICS REPORT 2024, June 17, 2024.
22. Jessie Levano, Predictive Policing in the AI Act، meaningful ban or paper tiger? 5 JULY 2024, EUROPEAN LAW BLOG,
23. KATARÍNA HIĽOVSKÁ and PETER KONCZ, "Application of Artificial Intelligence and Data Mining Techniques to Financial Markets", Acta všfs 6, 2012
24. Kazemi, General Data Protection Regulation, 29
25. KYODO, Kanagawa police to launch AI-based predictive policing system before Olympics, the Japan times, Jan 29, 2018.
26. Laux, J. Institutionalised distrust and human oversight of artificial intelligence، towards a democratic design of AI governance under the European Union AI Act. *AI & Soc* ,2023
27. Lee, YonJei, John Eck, O SooHyn, and Natalie Martinez. 2017. How concentrated is crime at places? A systematic review from 1970 to 2015. Crime Science 6
28. Leo Kelion; Crime prediction software 'adopted by 14 UK police forces', BBC, 4 February 2019.
29. Lopes, Giza, Marvin D. Krohn, Alan J. Lizotte, Nicole M. Schmidt, Bob E. Vasquez, and Jon G. Bernburg. Labelling and cumulative disadvantage، The impact of formal police Intervention on life chances and crime during emerging adulthood. Crime & Delinquency 58. 2012

30. Meijer, Albert, and Martijn Wessels. Predictive Policing; Review of Benefits and drawbacks. International Journal of Public Administration 42. 2019
31. MIN WANG and ZUOSU JIANG, "The Defining Approaches and Practical Paradox of Sensitive Data، An Investigation of Data Protection Laws in 92 Countries and Regions and 200 Data Breaches in the World", International Journal of Communication 11, 2017.
32. Miriam Jones, Predictive Policing a Success in Santa Cruz, Calif, Government Technology, October 08, 2012.
33. Patrick Breyer v Bundesrepublik Deutschland.EJC. C-582/14.16/5/2016 ECLI،EU،C،2016.
34. Pearsall, Beth. Predictive policing، The Future of Law Enforcement. National Institute of Justice Journal 266، 2010
35. Perry, Walter L., Brian McInnis, Carter C. Price, Susan Smith, and John S. Hollywood, Predictive Policing، The Role of Crime Forecasting in Law Enforcement Operations. Santa Monica, CA، RAND Corporation, 2013.
36. Portland State University (PSU). 2012. Predictive Policing، A Review of Literature. Criminology and Criminal Justice Senior Capstone Project, Paper 5
37. Predictive Policing Market by Technology (Crime Analysis, Facial Recognition Technology, Geo-Location Technology), End-Use (Detective Agencies, Law Enforcement Organization, Military & Defense) - Global Forecast 2024-2030.
38. Rick Sarre, Ben Livings; Artificial Intelligence and the Administration of Criminal Justice، Predictive Policing and Predictive Justice. Australia Report. University of South Australia. May 2023
39. Rosamunde Van Brakel and Paul De Hert,"Policing, surveillance and law in a pre-crime society، Understanding the consequences of technology based strategies", in Technology-led policing, eds, Piet Deelman, et al Antwerpen, Belgium، Maklu Publishers, 2011
40. Safat W, Asghar S, Gillani SA. Empirical analysis for crime prediction and forecasting using machine learning and deep learning techniques, IEEE Access 9 ,2021
41. Samah Samir; Detecting and Predicting Crimes using Data Mining Techniques، Comparative Study, Proceedings of 1st International Conference on Computers and Information, ICCI 2021
42. Sunde, Inger Marie. "AI-Based Law Enforcement Online، The Impact of the European Artificial Intelligence Act (AIA)". Bergen Journal of Criminal Law & Criminal Justice, vol. 10, no. 2, Dec. 2022,.
43. The data divide، Overcoming an increasing practitioner-academic gap, Larissa Fast, 2 November 2017
44. U.S. Department of Homeland Security, U.S. Customs and Border Protection, Washington, DC 20229, "U.S. Customs and Border Protection Passenger Name Record (PNR) Privacy Policy, (June 21, 2013). p. 1-8
45. Uspenski, V. A.. "To the Definition of Algorithms." ,1993.
46. Weisburd, David. The law of crime concentration and the criminology of place. Criminology 53، 2015.