دكتور/ أحمد عبد العزيز محمد أبو الحسن
باحث بمركز أبحاث القانون والتكنولوجيا الناشئة

الضوابط القانونية لاستعمال بعض تقنيات الذكاء الاصطناعي في إنفاذ القانون

المراسلة: د.أحمد عبدالعزيز محمد أبو الحسن
باحث بمركز أبحاث القانون والتكنولوجيا الناشئة

معرف الوثيقة الرقمي (DOI): jolets.v6i1.247/10.54873

البريد الإلكتروني: Ahmed.aboualhassan@bue.edu.eg

نسق توثيق البحث أحمد عبدالعزيز محمد أبو الحسن
الضوابط القانونية لاستعمال بعض تقنيات الذكاء الاصطناعي في إنفاذ القانون، المجلد السادس، العدد الأول، أبريل ٢٠٢٦

ملخص

تناول هذا البحث استخدام تقنيتي التعرف على الوجه والتنميط لأتمتة القرارات بالذكاء الاصطناعي في إنفاذ القانون، وبين منافع استخدام تلك التقنيتين في هذا المجال وتسريعها للنتائج النهائية ومكافحة الجريمة؛ ولهذا تزايد استخدامهما حول العالم وخاصة تقنية التعرف على الوجه المربوطة بالمنازل الذكية وأنظمة تأمين الممتلكات والمنازل الخاصة، وبين هذا البحث أيضا المخاطر وإشكاليات مشروعية استعمال تلك التقنيات في مجال إنفاذ القانون في كل مراحل تدريب وتشغيل تلك النماذج، حيث بين أن كل مرحلة من تلك المراحل تطرح مشاكلها الخاصة وتحتاج قواعدها الخاصة لضمان قانونيتها، كما طرح عدد من النماذج التشريعية حول العالم المتعلقة بتنظيم استخدام تلك التقنيات في إنفاذ القانون سواء داخل قوانين مخصصة للذكاء الاصطناعي عامة كقانون الاتحاد الأوروبي للذكاء الاصطناعي، أو قوانين متفرقة كاللائحة العامة الأوروبية لحماية البيانات الشخصية، أو قوانين بعض الولايات الأمريكية، وقد أوضح بعض تلك المخاطر والاشكاليات من خلال بعض القضايا المعاصرة وخاصة في مجال تعاون الشركات الخاصة مع جهات الأمن العام ومدي حدود استخدام البيانات وأنظمة المراقبة الذكية الخاصة في إنفاذ القانون والأمن العام، وخلص بنتائج من أهمها خطورة الاعتماد على تلك التقنيات في اتخاذ القرار النهائي وفائدتها في الأعمال الوسيطة وتسريع الإجراءات الجنائية وإنفاذ القانون، وأوصي بضرورة الحفاظ على قواعد المشروعية الإجرائية وخاصة ما يتعلق بالحقوق الفردية أثناء استعمال تلك التقنيات في إنفاذ القانون واقتصار استعمالها على الأعمال الوسيطة دون القرارات النهائية ومراجعة والرقابة المستمرة لاستعمالها وتطوير البنية التشريعية وقواعد ومدونات وتوجيهات إنفاذ القانون بما يتوافق مع مخاطر تلك التقنيات.

Abstract:

This research dealt with the use of facial recognition and profiling technologies to automate decisions with artificial intelligence in law enforcement, and showed the benefits of using these two technologies in this field and their acceleration of final results and fighting crime, which is why their use has increased around the world, especially facial recognition technology linked to smart homes and systems to secure property and private homes, and this research also showed the risks and legality issues of using these technologies in law enforcement in all stages of training and operating these models, as it showed that each of these stages presents its own issues and needs its own rules to ensure its legality. He recommended the need to preserve the rules of procedural legality, especially with regard to individual rights during the use of these technologies in law enforcement, limiting their use to intermediate work without final decisions, reviewing and continuously monitoring their use, and developing the legislative structure, rules, codes, and law enforcement guidelines in line with the risks of these technologies.

كلمات مفتاحية: التعرف على الوجه ، التنميط ، التحيز الخوارزمي، قانون الاتحاد الأوروبي للذكاء الاصطناعي، الثقة في الذكاء الاصطناعي، أتمتة القرارات.

Keywords: Facial recognition, profiling, algorithmic bias, EU AI law, trust in AI, decision automation.

مقدمه

انتشرت «دوائر الرقابة التليفزيونية المغلقة CCTV [١]"، سواء التقليدية أو الذكية»[٢]، عالميا لما لها من منافع متعددة لا يمكن إنكارها[٣]، سواء على شكل أنظمة موجهة للمنازل أو المؤسسات، وبربط تلك الأنظمة بتطبيقات "الذكاء الاصطناعي" كالمسح والتعقب والتحديد الجمعي للأشخاص باستخدام تقنيات «التعرف على نمط الوجه» عن طريق الحوسبة السحابية التي تتيح لها الاتصال المستمر بوحدات معالجة ضخمة تتيح لها استخدام تقنيات الذكاء الاصطناعي والرؤية الحاسوبية والتعرف على الأصوات واللغة الطبيعية وغيرها من الإمكانيات المتقدمة، وأيضا الصورة الأحدث والتي تدمج نماذج "الذكاء الصناعي ذات الغرض العام"[٤]، وخاصة نموذج CHAT GPT[٥]، كوسيلة للقيام بالمهام بشكل أقوى وأكثر سهولة، عظمت الفائدة العائدة على مالك تلك الأنظمة، وبالمقابل تزايدت المخاطر الواقعة على البيانات الشخصية بشكل مهول.

وأثيرت أيضا بشكل عملي قضايا تتعلق بمدى وحدود استخدام تلك الأنظمة لأغراض الأمن العام والمقاضاة والتعرف على المجرمين و تحديدهم ،فقد ظهر حول العالم عددٌ من القضايا التطبيقية التي أظهرت مدى خطورة استخدام تلك التطبيقات في أغراض الأمن العام، وما يحتاجه الأمر من تنظيم أكثر دقة من الموجود حاليا.

ولا يقتصر استعمال تطبيقات الذكاء الاصطناعي في إنفاذ القانون على تقنيات «تحديد الهوية والتتبع عن طريق التعرف على نمط الوجه» بل يمتد لأعمق من هذا حيث تستعمل قدرات نماذج الذكاء الاصطناعي الحديثة على التعرف وتحديد الأنماط على نطاق واسع في تحديد أنماط السلوكيات الإجرامية والتتبع والتنبؤ المستقبلي، وخاصة فيما يتعلق بمكافحة الجريمة المنظمة والعابرة للحدود، كل تلك الإمكانيات الكامنة في نماذج الذكاء الاصطناعي الحديثة لا يمكن تجاهلها ولكن فقط يجب تقنين استخدامها في مكافحة الجريمة وإنفاذ القانون لتحقيق مشروعية الإجراءات الجنائية والتوزان المبتغى بين الحقوق الفردية ومتطلبات الأمن العام وإنفاذ القانون.

وقد جاءت استراتيجية مصر للذكاء الاصطناعي (الاستراتيجية المصرية للذكاء الاصطناعي الإصدار الثاني ٢٠٢٥-٢٠٣٠) مركزة على سبل تطوير وتحقيق الريادة في مجال الذكاء الاصطناعي، وهو في رأينا شيئًا ضروريا، ولكنها لم تول الاعتبارات الحقوقية ما يكفي إلا ما جاء فيها من معايير عامة تنص على ضرورة احترام حقوق الإنسان أثناء تطوير تقنيات الذكاء الاصطناعي واستخدامها، ولهذا يأتي البحث في محور هام كمعايير استخدام تقنيات الذكاء الاصطناعي في مجال إنفاذ القانون كنقطة حيوية لابد من إيلائها القدر الكافي من الأهمية أثناء السعي المصري الحثيث للريادة في قطاع الذكاء الاصطناعي والتوسع في استخداماته، لتحقيق الاستدامة القانونية لمثل تلك الاستخدامات، وهو ما نسعى للمساهمة فيه بهذا البحث

---

١ أنظمة المراقبة التليفزيونية المغلقة: هي أنظمة حيث يتم ربط عدد من كاميرات الفيديو ببعضها، ويتم بث الصور الملتقطة لعدد من شاشات المراقبة التليفزيونية ولا يتم بثها للعموم Wakefield Alison ,Fleming Jenny ,The SAGE Dictionary of Policing ,states united ,SAGE ,٢٠٠٨ ,p: ٢٨

٢ وقد عرف اتحاد التصوير المؤتمت الأمريكي هذا النوع من كاميرات التصوير بأنها كاميرات بها بعض الإمكانيات المتعلقة بمعالجة الصور والتصوير وأيضا بها وحدة معالجة حاسوبية تستخدم لأغراض التصوير ومعالجة الصور، تقوم ببعض أنواع العمليات بشكل مؤتمت مثل تتبع الحركة بدون الحاجة لتدخل بشرى Belbachir Nabil Ahmed ,Smart Cameras ,London ,Springer Media Business & Science ,٢٠٠٩ ,p: ٣

3 Jean-Yves Dufour ,Intelligent Video Surveillance Systems ,New Jersey ,United States ,John Wiley& Sons ,2012 ,p1 :

4 Council of the European Union ,Interinstitutional File)2021/0106 :COD ,(Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence) Artificial Intelligence Act (and amending certain Union legislative acts5) ,aa .(Article44 ,3 b

5 Security camera network, A Chat-GPT Enabled Security Camera for just $35!?, last visited: 5/3/2024,

إشكالية البحث:

نتيجة لهذا وجب الإجابة على عدد من الإشكاليات التي تم طرحها نتيجة التطور المتسارع لتلك التقنيات:

١. ما هو تأثير هذه التطبيقات على حقوق الأفراد ومبادئ مشروعية الإجراءات الجنائية؟
٢. ما هي حدود استخدام تلك الأنظمة لأغراض إنفاذ القانون؟
٣. ما هي المخاطر الناجمة عن استخدام تلك الأنظمة لأغراض إنفاذ القانون؟
٤. ما هي الاتجاهات التشريعية لتنظيم استخدام تلك التقنيات لأغراض إنفاذ القانون؟
٥. ما هي الجهود الدولية لتنظيم استخدام تلك الأنظمة لأغراض إنفاذ القانون؟

أهداف البحث:

١. تعريف أنظمة المراقبة الذكية والتنميط بواسطة الذكاء الاصطناعي والتقنيات المستخدمة فيها.
٢. بيان المخاطر التي يمكن أن تطرحها تقنيات التعرف على الوجه والتنميط على الحقوق الفردية.
٣. بيان تأثير استخدام تقنيات الذكاء الاصطناعي على مبدأ المشروعية الإجرائية ودستورية أعمال التحقيق والاستدلال القائمة عليها.
٤. طرح أمثلة تطبيقه على أخطار استخدام أنظمة المراقبة الذكية والتنميط لأغراض الأمن العام.
٥. بيان التنظيم التشريعي لاستعمال تقنيات الذكاء الاصطناعي في إنفاذ القانون
٦. بيان الجهود الدولية لتنظيم استخدام أنظمة المراقبة الذكية لأغراض الأمن العام.

منهجية البحث:

للوصول لإجابة متكاملة –على قدر المستطاع– على إشكالية البحث، ونظرا لحداثة الموضوع ووجود فراغ تشريعي في التشريعات المصرية فيما يتعلق بهذا الموضوع فسيعتمد الباحث على أكثر من منهج لتحقيق أهداف البحث، كالآتي:

أولاً: المنهج الوصفي التحليلي: يُستخدم هذا المنهج في تفكيك وفهم الطبيعة التقنية والقانونية لأنظمة المراقبة الذكية وتقنيات التعرف على الوجه والتنميط. يهدف هذا التحليل إلى بيان تأثير هذه التقنيات المعقدة على مبادئ مشروعية الإجراءات الجنائية، واستعراض الإشكاليات والمخاطر التي تطرحها على الحقوق الفردية والحق في الخصوصية، تمهيداً للوقوف على أبعاد الظاهرة وتحديد نطاق التدخل التشريعي المطلوب.

ثانياً: المنهج التأصيلي (الاستقرائي): نظراً للحاجة الماسة إلى بلورة معايير قانونية دقيقة لاستخدام تقنيات الذكاء الاصطناعي في قطاع حساس كإنفاذ القانون، يعتمد البحث على استقراء الجهود الدولية والمواثيق والأطر التنظيمية المستحدثة. يُسهم هذا المنهج في تأصيل القواعد القانونية والأخلاقية التي يجب أن تحكم هذه التقنيات، واستنباط المبادئ الحاكمة لعمليات أتمتة القرارات، لبناء أساس نظري متين يوازن بين متطلبات الأمن العام والضمانات الدستورية لحقوق الإنسان.

ثالثاً: المنهج المقارن: يتصدى هذا المنهج للفراغ التشريعي القائم من خلال مقارنة متعمقة للاتجاهات التنظيمية المتقدمة، وتحديداً التشريعات الموحدة كقانون الذكاء الاصطناعي للاتحاد الأوروبي واللائحة العامة لحماية البيانات (GDPR)، إلى جانب التطبيقات التشريعية المتفرقة في الولايات المتحدة الأمريكية. سيتم إسقاط مخرجات هذا التحليل المقارن على الواقع القانوني المصري؛ بهدف استخلاص الدروس المستفادة، وصياغة سياسات استشرافية، وهندسة حلول تشريعية دقيقة تتوافق مع البيئة الدستورية الوطنية وتدعم الاستدامة القانونية للإجراءات الجنائية.

خطة البحث:

المبحث الأول: أسس ومخاطر استخدام تقنيات التنميط والتعرف على الهوية والتتبع من خلال التعرف على الوجه لأغراض إنفاذ القانون.

المطلب الأول: ماهية تقنيات التعرف على الوجه والمراقبة والتتبع اللحظي والتنميط لأغراض إنفاذ القانون

المطلب الثاني: مدي مشروعية الأدلة المتحصل عليها من خلال تقنيات الذكاء الاصطناعي

المبحث الثاني: التنظيم القانوني لاستخدام تقنيات التعرف على الهوية والتنميط لأغراض إنفاذ القانون

المطلب الأول: معايير استخدام أنظمة التعرف على الوجه والتنميط لأغراض الأمن العام في التشريعات الوطنية

المطلب الثاني: الجهود الدولية لتنظيم الذكاء الاصطناعي أثناء إنفاذ القانون

ويختتم بخاتمة بها النتائج والتوصيات.

المبحث الأول
أسس ومشروعية استخدام تقنيات التنميط والتعرف على الهوية والتتبع من خلال التعرف على الوجه لأغراض إنفاذ القانون

ظهرت في الفترة الأخيرة قفزة كبيرة في التركيب والاعتماد على أنظمة المراقبة وتأمين المنازل، وهذا في إطار ما يعرف بالمنازل الذكية[٦]، المعتمدة على ما يعرف بالأجهزة الذكية[٧] والتي تتبع ما يعرف ب "انترنت الأشياء internet of things"، والتي تزايدت الفوائد الناجمة منها من خلال ربطها بتقنيات الذكاء الاصطناعي، وتقديم جيل جديد من تلك الأنظمة يرتبط سحابيا بأنظمة ضخمة تتيح تقديم خدمات لم تكن متاحة للعامة سابقا، وخاصة فيما يتعلق بتحديد الهوية والأحداث، وعلى الرغم من تعاظم الفوائد الناجمة من هذا، إلا أن هذا يطرح إشكاليات كثيرة فيما يتعلق بالحقوق الفردية وخاصة الحق في البيانات الشخصية، وأيضا إمكانية استخدام تلك الأنظمة وشبكات المراقبة التي ستمتد لحدود تتعدي حدود أي نظام مراقبة عام حكومي لأغراض الأمن العام.

كما أن استعمال تقنيات الذكاء الاصطناعي لا يتوقف على التعرف على الوجه بل يمتد أيضا لتقنيات التنميط وهي ذات أثر أعمق وأكثر استمرارية –وإن كان غير مباشر أكثر– من تقنيات التعرف على الوجه، لما له من القدرة على التنبؤ والتحليل، بل قد يستعمل في أغراض غير قانونية كالتصنيف الجمعي.

وهو ما سنحاول إلقاء نظرة قانونية عليه في هذا المبحث، وهذا في مطلبين كالآتي:

المطلب الأول: ماهية تقنيات التعرف على الوجه والمراقبة والتتبع اللحظي والتنميط لأغراض إنفاذ القانون.

المطلب الثاني: مدي مشروعية الأدلة المتحصل عليها من خلال تقنيات الذكاء الاصطناعي

---

٦ تعرف «الأنظمة الذكية والمتصلة لإدارة وتأمين المنازل» على أنها «مجموعة من الأجهزة التي تؤتمت العمليات المنزلية، وتهدف لتحقيق راحة وأمن ورفاهية مستخدمها داخل منزله، من خلال قدرتها على إدارة نفسها وأتمتة العمليات المنزلية بأقل قدر من التدخل البشري، وهذا من خلال تقنيات مستحدثة كإنترنت الأشياء والأتمتة»، أنظر: Mehdi Rahmani-Andebili, Operation of Smart Homes, Power Systems, united states, Springer Nature, 2021, p: 2

7 Eu, Regulation (EU) 2024/2847 Cyber Resilience Act, article 3, 'product with digital elements' means a software or hardware product and its remote data processing solutions, including software or hardware components being placed on the market separately;

المطلب الأول
ماهية تقنيات التعرف على الوجه والمراقبة والتتبع اللحظي والتنميط لأغراض إنفاذ القانون

تزايد الاقبال على شراء وتركيب تقنيات تأمين ومراقبة للممتلكات والمساحات الخاصة بشكل ملحوظ، وترافق هذا مع زيادة أعداد الأنظمة المخصصة لهذا وتنوعها من حيث الإمكانيات والأسعار، وعلى الرغم من وجود بعض المعايير القانونية لتركيب مثل تلك الأنظمة[٨]، إلا أن دمج تلك الأنظمة مع تقنيات الذكاء الاصطناعي يعتبر نقلة نوعية لمثل هذه النوعية من الأنظمة لما تقدمه تطبيقات الذكاء الاصطناعي من إمكانيات متقدمة تزيد من مخاطر تلك الأنظمة بشكل كبير، مما يوجب تخصيص دراسات متخصصة في تلك التقنيات الحديثة والمعروفة ب (التعرف على الأشخاص من خلال نمط الوجه وأيضا التتبع اللحظي للأفراد facial recogni- tion and real time tracking of individual's)،

هذا من ناحية المستهلك والتقنيات التي يمكن طرحها للمستهلك العادي، أما من ناحية المتخصصين والمحترفين فإن كل البيانات التي يتم جمعها من الانترنت وحتى شبكات التعرف على الوجه تدخل في دورة من التحليل والمعالجة المستمرة، بل والتصنيف التلقائي ويتم تغذية وتدريب نماذج الذكاء الاصطناعي بها أو حتى البرمجيات العادية للمساعدة في الوصول لنتائج مختلفة متغيرة منها ما يتعلق بأتمتة القرارات وتصنيف الأشخاص.

وهو ما سنحاول بحثه في هذا المطلب، كالآتي:

الفرع الأول: ماهية تقنيات التعرف على الهوية من خلال مسح الوجه والتنميط

الفرع الثاني: إشكاليات تطوير تقنيات التعرف على الوجه والتنميط

الفرع الأول
ماهية تقنيات التعرف على الهوية من خلال مسح الوجه والتنميط

أولا: ماهية تقنيات التعرف على الوجه وارتباطها بإنفاذ القانون:

أ: ماهية تقنيات التعريف على الهوية من خلال مسح نمط الوجه:

لا يمكن إنكار أهمية هذه التقنية وخصوصا في قطاعات الأمن والتأمين، ولهذا فهي من أكثر تقنيات وأجهزة التأمين والأمن البيومترية جذبا لمطوري أجهزة ونظم المراقبة والتأمين[٩]، وقد عرف التعرف على الوجه على أنه "المعالجة التلقائية للصور الرقمية التي تحتوي على وجوه الأفراد بغرض تحديد الهوية، التوثيق, التحقق أو التصنيف لهؤلاء الأفراد . وهي عملية تتكون من عدد من العمليات الفرعية المنفصلة: الحصول على الصور التي تحتوي على وجوه الأشخاص، تحديد الوجه، مسح المتغيرات البسيطة وتحسين الوجه، تحديد النقاط المفتاحية للوجه، إدخال بيانات الوجه ضمن نظام التعرف على الهوية، المقارنة والتعريف"[10].

٨ كقانون دولة الكويت رقم ٦١ لسنة ٢٠١٥ في شأن تنظيم وتركيب كاميرات وأجهزة المراقبة الأمنية الذي يتعامل مع أنظمة المراقبة الفيديوية التقليدية، قانون المحال العامة المصري رقم ١٥٤ لسنة ٢٠١٩/، م: ٢٣ قانون أساسي عدد ٦٣ لسنة ٢٠٠٤ مؤرخ في ٢٧ جويلية ٢٠٠٤ يتعلق بحماية المعطيات الشخصية، القسم الرابع – في معالجة المعطيات الشخصية لأغراض المراقبة البصرية

9 Stan Z. Li, Anil K. Jain. Handbook of Face Recognition. United states, Springer Science & Business Media, 2005. P: 1, Asit Kumar Datta, Madhura Datta, Pradipta Kumar Banerjee. Face Detection and Recognition: Theory and Practice. United States, CRC Press, 2015. P: 4

10 article 29 data protection working party. opinion 02/2012 on facial recognition in online and mobile services. Brussels, 22 March 2012. P: 2

ب: استعمال تقنيات التعرف على الوجه والتتبع في ارتكاب الجرائم:

-نظرا لتزايد استخدام تلك التقنيات في الأجهزة الذكية المتصلة كالهواتف المحمولة الذكية والحواسيب وحتى أجهزة البيوت الذكية كوسيلة للتعرف على الهوية وأحيانا تلقى أوامر التشغيل عن طريق حساسات ومستقبلات الصوت، كذلك بالتبعية تزايد استخدامها في الأغراض الإجرامية عن طريق اختراق تلك الأجهزة وسحب البيانات المولدة والمخزنة أو الولوج للأنظمة نفسها من أجل تعقب الحركات والأفعال الشخصية للأشخاص واستعمالها للابتزاز بأشكال متعددة تتنوع بتنوع وامتداد البيانات التي تجمعها تلك الأجهزة، وهو ما يعرف ب «اختراق السرية لأنظمة الأجهزة الذكية»[11].

ج: استعمال تقنيات التعرف على الوجه والتتبع في مكافحة الجريمة:

هذا من ناحية أما من الناحية الأخرى فإن تقنيات التعرف على الهوية باستخدام نمط الوجه من أكثر تقنيات الذكاء الاصطناعي استخداما في أعمال الأمن العام، فباستخدام تلك التقنيات يمكن لقوات الأمن والجهات المختصة التعرف وتحديد أماكن المجرمين وضحايا الجريمة والأشخاص المختفية على حد سواء، فمن خلال ظهورهم في الصور الملتقطة بواسطة دوائر المراقبة الفيديوية المغلقة يمكن تحديد أماكن تواجدهم إما بواسطة تحديد معالم محيط هذا الظهور أو تحديد موضع الكاميرا التي التقطتهم[12]، كما يمكن التتبع الفوري واللحظي لحركاتهم ورسم خرائط مكانية عن طريق شبكات المراقبة الذكية الخاصة مثلا كأنظمة جرس الباب الذكي رينج ring، أو العامة كالتابعة لجهة أمن عام مثلا كشرطة نيويورك بأمريكا.

وقد تم تبنى تقنيات التعرف على الوجه واستخدام الذكاء الاصطناعي لمسح وتكوين قواعد بيانات لقوالب الوجوه والمسح الفوري وتحديد الهويات في الولايات المتحدة، فمثلا استخدمت المباحث الفيدرالية وإدارة الهجرة والمنافذ بالولايات المتحدة قواعد بيانات مكاتب إدارة المركبات بالولايات المتحدة لتعدين واستخراج قوالب الوجوه من صور «رخص المرور»، وقامت إدارة المرور بنيويورك بتركيب أجهزة للتعرف على قوالب الوجوه على كل الأنفاق والكباري للتعرف الفوري واللحظي على هويات السائقين من خلال قوالب وجوههم[13].

وواحدة من أكثر تقنيات الذكاء الاصطناعي المرتبطة بالتعرف على الهوية وقوالب الوجوه إثارة للاهتمام فيما يخص تتبع وتعقب واستعادة الأشخاص والأطفال المفقودين و حتى لو بعد اختفائهم لفترة طويلة، هي تقنيات «شيخوخة الطفل وتجديد شبابه» والتي تمكن من عمل نماذج للطفل المختفي أو ضحية الاتجار بالبشر في مراحل عمره المختلفة بنسبه خطأ صغيرة للغاية، مما يساعد وبشده في استعادة وتتبع هؤلاء الضحايا ولو بعد مدة زمنية كبيرة والتغير المصاحب للزمن في ملامح الوجه[14].

وأيضا يمكن استخدام شبكات المراقبة الذكية للتتبع الفوري واللحظي لمسار الأشخاص، فلقد استخدم قسم شرطة ولاية لوس انجلوس بكاليفورنيا أمريكا شبكات كاميرات أجراس الباب الذكية المباعة من قبل شركة «رينج الأمريكية التابعة لشركة أمازون» لتتبع متظاهري مظاهرات حركة «الحياة السوداء تهم black live matters" عام 2021 بالولايات المتحدة، وهذا من خلال برنامج «الضواحي»[15] عن طريق تحليل صور تتعلق بتلك التظاهرات التقطتها كاميرات أجراس المنازل الذكية، مما استخدم في تعقب المتظاهرين بدمج مسارات كاميرات

11 David Buil-Gil, Steven Kemp, Stefanie Kuenzel, Lynne Coventry, Sameh Zakhary, Daniel Tilley, James Nicholson, The digital harms of smart home devices: A systematic literature review, Computers in Human Behavior, Volume 145, August 2023, 107770, accessed from: sciencedirect, last visited: 13/4/2024, https://shorturl.at/xHQY0

12 Ibrahim Ali Mohammed, An Exploratory Study Into The Face Detection And Recognition System To Strengthen Security Precautions Using An Artificial Intelligence System, International Journal of Creative Research Thoughts, Volume 1, Issue 1 February 2013, p: 140.

13 Rosario Girasa, Gino J. Scalabrini, Regulation of Innovative Technologies: Blockchain, Artificial Intelligence and Quantum Computing, united states, springer nature, 2023, p: 94.

14 Praveen Kumar Chandaliya, Neeta Nain, ChildGAN: Face aging and rejuvenation to find missing children, Pattern Recognition, Volume 129, September 2022, accessed from science direct, last visited: 13/4/2024, https://t.ly/N9JHH

١٥ برنامج انعقد بين شركة أمازون المالكة لشركة رينج يتيح لقوات الأمن العام الأمريكية الولوج لقواعد بيانات التغذية المرسلة من الكاميرات الذكية التي تبيعها الشركة.

المنازل المربوطة بشبكة ذكاء اصطناعي واحدة تابعة للشركة الأم «أمازون الأمريكية»[16]، وهو ما أدي إلى تصاعد حدة الانتقادات الموجهة لهذا النوع الجديد من المراقبة الأمنية، بعد ظهور استخدامها بشكل يقمع الأفراد عن ممارسة حقوقهم الدستورية كالحق في التظاهر، مما ينقلنا للنقطة التالية.

ثانيا: ماهية تقنيات التنميط وارتباطها بإنفاذ القانون

أ: تعريف التنميط:

يعرف التنميط على أنه "أي شكل من أشكال المعالجة الآلية للبيانات الشخصية التي تتألف من استخدام البيانات الشخصية لتقييم جوانب شخصية معينة تتعلق بشخص طبيعي، ولا سيما لتحليل أو التنبؤ بالجوانب المتعلقة بأداء ذلك الشخص الطبيعي في العمل، أو الوضع الاقتصادي، أو الصحة، أو التفضيلات الشخصية، أو المصالح، أو الموثوقية، أو السلوك، أو الموقع، أو الحركات"[17].

ب: استعمال التنميط في ارتكاب الجرائم:

ومن هنا يمكننا أن نرى الوسائل المتعددة التي يمكن أن تستخدم فيها تقنيات التنميط في الجرائم، فعن طريق البحث المكثف وهندسة البيانات المجمعة من الإنترنت ومنصات التواصل الاجتماعي، يمكن استهداف الأشخاص بسلوكيات إجرامية متعددة ابتداء من الجرائم الفردية كالابتزاز والسرقة والقتل، كما يمكن أن تستخدم النتائج الخارجة من عمليات التنميط والتصنيف أيضا لوضع خطط لعمليات إجرامية معقدة ومستمرة وتتبع الأشخاص، ولكن عادة ما ينتشر استخدام تلك التقنيات في العمليات الاجرامية المنظمة وخاصة الاتجار بالبشر حيث يتم تقسيم الأشخاص لفئات مستهدفة لأغراض الاتجار بالبشر المتعددة سواء العمالة القسرية أو غير الشرعية أو الاتجار الجنسي أو حتى الاستغلال الجنسي والغير قانوني للأطفال[18].

ج: استعمال التنميط لمكافحة الجريمة:

في ورشته المنعقدة بفيينا عام ٢٠٠٨ أكد مكتب الأمم المتحدة للجريمة والمخدرات وجود فوائد متعددة لاستخدام تقنيات «التنميط الجنائي» أو «تقنيات التحليل التحقيق الجنائي» أو بمسمى آخر «التحليل الجنائي الذكي» بمكافحة الجريمة وخاصة الاتجار بالبشر، عن طريق تحليل أنماط السلوك والأساليب والخصائص المنهجية والمنطقية للمجرمين والمنظمات الإجرامية، فالملامح الجنائية المقدمة بواسطة التحليل الجنائي قد تساعد قوات الشرطة والجمارك في تحديد المحتجزين واعتراضهم عند دخولهم ومرورهم من نقاط الحدود، وجاءت الورقة بجدول به عشر مجموعات وظيفية ومحددة الأدوار التي قد تلعبها هذه المجموعات في جميع مراحل وخطوات جريمة الاتجار بالبشر من التجنيد للاستغلال وحتى المكافحة من الإبلاغ للتعافي[19]، والحقيقة أن تلك الورقة كلها تعتبر ملف تنميطي كبير محدد فيه مجموعة كبيرة من المجموعات الوظيفية على مدار الورقة ودورها إما في عملية الاتجار أو مكافحتها.

كما نشر نفس المكتب «الأداة رقم ٩,١٤ الاستراتيجيات الاستباقية المانعة: استهداف المهربين» والتي تؤكد باتفاق عدد كبير من المنظمات والجهات الدولية المختصة على أهمية ونفعية استعمال تقنيات «التنميط» بتكوين ملفات تحتوي على بيانات تحدد أنماط مختلفة تتعلق بجريمة الاتجار بالبشر، من ناحية الضحايا وتكوين ملفات تحتوي على أنماط معينة من الضحايا، والمجرمين من المهربين وأعوانهم والتي تحتوي على أنماط لعملياتهم وطرقهم وهم أنفسهم ومعاونوهم[20].

---

16 atthew guariglia, dave maassfebruary. lapd requested ring footage of Black Lives Matter protests. Electronic Frontier Foundation. Web site, 2021, last visited: 13/9/2022. https://t.ly/yaeIH

17 Information commissioner office, What is automated individual decision-making and profiling?, last visited: 10/4/2024, https://t.ly/4nVY3

18 United Nations, Working Group on Trafficking in Persons, Conference of the Parties to the United Nations Convention against Transnational Organized Crime, CTOC/COP/WG.4/2021/2, Successful strategies for addressing the use of technology to facilitate trafficking in persons and to prevent and investigate trafficking in persons, p: 4.

19 United Nations Office on Drugs and Crime, Anti-Human Trafficking Unit, 016 Workshop: Profiling the Traffickers, The Vienna Forum to fight Human Trafficking 13-15 February 2008, Austria Center Vienna, UN.GIFT B.P.: 016, p: 2-3

٢٠ United Nations Office on Drugs and Crime, Anti-Human Trafficking Unit, tool 9.14 Proactive prevention strategies: targeting traffickers, Vienna,

الفرع الثاني
الإشكاليات القانونية المتعلقة بتطوير تقنيات التعرف على الوجه والتنميط

أولا: المخاطر الناجمة من عدم حوكمة البيانات

يعمد مطورو تلك البرامج على تقنيات متعددة تستخدم ما يعرف بكتل البيانات الضخمة[21] لتغذية وتطوير برمجياتهم، وتعتمد هذه التقنيات على مطابقة ومعالجة كمية ضخمة من الصور للتعرف على أنماط للوجه يتم تخزينها واستخدامها لاحقا لتحديد الهوية، وهو ما يتم الحصول عليه عادة باستخدام برامج الجمع والتنقيب الآلية crawler bots والتي تدخل على قواعد البيانات الخلفية لمواقع الانترنت وتسحب كل البيانات الموجودة في تلك القواعد، وفي أحيان كثيرة يتم هذا بدون علم وموافقة صاحب تلك البيانات، وهذا يتعارض مع عدد كبير من الضوابط القانونية للمعالجة المشروعة للبيانات الشخصية، مثل الموافقة المسبقة للمعنى بالبيانات الشخصية، ومحدودية ومشروعية جمع البيانات، ومحدودية المعالجة، وغيرها الكثير.

كما ظهر العديد من الممارسات الحديثة في قطاع الذكاء الاصطناعي التي تعتمد على تدريب نماذج الذكاء الاصطناعي على قواعد بيانات مفتوحة المصدر مثل LAION-5B[22] مثلا والذي يستخدم كثيرا لتدريب نماذج الذكاء الاصطناعي الموجهة لتوليد الرسوم، وأيضا تدريبها على نماذج مولدة حاسوبيا من البيانات تفاديا للامتثال لقوانين حماية البيانات الشخصية ولكنه أيضا يولد العديد من الإشكاليات حول مدي حوكمة ودقة تلك البيانات وخاصة في مجال شديد المخاطر كإنفاذ القانون حيث يمكن أن يسبب خطأ واحد العديد من الإشكاليات للأشخاص التي قد يتم اتهامها خطأ نتيجة لخطأ في النتيجة المولدة بشكل مؤتمت من خلال برنامج الذكاء الاصطناعي[23].

وفي سياق متصل، أُقيمت دعوى جماعية (Class Action) ضد شركة 'OpenAI' –المدعومة من شركة مايكروسوفت– يزعم فيها المدعون استيلاء الشركة بصورة غير مشروعة على 'بيانات التعريف الشخصية' (PII) عبر عمليات المسح الشامل لشبكة الإنترنت. وتستند الدعوى إلى انتهاك الشركة لعدة تشريعات محورية؛ أبرزها قانون ولاية كاليفورنيا لغزو الخصوصية[24]، والقانون الفيدرالي الأمريكي لخصوصية الاتصالات الالكترونية لعام 1986[25]، والقانون الفيدرالي لجرائم النصب وإساءة استخدام الكمبيوتر لعام ١٩٨٦[26]، ذلك لقيام الشركة بجمع بيانات تدريبية لإنشاء قواعد بيانات لبرمجيات التعرف على الوجوه، مما يُشكل اعتداءً جسيماً على خصوصية الأفراد. والجدير بالذكر أن هذه الدعوى المتداولة حالياً أمام المحكمة الفيدرالية في

.United Nations Office on Drugs and Crime, p: 503

٢١ "البيانات الضخمة هي وسيلة لتخزين ومعالجة كمية ضخمة من البيانات، لإكتشاف أنماط ومعلومات مخفية، قد لا تظهر بطرق المعالجة العادية والمفردة للبيانات، بما يرفع قيمة هذه البيانات، وينتج عنه اتخاذ قرارات أفضل" أنظر: Maria Tzanou, Health Data Privacy under the GDPR: Big Data Challenges and Regulatory Responses, Routledge Research in the Law of Emerging Technologies, united states: Routledge, 2020, p: 1 preface

٢٢ LAION–5B: اختصار لـ (Large–scale Artificial Intelligence Open Network)، وهي قاعدة بيانات مفتوحة المصدر تُعد الأضخم عالمياً، تشتمل على ٥,٨٥ مليار زوج من (الصور والنصوص) المفلترة تقنياً. أُطلقت من قبل منظمة «LAION» الألمانية غير الربحية لتمكين الباحثين من تدريب نماذج الذكاء الاصطناعي التوليدي (مثل Stable Diffusion). وتكمن أهميتها القانونية في كونها تعتمد على «كشط البيانات» (Data Scraping) من شبكة الإنترنت، مما يثير إشكاليات معاصرة حول حقوق الملكية الفكرية والخصوصية، للمزيد أنظر: Schuhmann, C., et al. (٢٠٢٢). «٥B: An open large–scale–LAION dataset for training next generation image–text models». arXiv preprint arXiv:٢٢١٠,٠٨٤٠٢ https://doi.org/10.48550/arXiv.2210.08402 .

23 United Nations University, Recommendations on the Use of Synthetic Data to Train AI Models, last visited: 17\4\2025, https://unu.edu/publication/recommendations-use-synthetic-data-train-ai-models#:~:text=Using%20synthetic%20or%20artificially%20generated,quality%2C%20security%20and%20ethical%20implications.

24 2005 California Penal Code Sections 630-637.9 CHAPTER 1.5. INVASION OF PRIVACY, PENAL CODE SECTION 630-637.9

25 United states of America, Electronic Communications Privacy Act of 1986 (ECPA)

26 United states of america, The Computer Fraud and Abuse Act of 1986 (CFAA), Title 18, United States Code, Section 1030.

سان فرانسيسكو[27]، وهي ما هي إلا نموذج لسلسلة من القضايا المنظورة أمام القضاء الأمريكي ضد شركات الذكاء الاصطناعي، والتي تتنوع موضوعاتها ما بين انتهاك الخصوصية والتعدي على حقوق الملكية الفكرية[28].

ثانيا: المخاطر الناجمة عن تحيز الذكاء الاصطناعي:

يعرف تحيز الذكاء الاصطناعي بأنه: "عندما تتخذ أو توصي أنظمة الذكاء الاصطناعي باتخاذ قرارات غير عادلة ضد مجموعات معينة، نتيجة لعدد كبير من العوامل أهمها التحيز الخوارزمي وعدم حوكمة البيانات والتدريب"[29]، وقد جاءت العديد من الدراسات والنتائج التي تؤكد وجود نسبة من التحيز والتمييز ضد أنواع معنية من الوجوه كوجوه الأطفال مثلا وألوان البشرة كأصحاب البشرة ذات الألوان الداكنة مثلا[30]، ولو حتى لأسباب تقنية تتعلق بالإضاءة أو بالمعالجة أو بوسيلة التصوير[31]، مما يعرض هؤلاء لنسب خطأ أكبر من غيرهم كالذكور القوقازيين البالغين مثلا، ولكن هذا ما يزيد من نسب المخاطر التي يتعرض لها أصحاب البشرة أو الوجوه التي تزيد بها حالات التمييز ونسبة الخطأ بها بلغت في عام ٢٠١٨ ل ٢٠,٨ إلى ٣٤,٥ بالمائة للنساء ذوات البشرة الغامقة، وأيضا تسببت في حالات استهداف عنصرية أو غير حقيقية من قبل قوات الشرطة بمدينة نيويورك الأمريكية ضد تجمعات المهاجرين الأسبان والمسلمين، وقد تسبب هذا في عدد من الفضائح داخل الولايات المتحدة للشركات وقوات الأمن التي تستخدم هذه التقنيات، وقد أدى هذا إلى أن توقف شركة مايكروسوفت وشركة أمازون للخدمات السحابية خدمات التعرف على الوجه التي تطورها من قبل جهات الأمن[32]، وأيضا شركات رينج وكلير فيو الأمريكية[33]، والتي تم مقاضاتها بسبب استخدامها لبرامج المسح الشامل للإنترنت لتكوين قواعد بيانات برامج التعرف على الوجه التي تؤجرها لقوات الأمن[34].

ثالثا: المخاطر الناجمة عن عدم دقة الأنظمة والأدلة المتحصلة منها:

على الرغم من الإمكانيات الهائلة التي توفرها هذه التقنية في مجال الأمن الخاص والعام، إلا أن العديد من الجهات الدولية قد وجهت انتقادات واسعة للتأثير الخطير ل "تقنيات التعرف المؤتمت على الوجه» منها الخطورة البالغة للاعتماد على مثل هذه التقنيات الحديثة في مجال إنفاذ القانون والأمن العام، فقد أشارت "وكالة الاتحاد الأوروبي للحقوق الأساسية" أنه حتى مع نسبة خطأ تبلغ واحد في المائة فهذا يعني تعرض الآلاف للاحتجاز وتوجيه التهم الجنائية عن طريق الخطأ[35]، كما أشار "المجلس الأوروبي للبيانات الشخصية" أن هذه التقنيات لا توفر نتائج موثوق بها، وهذا يرجع لحاجتها لصور متعددة الجوانب للوجه الواحد لزيادة دقة البيانات البيومترية الناجمة عنها، وعليه فإنه من الخطر الاعتماد عليها في أعمال خطيرة كالتحقيقات الجنائية وتوجيه التهم الجنائية للأشخاص[36].

27 UNITED STATES DISTRICT COURT, NORTHERN DISTRICT OF CALIFORNIA, CLASS ACTION COMPLAINT, Case 3:23-cv-03199, Filed 06/28/23

28 OpenAI and ChatGPT Lawsuit List, last visited: 7/3/2024, https://shorturl.at/gnFO2

٢٩ للمزيد نرجو مراجعة الدراسة التي أعدتها الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا)، التحيز في أنظمة الذكاء الاصطناعي تحديات وحلول، يناير ٢٠٢٥.

30 Nisha Srinivas, Karl Ricanek, Dana Michalski, David S. Bolme, Michael King, Face Recognition Algorithm Bias: Performance Differences on Images of Children and Adults, 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), IEEE, p: 1.

31 David Leslie, Understanding bias in facial recognition technologies, the Alan Turing institute, 2020, p: 12-15.

32 Ibid: Rosario Girasa, Gino J. Scalabrini, Regulation of Innovative Technologies: Blockchain, Artificial Intelligence and Quantum Computing, p: 95.

٣٣ : احمد عبد العزيز محمد أبو الحسن، الاشكاليات الناجمة عن أنظمة المراقبة الذكية من منظور حماية البيانات الشخصية وتنظيم الذكاء الاصطناعي، ملتقى دولي حول الذكاء الاصطناعي والأمن القومي: الرهانات القانونية.، الجزائر، ٢٠٢٣، ص: ٨-١٠

34 Mutnick v. Clearview AI, Inc. et al, No. 1:2020cv00512 - Document 86 (N.D. Ill. 2020) urt Description: MEMORANDUM Opinion and Order: The Court denies defendants' Rule 12(b)(2) and § 1404(a) motions [29, 45]. Signed by the Honorable Sharon Johnson Coleman on 8/12/2020. Mailed notice. (ym,)

35 the EU fundamental rights agency. facial recognition technology: fundamental rights considerations in the context of law enforcement. Austria, fra – European union agency for fundamental rights, 2019. P: 9

36 The European Data Protection Board. Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement. Brussel, 27 June 2022. P: 11

كما نادى «اتحاد الحريات المدنية الأمريكي» بوقف استخدام هذا البرنامج لأغراض الأمن العام بواسطة قوات إنفاذ القانون الأمريكية بناء على هذه الدراسات، واستشهد بحالة قام بها برنامج تعرف على الهوية بتحديد عدد ٢٨ نائب كونجرس أمريكي على أنهم مجرمون من أصل خمسين نائبا تعرضوا لتلك الدراسة[٣٧].

رابعا: الإشكاليات الناجمة عن أتمتة القرارات:

تعرف أتمتة القرارات بأنها: "اتخاذ القرارات بواسطة وسائل الأتمتة وبدون أي تدخل أو انخراط للعامل البشري، وهو ما يمكن أن يكون نتاج لبيانات واقعية أو بيانات مستنبطة وملفات شخصية تم توليدها عن الأشخاص»[٣٨].

ويتم اللجوء للأتمتة في العديد من جوانب العمل الأمني ابتداء من أتمتة عمليات المراقبة والجمع للبيانات، وانتهاء بعمليات أتمتة قرارات الاتهام والتعرف على الأشخاص، مرورا بأتمتة عمليات الفحص والمراقبة وعمل المسيرات ونظم المراقبة، وقد عددت "وكالة ايروبول" في تقريرها المعنون " الذكاء الاصطناعي والشرطة ": فوائد الذكاء الاصطناعي وتحدياته بالنسبة لأجهزة إنفاذ القانون" العديد من استخدامات الأتمتة في عمليات إنفاذ القانون، مثلا ما تناوله التقرير من نزوح العديد من وكالات الأمن حول العالم لاستخدام تقنيات الأتمتة في العديد من مراحل العمل الجنائي مثل : إعادة تحليل الاستخبارات وبناء البصمات وسبر تطبيقات الويب للكشف عن التهديدات الأمنية والعديد من الاستخدامات التي توفر إمكانيات لا حصر لها في مجال إنفاذ القانون[٣٩].

والحقيقة أن أتمتة الأعمال بواسطة تقنيات الذكاء الاصطناعي هو من أبسط الاستخدامات لهذه التقنيات المتطورة وقد ظهرت في مراحل متقدمة عن ظهور نماذج «المتحولات المنطقية transformers" و"نماذج اللغة الكبيرة LLM" في هيئة المساعدات الذكية كسيري واليكسا وغيرها وهي درجات منخفضة الخطورة من الذكاء الاصطناعي low risk level bots، ولكن ما زاد من خطورة الأمر هو إمكانية اعتماد الأشخاص والجهات على تلك التقنيات لاتخاذ قرارات نهائية بدون مراجعة وتقييم بشري للقرار، أو حتى زيادة الاعتمادية على تلك القرارات التي تولدها تلك النماذج بصورة غير واعية بناء على الاعتقاد بدقة تلك النماذج أو حياديتها المفترضة، مما يفرض مخاطر كبيرة وخاصة في مجال إنفاذ القانون حيث أنه حتى بدون التطرق للذكاء الاصطناعي فإن الخطأ في البيانات الجنائية قد يؤدي إلى مخاطر وآثار وخيمة للأفراد عن طريق الاتهام والملاحقة الأمنية وأحيانا الأحكام القضائية المبنية على بيانات خاطئة، وهو ما يزيد بشكل كبير في ظل الاعتماد على أنظمة الذكاء الاصطناعي.

37 Danny Caine. How to Resist Amazon and Why: The Fight for Local Economics, Data Privacy, Fair Labor, Independent Bookstores, and a People-Powered Future!. United states, Microcosm Publishing, 2022. P: 152

38 Information Commissioner's Office, What is automated individual decision-making and profiling?, last visited: 19\4\2025, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/automated-decision-making-and-profiling/what-is-automated-individual-decision-making-and-profiling/#:~:text=Automated%20decision%2Dmaking%20is%20the,to%20award%20a%20loan%3B%20and

المطلب الثاني
مدي مشروعية الأدلة المتحصل عليها من خلال تقنيات الذكاء الاصطناعي

نظرا للمخاطر التي يمكن أن تقع على الأفراد نتيجة التعقب والتحديد الجنائي، فقد حرصت جميع النظم القانونية المعاصرة على إحاطة أعمال الاستدلال والتحقيق الجنائي بعدد من القواعد التي تضمن مشروعيته وهي ما تعرف «بالمشروعية الجنائية»[٤٠] التي تعمل على الحفاظ على دستورية أعمال التحقيق والاستدلال الجنائي من خلال الحفاظ على المبادئ الدستورية المنظمة لهذا، ومن أهمها ما يتعلق بحقوق الأفراد وخاصة ما يتعلق بحقهم في سلامة الجسد، والخصوصية، وغيرها من الحقوق الأساسية التي يجب مراعاتها أثناء مرحلة التحقيق والاستدلال، ليحوز الدليل الجنائي على حجيته وصحته أمام القضاء في مرحلة الدعوى الجنائية، وإلا تعرض لما يعرف باستبعاد الأدلة الجنائية[٤١]، وقد تتعارض وسائل جمع الأدلة الجنائية عن طريق أنظمة الذكاء الاصطناعي مع قاعدة المشروعية الإجرائية في عدد من النقاط، منها ما يتعلق بالحقوق الأساسية للأفراد، ومنها ما يتعلق بمشروعية تحصل الجهات الأمنية على البيانات والأدلة من أنظمة المراقبة الأمنية الخاصة.

الفرع الأول: تأثير تقنيات التعرف على الوجه على الحق في البيانات الشخصية

الفرع الثاني: المخاطر التي يثيرها التعاون بين مشغلي أنظمة المراقبة الذكية للمنازل وبين جهات الأمن العام

الفرع الثالث: قواعد أتمتة القرارات في قوانين حماية البيانات الشخصية

الفرع الأول
تأثير تقنيات التعرف على الوجه على الحق في البيانات الشخصية

1: المخاطر الناجمة من عدم وعي الشخص المعني بالبيانات بالتقاط بياناته والتعرف عليه:

يري الباحث أن تقنيات "التعرف على الهوية من خلال مسح نمط الوجه" من أخطر تقنيات التعرف البيومترية من وجهة نظر حماية البيانات الشخصية، كونها لا تتطلب تفاعلا واعيا بين الشخص المعنى بالبيانات والآلة التي تتعرف عليه، فالعديد من تلك الآلات يمكنها التعرف على هوية الشخص المعنى بالبيانات بمجرد وجوده في نطاقها الذي يمكن أن يمتد لمئات الأمتار.

وفي حالات أخرى يمكن مسح والتعرف على هوية الأشخاص بدون حتى أي تفاعل مادي بين الشخص المعنى بالبيانات والآلة المعرفة للهوية، أو حتى علم الشخص المعنى بالبيانات، مما يثير مشكلة العابرين، فالإشكالية الأساسية هنا هي قيام تلك الأجهزة بجمع بيانات كل من يدخل في نطاقها بشكل متزامن وعشوائي بدون تحديد أو اقتصار على بيانات مالكها، فسواء كانوا من أفراد الأسرة أو غيرهم من الآخرين المتواجدين بشكل شرعي أو غير شرعي في نطاق هذه الأنظمة، وهذا لا يمكن حظره ابتداء كونه يعتبر جزءا من وظائفها الأساسية، ولهذا يرى الباحث ملاءمة اقتصار التدخل التشريعي والقانوني عامة علي تكييف مشروعية استخدامه وحدود رخصة المتحكم في معالجة بيانات هؤلاء العابرين والمتواجدين بنطاق تلك الأنظمة.

2: حالات الأشخاص المعنية بالبيانات من غير مالك الجهاز (مفهوم العابرين):

يؤثر الجمع المتزامن والغير محدد لجميع البيانات الشخصية لكل من يدخل في نطاق هذه الأنظمة على تحديد

٤٠ عرف مبدا المشروعية الإجرائية او مبدأ مشروعية الدليل الجزائي على أنه « ضرورة اتفاق الإجراء مع القواعد القانونية والأنظمة الثابتة في وجدان المجتمع المتحضر» محمد لطفي عبد الفتاح، القانون الجنائي واستخدامات التكنولوجيا الحيوية: الهندسة الوراثية، البصمة الوراثية، الاستنساخ، المنصورة، دار الفكر والقانون، ٢٠١٢، ص: ١٨٧.

٤١ استبعاد الأدلة الجنائية غير المشروعة هو جزاء إجرائي يهبط بقيمة الدليل الإثباتية هبوطاً يصل الى حد إهداره وعدم الاعتداد به كدليل إدانة من دون البراءة، بسبب عيب أعترى طريقة تحصيله، أنظر: عبد الحسن دويخ خفيف، استبعاد الأدلة الجنائية غير المشروعة: دراسة مقارنة، رسالة ماجستير، العراق، كلية القانون، جامعة ذوقار، ٢٠١٨، ص: ٣٤.

المراكز القانونية للأشخاص المعنية بالبيانات، فعلى حين يمكن القول بواحدية العلاقة بين الشخص المعني بالبيانات والمتحكم فيها لأغراض التصفح وتقديم الخدمات والتعاقد عليها، إلا أن هذا لا ينطبق على الأنظمة الذكية لإدارة المنازل وتأمينها، والتي تقوم بالجمع والمعالجة المستمرة للبيانات الشخصية لكل من يقع في نطاق مستشعراتها، لذا لا يمكن القول بواحدية «الشخص المعني بالبيانات»، بل يجب افتراض تعدديتهم طوال الوقت

ويكمن طرح مثال تطبيقي على هذا المفهوم الحديث من خلال عرض الدعوي الجماعية التي رفعتها المواطنة الأمريكية «ميشيل وايس» على شركة «رينج التابعة لأمازون» عام ٢٠٢٠ والتي مثلت فيها مجموعة من الأفراد الذين لا يملكون أجهزة تابعة لتلك الشركة[42]، ولكن زعموا أنهم تعرضوا لانتهاك خصوصيتهم جراء مسح صورهم والتعرف على هوياتهم أثناء عبورهم في نطاق تلك الأجهزة، وهذا بدون إذنهم وموافقتهم مما نجم عنه امتلاك تلك الشركة لبياناتهم الشخصية وخصوصا قوالب وجوههم والتي تستخدم في تقنيات التعرف على الهوية من خلال مسح قوالب الوجه التابعة للشركة بدون علمهم أو موافقتهم[43]، واستعانت المدعية ببراءة الاختراع المملوكة للشركة والمتعلقة بتقنيات التعرف على الوجه والتي تملكها الشركة وقد طعنت الشركة على الدعوى تأسيسا على سابقة قضائية أخرى وهي «زيلمر ضد فيس بوك[44]، وقد رفض طعن الشركة وما زالت القضية معروضة أمام القضاء الأمريكي[45].

وحالة أخرى تتمثل فى قضية "زيلمر ضد فيس بوك" وهي "دعوى جماعية" رفعتها مجموعة من غير مستخدمي منصة التواصل الجماعي "فيس بوك" لزعمهم أن الشركة قامت بانتهاك خصوصياتهم حين احتفظت بقوالب لوجوههم أنتجتها باستخدام تقنيات الذكاء الصناعي لديها المفعلة ذاتيا أثناء مسح الشركة للصور التي يرفعها مستخدمي المنصة بالميزة المعروفة باسم «الوسم tagging"."[46]

وقد تداولت المحاكم هذه الدعوى في أرجاء المحاكم الأمريكية منذ عام 2015 وانتهت بأضخم تسوية في تاريخ القضاء الأمريكي فيما يتعلق بقضايا مخالفات الخصوصية حيث وافقت شركة فيس بوك على دفع ما يقرب من تسعة وسبعين مليون دولار أمريكي ونصف المليون كإجمال نهائي للتسوية تقسم على المدعين بحيث يحصل كل مدع على ثلاثمائة وخمسة وأربعين دولارا، وهو على حسب الحكم النهائي بالموافقة على التسوية أقل من المقدار المفرَوض حال السريان في الدعوى وفرض غرامات جنائية على شركة فيس بوك لمخالفتها قانون ولاية الينوى الأمريكية لخصوصية البيانات البيومترية لعام 2008 والتي تتراوح بين ألف دولار وخمسة آلاف دولار لكل مخالفة[47].

كما ظهر البعد الحقيقي للمخاطر التي تمثلها تلك التقنيات على مشروعية الأدلة المستقاة منها وخاصة تماسها مع الحق في البيانات الشخصية في قضايا عدة، مثلا قضية "كلير فيو clear view" الأمريكية التي تمتلك برنامجا للتعرف على الهوية من خلال نمط الوجه، حيث تواردت تقارير تؤكد قيام مؤسس الشركة ومبرمج البرنامج "هون تون " بحصاد بيانات شخصية مجمعة من على الانترنت لتدريب برنامج للتعرف على الوجوه خاصته، متجاوزا جميع قواعد معالجة البيانات الشخصية التي تتعلق بمشروعية المعالجة ومحدوديتها وعلم الأشخاص المعنيين بالبيانات واستخدام البيانات الشخصية لأغراض الذكاء الصناعي والتربح[48].

42 Wise v. Ring LLC, W.D. Wash., No. 2:20-cv-01298, 8/3/22

43 Samantha Hawkins. Ring Loses Bid to Dismiss Biometric Claims Over Doorbell Cameras. Bloomberglaw, web site, Aug. 4, 2022, last visited: 13/9/2022, https://news.bloomberglaw.com/privacy-and-data-security/ring-loses-bid-to-dismiss-biometric-claims-over-doorbell-cameras

44 Zellmer v. Facebook, Inc. (3:18-cv-01880) District Court, N.D. California, March 27, 2018 وسيتم تفصيلها لاحقا

45 JOHN C. COUGHENOUR, District Judge order on 3/8/2022 on Case No. C20-1298-JCC.

46 Kristin L. Bryan, David J. Oberly. Recent BIPA Opinion May Have Significant Implications on The Scope of Section 15(b) Claims Moving Forward. the National Law Review's, September 13, 2022, Volume XII, Number 256, last visited: 13/9/2022, https://shorturl.at/qGVZ7

47 UNITED STATES DISTRICT COURT, NORTHERN DISTRICT OF CALIFORNIA. RE FACEBOOK BIOMETRIC INFORMATION PRIVACY LITIGATION Case No. 15-cv-03747-JD. ORDER RE FINAL APPROVAL ATTORNEYS' FEES AND COSTS, AND INCENTIVE AWARDS Re: Dkt. Nos. 499, 517. 02/26/21. https://shorturl.at/jmzPT

48 Alexander L. Vuving. Hindsight, Insight, Foresight: Thinking About Security in the Indo-Pacific. United states, Asia-Pacific Center for Security Studies, 2020. P: 52, Martin Ford. Rule of the Robots: How Artificial Intelligence Will Transform Everything. United Kingdom, Hachette UK, 2021. P: 54, Ronald J. Deibert. Reset: Reclaiming the Internet for Civil Society. United Kingdom. September Publishing, 2020.

مما نجم عنه رفع المواطن الأمريكي متنيك دعوي جماعية ضد الشركة على أسس هذه الممارسات MUTNICK VS CLEARVIEW AI INC[49]، والتي تم رفضها لعدم وجود نص قانوني يجرم ممارسات تلك الشركة، ولكن رغم هذا فقد فسخت شركة "كلير فيو" كل تعاقداتها عدا هذه الموقعة مع قوات الأمن العام، والتي فسختها داخل ولاية الينوي لوجود قانون الينوي لحماية البيانات البيومترية[50].

وفي هذا السياق يجب إيضاح الوضع الخاص لقوانين الخصوصية في الولايات المتحدة التي يوجد بها قانون الخصوصية الأمريكي لعام 1974 الذي يخاطب فقط الحكومة الفيدرالية والجهات التابعة لها بما فيه قوات الأمن العام وقوات إنفاذ القانون الفيدرالية مما يحد من قدرات تلك الجهات من تكوين وإدارة نماذج ذكاء اصطناعي للتعرف على الوجه، مما يدفع تلك الجهات لتفادي تلك القيود القانونية بالتعاقد مع مقدمي خدمات من القطاع الخاص، كحالة شركة" كلير فيو" الأمريكية، التي تؤجر خدماتها بشكل حصري لقطاع الأمن العام، والذي يعتمد على مثل تلك التقنيات لسد حاجاته المتنامية لتحديد الهوية والتعرف على المتهمين، نجدها تقدم أبلغ مثال للمخاطر التي يمكن أن يتعرض لها الأبرياء جراء عدم تنظيم عمل هذه الشركات.

ففي حين تملك الشركة قاعدة بيانات تحتوي على ثلاثة بليون صورة، فإن قاعدة بيانات وكالة الاستخبارات الفيدرالية الأمريكية تحتوي على ستمائة وأربعين مليون صورة فقط، كونها مقيدة بمعايير قانونية أعلى من الشركة الخاصة بموجب قوانين الخصوصية الأمريكية التي تحكم القطاع العام، على عكس الشركات الخاصة كشركة "كلير فيو" الغير خاضعة لقوانين شاملة تنظم أعمالها فيما يتعلق بالخصوصية وحماية البيانات الشخصية[51]، وهذا راجع لعدم وجود قوانين تخاطب القطاع الخاص فيما يتعلق بالخصوصية وحماية البيانات الشخصية بأمريكا[52]، ولهذا اعتبر الكثيرون استخدام السلطات العامة الأمريكية لمقاولين من القطاع الخاص لتولي أعمال المراقبة وتحليل البيانات الشخصية تحايلا على القواعد القانونية الحاكمة لها، وهو ما حدث بالضبط في حالة فضيحة برنامج "بريزم الأمريكية" الشهيرة والتي فضحها "سنودن"[53].

وهذا يؤكد ضرورة تناول هذا الموضوع بشكل تشريعي يحده ويحافظ على التوازن اللازم بين اعتبارات الأمن سواء العام أو الخاص، وبين الحق في البيانات الشخصية.

P: 52

49 Mutnick v. Clearview AI, Inc. et al, No. 1:2020cv00512 - Document 86 (N.D. Ill. 2020) urt Description: MEMORANDUM Opinion and Order: The Court denies defendants' Rule 12(b)(2) and § 1404(a) motions [29, 45]. Signed by the Honorable Sharon Johnson Coleman on 8/12/2020. Mailed notice. (ym,)

50 Henry H. Perritt. Digital Communications Law. Revised / 2020. United states, Wolters Kluwer, 2010, 2020 edition. P: 13-170 , ibid: Alexander L. Vuving. Hindsight, Insight, Foresight: Thinking About Security in the Indo-Pacific ., p: 48

51 Roland Vogl. Research Handbook on Big Data Law, Research Handbooks in Information Law series. United states, Edward Elgar Publishing, 2021. P: 35

52 Roberto J. Rodrigues, Petra Wilson, Stephen J. Schanz, The Regulation of Privacy and Data Protection in the Use of Electronic Health Information: An International Perspective and Reference Source on Regulatory and Legal Issues Related to Person-identifiable Health Databases, Washington, D.C., United States: Pan American Health Organization, 2001, p: 38, Jacqueline Klosek, Data Privacy in the Information Age, Westport/ Connecticut/ United States: Greenwood Publishing Group, 2000, p: 190, United States. Congress. House. Committee on Energy and Commerce, The EU Data Protection Directive: Implications for the U.S. Privacy Debate : Hearing Before the Subcommittee on Commerce, Trade, and Consumer Protection of the Committee on Energy and Commerce, House of Representatives, One Hundred Seventh Congress, First Session, March 8, 2001, Volume 4, U.S., Washington, D.C./ United States: Government Printing Office, 2001, p: 4, Curtis Frye, Privacy-enhanced Business: Adapting to the Online Environment, Westport/ Connecticut/ United States: Greenwood Publishing Group, 2001, p: 71

53 T.C. Sottek, Janus Kopfstein. everything you need to know about prism, a cheat sheet for the nsa's unprecedented surveillance programs. The verge, 17/7/2013, https://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet

الفرع الثاني
المخاطر التي يثيرها التعاون بين مشغلي أنظمة المراقبة الذكية للمنازل وبين جهات الأمن العام

أولا: حالة شركة رينج التابعة لأمازون

أثارت ما كشفته شركة أمازون الأمريكية في شهر يوليو 2022 عن التعاون القائم بين شركتها التابعة «رينج" والتي تقدم منتجات للرقابة والإدارة المنزلية الذكية smart home وجهات الأمن العام، حالة من القلق العام وسط الأمريكيين سواء من الجمهور أو المتخصصين أو السياسيين.

وقد صرحت الشركة أنها تشارك مقاطع الفيديو والبيانات الشخصية المولدة بواسطة أجهزة "جرس الباب الذكي" التي تبيعها الشركة بشكل مستمر مع جهات الأمن العام المحلية بذريعة التعاون مع تلك الجهات في الحفاظ على سلامة الضواحي الأمريكية، وهو برنامج يغطي جميع شبكة وقواعد بيانات الشركة الممتدة في جميع أنحاء أمريكا[54].

جاء هذا التصريح بعد سلسلة من المخاطبات والتساؤلات بشأن هذا الموضوع[55]وجهها السيناتور / عضو مجلس الشيوخ الأمريكي "ادوارد جي ماركي" السيناتور الديموقراطي لولاية ماساتشوستس الأمريكية لشركة أمازون، حول سياسات شركة "رينج" فيما يخص البيانات الشخصية التي تجمعها أجهزتها والتي تقدر بعشرة ملايين جهاز حول أمريكا[56].

والذي أقلق العامة في أمريكا حول هذا التصريح أنه أولا يأتي بدون علم أو موافقة ملاك تلك الأجهزة، فطبقا لتصريحات شركة "أمازون" فهي تشارك الصور ومقاطع الفيديو مع قوات إنفاذ القانون بدون علم أو موافقة عملائها، أو طبقا لتصريح أو إذن قضائي[57]، وأيضا بالمخالفة لسياساتها المعلنة حول شراكتها مع جهات إنفاذ القانون المحلية[58]، والذي أعلنت فيه أنها تشارك البيانات الشخصية مع جهات الأمن العام بناء على ما أسمته دواعي الطوارئ والمحافظة على حياة وأمن الأفراد فقط .

وقد أثار هذا التصريح استياء العديد من عملاء الشركة، وخصوصا في ظل الاطارين القانوني والثقافي الأمريكي الذي لا يحبذ على الإطلاق فكرة تدخل جهات إنفاذ القانون المحلية في شئون المواطنين وخصوصياتهم بدعوى توفير الخدمات الأمنية، ودعوا شركة أمازون لوقف برامج التعاون هذه التي تسمح بالشراكة المفتوحة لتلك البيانات المعرفة للشخصية PII personal identifiable information بين الشركة وقوات إنفاذ القانون بدون ضوابط قانونية معروفة للمستخدمين وبدون موافقتهم أو تصريح قضائي.

واستجابة لتلك الدعوات أوقفت شركة أمازون تعاونها مع قوات الأمن المحلية منذ عام 2020 حتى تاريخه، داعية الحكومات لتقديم قوانين أكثر صرامة لاستخدام تلك الجهات لبرامج التعرف على الوجوه وتحديد الهوية بالذكاء الاصطناعي[59].

وقد كشفت بعض المنظمات الحقوقية كمنظمة الحقوق الأمريكية الرائدة "مؤسسة الحدود الإلكترونية" في عام

54 alfred ng, amazon gave ring videos to police without owners' permission, politico, 07/13/2022, last visited: 11/9/2022, https://shorturl.at/dsJU8b

٥٥ وهذه المخاطبات استرمت من سنة ٢٠١٩ حتى الآن نتيجه للسمعة المسبقة حول شراكة امازون مع جهات انفاذ القانون المحلية وسيتم تفصيلها لاحقا

56 Edward J. Markey, a letter to Andrew jassy, united states, June , 2022, p: 1, you can download the letter from, https://www.markey.senate.gov/download/senator-markey-letter-to-amazon-on-ring-audio-and-law-enforcement

57 Weird, Amazon Handed Ring Data to Police Without Warrants, last visited: 11/9/2022, https://www.wired.com/story/amazon-ring-police-videos-security-roundup/

58 Ring, How Public Safety Agencies Use Neighbors, last visited, 11/9/2022, https://support.ring.com/hc/en-us/articles/360031595491

59 Amazon, We are implementing a one-year moratorium on police use of Rekognition, June 10, 2020, last visited: 13/9/2022, https://www.aboutamazon.com/news/policy-news-views/we-are-implementing-a-one-year-moratorium-on-police-use-of-rekognition

2021 أن قسم شرطة ولاية لوس أنجلوس بكاليفورنيا أمريكا طلب من خلال برنامج "الضواحي" صور تتعلق بمظاهرات "حياة السود تهم black live matters" المشهورة الموجهة ضد عنف الشرطة تجاه أصحاب البشرة الملونة من الأمريكيين ذوي الأصول الأفريقية[60]، مما صعد من حدة الانتقادات الموجهة لهذا النوع الجديد من المراقبة الأمنية، بعد ظهور استخدامها بشكل يقمع الأفراد من ممارسة حقوقهم الدستورية كالحق في التظاهر.

ومن ناحية أخري فقد أظهرت العديد من الدراسات والأبحاث عدم معصومية تلك البرامج من ارتكاب الأخطاء وخصوصا في حالات معينة تتعلق بالتعرف على أصحاب البشرة الملونة كالأمريكيين من أصل أفريقي وغيرهم من أصحاب الخلفيات الإثنية، وأيضا النساء والصغار[61]، كما نادى "اتحاد الحريات المدنية الأمريكي" بوقف استخدام هذا البرنامج لأغراض الأمن العام بواسطة قوات إنفاذ القانون الأمريكية بناء على هذه الدراسات واستشهد بالذات بدراسة قام بها هذا البرنامج بالتعرف على 28 نائب كونجرس أمريكي على أنهم مجرمين[62].

ثانيا: حالة تقديم خدمات التعرف على الهوية من خلال مسح بيانات الوجه (أمازون ريكونجشن)

لم تقتصر شراكة شركة أمازون مع أجهزة الأمن الأمريكية على ما أثير في فضيحة شركة رينج، ولكن للشركة تاريخ قديم في تقديم خدمات التعرف على الوجه التابعة لها "أمازون ريكوجنكشن" لهذه الأجهزة، وهي جزء من خدمات الحوسبة السحابية التابعة أيضا لأمازون والمعروفة ب "خدمات أمازون المقدمة عبر شبكة المعلومات العالمية (amazon web services (AWS"، وهذا البرنامج من المعروف عنه استخدامه لقاعدة واسعة من الصور المخزنة حاسوبيا للتعرف بسرعة ودقة على الوجوه والهويات، وهو يقدم عددا من الخدمات الفرعية تتنوع بين التعرف على العمر والنوع من خلال البحث عن بعض العلامات المميزة في تركيبة الوجه وتدعى " تحديد الوجه DEDECT FACE" و التعرف على الوجه من خلال مطابقته بقاعدة بيانات ضخمة يحتويها البرنامج ترتبط بخدمات أمازون السحابية "INDEX "FACE AND SEARCH FACES[63].

حيث خصصت أمازون جزءا من تلك البنية الحاسوبية الحوسبية للقطاع الأمني ابتداء من أواخر عام 2017، مما أثار حفيظة عدد من المنظمات الحقوقية الأمريكية، وجعلهم يطالبون "أمازون" بإيقاف هذا التعاون متعللين باستخدام جهات الأمن العام لتلك التقنيات بشكل غير قانوني يهدد مصالح وحقوق الأفراد[64]، بما يتنافى مع القيم الدستورية الأمريكية[65]، وأيضا ردا على عدد من الدراسات التي أكدت على خطورة الاعتماد على هذه التقنيات الحديثة في أعمال شديدة الخطورة كالتحقيقات الجنائية [66].

60 matthew guariglia, dave maassfebruary. lapd requested ring footage of Black Lives Matter protests. Electronic Frontier Foundation. Web site, 2021, last visited: 13/9/2022. https://www.eff.org/deeplinks/2021/02/lapd-requested-ring-footage-black-lives-matter-protests

61 Rosario Girasa. Artificial Intelligence as a Disruptive Technology: Economic Transformation and Government Regulation. Switzerland, Springer Nature, 2020. P: 114-115

62 Danny Caine. How to Resist Amazon and Why: The Fight for Local Economics, Data Privacy, Fair Labor, Independent Bookstores, and a People-Powered Future!. United states, Microcosm Publishing, 2022. P: 152

63 Neha Sharma, Amlan Chakrabarti, Valentina Emilia Balas, Jan Martinovic, Data Management, Analytics and Innovation: Proceedings of ICDMAI 2020, Volume 1, singapore, Springer Nature, 2020, p: 283

64 Stephen J.A. Ward. Handbook of Global Media Ethics. Switzerland, Springer Nature, 2021. P: 525

65 Elizabeth Dwoskin. Amazon is selling facial recognition to law enforcement — for a fistful of dollars. The Washington post. May 22, 2018, web site, last visited: 13/9/2022, https://www.washingtonpost.com/news/the-switch/wp/2018/05/22/amazon-is-selling-facial-recognition-to-law-enforcement-for-a-fistful-of-dollars/

66 Karen Haoarchive. The two-year fight to stop Amazon from selling face recognition to the police. united states, MIT Technology Review, June 12, 2020, MIT (Massachusetts Institute of Technology). Last visited: 13/9/2022, https://www.technologyreview.com/2020/06/12/1003482/amazon-stopped-selling-police-face-recognition-fight/

الفرع الثالث
قواعد أتمتة القرارات في قوانين حماية البيانات الشخصية

من أهم الأعمال التي تستخدم فيها آليات الذكاء الصناعي والتي تشكل خطورة متعاظمة على البيانات الشخصية وحقوق الأفراد المعنية بالبيانات، هي استخدام البيانات الشخصية لأغراض التنميط أو أتمتة/ ميكنة اتخاذ القرارات بناء البيانات الشخصية، وهذا الاستخدام قد يترتب عليه عواقب جسيمة للشخص موضع البيانات، فعلي سبيل المثال عند تقييم الموقف الائتماني للعميل عن طريق قراءة تاريخه الائتماني فقط ، أو رفع قيمة التأمين على الحياة بناء على التاريخ المرضي للشخص موضع البيانات، ولهذا خصه بعض المشرعين بنصوص خاصة.

وهذا الحق موجود فقط في كل من اللائحة العامة لحماية البيانات الشخصية والقانون البحريني لحماية البيانات الشخصية، ولم يذكر في القانون المصري، فالقانون البحريني حدد حالات معينة يمكن فيها ل «الشخص صاحب البيانات» و «محل القرار» أن يطالب مدير البيانات أو النظام أو طالب القرار اللجوء لأسلوب آخر للوصول لهذا القرار، وهذه الحالات تتعلق إما بالتقييم الوظيفي والمالي أو التأميني، وقيد هذا الحق في حالات تنفيذ العقود أو الالتزامات الناشئة عنها، ويسري على هذا الحق ما يسري على بقية الحقوق السابقة[67].

وعلى عكس هذا جاءت اللائحة العامة موسعة لحق الشخص في الاعتراض على جميع القرارات المتخذة آليا بصورة حصرية ؛ و التوصيف / التنميط (المعالجة الآلية للبيانات الشخصية لتقييم أشياء معينة عن الفرد)، فقد شملت في أحكامها جميع أنواع الاتخاذ المؤتمت للقرارات من ضمنها التنميط أيضا[68]، وحظرت اللائحة هذه الأنواع من المعالجة ابتداء واستثنت فقط هذا في حالات معينة مثل العلاقات العقدية أو السماح بهذا من قبل قانون اتحادي أو وطني أو الموافقة الصريحة ل «الشخص موضع البيانات» وأخيرا المصلحة العامة[69]، كما فرضت على «المتحكم في البيانات» آليات معينة عند إعماله لمثل هذه الآليات المؤتمتة لاتخاذ القرارات وهي أن يتاح للشخص موضع البيانات معلومات كافية وبسيطة توضح كيفية عمل هذه الآليات، وضع وسائل واضحة وسهلة لطلب "الأشخاص موضع البيانات» التدخل البشري، وأن يمكنوا الأشخاص موضع البيانات من إيضاح وجهة نظرهم ونقاط الخلاف أو يعترضوا على القرارات الناجمة عن هذه الآليات المؤتمتة، كذا يجب أن يقوموا بوضع آليات وسبل للصيانة والمتابعة المستمرة والدورية لهذه الأنظمة للتأكد من عملها بالصورة المقصودة منها، وأخيرا تأمين البيانات الشخصية بطريقة تتناسب مع المخاطر التي يمكن أن تهدد مصالح الفرد وحقوقه ، وتمنع الآثار التمييزية التي يمكن أن تنجم عن مثل هذه المعالجات[70].

---

٦٧ القانون البحريني: مادة (٢٢) الحق في الاعتراض على القرارات التي تتم بناءً على المعالَجة الآلية.

68GDPR :Art 22 .GDPR Automated individual decision-making ,including profiling ,Recitals(71) Profiling (72) Guidance of the European Data Protection Board regarding profiling (91) Necessity of a data protection impact assessment ,information commissioner office ,Rights related to automated decision making including profiling) ,Wilmslow :information commissioner office ,(2109 ,accessed from ico website :http//:bit.ly/icortautodmأتمتة , الاتخاذ المؤتم للقررات والتنميط هما موضوعات منفصلان في القوانين الأوروبية القرار يشير فقط لألية المعالجة النهائية والنتيجة الخارجة من هذه المعالجة، وتزيد عن هذا عملية التنميط في كونها تسعي إلي for قولبة أو وضع الأشخاص الطبيعين في فئات مختلفة مما قد يؤثر على حقوقهم الأساسية ويعرضهم للتمييز العرقي والعنصري more in this supject, please see :Martin Ebers ,Susana Navas ,Algorithms and Law ,Diana sancho ,Automated processing ,profiling and automated decision -making ,Cambridge /United Kingdom :Cambridge University Press ,2020 ,p , 138 :Ronald Leenes ,Rosamunde van Brakel ,Serge Gutwirth ,Paul de Hert, Data Protection and Privacy :The Age of Intelligent Machines ,Computers ,Privacy and Data Protection, London ,England :Bloomsbury Publishing ,2017 ,p , 154 :Mireille Hildebrandt ,Serge Gutwirth ,Profiling the European Citizen :Cross-Disciplinary Perspectives ,Berlin/Heidelberg /Germany :Springer Science& Business Media ,2008 ,p.34-43 :

69 Michèle Finck, Smart Contracts as a Form of Solely Automated Processing under the GDPR, Max Planck Institute for Innovation and Competition Research Paper No. 19-01, München/ Germany: Max Planck Institute for Innovation and Competition, p: 6

70 information commissioner office, Rights related to automated decision making including profiling, 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, Vol 8, No 3, Berlin/ Heidelberg/ Germany: Springer Science+Business Media, 2017, p: 2

وعليه يوصي الباحث بشدة إدراج نصوص مشابهة تنظم استخدام البيانات الشخصية لأغراض التنميط والاتخاذ المؤتمت للقرارات حماية للأشخاص الطبعيين من المخاطر التي قد تنجم عن هذا الاستخدام، مثل التمييز العنصري، والمصالح المالية، والمعنوية، وغيرها.

المبحث الثاني
التنظيم القانوني لاستخدام تقنيات التعريف على الهوية والتنميط لأغراض إنفاذ القانون

إزاء المخاطر المحتملة والمصاحبة لاستخدام تقنيات التعرف على الوجه والتنميط في عمليات إنفاذ القانون، ظهر العديد من الجهود القانونية لتنظيم استعمال تلك التقنيات في إنفاذ القانون نظرا لما تمثله تلك التقنيات من مخاطر في حد ذاتها بالإضافة للطبيعة الحساسة لعمليات إنفاذ القانون، وقد تمثلت تلك الجهود في قوانين وطنية وتوصيات دولية متعددة سنستعرض بعضها هنا، وهذا في مطلبين كالآتي:

المطلب الأول: معايير استخدام أنظمة التعرف على الوجه والتنميط لأغراض الأمن العام في التشريعات الوطنية

المطلب الثاني: الجهود الدولية لتنظيم الذكاء الاصطناعي أثناء إنفاذ القانون

المطلب الأول
معايير استخدام أنظمة التعرف على الوجه والتنميط لأغراض الأمن العام في التشريعات الوطنية

للمخاطر المترتبة على استخدام التقنيات الحديثة للتعرف الآلي وأتمتة عمليات تتبع الأشخاص بالذكاء الاصطناعي، حرص عدد من القوانين على تقديم منظومة متكاملة لهذه الأنظمة تشمل قواعد تدريب وجودة البيانات وحدود الاستخدام، أو تشمل قواعد عامة لأنظمة المراقبة، أما بالنسبة لعمليات التنميط فهي لم تجد الاهتمام المماثل لتقنيات التعرف على الوجه، وسوف نلقي نظرة هنا على بعض من نماذج تلك القوانين، وهذا في فرعين كالآتي:

الفرع الأول: تنظيم استخدام تقنيات التعرف على الهوية والتنميط في قوانين الاتحاد الأوروبي

الفرع الثاني: الوضع التشريعي لاستخدام تقنيات الذكاء الاصطناعي لإنفاذ القانون في الولايات المتحدة

الفرع الأول

تنظيم استخدام تقنيات التعرف على الهوية والتنميط في قوانين الاتحاد الأوروبي

يعتبر قانون الذكاء الاصطناعي[٧١] للاتحاد الأوروبي –كعادة التشريعات الصادرة من الاتحاد الأوروبي– منظومة متكاملة اهتمت بتقديم تنظيم قانوني واداري وفني مميز لدعم قطاع الذكاء الاصطناعي في الاتحاد الأوروبي من ناحية، ومن ناحية أخرى العمل على تنظيم نماذج الذكاء الاصطناعي، ومن ضمن هذه الاستخدامات التي اهتم بها قانون الذكاء الاصطناعي الأوروبي هو استخدام الذكاء الاصطناعي لأغراض الأمن العام وإنفاذ القانون، وقد تناثرت قواعد هذه الاستخدامات في جميع أنحاء القانون كمثلا تصنيف هذه الاستخدامات ثم وضع قواعد استخدام التقنيات التي اباح استخدامها، وهو ما سنبينه كالآتي:

٧١ جاء القانون مركزا على استخدامات الذكاء الاصطناعي لا التقنيات ذاتها ودعم الثقة في الذكاء الاصطناعي

أولا: تصنيف نماذج الذكاء الاصطناعي لأغراض انفاذ القانون في قانون الذكاء الاصطناعي الأوروبي

أ: التقنيات المحظورة في قانون الذكاء الاصطناعي الأوروبي:

1: حظر تقنيات المسح والجمع العشوائي لبيانات الوجه في قانون الذكاء الاصطناعي الأوروبي:

يمكن التماس صعوبة تحديد اتجاه تشريعي يحافظ على التوزان بين الحقوق الفردية المرتبطة والضرورات الأمنية، فيما يتعلق باستعمال تقنيات التعرف على الوجه وأنظمة المراقبة المزودة بالذكاء الاصطناعي بما حدث من مداولات مكثفة واعتراضات متعددة قسمت جبهة التوافق السياسي أثناء المداولات الأخيرة لقانون الذكاء الاصطناعي الأوروبي، حيث كانت تلك النقطة من أكثر نقاط القانون جدلا بين دول أعضاء الاتحاد بين مؤيد ومعارض[72]، وقد جاء القانون بعد ذلك ناصا على منع تلك التقنيات من الأصل حيث منع طرح نماذج أنظمة الذكاء الاصطناعي التي تنشئ أو توسع قواعد بيانات التعرف على الوجه من خلال تجميع أو التنقيب العشوائي لصور الوجه من الإنترنت أو لقطات كاميرات المراقبة[73]، ولكنه نظم تقنيات المراقبة ذاتها كما سنعرض فيما بعد، أي أن المشرع الأوروبي اعتبر تقنيات المسح والجمع العشوائي للإنترنت لتكوين قواعد البيانات التي سيدرب عليها نموذج الذكاء الاصطناعي أكثر خطرا من تقنيات المتابعة ذاتها، وهو ما نؤيده حيث أن مرحلة جمع البيانات والتدريب من أخطر مراحل إنشاء نموذج الذكاء الاصطناعي مما يوجب حوكمتها بشكل صارم تفاديا لأي أخطاء أثناء التشغيل والاعتماد على نموذج الذكاء الاصطناعي ذاته.

2: حظر تقنيات التنميط في قانون الذكاء الاصطناعي الأوروبي:

حظر قانون الذكاء الاصطناعي للاتحاد الأوروبي عامة طرح أي برنامج ذكاء اصطناعي يستخدم بشكل أساسي ومستقل لتحديد إمكانية انخراط أو التنبؤ بإمكانية انخراط شخص طبيعي في الأنشطة الإجرامية بناء على التنميط الشخصي، وهذا الحظر لا يسري على البرامج التي تستخدم كوسائل مساعدة لآليات مكافحة الجريمة وتقييم انخراط الأشخاص في الأنشطة الإجرامية، في حين يكون التقييم نفسه مبنى على تقييم بشرى موضوعي للجريمة والأنشطة الإجرامية[74].

ب: التقنيات العالية المخاطر في قانون الذكاء الاصطناعي:

صنف قانون الذكاء الاصطناعي الأوروبي نماذج الذكاء الاصطناعي التي تعتمد على تحليل البيانات البيومترية أو التنميط والتصنيف لإخراج نتائج مؤتمتة نهائية كتقنيات محظورة ابتداء، ولكنه استثنى بعضا منها لأغراض محددة من أهمها استعمالها لأغراض إنفاذ القانون والأمن العام، وهو لا يعني استثناءها بالكلية من المعايير المشددة للقانون، ولكنه فقط خفف من تصنيفها من التقنيات المحظورة للتقنيات عالية المخاطر، وهو ما يعني إمكانية استعمالها ولكن وجوب أن يخضع مستعملها للعديد من الاعتبارات الصارمة، والتي من أهمها هنا هو حظر الاستعمال لكل استخدام غير متعلق بإنفاذ القانون والأمن العام وكل من هو ليس جهة إنفاذ قانون مخولة بموجب سلطاتها القانونية للقيام بتلك الأعمال، بالإضافة للعديد من الالتزامات التي سنفصلها في موضعها.

وقد نصت المادة السادسة على أن اعتبار أي نموذج للذكاء الاصطناعي يستخدم لتنميط وتصنيف الأشخاص الطبيعية كنموذج عالي المخاطر[75]، كما جاء الملحق الثالث من القانون ناصا على أن أي ذكاء اصطناعي

72 Euronews ,Could the EU's Artificial Intelligence Act increase mass surveillance systems?, last visited: 12/4/2024, https://t.ly/zYnTY

73 Eu, Regulation (EU) 2024/1689 Artificial Intelligence Act, article 5: Prohibited AI practices: 1. The following AI practices shall be prohibited: e: the placing on the market, the putting into service for this 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;

74 Eu, Regulation (EU) 2024/1689 Artificial Intelligence Act, article 5\1\d.

75 Eu, Regulation (EU) 2024/1689 Artificial Intelligence Act, article 6: Notwithstanding the

مستخدم بواسطة قوات الأمن أو إنفاذ القانون التابعين للاتحاد الأوروبي أو دوله بنفسهم أو لمصلحتهم وغاياتهم، يعتبر ذو خطورة عالية إذا استخدم لغايات تحديد خطورة شخص طبيعي أو إدانته أو إعادة إدانته إذا استخدم «التنميط» بشكل أساسي أو لم يستخدمه بشكل أساسي[76].

كما شدد القانون في أكثر من موضع وجوب مراعاة قاعدة «الافتراض المبدئي للبراءة»، وأن مواطني الاتحاد الأوروبي يجب ألا يتعرضوا لأي نوع من أنواع الإدانة والاتهام الجنائي المبنى فقط وأساسيا على أتمتة القرار بواسطة آليات الذكاء الاصطناعي[77].

وبالنسبة لنماذج الذكاء الاصطناعي التي تستعمل البيانات البيومترية فهي من النماذج عالية المخاطر إذا استعملت لتحديد الهوية من على بعد، أو أنظمة الذكاء الاصطناعي المخصصة للاستخدام في التصنيف البيومترية، وفقًا لسمات أو خصائص حساسة أو محمية بناءً على الاستدلال على تلك السمات أو الخصائص; أنظمة الذكاء الاصطناعي المخصصة للاستخدام في التعرف على المشاعر[٧٨].

ثانيا: شروط استخدام تقنيات التتبع المعتمد على التعرف على قوالب الوجوه في قانون الاتحاد الأوروبي للذكاء الاصطناعي:

إزاء رغبة بعض الدول الأعضاء كفرنسا في تعزيز أمن المناطق العامة بها وخاصة خلال الأحداث الكبرى[79]، وضع قانون الاتحاد الأوروبي بعض المعايير الصارمة لاستعمال تقنيات المراقبة المباشرة للأماكن العامة المزودة بقدرات التعرف المباشر والتلقائي والتتبع للأشخاص بناء على أنماط الوجه، حيث اشترط الآتي:

١. أن تستخدم تلك الأنظمة حصريا ل: (١- البحث عن ضحايا محددين من ضحايا الاختطاف أو الاتجار بالبشر أو الاستغلال الجنسي للبشر، وكذلك البحث عن الأشخاص المفقودين; 2- منع أو إيقاف التهديدات الكبرى المرتبطة بحياة الأفراد أو سلامتهم البدنية أو الهجمات الإرهابية. 3- تعقب مرتكبي الجرائم الجنائية أو المشتبه في ارتكابهم جرائم معنية لا تقل عقوباتها عن أربع سنوات على الأقل (جرائم كبرى) لأغراض التحقيقات أو القضاء أو تنفيذ العقوبات الجنائية).

٢. أن تستخدم تلك التقنيات لتتبع أشخاص معينين وتأكيد هويتهم، مع الأخذ في الاعتبار التوازن بين خطورة الحدث والأضرار المتوقعة عن حدوثه، والمخاطر الناجمة على حقوق وحريات الأفراد.

٣. ويجب أيضا أن يتم مراعاة أي ضوابط قانونية وطنية وأن تقوم سلطة إنفاذ القانون بعمل تقييم للمخاطر الواقعة على الحقوق الفردية الأساسية، وأن تسجل الاستخدام في القاعدة الاتحادية لمثل تلك الحالات فورا أو في أقرب وقت ممكن.

٤. يجب الحصول على إذن قضائي مسبق أو صادر من جهة إشرافية مستقلة، وفي حالات الاستعجال المبررة يجب ألا يتجاوز وقت تقديم الإذن عن أربع وعشرين ساعة، وفي حالة رفض الطلب وتم تشغيل الأنظمة والبدء في التتبع يجب إيقاف العملية فورا ومحو كل البيانات التي تم تجميعها.

٥. يجب إخطار سلطات مراقبة السوق وحماية البيانات الشخصية بكل عملية تتبع ومسح.

٦. إخطار المفوضية سنويا بكل حالات التتبع التي تم إجراؤها، وتصدر المفوضية

first subparagraph, an AI system referred to in Annex III shall always be considered to be high-risk where the AI system performs profiling of natural persons.

76 Eu, Regulation (EU) 2024/1689 Artificial Intelligence Act, ANNEX III, 6

77 Eu, Regulation (EU) 2024/1689 Artificial Intelligence Act, recital 42, recital 48, recital 59.

78 Eu, Regulation (EU) 2024/1689 Artificial Intelligence Act, ANNEX III, 1

79 Investigate europe, France spearheads member state campaign to dilute European AI regulation, last visited: 8\4\2025, https://www.eu/posts/france-spearheads-member-state-campaign-dilute-european-artificial-intelligence-regulation

تقرير سنوي متاح للجمهور بكل تلك العمليات، بحيث لا يشمل التقرير على معلومات تشغيلية حساسة[80].

وتشمل الجرائم المنصوص عليها منع احتمالات حالية ومحددة للتهديدات الإرهابية، تعقب وتحديد شخص متهم في الجرائم المحددة سلفا في القانون وهي: ("الإرهاب ؛ الاتجار بالبشر ؛ الاستغلال الجنسي للأطفال واستغلال الأطفال في المواد الإباحية ؛ الاتجار غير المشروع بالمخدرات والمؤثرات العقلية ؛ الاتجار غير المشروع بالأسلحة والذخائر والمتفجرات ؛ القتل والإصابة الجسدية الخطيرة ؛ الاتجار غير المشروع بالأعضاء والأنسجة البشرية ؛ الاتجار غير المشروع بالمواد النووية أو المشعة ؛ الاختطاف وضبط النفس غير القانوني وأخذ الرهائن ؛ الجرائم التي تدخل في اختصاص المحكمة الجنائية الدولية ؛ الاستيلاء غير المشروع على الطائرات/السفن ؛ الاغتصاب ؛ الجريمة البيئية ؛ السطو المنظم أو المسلح ؛ التخريب ؛ المشاركة في منظمة إجرامية ضالعة في جريمة أو أكثر من الجرائم المذكورة أعلاه)[81]، أو بجناية معاقب عليها بعقوبة تقدر بأربع سنوات، مع مراعاة أحكام المادة التاسعة من اللائحة العامة لحماية البيانات الشخصية[82]، وهي المادة الخاصة بمعالجة الفئات الخاصة من البيانات الشخصية[83].

ثالثا: الضوابط القانونية لاستعمال تقنيات التنميط لأغراض إنفاذ القانون:

يعتبر التنميط من الأنشطة التي توليها القوانين المختلفة عناية خاصة تبدأ من اشتراطات معينة لاستخدام البيانات الشخصية فيها، حيث نصت اللائحة العامة لحماية البيانات الشخصية على ضرورة حماية الأشخاص المعنية بالبيانات من المراقبة السلوكية والتتبع على الإنترنت والتنميط[84]، كما جاء قانون الذكاء الاصطناعي للاتحاد الأوروبي واضعا أي تطبيق من تطبيقات الذكاء الاصطناعي والذي يستعمل التنميط في عملياته في مستوى العمليات عالية الخطورة والتي وضع على مطوريها وطارحيها في السوق التزامات خاصة[85].

وقد منح كلا من اللائحة العامة وتوجيه البوليس ونسخهم السابقة من تشريعات الاتحاد الأوروبي المتعلقة بحماية البيانات الشخصية، الشخص المعنى بالبيانات الحق في الاعتراض على أي قرار اتخذ بشكل مؤتمت بناء على تنميط البيانات الشخصية أو معالجة البيانات الشخصية[86].

وأيضا نص التوجيه[87] الأوروبي ٦٨٠ لسنة ٢٠١٦ المعروف بتوجيه البوليس (حماية البيانات الشخصية بما يتعلق بأعمال سلطات التحقيق وإنفاذ القانون) على وجوب حظر الاتخاذ المؤتمت للقرارات بناء على التنميط ومعالجة البيانات الشخصية فقط إلا لو سمح بهذا تشريعيا سواء على مستوى الاتحاد أو على المستوى الوطني مع إيلاء التدابير القانونية اللازمة للحفاظ على حقوق الأشخاص المعنية بالبيانات الشخصية، وأيضا حظر أي معالجة للبيانات عن طريق «التنميط» والتي قد تؤدى إلى التمييز ضد الأشخاص الطبيعية بناء على معالجة الفئات الخاصة من البيانات الشخصية[88]، كما نص التوجيه على وجوب أن يحتفظ المتحكم في البيانات (هيئات إنفاذ القانون) بسجلات لعمليات المعالجة بما فيها سجل لعمليات التنميط[89].

80 Eu, Regulation (EU) 2024/1689 Artificial Intelligence Act, article 5

81 Eu, Regulation (EU) 2024/1689 Artificial Intelligence Act, ANNEX II, List of criminal offences referred to in Article 5(1), first subparagraph, point (h)(iii)

82 Eu, Regulation (EU) 2024/1689 Artificial Intelligence Act, recital 70.

83 Gdpr, Art. 9, Processing of special categories of personal data

84 daniel J. Solove, Paul M. Schwartz, EU Data Protection and the GDPR: [Connected EBook], united states of America, Aspen Publishing, 2023, p: 100, gdpr, recital: 24

85 European Commission, Why do we need to regulate the use of Artificial Intelligence?, lastvisited: 10/4/2024, https://t.ly/thJZa , Council of the European Union, Interinstitutional File: 2021/0106(COD), Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, (5aa). Article 6, d.

86 David Wright, Serge Gutwirth, Michael Friedewald, Elena Vildjiounaite, Yves Punie, Safeguards in a World of Ambient Intelligence, united states, springer, 2010, p: 58

٨٧ تنقسم البنية القانونية للقوانين الإتحادية للاتحاد الأوروبي ل «لائحة» وهي نافذة نفاذا مباشرا بحق الدول الأعضاء، و «توجيه» وهو يحتاج إلى قوانين وطنية تفعله ويوفر فقط الخطوط الأساسية التي يجب أن يتم التشريع بناء عليها.

88 EU, Directive (EU) 2016/680, article 11,

89 EU, Directive (EU) 2016/680, article 24/e

وأخيرا فإن اللائحة العامة قد اشترطت على أي مستخدم لآليات «التنميط»، أن يؤمن البيانات الشخصية وأن يمنع استخدامها بما يمكن أن يؤدى للتمييز غير العادل للأشخاص، وأن يعلم الشخص المعنى بالبيانات بوسائل اتخاذ تلك القرارات، وأن يتاح له فرصة المراجعة والاعتراض عليها، ووجود مختص بشرى لمراجعتها والاستماع لاعتراضاته[90].

ومن هنا نرى أنه على الرغم من مزايا استخدام «التنميط» في إنفاذ القانون، إلا أنه يجب مراعاة حقوق الأشخاص الموجه إليهم التهم أو الملاحقين بغرض إيقاف أو التحري عن ارتكاب هذه الجرائم، فيجب ألا يتم اتخاذ قرار الاتهام والمحاكمة والحكم القضائي بناء على قرار مؤتمت بواسطة الذكاء الاصطناعي بارتكاب تلك الجريمة بناء على تنميط وتكوين ملف جنائي بناء على تحليل البيانات الشخصية والخلفية الجنائية والمكونات والخصائص الشخصية للمتهم فقط ، بل يجب أن يعلم المتهم بأنه تم ملاحقته بناء على تحليل مستخدم به «التنميط» ليتمكن من الاعتراض على هذا التحليل والخضوع لمراجعة بشرية لكيفية الوصول لهذا القرار ، ويجب أيضا ألا توكل جهود المكافحة بشكل حصري وكامل للذكاء الاصطناعي بل يمكن الاستعانة به فقط كوسيلة للتسريع والمساعدة في الجهود البشرية الأصلية لمكافحة هذه الجرائم.

ومن هنا أيضا يمكننا تبين النسق العام للضوابط القانونية لاستعمال تطبيقات الذكاء الاصطناعي عامة، وهي ضرورة وضع حدود للتوازن بين الفوائد المحتملة والأخطار المتوقعة، وخصوصا تلك الواقعة على الأفراد وحقوقهم وحرياتهم، من خلال نماذج تشريعية تتبع إطار حقوقي مدعم بأدوات امتثال قوية يمكن تنفيذها بدون أن تعيق حركة التطور العلمي البشرى وما قد يعود منها من فوائد ومنافع جمة.

رابعا: ضوابط أتمتة القرار في قانون الذكاء الاصطناعي:

ربط قانون الذكاء الاصطناعي للاتحاد الأوروبي بين تعريف الذكاء الاصطناعي المعني به بقدرة الأنظمة على الاستنتاج INFER وهو أن يقدر النظام على إخراج استنتاج وإخراج مخرجات قد توثر على العالم الخارجي، وميزها عن مجرد البرامج القادرة على الأتمتة بناء على محددات تم برمجته بها قبلا[91]، كما ربط بين أنظمة تحديد الهوية بواسطة الذكاء الاصطناعي وبين قدرة تلك الأنظمة على القيام بعملية التعرف وتحديد الهوية بشكل مؤتمت بالارتكاز لمقارنة المحددات البيومترية التي تضمن ولا تقف على الوجه بالمحددات البيومترية المسجلة للفرد على قواعد البيانات[92].

وأوضح القانون أن ليس كل استعمال لبرامج الذكاء الاصطناعي لا يترتب عليه مخاطر كبري على حقوق الإنسان المرتبطة، فحالات استعمال نماذج الذكاء الاصطناعي بشكل لا يوثر على القرار النهائي لا يمكن اعتبارها من الحالات التي يمكن اعتبارها تمثل خطورة على الحقوق المرتبطة كمثلا استعمال نماذج الذكاء الاصطناعي لفهرسة وترتيب البيانات وتصنيفها وغيرها من الاستعمالات الوسيطة ويجب تصنيف تلك الحالات كحالات قليلة المخاطر لا عالية المخاطر ، وعليه يكون المعيار الأوحد هو مدي تأثير استخدام نماذج الذكاء الاصطناعي على القرار البشري لا مجرد عمل مهام تحضيرية أو وسيطة[93].

وقد نص قانون الذكاء الاصطناعي الأوروبي على ضرورة أن تصمم أنظمة الذكاء الاصطناعي بما يسمح الاشراف والمراجعة البشرية لأغراض تقليل المخاطر على الحقوق البشرية الفردية، ومن اللافت أيضا أن القانون أثناء تناوله لقواعد الاشراف البشري على النتائج المؤتمتة المخرجة من نموذج الذكاء الاصطناعي قد أوجب أن يتم الأخذ في الاعتبار ميل المشرف للاعتماد على المخرجات المؤتمتة المخرجة من نماذج الذكاء الاصطناعي وخاصة تلك عالية المخاطر[94].

كما نص القانون على أن جميع الضوابط المنصوص عليها بشأن أتمتة اتخاذ القرار أو الخاصة بحماية الشخص المعني بالبيانات من آثار تلك الأتمتة كالمنصوص عليها في كلا من اللائحة الأوروبية العامة لحماية البيانات الشخصية وتوجيه البوليس تظل سارية ويتمتع بها الأشخاص فيما يتعلق بحقوقهم أثناء أتمتة اتخاذ القرارات المتعلقة بهم، وخاصة فيما يتعلق بإنفاذ القانون[95].

90 GDPR, article 22Automated individual decision-making, including profiling (71) , recitals: Profiling (72) Guidance of the European Data Protection Board Regarding Profiling (91) Necessity of a Data Protection Impact Assessment

91EU AI ACT, recital 12.

92 EU AI ACT, recital 15.

93 EU AI ACT, recital 73.

94 EU AI ACT, article 14 human oversight

95 EU AI ACT, recital 10.

الفرع الثاني
الوضع التشريعي لاستخدام تقنيات الذكاء الاصطناعي لإنفاذ القانون في الولايات المتحدة

أولا: على المستوى الاتحادي:

تتبع الولايات المتحدة عادة منهج عدم التدخل التشريعي في القطاع التقني وقطاع الاتصالات[٩٦]، وعلى خلفية النقلة المعاصرة في تقنيات الذكاء الاصطناعي أصدرت إدارة الرئيس الأمريكي السابق «بايدن" الأمر التنفيذي رقم 14110 بشأن تطوير الذكاء الاصطناعي واستخدامه بطريقة آمنة ومأمونة وجديرة بالثقة، والذي تناول عددا من النقاط فيما يخص استعمال الذكاء الاصطناعي في مجال إنفاذ القانون، ومنها وجوب مراعاة الحقوق المدنية وعدم التمييز عند استعمال أدوات الذكاء الاصطناعي في مجال إنفاذ القانون وخاصة: (يجب على الجهات المعنية استخدام مكاتبها وسلطاتها المعنية بالحقوق المدنية والحريات المدنية – حسب الاقتضاء وبما يتسق مع القانون المعمول به – لمنع ومعالجة التمييز غير القانوني وغيره من الأضرار التي تنتج عن استخدامات الذكاء الاصطناعي أثناء استعمالها في الأغراض الحكومة الفيدرالية. لا ينطبق هذا التوجيه على سلطات الإنفاذ المدنية أو الجنائية للوكالات. يجب على الوكالات أن تنظر في الفرص المتاحة لضمان استشارة مكاتب الحقوق المدنية والحريات المدنية الخاصة بها على النحو المناسب بشأن قرارات الوكالات الفيدرالية المتعلقة بتصميم الذكاء الاصطناعي وتطويره واقتنائه واستخدامه. لتعزيز هذه الأهداف، تنظر الوكالات الفيدرالية أيضًا في فرص زيادة التنسيق والتواصل والمشاركة بشأن الذكاء الاصطناعي حسب الاقتضاء مع المنظمات المجتمعية؛ ومنظمات الحقوق المدنية والحريات المدنية؛ والمؤسسات الأكاديمية؛ والصناعة؛ وحكومات الولايات والحكومات المحلية والقبلية والإقليمية؛ وغيرها من أصحاب المصلحة)، وقد أوصى بأن يعمل مكتب المحامي العام على تطوير استراتيجيات وتوظيف كفاءات تعمل على تطوير استخدام تقنيات الذكاء الاصطناعي وتطوير استراتيجيات وخطط لتقليل مخاطر استعمال تقنيات الذكاء الاصطناعي أثناء إنفاذ القانون[٩٧]، ومن الجدير بالذكر أن الرئيس الأمريكي الحالي «ترامب» قد ألغي هذا القرار التنفيذي وجميع آثاره التي تتضمن أن تقوم جميع الجهات المعنية بدراسة جميع آثار الذكاء الاصطناعي في جميع المجالات[٩٨].

ثانيا: على مستوى الولايات:

في ولاية ماساتشوستس الأمريكية تم إضافة القسم ٢٢٠ للقانون العام للولاية والخاص بالبحث بواسطة تقنيات التعرف على الوجه، فطبقا لهذا القانون يجب على وكالات إنفاذ القانون التي تريد أن تجرى فحصا بواسطة تقنيات فحص الوجه أن تقدم طلبا إلى مسجل السيارات، إدارة شرطة الولاية، أو مكتب التحقيقات الاتحادي، وهذا الطلب يجب أن يكون لتنفيذ أغراض محددة فقط وهي: تنفيذ أمر قضائي بناء على معلومات واعتقاد أو حقائق ملموسة أن المعلومات المطلوبة ستفيد في تحقيق جنائي قائم، أن يكون الطلب يتعلق بتحديد هوية شخص متوفى، أن يكون الطلب يتعلق بمنع حدوث أمر طارىء قد يؤثر على حياة أو يعرض أحد الأشخاص للخطر ويجب أن يكون الطلب محددا تماما لهذه الوقائع[99].

وأوجب على كل السلطات التي تجرى بحثا باستخدام تقنيات التعرف على الوجه أن تسجل جميع هذه العمليات بما يشمل: التاريخ، نسخة من طلب البحث، عدد المطابقات، وقواعد البيانات المستخدمة، أسماء القائمين عليها والمطلوب ومطابقتهم أو التعرف على هويتهم، البيانات المرتدة على أن تحفظ ولا تنشر ، وأن تقدم بها تقريرا ربع

---

٩٦ وهذا يرجع لتاريخ طويل للمزيد يرجي مراجعة Tim Wu, A Brief History of American Telecommunications Regulation, n, OXFORD INTERNATIONAL ENCYCLOPEDIA, VOL. 5, P. 95, 2009 (2007), p:5.

97 The white house, Executive Order 14110 of October 30, 2023 Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, sec 7: Advancing Equity and Civil Rights

98 AMERICAN PSYCHOLOGICAL ASSOCIATION, Trump administration rolls back Biden AI executive order and launches Stargate project, last visited: 18\4\2025, https://www.apaservices.org/practice/business/technology/on-the-horizon/ai-executive-orders

99 The 193rd General Court of the Commonwealth of Massachusetts, General Law - Part I, Title II, Chapter 6, Section 220

سنوي للمكتب التنفيذي للأمن والسلامة العامة، والذي عليه أن ينشر تقريرا سنويا عنها[100].

وهناك أيضا قانون ولاية إلينوي الأمريكية المعرف بقانون خصوصية المعلومات البيومترية الذى عرف «المعرف البيومتري" على أنه "مسح شبكية العين أو قزحية العين، أو بصمة الإصبع، أو البصمة الصوتية، أو مسح هندسة اليد أو الوجه"[101]، وقد سن هذا القانون عام ٢٠٠٨ وهو يشمل جمع واستخدام وحماية ومناولة وتخزين وحفظ وتدمير محددات الهوية والمعلومات البيومترية، ويلزم الشركات بأن تقدم للشخص المعنى بالبيانات إشعارا كتابيا – بما في ذلك الغرض من الجمع وطول الفترة الزمنية التي سيتم فيها الاحتفاظ بمحدد الهوية، كما يحظر أيضًا على أشخاص القانون الخاص الذين يمتلكون معرفات أو معلومات بيومترية من الكشف عن هذه المعلومات ، أو الاستفادة منها دون موافقة الشخص[102]، وقد أعطى هذا القانون للأشخاص الحق الفردي في مقاضاة أي شركة أو جهة لا تلتزم بهذه الالتزامات مما أدى إلى رفع دعاوى قضائية ونجم عنها تسويات كبيرة بناءً على الغرامات القانونية المفروضة على كل انتهاك[103].

الفرع الثالث
الوضع القانوني في جمهورية مصر العربية

على النقيض من المساعي التشريعية الأوروبية المتمثلة في قانون الذكاء الاصطناعي للاتحاد الأوروبي، يفتقر البنيان التشريعي المصري الحالي إلى تنظيم قانوني خاص ومباشر يحكم توظيف تقنيات التعرف البيومتري أو التنميط الخوارزمي في قطاع إنفاذ القانون. ومع ذلك، يمكن تلمس إرادة المشرع نحو بناء سياج حمائي أولي لحقوق الأفراد في مواجهة هذه التقنيات، وذلك من خلال القراءة التحليلية للائحة التنفيذية لقانون حماية البيانات الشخصية[١٠٤]. وقد حاولت اللائحة تقييد عمليات المراقبة البصرية والتتبع السلوكي، إلا أن هذا الإطار التنظيمي يعتريه بعض القصور الهيكلي عند وضعه في ميزان المقارنة مع المعايير الدولية.

فمن جهة أولى، أقرت اللائحة التزاماً صريحاً بضمان عدم ترتب أي ضرر على الشخص المعني بالبيانات جراء استخدام بياناته في عمليات «تدريب الذكاء الاصطناعي والتقنيات الناشئة والمبتكرة»[١٠٥]. ورغم أهمية هذا النص كأول إشارة تنظيمية صريحة للذكاء الاصطناعي في المنظومة التشريعية للبيانات في مصر، إلا أنه يعاني من خلل تشريعي في "توزيع المسؤولية الفنية والقانونية"؛ إذ ألقى بعبء ضمان عدم الإضرار على عاتق "المعالج" (وهي غالباً الشركات التقنية المطورة للأنظمة)، متجاهلاً الدور المحوري لـ "المتحكم" (والذي يمثل هنا الجهة السيادية أو الأمنية) الذي يحدد سياق وغرض استخدام تلك الخوارزميات في اتخاذ القرارات المؤتمتة أو التنميط، وهو ما يخالف التوجهات الأوروبية التي تُحمل "المتحكم" المسؤولية التضامنية أو الأساسية عن تقييم المخاطر (Data Protection Impact Assessment).

ومن جهة ثانية، تطرقت اللائحة إلى تنظيم استخدام وسائل المراقبة البصرية في الأماكن العامة، حيث حظرت إجراء أي معالجة تهدف للوصول للبيانات الشخصية عبر «تقنيات تمييز الوجوه» (Face Recognition) أو التقنيات المماثلة، إلا في الأحوال المقررة قانوناً أو بموافقة صريحة[106]. كما قيدت بشدة استخدام بيانات الأطفال في عمليات "التصنيف أو التتبع أو المراقبة السلوكية" (Profiling and Behavioral Tracking)

100 The 193rd General Court of the Commonwealth of Massachusetts, General Laws/ Part I/ Title II/ Chapter 6/ Section 220: Facial recognition searches; requests; valid purposes; documentation; reporting; exceptions, c,d, Rachel Harmon, The Law of the Police: [Connected EBook], united states, Aspen Publishing, 2024, p: 130-131.

101 Illinois general assembly, CIVIL LIABILITIES (740 ILCS 14/) Biometric Information Privacy Act, Sec. 10. Definitions. In this Act

102 Amie Taal, The GDPR Challenge: Privacy, Technology, and Compliance in an Age of Accelerating Change, united states, CRC Press, 2021, p: 166.

103 Daniel J. Solove, Paul M. Schwartz, Information Privacy Law, united states, Aspen Publishing, 2022, p: 975.

١٠٤ اللائحة التنفيذية لقانون حماية البيانات الشخصية الصادرة بقرار وزير الاتصالات وتكنولوجيا المعلومات رقم ٨١٦ لسنة ٢٠٢٥، الوقائع المصرية، العدد ٢٤٤ تابع (أ) في أول نوفمبر سنة ٢٠٢٥.

١٠٥ المرجع السابق، المادة (٤) أولاً بند ٧.

١٠٦ المرجع السابق، المادة (٤) أولاً بند ٧.

.[107]

إلا أنه، وعلى الرغم من هذه الملامح التنظيمية الإيجابية، يظل هذا الإطار قاصراً عن معالجة إشكاليات توظيف تقنيات التنميط والتعرف البيومتري في قطاع «إنفاذ القانون» تحديداً. ويرجع ذلك إلى عائق هيكلي رئيسي يتمثل في المادة (٣) من قانون حماية البيانات الشخصية المصري، والتي استثنت صراحةً وبشكل مطلق من نطاق تطبيق القانون البيانات التي تتم معالجتها لاعتبارات «الأمن القومي»[108].

وهنا تبرز الفجوة مقارنة بالتشريعات المقارنة؛ فبينما يضع قانون الذكاء الاصطناعي الأوروبي قيوداً واشتراطات صارمة تتعلق بالشفافية والتناسب حتى على استخدامات الأمن العام (مثل قصرها على جرائم محددة واشتراط الإذن القضائي المسبق)، يترك الاستثناء المطلق في القانون المصري الباب مفتوحاً أمام استخدام السلطات لتقنيات الذكاء الاصطناعي التنبؤي دون ضوابط إجرائية واضحة للشفافية أو تقييم الأثر الحقوقي. وهو ما يُبقي الحاجة ملحة لتدخل تشريعي مستقل، أو صياغة مدونات سلوك ملزمة، تنظم استخدام السلطات العامة لخوارزميات الذكاء الاصطناعي في التحقيق الجنائي، لضمان التوازن الدقيق بين مقتضيات حماية الأمن القومي من جهة، وصيانة الحقوق الدستورية ومبدأ المشروعية الإجرائية من جهة أخرى.

المطلب الثاني
الجهود الدولية لتنظيم الذكاء الاصطناعي أثناء إنفاذ القانون

نتاجا لهذه المخاوف المتزايدة[109]، قامت العديد من المنظمات الدولية بدعوة الحكومات للحد من تدخلها في أنشطة معالجة البيانات الشخصية التي يجريها القطاع الخاص، ومطالبتها للشركات بتسليم تلك البيانات للجهات الحكومية سواء كانت أمنية أم غير أمنية لتستخدمها لأغراضها الخاصة.

الفرع الأول: الجهود الدولية المتعلقة بحوكمة الذكاء الاصطناعي

الفرع الثاني: جهود دولية متعلقة بنظم استعمال الذكاء الاصطناعي في إنفاذ القانون

الفرع الأول
الجهود الدولية المتعلقة بحوكمة الذكاء الاصطناعي

أولا: تقرير الأمم المتحدة (حوكمة الذكاء الاصطناعي من أجل الإنسانية):

أصدرت الهيئة الاستشارية رفيعة المستوى المعنية بالذكاء الاصطناعي التابعة للأمم المتحدة تقريرها عن كيفية ومعايير حوكمة الذكاء الاصطناعي في ٢٠٢٤، وفيما يتعلق باستخدام الذكاء الاصطناعي من أجل إنفاذ القانون سواء على المستوى الوطني أو الدولي، حيث شددت على المخاطر القصوى المتعلقة باستخدام الذكاء الاصطناعي فيما يتعلق بإنفاذ القانون حيث يجب أن يتم مراعاة المعايير المتفق عليها في القانون الدولي لحقوق الإنسان فيما يتعلق بالمساءلة والمحاسبة حين يتم استعمال تلك التقنيات التي يمكن أن يترتب عليها مخاطر كبرى على الحقوق الفردية، ومراعاة كرامة الانسان ومنع ممارسات التلاعب النفسي المتضمنة: (التلاعب أو الخداع أو الحث أو إصدار الأحكام أو الاستغلال أو التمييز أو المساواة في المعاملة أو المقاضاة أو المراقبة أو فقدان استقلالية الإنسان أو الاستهداف بمساعدة الذكاء الاصطناعي)، وأيضا الالتزام بالمعايير الأساسية لحقوق الإنسان ك: (مثل الحق في افتراض البراءة (على سبيل المثال الخفارة التنبؤية)، والحق في محاكمة عادلة على سبيل المثال، التنبؤ بالعودة إلى الإجرام والاعتراف بالذنب، والعودة إلى الإجرام، والتنبؤ، والمحاكمات المستقلة)، وحرية التعبير والمعلومات (على سبيل المثال، الحث، والمعلومات المخصصة، وفقاعات المعلومات)، والخصوصية (على سبيل المثال، تكنولوجيا التعرف على الأشخاص من سمات وجوههم وحرية التجمع والتنقل على سبيل المثال، تكنولوجيا التتبع في الأماكن العامة)، واحترام سيادة القانون وعدم

١٠٧ المرجع السابق، المادة (١٤) بند ٣.

١٠٨ تُراجع المادة (٣) من قانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠.

109 Aurelia Tamò-Larrieux, Designing for Privacy and its Legal Framework: Data Protection by Design and Default for the Internet of Things, Volume 40 of Law, Governance and Technology Series, Issues in Privacy and Data Protection, Germany: Springer, 2018, p: 8

التحيز ضد جماعات أو فئات بعينها[١١٠].

ونهاية فإن هذا التقرير أورد التقرير الحاجة إلى الحوكمة العالمية لنظم والاتجاهات السياسية لتطوير الذكاء الاصطناعي[١١١].

ثانيا: توصيات منظمة اليونسكو بشأن أخلاقيات الذكاء الاصطناعي:

أصدرت منظمة اليونسكو كالمنظمة الأممية المسئولة عن التعليم والعلم والثقافة توصياتها عن أخلاقيات الذكاء الاصطناعي كنتاج لمؤتمرها العام الواحد والأربعين المنعقد في الفترة من ٩ إلى ٢٤ نوفمبر ٢٠٢١، وقد تناولت هذه التوصيات العديد من جوانب الذكاء الاصطناعي، ومنها ما يتعلق باستخداماته في حقل إنفاذ القانون حيث أوصت الدول الأعضاء في المنظمة الذين يستعملون نماذج الذكاء الاصطناعي لغايات تمس حقوق الإنسان بشكل مباشر مثل إنفاذ القانون وغيرها أن يتبنوا وينشئوا آليات لرصد الأثر الاجتماعي والاقتصادي لهذه الأنظمة من قبل سلطات الرقابة مناسبة، بما في ذلك سلطات مستقلة لحماية البيانات, والجهات الرقابية على قطاعات مخصصة[١١٢].

كما أوصت الدول الأعضاء أن تضع ضمانات مناسبة لحماية الحق في الخصوصية وفقا للقانون الدولي، بما في ذلك معالجة قضايا ذات حساسية خاصة كسياسات المراقبة لأغراض الأمن العام. كما أوصت الدول الأعضاء اعتماد أو إنفاذ أطر تشريعية توفر الحماية المناسبة، بما يتوافق مع القانون الدولي. كما أوصت الدول الأعضاء أن تشجع بقوة جميع الجهات الفاعلة، بما في ذلك الأشخاص الاعتبارية الخاصة، أن يتبعوا المعايير الدولية القائمة، وعلى وجه الخصوص، إجراء تقييمات ملائمة لأثر الخصوصية، كجزء من تقييمات الأثر الأخلاقي، والتي تأخذ في الاعتبار الأثر الاجتماعي والاقتصادي الأوسع نطاقًا لمعالجة البيانات المقصودة، وتطبيق الخصوصية حسب التصميم في أنظمتها. وينبغي احترام الخصوصية وحمايتها وتعزيزها طوال دورة حياة أنظمة الذكاء الاصطناعي[١١٣].

ثالثا: تقرير منظمة التعاون الاقتصادي والتنمية عن مراجعة وضع الذكاء الاصطناعي في مصر:

ذكر تقرير منظمة التعاون الاقتصادي والتنمية عن وضع الذكاء الاصطناعي في مصر أخطار استعمال تقنيات الذكاء الاصطناعي في حفل إنفاذ القانون والاستعانة بتقنيات التعرف على الوجه والمراقبة، وأيضا الاعتماد على تلك التقنيات بدون الحاجة لتدخل ومراجعة بشرية، مما يثير إشكاليات تتعلق بحقوق الإنسان وخاصة الحق في الخصوصية ومخاطر التحيز وغيرها من المخاطر، والحاجة لصياغة ووضع قوانين وقواعد لاستخدام تلك التقنيات فيما يتعلق بإنفاذ القانون، وقد أشار هذا التقرير أن الميثاق المصري فيما يتعلق بالذكاء الاصطناعي المسئول لم يتطرق لتلك الإشكاليات، ولكنه في ذات الوقت حض على احترام حقوق الإنسان ورفاهية المواطنين فيما يتعلق باستخدامات وتطبيقات الذكاء الاصطناعي، وخاصة بالنسبة للاستخدامات الحكومية لمثل تلك التقنيات[١١٤].

---

١١٠ الهيئة الاستشارية رفيعة المستوي المعنية بالذكاء الاصطناعي التابعة للأمم المتحدة، تقرير الأمم المتحدة (حوكمة الذكاء الاصطناعي من أجل الإنسانية)، ٢٠٢٤، ص: ٣٠-٣١.

١١١ الهيئة الاستشارية رفيعة المستوي المعنية بالذكاء الاصطناعي التابعة للأمم المتحدة، تقرير الأمم المتحدة (حوكمة الذكاء الاصطناعي من أجل الإنسانية)، ٢٠٢٤، ص: ٣٧.

112 UNESCO, Recommendation on the Ethics of Artificial Intelligence, Adopted on 23 November 2021, p: 27.

113 UNESCO, Recommendation on the Ethics of Artificial Intelligence, Adopted on 23 November 2021, p: 29.

114 OECD, OECD Artificial Intelligence Review of Egypt, OECD Publishing, Paris, p: 21, https://doi.org/10.1787/2a282726-en

الفرع الثاني
جهود دولية متعلقة بنظم استعمال الذكاء الاصطناعي في إنفاذ القانون

أولا: قرار الجمعية العامة للأمم المتحدة «الحق في الخصوصية في العصر الرقمي» لعام ٢٠١٨

ومن ضمن هذا الجهود المتواصلة التي قامت بها الأمم المتحدة بعد فضيحة التجسس الأمريكية المشهورة ب "بريزم prism" في عام 2012، والتي انتهت بإصدار قرار الجمعية العامة للأمم المتحدة "الحق في الخصوصية في العصر الرقمي" لعام 2018[115], والذي أوصت فيه الأمم الأعضاء ب: (احترام واتخاذ التدابير اللازمة لاحترام الحق في الخصوصية وخصوصا في قطاع الاتصالات الرقمية، وإعادة النظر في إجراءات جمع ومعالجة البيانات الشخصية ومراقبة الاتصالات الرقمية، وإنشاء وتعزيز آليات الرقابة البرلمانية والقضائية المستقلة وتزويدها بالموارد والقدرات اللازمة لممارسة عملها، وإتاحة تعويض مناسب للمتضررين، سن تشريعات مناسبة ومتخصصة تضمن احترام المبادئ الدولية بهذا المجال، وغيرها من التوصيات)[116].

وأهاب القرار الشركات بالعمل على تنفيذ معايير إطار الأمم المتحدة المعنون" الحماية والاحترام والانتصاف"[117]، وأن توفر لمستخدميها قواعد الشفافية والانتصاف اللازمين لحمايتهم وحماية بياناتهم الشخصية ضد المخاطر التي قد تتعرض لها، وأن تعمل على دمج آليات عمل رقابية وفنية وإدارية تضمن تجهيز البيانات، وأن تحترم الحق في الخصوصية أثناء تصميمها لتكنولوجيات أتمتة اتخاذ القرارات والذكاء الصناعي وتشغيلها وتقييمها والرقابة عليها، ومعالجة انتهاكات حقوق الإنسان التي تكون قد تسببت أو أسهمت فيها[118].

ثانيا: دليل الإتحاد الأوروبي بالأخلاقيات الخاصة بتطوير ونشر نماذج وأنظمة الذكاء الاصطناعي فيما يتعلق بمنع استخدامها بالإتجار بالبشر

نص هذا الدليل على أكثر من التزام لمطوري وناشري نماذج الذكاء الاصطناعي، والتي يمكن أن تؤدى لتقليل استخدامه في ارتكاب الجرائم عامة والاتجار بالبشر خاصة، ومن ضمنها:

"مبدأ منع الضرر": وينص على ضرورة ألا يباح نموذج الذكاء الاصطناعي للاستخدامات غير القانونية أو التي قد تسبب ضرر، مع إيلاء اهتمام خاص لحماية الفئات الضعيفة في المجتمع كالأطفال والنساء، وهو ما يساهم بشكل مباشر في تقليل تعريض تلك الفئات لمخاطر الاستغلال غير القانوني[119].

كما نص أيضا على وجوب أن يتم وضع **«مبدأ المساءلة والمراجعة» و «حقوق الإنسان»** في الحسبان أثناء تحقيق نموذج للذكاء الاصطناعي وخاصة الخصوصية وحوكمة البيانات[120]، والتي يرى الباحث أنها عامل مهم جدا لمنع استخدام نماذج الذكاء الاصطناعي في الإتجار بالبشر حيث أن تلك الأنشطة مثل أي أنشطة تتم حاسوبيا وتتعلق بالبشر تكون البيانات الشخصية هي مفتاح ونقطة ابتداء النشاط الإجرامي.

١١٥ الأمم المتحدة – الجمعية العامة , قرار الجمعية العامة للأمم المتحدة رقم (١٧٩\٧٣) للعام ٢٠١٨ الحق في الخصوصية في العصر الرقمي, (نيويورك: الأمم المتحدة – الجمعية العامة, الدورة الثالثة والسبعون/ الجلسة العامة ٧٠, ٢١ January ٢٠١٩), وثيقة رقم ١٧٩/٧٣/RES/A ,مستخرج من الموقع الرسمي لوثائق الأمم المتحدة: http://:unrtpidage١٨/ly.bit

١١٦ من التقرير صفحة ٧ من البند السادس يرجي مراجعة: (ن) أن تنظر في وضع التشريعات والتدابير الوقائية ووسائل الانتصاف اللازمة لمعالجة الضرر الناجم عن تجهيز البيانات الشخصية أو استخدامها أو بيعها أو إعادة بيعها لمرات متعددة أو تداولها بشكل آخر بين المؤسسات التجارية دون موافقة صريحة يعطيها الفرد بحرية وعن بينة من الأمور، أو في مواصلة تنفيذ تلك التشريعات والتدابير ووسائل الانتصاف؛ ص ٦–٧ بند ٦ خاص بالدول

١١٧ الأمم المتحدة – الجمعية العامة , تقرير الممثل الخاص للأمين العام المعني بمسألة حقوق الإنسان والشركات عبر الوطنية وغيرها من مؤسسات الأعمال، جون روغي مبادئ توجيهية بشأن الأعمال التجارية وحقوق الإنسان: تنفيذ إطار الأمم المتحدة المعنون «الحماية والاحترام والانتصاف», (نيويورك: الأمم المتحدة – الجمعية العامة, الدورة السابعة عشرة/ الجلسة العامة ٧٠, ٢١ March ٢٠١١), مستخرج من الموقع الرسمي لوثائق الأمم المتحدة: http://:unarc١٧٣١/ly.bit

١١٨ مرجع سابق, ص ٧-٨, بند خاص بالشركات

119 European Commission, High-Level Expert Group on Artificial Intelligence, ETHICS GUIDELINES FOR TRUSTWORTHY AI, B-1049, Brussels, AI HLEG, 2019, p: 12.

120 IBID, ETHICS GUIDELINES FOR TRUSTWORTHY AI, P: 14

"التصميم حسب القانون": هذا المفهوم المتوسع والذى تبناه الإتحاد الأوروبي في قوانينه المختلفة المتعلقة بالتقنية مثل مبدأ «التصميم حسب الخصوصية privacy by design" في اللائحة العامة لحماية البيانات الشخصية، والذى يعنى أن يتم مراعاة الالتزامات القانونية أثناء تصميم البنى الفنية والمعلوماتية لأي عملية تشغيلية، فمن ناحية «التصميم حسب الخصوصية» فهو يعنى مراعاة الالتزامات المنصوص عليها في اللائحة العامة لحماية البيانات الشخصية أثناء تصميم وتنسيب وتشغيل البنى الفنية لمعالجة البيانات، وهو التزام مستمر مسابق ويتعلق بالامتثال، وقد توسعت هذه التوجيهات في هذا المفهوم فأسمته «التصميم حسب القانون» وهو ما يعنى أن يصمم النموذج التشغيلي للذكاء الاصطناعي بما يؤكد فيه امتثاله للقوانين المتعلقة بأعماله، وهو ما يترجم من ناحية الإتجار بالبشر إلى ضرورة عمل نموذج تمثيلي لأنماط الجريمة ووسائل منعها ووضع التزامات تترجم لأكواد وأوامر تشغيلية تمنع من إكمال العمليات التي تؤدى إلى المساعدة في تلك الجرائم، والإبلاغ عن مرتكبيها[121].

ثالثا: تقرير المقررة الخاصة المعنية بالأشكال العنصرية واستخدام التكنولوجيات الرقمية في إنفاذ إجراءات الحدود والهجرة:

قدم هذا التقرير في الدورة الثامنة والأربعين لمجلس حقوق الإنسان، حيث تناول فوائد استخدام التقنيات الحديثة وخاصة الذكاء الاصطناعي في إنفاذ ومراقبة الحدود، ولكن أيضا مخاطرها وخاصة فيما يتعلق بالمحايدة والتمييز العرقي والاثني، وأشار إلى المخاطر التي تنجم عن تصميمها المتحيز وخاصة فيما ينجم عن التنميط والتصنيف لأصحاب البشرات المختلفة سواء سمراء أو أسيوية وأشار إلى أسباب مختلفة منها التحيزات الأيدلوجية وعداء الأجانب والمخاوف الأمنية المقترنة من العداء الصريح للمهاجرين وأيضا السعي وراء تحقيق كفاءة تشغيلية وإدارية بدون الأخذ في الحسبان حقوق الإنسان والتصميم المراعي للحقوق وأيضا العديد من المعايير القانونية أثناء تصميم وتدريب نماذج الذكاء الاصطناعي المستخدمة فيما يعرف ب (الحدود الرقمية)[122].

121 IBID, ETHICS GUIDELINES FOR TRUSTWORTHY AI, P: 21

١٢٢ المقررة الخاصة المعنية بالأشكال المعاصرة للعنصرية والتمييز العنصري وكره الأجانب وما يتصل بذلك من تعصب، التمييز العنصري وكره الأجانب واستخدام التكنولوجيات الرقمية في إنفاذ إجراءات الحدود والهجرة، HRC/A/٧٦/٤٨، ص: ٤-٥.

خاتمة

على الرغم من الاتجاه الدولي المتسارع لريادة الذكاء الاصطناعي، سعيا لتحقيق أقصى استفادة ممكنة منه أو تفادي مخاطره، إلا أن اللهاث وراء صرعات الاستهلاك الحالية بدون الالتفات للمعايير الواجبة نحو حوكمة وضبط تلك الأنظمة حفاظا على الحقوق الفردية المرتبطة وفي حالة البحث الضوابط والمبادئ الدستورية للمشروعية الإجرائية والعدالة الجنائية قد ينجم عنه عواقب وخيمة قد لا يدركها أو يغض عنها الطرف من يدعون لعدم تقنين تقنيات الذكاء الاصطناعي.

وباستطلاع بعض التقنيات المعتمدة على الذكاء الاصطناعي والمستخدمة في إنفاذ القانون يتبين لنا مدي اصطدامها بالعديد من معايير المشروعية الإجرائية مما يوجب اتباع إما القواعد التشريعية المخصصة لتصميم تلك النماذج وتشغيلها أو القواعد العامة التي يمكن أن تغطي العديد من جوانب تدريب وتشغيل تلك النماذج، ولكن بطبيعة الحال ستترك الموضوع عرضة للتفسير القضائي الذي يأخذ مكانه الطبيعي بعد وقوع الضرر، وهو منهج غير مناسب مع الأخطار التي تصاحب تلك التقنيات، لذا يجب أما تغيير البنية التشريعية الحالية سواء باتباع نهج قطاعي كتعديل قانون الإجراءات الجنائية مثلا، أو اتباع نهج موحد باستحداث قانون للذكاء الاصطناعي يشمل فيما يشمله قواعد لاستعمال تقنيات الذكاء الاصطناعي في مجال إنفاذ القانون وأيضا والأهم بنية تنظيمية وإشرافيه وفنية متكاملة تعمل على تقليل الأخطار ومنعها المسبق، وهو الاتجاه الذي يفضله الباحث، وبناء عليه نخلص لبعض النتائج والتوصيات في نهاية هذا البحث، وهي:

النتائج:

١. تقنيات «التعرف على الهوية من خلال مسح نمط الوجه» من أخطر تقنيات التعرف البيومترية من وجهة نظر حماية البيانات الشخصية، كونها لا تتطلب تفاعلا واعيا بين الشخص المعنى بالبيانات والألة التي تتعرف عليه، كما أن نسب الأخطاء المرتبطة باستخدامها تزيد من نسب عدم مشروعية الإجراءات الجنائية المعتمدة عليها.
٢. تتنوع أخطار تقنيات التنميط حسب درجة استخدامها داخل أنظمة انفاذ القانون ابتداء من درجات المساعدة الفاعلة في تصنيف المعلومات والأنماط حتى الأخطر وهو استخدامها لاتخاذ القرار النهائي.
٣. تعتبر بعض السلوكيات المتبعة أثناء تطوير تقنيات الذكاء الاصطناعي كالمسح العام للإنترنت لتكوين قواعد بيانات التدريب للنماذج من أخطر السلوكيات المرتبطة عامة بتطوير نماذج الذكاء الاصطناعي.
٤. ترتبط بجميع مراحل تطوير وتدريب وطرح وتشغيل نماذج الذكاء الاصطناعي لأغراض انفاذ القانون أخطار ترتبط بتلك المرحلة بداية من مشروعية جمع البيانات انتهاء بمشروعية اتخاذ القرارات بصفة مؤتمتة اعتمادا عليها.
٥. يطرح استعمال نماذج الذكاء الاصطناعي في مجال انفاذ القانون العديد من المخاطر على الافراد من أهمها المخاطر المتعلقة بالحق في البيانات الشخصية والخصوصية، التحيز، عدم دقة النتائج، والخضوع لقرارات مؤتمتة غير مدققة ومراجعة.
٦. جاءت النظم القانونية لتنظيم استخدام تقنيات الذكاء الاصطناعي لأغراض انفاذ القانون متفقة على الاخطار المتعلقة بهذه الأنظمة وواضعة معايير مختلفة لحفظ التوزان بين الفوائد المرجوة من تلك النماذج والأخطار المرتبطة بها.

التوصيات:

١. يوصي الباحث المعنيين بالتشريع في جمهورية مصر العربية بوضع تشريعات تشمل جميع مراحل تدريب وتطوير وتشغيل نماذج الذكاء الاصطناعي لإنقاذ القانون تحافظ على التوازن القانوني ومشروعية الإجراءات الجنائية المعتمدة على الذكاء الاصطناعي

٢. يدعو الباحث للتعاون بين المختصين بعلوم الذكاء الاصطناعي والقانونين والحقوقيين والأمنيين وتكوين مراكز خبرة ومجامع تفكير مشتركة تطور من قواعد وسلوكيات استعمال الذكاء الاصطناعي في مجال انفاذ القانون.

٣. يوصي الباحث الجهات المعنية بالأمن وانفاذ القانون بمراعاة مبادئ الشفافية والمراقبة الداخلية التي تراعي الطبيعة الخاصة لأعمالها من خلال انشاء قطاعات داخلية لتطوير قواعد سلوك ورقابة سابقة ومستمرة على اعمال الجمع والاستدلال وانفاذ القانون باستعمال الذكاء الاصطناعي.

٤. يوصي الباحث السلطة القضائية ووزارة العدل بتكثيف جهودها البحثية وتوجيهاتها لضبط معايير استخدام نماذج الذكاء الاصطناعي اثناء التحقيق والتقاضي الجنائي المعتمد على الذكاء الاصطناعي بما يحافظ على مبادئ المشروعية الإجرائية والتقاضي العادل.

٥. أن يتم مراعاة التوازن بين الحقوق الفردية واعتبارات الأمن العام في أي قوانيين أو مدونا سلوك أو توجيهات داخلية تتعلق باستخدام الذكاء الاصطناعي لأغراض الأمن العام.

٦. ان يتم الاقتصار في استعمال تقنيات الذكاء الاصطناعي في مجال انفاذ القانون على المساعدة في عمليات الاستدلال المبدئية أو الاعمال الوسيطة لجمع وتحليل البيانات والانماط، لا الاعتماد عليها لاتخاذ قرارات نهائية.

٧. وجوب خضوع جميع أعمال التحري والاستدلال والتحقيق وانفاذ القانون المعتمدة والتي تتم بمساعدة الذكاء الاصطناعي بمراقبة مستمرة وتقييم بشري ومراجعة للقرارات والنتائج، وأن تتم بواسطة السلطات القانونية والعاملين فيها بعد تدريبهم على كلا من الجوانب القانونية والأمنية المتعلقة بهذه الاستعمالات.

المراجع

أولاً: مراجع عربية

أولا: الكتب

١. محمد لطفي عبد الفتاح، القانون الجنائي واستخدامات التكنولوجيا الحيوية: الهندسة الوراثية، البصمة الوراثية، الاستنساخ، المنصورة، دار الفكر والقانون، ٢٠١٢،

ثانيا: الأبحاث

١. احمد عبد العزيز محمد أبو الحسن، الاشكاليات الناجمة عن أنظمة المراقبة الذكية من منظور حماية البيانات الشخصية وتنظيم الذكاء الاصطناعي،, ملتقى دولي حول الذكاء الاصطناعي والأمن القومي: الرهانات القانونية.، الجزائر، ٢٠٢٣

ثالثا: رسائل جامعية

١. عبد الحسن دويخ خفيف، استبعاد الأدلة الجنائية غير المشروعة: دراسة مقارنة، رسالة ماجستير، العراق، كلية القانون، جامعة ذوقار، ٢٠١٨

ثانيا: مراجع اجنبية

1/ Books:

1. Ahmed Nabil Belbachir, Smart Cameras, London, Springer Science & Business Media, 2009
2. Alexander L. Vuving. Hindsight, Insight, Foresight: Thinking About Security in the Indo-Pacific, united states, Asia-Pacific Center for Security Studies, 2020
3. Alexander L. Vuving. Hindsight, Insight, Foresight: Thinking About Security in the Indo-Pacific. United states, Asia-Pacific Center for Security Studies, 2020
4. Alison Wakefield, Jenny Fleming, The SAGE Dictionary of Policing, united states, SAGE, 2008
5. Asit Kumar Datta, Madhura Datta, Pradipta Kumar Banerjee. Face Detection and Recognition: Theory and Practice. United States, CRC Press, 2015
6. Aurelia Tamò-Larrieux, Designing for Privacy and its Legal Framework: Data Protection by Design and Default for the Internet of Things,

Volume 40 of Law, Governance and Technology Series, Issues in Privacy and Data Protection, Germany: Springer, 2018
7. Curtis Frye, Privacy-enhanced Business: Adapting to the Online Environment, Westport/ Connecticut/ United States: Greenwood Publishing Group, 2001
8. Danny Caine. How to Resist Amazon and Why: The Fight for Local Economics, Data Privacy, Fair Labor, Independent Bookstores, and a People-Powered Future!. United states, Microcosm Publishing, 2022
9. Henry H. Perritt. Digital Communications Law. Revised / 2020. United states, Wolters Kluwer, 2010, 2020 edition
10. Jacqueline Klosek, Data Privacy in the Information Age, Westport/ Connecticut/ United States: Greenwood Publishing Group, 2000
11. Jean-Yves Dufour, Intelligent Video Surveillance Systems, New Jersey, United States, John Wiley & Sons, 2012
12. Mehdi Rahmani-Andebili, Operation of Smart Homes, Power Systems, united states, Springer Nature, 2021
13. Maria Tzanou, Health Data Privacy under the GDPR: Big Data Challenges and Regulatory Responses, Routledge Research in the Law of Emerging Technologies, united states: Routledge, 2020
14. Martin Ford. Rule of the Robots: How Artificial Intelligence Will Transform Everything. United Kingdom, Hachette UK, 2021
15. Neha Sharma, Amlan Chakrabarti, Valentina Emilia Balas, Jan Martinovic, Data Management, Analytics and Innovation: Proceedings of ICDMAI 2020, Volume 1, singapore, Springer Nature, 2020
16. Roberto J. Rodrigues, Petra Wilson, Stephen J. Schanz, The Regulation of Privacy and Data Protection in the Use of Electronic Health Information: An International Perspective and Reference Source on Regulatory and Legal Issues Related to Person-identifiable Health Databases, Washington, D.C., United States: Pan American Health Organization, 2001
17. Roland Vogl. Research Handbook on Big Data Law, Research Handbooks in Information Law series. United states, Edward Elgar Publishing, 2021
18. Ronald J. Deibert. Reset: Reclaiming the Internet for Civil Society. United Kingdom. September Publishing, 2020
19. Rosario Girasa. Artificial Intelligence as a Disruptive Technology: Economic Transformation and Government Regulation. Switzerland, Springer Nature, 2020
20. Stan Z. Li, Anil K. Jain. Handbook of Face Recognition. United states, Springer Science & Business Media, 2005
21. Stephen J.A. Ward. Handbook of Global Media Ethics. Switzerland, Springer Nature, 2021
22. United States. Congress. House. Committee on Energy and Commerce. Subcommittee on Commerce, Trade, and Consumer Protection, The EU Data Protection Directive: Implications for the U.S. Privacy Debate : Hearing Before the Subcommittee on Commerce, Trade, and Consumer Protection of the Committee on Energy and Commerce, House of Representatives, One Hundred Seventh Congress, First Session, March 8, 2001, Volume 4, U.S., Washington, D.C./ United States: Government Printing Of-

fice, 2001

2/ Formal documents:

1. article 29 data protection working party. opinion 02/2012 on facial recognition in online and mobile services. Brussels, 22 March 2012
2. Council of the European Union, Interinstitutional File: 2021/0106(COD), Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts
3. Edward J. Markey, a letter to Andrew jassy, united states, June , 2022
4. the EU fundamental rights agency. facial recognition technology: fundamental rights considerations in the context of law enforcement. Austria, fra – European union agency for fundamental rights, 2019.
5. The European Data Protection Board. Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement. Brussel, 27 June 2022.
6. European Commission, High-Level Expert Group on Artificial Intelligence, ETHICS GUIDELINES FOR TRUSTWORTHY AI, B-1049, Brussels, AI HLEG
7. UNESCO, Recommendation on the Ethics of Artificial Intelligence

3/ cases:

1. CJEU judgment in the Schrems II case, 2020
2. JOHN C. COUGHENOUR, District Judge order on 3/8/2022 on Case No. C20-1298-JCC
3. Mutnick v. Clearview AI, Inc. et al, No. 1:2020cv00512
4. NORTHERN DISTRICT OF CALIFORNIA, CLASS ACTION COMPLAINT, Case 3:23-cv-03199, Filed 06/28/23
5. NORTHERN DISTRICT OF CALIFORNIA. RE FACEBOOK BIOMETRIC INFORMATION PRIVACY LITIGATION Case No. 15-cv-03747-JD
6. Wise v. Ring LLC, W.D. Wash., No. 2:20-cv-01298, 8/3/22
7. Zellmer v. Facebook, Inc. (3:18-cv-01880) District Court, N.D. California, March 27, 2018
8. California Penal Code Sections 630-637.9 CHAPTER 1.5. INVASION OF PRIVACY, PENAL CODE SECTION 630-637.9
9. United states of America, Electronic Communications Privacy Act of 1986 (ECPA)
10. United states of america, The Computer Fraud and Abuse Act of 1986 (CFAA), Title 18, United States Code, Section 1030