ورقة بحثية

تقنية التعرّف على الوجه وواقع الخصوصية

محمد معاذ*

زميل غوغل وباحث في مجال الذكاء الاصطناعي. كاتب تقني. يرتكز عمله المهني على توفير المهارات الإستراتيجية لدعم وفهم تقنية الذكاء الاصطناعي في المنطقة العربية. أنجز العديد من الدراسات والمقالات العلمية في الذكاء الاصطناعي، وتركّز أبحاثه على التأثير الحقيقي لهذه التقنية في مختلف المجالات.

*mohamadmaaz1991@gmail.com

الملخّص

تقنية التعرف على الوجه هي نظام للتعرّف التلقائي يتعرّف على الأفراد من خلال تصنيف ميزات محددة لهيكل الوجوه، بهدف ربط المعلومات الممسوحة ضوئيًّا بالبيانات المخزّنة. وقد تمّ تطبيقها خلال العقود القليلة الماضية على نطاقٍ واسعٍ بحجة زيادة التدابير الأمنية وتحقيق الأمن. إلّا أنّ هذا الاستخدام المكثّف لهذه الأنظمة خلق تحديات ومخاوف مرتبطة بالخصوصية. تتناول هذه الورقة البحثية تقنية التعرّف على الوجه، وماهيتها إضافةً إلى البحث في مسألة الخصوصية ومدى الالتزام باحترام البيانات في هذا الحقل التكنولوجي. وتخلص الدراسة إلى أنه لا بدّ من التحكّم في تكنولوجيا المعلومات والأنظمة الرقمية لمنع سوء الاستخدام والاستغلال لبيانات المستخدمين، لا سيّما وأن التطورات التقنية المتسارعة باتت تتيح قدرةً أكبر على معالجة وتصنيف كمياتٍ هائلة من البيانات التي يتم إنشاؤها بواسطة الأجهزة الإلكترونية التي يستخدمها الأشخاص حول العالم.

الكلمات المفتاحية: الذكاء الاصطناعي، التعرّف على الوجه، الخصوصية، البيانات.

1. المقدمة

ليس هناك أكثر من التفكير الأورويلي الذي يشير إلى أنّ "الأخ الأكبر يراقبك". تلك الفكرة التي سبق وتنبّأ بها الكاتب الإنجليزي جورج أورويل في روايته "1984"، والتي فيها يراقب الأخ الأكبر كل شاردة وواردة، ويحدّ من الحريات الفردية والشخصية، تحت غطاء الحفاظ على أمن وسلامة المجتمع. وحتى بدون تحديد كيفية مراقبة الأشخاص - سواء من خلال تتبّع الهواتف المحمولة، أو تحديد سلوك التصفّح عبر الإنترنت - فمن المنطقي تخيّل المراقبة المستمرة. وعندما يصبح المفهوم مطبّقًا حرفيًا في العالم الواقعي، ويعتقد الناس أنّ الكاميرات تراقبهم في كل مكانٍ يذهبون إليه، حتى في منازلهم ربّما، فالنتيجة ستكون تأثيرًا مخيفًا على الأفراد الذين قد لا يشعرون بالحرية في عيش حياتهم بالطريقة التي يريدونها.

لكن، ماذا يعني ذلك للأشخاص الذين يتعاملون مع أنظمة التعرّف على الوجه التي باتت تظهر في كل مكان؟

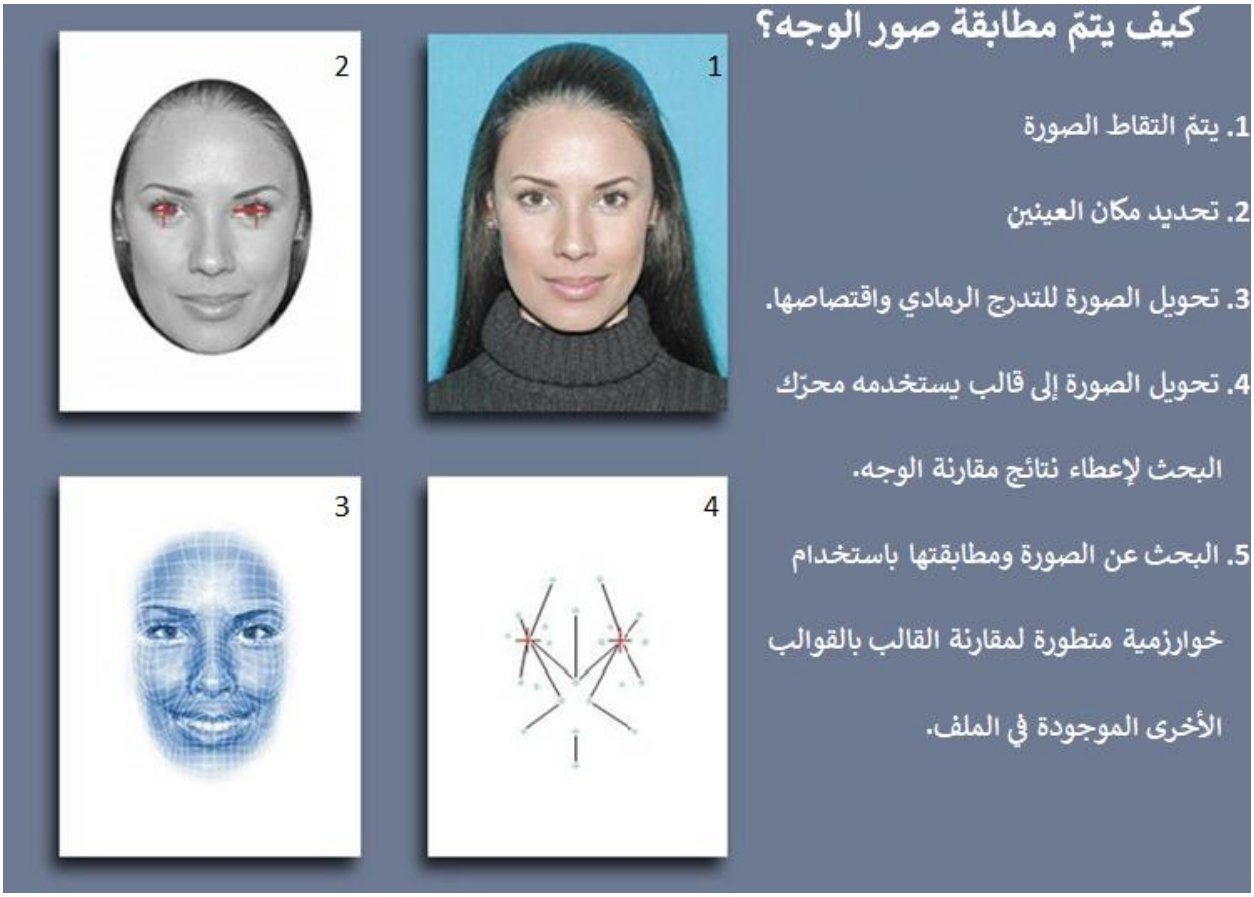
يمكن للأفراد استخدام هذه التقنية لفتح هواتفهم الذكية، والوصول إلى حساباتهم المصرفية، وتفويض الإذن بدفع المستحقات المالية وأنشطة أخرى عبر شبكة الانترنت. وتلجأ الشركات والمنظّمات للاستعانة بهذه الأنظمة الذكية في إدارة صلاحيات الدخول إلى المرافق، ومراقبة الحشود وغيرها. كما تستخدمها الحكومات في تتبّع الخارجين عن القانون والمجرمين، وضبط أمن الحدود، وكذلك في التحقيقات الجنائية[1]. ومع مرور الوقت، تتعدّد الاستخدامات لهذه الأنظمة ويجري تطويرها باستمرار. إلا أنّ العديد من الأسئلة تطرح نفسها حيال ذلك: هل هذه التقنية جيدة؟ ألا تبعث على القلق؟ وهل ينبغي التوقّف عن استخدامها كليًّا؟ وغيرهامن الأسئلة. وفي حين تعلو بعض الأصوات في الوسط البحثي والعلمي، للتوقف عن استعمال أنظمة التعرّف على الوجه، إلى حين وضع معايير وقواعد واضحة تنظّم عمليات الاستخدام، يبدو أنه من غير المرجّح حدوث ذلك.

2. التعرّف على الوجه

متى يكون الوجه مجرد صورة ومتى يكون "معرّفًا بيومتريًا" والذي يعني تحديد الهوية من خلال نظام القياس والاستدلال الحيوي؟ يعتبر فهم كيفية عمل الأنظمة التقنية أساسًا مهمًا لتقييم مخاطر التعرّف على الوجه بشكلٍ فاعل. وفي حين هناك العديد من الخيارات المرتبطة بأنظمة القياس الحيوي للتحقّق من الهوية، مثل مسح شبكية العين، أو التعرّف على كفة اليد أو بصمات الأصابع، وغيرها إلّا أنّ الورقة البحثية تركّز على تقنية

التعرّف على الوجه. وعلى الرغم من وجود العديد من المزايا لهذا النوع من التقنيات لكن لها سلبيات مختلفة، والأمر يتوقّف على طريقة الاستخدم.

إنّ نظام التعرّف على الوجه لا يرتكز على إنشاء الصور. بل يقوم بخلق نماذج (Templates) تستخدم الخوارزميات الحسابية[2]. وهذا يعني أنّه عندما يتمّ مسح الوجه ضوئيًا، لا يعمد النظام لالتقاط الصورة الخاصة بالشخص، وإنّما يخلق تصميمًا بناءً على بنية الوجه. ومن أجل عملية تسجيل شخصٍ ما في قاعدة بياناتٍ لأغراض التعرّف على الوجه، يتمّ إجراء مسحٍ على الوجه الحقيقي للفرد، وتحديد التفاصيل المميزة والفريدة فيه، أمّا الخطوة الثانية فهي قراءة هندسة الوجه، وهي تشمل المسافة بين العينين وكذلك البعد من الجبهة إلى الذقن. تُعرف النتيجة باسم "توقيع الوجه" (individual signature)[3].(أنظر الشكل رقم 1 أدناه). ليجري بعدها تخزين النموذج، إلى جانب وسمٍ أو رمز (Code) يتيح السجلّ الكامل لأيّ معلوماتٍ شخصية أخرى تمّ جمعها أو الاحتفاظ بها عن الشخص. وإذا كانت الصورة الفعلية للشخص تشكّل جزءًا من السجلّ، فعادةً ما يتمّ التقاطها وتخزينها بشكلٍ منفصلٍ تمامًا عن النموذج[4]. وفي وقتٍ لاحقٍ، عندما يجري تحديد هوية الشخص أو تحديد صورة من مقطع فيديو لمحاولة التعرّف عليها، يقوم النظام بمسحٍ للصورة أو الشخص، وتحويل ذلك إلى بياناتٍ رقمية لإنشاء نموذجٍ جديد، ومن ثمّ تشغيل هذا النموذج من خلال صيغةٍ حسابية، ثم مقارنة النموذج الجديد مع الملف المسجّل سابقًا للشخص. وبناءً على تشابه النموذج الذي تمّ التقاطه والبيانات التي جرى العثور عليها، يمكن إجراء تطابقٍ بين الصورة الملتقَطة بواسطة كاميرا المراقبة وبين صورة معينة في قاعدة بيانات الوجوه[5]. وفي هذه الحالة يتمّ تحديد هوية الشخص، في عمليةٍ تستغرق عادةً أقلّ من ثانية.



الشكل رقم (1): خطوات التعرّف على الوجه[6]

3. مستويات أنظمة التعرّف على الوجه

ليست كل الكاميرات التي تدير نوعًا من برامج الوجه هي في الواقع أنظمة تعرّف. هناك أربعة مستويات على الأقلّ من برمجيات صور الوجه، ولكلٍّ منها حالات استخدام مختلفة، ومزايا، ومخاطر، وآثار على الخصوصية. وتتلخّص هذه المستويات، في ترتيبٍ تصاعدي بناءً على تعقيدها وهي: الاكتشاف، التوصيف، التحقّق، والتعرّف[7].

أ. الاكتشاف

يعدّ اكتشاف الوجه من أبسط المستويات، مثلما قد يُرى من خلال الكاميرا - المربّع الصغير الذي يتحرّك لتأطير وجوه الأشخاص في مجال الرؤية. ويرتكز هذا المستوى على إيجاد الوجه البشري

وتمييزه، وذلك للسماح للكاميرا بالتركيز عليه، أو قد يكون لإحصاء الأشخاص الذين يمرون في نقطةٍ معينة، أو غيرها من التطبيقات[8].

ب. التوصيف

في هذه الحالة، تقوم الكاميرا بجمع وتسجيل معلوماتٍ أكثر تفصيلًا ممّا هو عليه في مرحلة اكتشاف الوجه، إلّا أنها لم تنشئ بعد سجلًا شخصيًا[9]. ومن الأمثلة على ذلك، لوحة الإعلانات التفاعلية في محطةٍ للحافلات، أو شاشة مثبّتة فوق شاشة عرض منتجات التي قد تستخدم لجمع معلومات مثل نوع الجنس، والعمر التقريبي، والمؤشرات العاطفية المحتملة (مبتسم، حزين..)؛ ويمكن بعد ذلك الجمع بين هذه المعطيات مع بياناتٍ أخرى مثل المدّة التي نظر فيها الشخص إلى الشاشة، أو أين تنقّل داخل المتجر وغيرها. وقد توفّر هذه البيانات للمعلنين معلوماتٍ حول ردود أفعال المتسوّقين، إستنادًا إلى النوع: استجابة الإناث بشكلٍ إيجابي، فيما نظر الرجال الأكبر سنًّا بشكلٍ سريع. ولا يقوم أيّ من أنظمة اكتشاف وتوصيف الوجه بإنشاء أو جمع معلومات تعريفٍ شخصية، وبالتالي فإنّ مخاطر الخصوصية تعدّ منخفضة[10].

ج. التحقّق

هو عبارة عن نظام مطابقة مثلما يحدث عند محاولة الدخول إلى الهاتف، إذ تقوم الشاشة بفحص الوجه، وتحاول مطابقة النموذج أو القالب الذي سبق وتمّ حفظه على الهاتف الذكي. بمعنى آخر، يمكن تلخيص عملية التحقّق بسؤالٍ مفاده: "هل هذا هو الشخص المعني الذي يدّعي أنّه هو أم لا؟". وفي مثالٍ آخر على التحقّق: قد تحتفظ شركة ما بقاعدة بياناتٍ تضمّ نماذج بيانات الموظفين تمّ إنشاؤها وتخزينها. وعندما يحاول الموظف دخول مبنى الشركة، تقوم الكاميرا بمسح وجهه، ويتحقّق فاحصٌ رقميّ من بطاقة هويته. وفي هذه الحالة، تعرّف بطاقة الهوية عن الشخص، ويتمّ محاولة مطابقة المسح الضوئي مع هذا النموذج حصرًا. وفي حال التطابق، يُسمح للشخص بدخول المبنى. أمّا إذا لم يحدث ذلك، يتمّ إعادة التوجيه إلى موظّف استقبالٍ أو نظامٍ بديل آخر للتقييم. وهذا أيضًا هو نوع النظام الذي يتمّ العمل به في المطارات فيما يتّصل بالرحلات الدولية، فهو يقارن

بين هوية المسافرين المعروضة (الوجوه، إلى جانب بطاقة الهوية) وبين النموذج المسجّل المرتبط بصور الركاب على قائمة الصعود. والنتيجة هي إمّا "نعم" أو "لا" للتحقّق من صحّة هوية الأشخاص.

د. التعرّف

هو المستوى الرابع للتعرّف على الوجه. ويمكن تلخيصه على النحو التالي:"هل يستطيع البرنامج أن يحدّد من هو هذا الشخص المجهول؟" هذا النوع من الأنظمة هو ما تستخدمه الجهات المعنية بتطبيق القانون كالشرطة، ويمكن أن يتمّ ذلك من خلال فحص صورةٍ في قاعدة بياناتٍ تحوي أصحاب سوابق جرمية مسجّلين، أو حاملي رخصة القيادة، أو مجموعات البيانات الأخرى (Dataset) المحدّدة مسبقًا. ويقوم النظام بمسح الصورة - قد يكون من خلال مقطع فيديو في مكانٍ عام، أو صورة من كاميرا في مكان وقوع حادثٍ ما- ويحاول مطابقة النموذج في أيّ مجموعة بيانات متاحة لهذا الغرض[11]. ومن المرجّح أن يعود النظام بعمليات مطابقةٍ محتملة. لكن، في نهاية المطاف، سيعود القرار للعنصر للبشري في مراجعة وتقييم أيّ تطابقٍ قد اقترحه النظام، لاتّخاذ قرارٍ نهائي بشأن ما إذا كان قد تمّ التعرّف على هذا الشخص بنجاحٍ أم لا.

ويعدّ استخدام التعرّف على الوجه شائعًا في مجال الأمن، مثل تحديد شخصٍ ما قام بسرقة متاجر في مجموعة بياناتٍ تضمّ أصحاب سوابق في سرقة المتاجر. كما أنّ هذا النوع من الأنظمة هو المستخدَم في التحقيقات الجنائية. وحتى يتسنّى لجهات نفاذ القانون الاطّلاع على مثل هذه الصور، يجب تنفيذ أمرٍ قضائي أو ما شابه ذلك، بناءً على السياق والقوانين المنصوص عليها في البلاد. وبمجرد استيفاء المعيار القانوني، يحتاج الأمر إلى بعض الوقت للتدقيق في الصور. وعلى عكس ما يُروَّج في الأفلام والبرامج، لا يمكن إنشاء معرّف في غضون ثوانٍ. وبدلًا من ذلك، تقوم السلطات أولًا بالحصول على مقاطع الفيديو ثم استخدام برنامج أوّلي لتشغيلها، وإنشاء سلسلة من الصور الخام لجميع الأشخاص الموجودين في المقاطع. وهذه الصور ستكون ذات جودةٍ أقل، حيث يتمّ فصل وعزل صور الأشخاص الذين يضعون قبّعات، أو تلك الملتقَطة من زوايا غير مألوفة وما إلى ذلك. بعدها، يجري تشغيل نماذج هذه الصور مع مجموعة بيانات ترى الشرطة بأنها قابلة للتطبيق عليها، مثل سجلّات إدارة المركبات الآلية المحلية أو غيرها. ومن شبه المؤكّد أنّ أيّ تطابقٍ محتمل سيكون في مستوياتٍ منخفضة من اليقين، لذلك سيتعيّن على المسؤول البشري كما ذكرنا سابقًا إلى مراجعتها

لمعرفة ما إذا كان هناك تطابقًا يبدو موثوقًا بدرجة كافية للمتابعة، واتّخاذ مزيدٍ من الإجراءات. ولا بدّ من الإشارة إلى أنّ مستوى الدقة المطلوبة في أيّ نظام تعرّف على الوجه يختلف بناءً على التطبيق والسياق. فبالنسبة لجهاز آيفون على سبيل المثال والذي يسمّى بنظام التعرّف على الوجه (Face ID) يتمّ الاعتماد على كاميرا تعمل بالأشعة تحت الحمراء، ومستشعِر، وكذلك جهاز عرض للنقاط لرسم 30 ألف نقطة على الوجه وإنشاء مسح ثلاثيّ الأبعاد بهدف القيام بعملية التعرف على الوجه[12]. وتعدّ التقنية ثلاثية الأبعاد إحدى الطرق التي تمنع وصول شخص آخر ببساطة من الوصول إلى الهاتف[13].

4. بين التعرّف على الوجه وكلمات المرور

يُعدّ أمان البيانات من أكثر المواضيع إثارةً للجدل بالنسبة لأولئك المهتمّين بأنظمة التعرّف على الوجه. وهناك عدّة أوجه في النظر لمستويات الأمان[14]. أوّلها في مدى إمكانية انتحال الصفة (الحصول على صلاحية الوصول بدون وجود وجه الشخص الفعلي) أو اختراقها (الوصول إلى الملفات المخزّنة من النماذج أو القوالب). ويتمّ تقييم أنظمة التعرّف على الوجه على هذا الأساس، مع التأكيد على أنّه لا يوجد نظام مثالي. ويرى المنتقدون لهذه التقنية بأنّ النسبة الصغيرة من المخرجات غير الصحيحة لمثل هذه الأنظمة، كفيلة أن تجعلها أنظمة محفوفة بمخاطر غير معقولة أبرزها التحيّز[15]. وفي هذا السياق، لا بدّ من تناول البدائل المتاحة للتعرّف على الوجه وعلى رأسها كلمات المرور وإجراء مقارنة بينها وبين هذه الأنظمة.

من شبه المؤكد أنّ البيانات البيومترية المتأتّية من أنظمة التعرّف، والواردة في قاعدة بيانات الأفراد المسجلين، تعدّ خيارًا أكثر أمانًا من كلمات المرور. إذ يمكن اختراق هذه الكلمات بسهولةٍ إلى حدّ ما من خلال أساليب "هجوم القوة العمياء" (Brute Force Attack) وهو مصطلحٌ يشير إلى عمليات الهجوم بطريقة التخمين التي يتمّ الاعتماد عليها لمحاولة استحصال معلوماتٍ معيّنة كإسم المستخدم وكلمة السرّ أو الرقم التعريفي الشخصي عن طريقة تخمين مجموعة من الاحتمالات المتوقعة وكذلك إيجاد المفتاح لفك شيفرات الرسائل والبيانات[16]. ويميل الأشخاص إلى إعادة استخدامها، لذا فإنّ الحصول على كلمة مرور شخصٍ ما لحسابٍ واحد، من شأنه أن يوفّر احتمالية الوصول لحساباتٍ أخرى أيضًا، الأمر الذي يؤدّي إلى أن تكون

كلمة المرور غير آمنة، وبالتالي إضعاف النظام الذي يتمّ تخزينها عليه. وفي هذه الحالة، يتبادر سؤال: إذا ما تمّ اختراق خادم كلّ من كلمات المرور وقوالب المقاييس الحيوية، ما هي المخاطر المترتّبة على ذلك؟

إنّ الاستحواذ على كلمات المرور يؤدي إلى الحصول على معلوماتٍ يمكن استخدامها للوصول مباشرة إلى الحسابات الفردية. وكما ذُكر سابقًا، قد تكون كلمة المرور تسمح بالوصول إلى حساباتٍ أخرى أيضًا. في المقابل، فإنّ خرق قاعدة البيانات البيومترية سوف ينتج عنها فقط الحصول على تلك الأعداد الثنائية (Binary Numbers) التي لا يمكن بسهولة - إن وجدت - "إعادة هندسة" القالب أو الصورة الأصلية[17]. ولا يمكن استخدام هذه البيانات التي تمّ تحصيلها نتيجة الخرق للوصول إلى الحساب المرتبط. كما أنّه ليس من المحتمل أن تكون هذه المعلومات مفيدة للوصول إلى أيّ حساباتٍ أخرى كما هو الحال مع كلمات المرور، وذلك نظرًا لأن كلّ منصة بيومترية ترتكز على مزوّدٍ مختلف، كما أنّ الخوارزميات غير قابلة للتشغيل المتبادل. وفي الواقع، قد يكون اختراق قاعدة بيانات بيومترية مرتبطًا بالأمان العام للشبكة، ولكن إذا ما تمّ اختراقها، فهناك احتمال أكبر بأنّ البيانات سيكون من الصعب جدًا استغلالها بأيّ طريقةٍ منهجية[18]. وتعدّ القياسات الحيوية دائمًا جزءًا من نظام، ما يعني أنّها جزءٌ واحد فقط من عملية وصول متعدّدة الخطوات، وبالتالي فإنّ مجرد الحصول على البيانات القياسية الحيوية لا يكفي للوصول كما الحال مع كلمات المرور.

5. الخصوصية مقابل الأمن

يُعرَف مبدأ الخصوصية باسم "جودة وسلامة البيانات"، وهو يشترط أن تكون البيانات الفردية ومجموعات البيانات "دقيقة وذات صلة وكاملة"[19]. ويكمن التحدّي الذي تواجهه النظم الحالية للتعرّف على الوجه في تحقيق الدقّة الكافية، ومراعاة الاختلافات الديموغرافية مثل العرق ونوع الجنس وغيرها، على الرغم من أنها تتحسّن مع مرور الوقت. ومع ذلك، فإنّ الطرق التي أخفقت فيها أنظمة التعرف على الوجه، أدت إلى تحفظاتٍ كبيرة حول موثوقيتها من منظور الخصوصية والعدالة الاجتماعية والحريات المدنية، وهذا ما أكّدته دراسة المعهد الوطني الأميركي للمعايير والتكنولوجيا (NIST) ودعت إلى بذل الجهود للتخفيف من الآثار المترتبة حيال ذلك[20].

ويبدو أنّ الصين، على وجه الخصوص، حريصة على استخدام التعرف على الوجه في كل شيء بدءًا من تحديد المشاة[21]. وبالتزامن مع انتشار جائحة "كوفيد 19"، انتشر استخدام هذه التقنية بشكلٍ أكبر في مجال

الرقابة، بهدف منع انتشار الفيروس، وتحقيق الأمن العام كما تقول الحكومة الصينية. وفي آذار/ مارس من العام الماضي، تمّ تجهيز كاميرات التعرّف على الوجه بتقنية الكشف عن درجة حرارة الجسم في الأماكن العامة لمنع الأشخاص الذين قد يكونون مصابين بالفيروس من السفر. وقد ازداد عدد كاميرات التعرّف المستخدمة في الصين من 176 مليونًا في عام 2017 إلى 626 مليونًا حتى عام 2020[22]. كما وضعت الحكومة بعض التدابير لتنظيم "أمن البيانات الحيوية" التي تمّ جمعها، حيث أنّ هذه البيانات البيومترية تعدّ محمية تحت مسمّى "أمن المعلومات الشخصية". وتنصّ التدابير على أنّ جمع المعلومات الشخصية ينبغي أن يكون "لأغراضٍ قانونية ومبررة وضرورية ومحددة"، مما يتطلب في كثيرٍ من الأحيان الموافقة، كما يجب الحرص على أن تظلّ آمنة. إلّا أنّ الواقع الحالي بوضع الكاميرات في الأماكن العامة لا يحاول الحصول على الموافقة أو الالتزام بحماية أمن وسلامة البيانات كما ينبغي[23].

وكان العديد من الباحثين والأكاديميين قد أجروا مراجعاتٍ عميقة لتأثير تكنولوجيا المراقبة عل المجتمع وكذلك على الأقليات وغيرها من الجماعات مع تطبيق هذه التقنية من قبل السلطات[24]. وفي هذا السياق، لا يمكن تجاهل المواقف المرتبطة بأولئك الذين يسيرون في حركات احتجاجية لصالح قضية معينة في مكانٍ عام. صحيح أنّ المحتجّين قد يدركون أنّ الناس سوف تراهم وربما تتعرّف عليهم، كما قد يجري التقاط صور لهم ونشرها عبر الإنترنت. لكن، فإن ما قد لا يتوقّعونه على الأرجح هو أن تكون لدى السلطات كاميرات أو تغطية تمكنّها لاحقًا من جمع وتحديد صور العديد أو معظم الأشخاص الحاضرين، والاحتفاظ بها على شكل ملفّات كنوع من السجلّات في المستقبل، خصوصًا في البلدان التي لا تتمتع بقدرٍ كافٍ من الحماية القانونية بخصوص المراقبة الشاملة والخصوصية. ومن جهةٍ أخرى، إنّ التعرّف الخاطئ من قبل الجهات الحكومية يمكن أن يؤدي إلى تسجيل أشخاصٍ أبرياء على قوائم المراقبة، خصوصًا مع ازدياد المخاوف من وقوع انتهاكات أو تجاوزات قد تمسّ الأقليات وغيرها من الفئات في المجتمع. وقد ثبت تاريخيًا أنّ قدرة الحكومة على تتبّع مواطنيها تسمح بالتمييز ضد الجماعات أو الأفراد المستهدفين تحت مسميات الأمن.

6. الخصوصية وقطاع الأعمال

لا تقتصر مخاوف الخصوصية على المجال الحكومي بل تتعدّاه لتشمل قطاع الأعمال أيضًا. وقد تستخدم الشركات التجارية تقنية التعرّف على الوجه، لجمع المعلومات البيومترية بدون موافقة الأفراد. في الولايات المتحدة الأمريكية، أصدرت المحكمة الفيدرالية حكمًا بتغريم شركة فيسبوك مبلغ 650 مليون دولار لصالح

سكان من ولاية "إلينوي" الأميركية، وذلك لاستخدام منصّة فيسبوك هذه التقنيّة وجمع البيانات البيومترية الخاصة بهم دون إذنهم[25]. ويعدّ قانون خصوصية المعلومات الحيوية في إلينوي (BIPA) من بين أكثر القوانين صرامةً في الولايات المتحدة، ويتطلّب من الشركات الحصول على إذن وموافقة صريحة من المستهلك قبل جمع أو تقاسم أي معلومات بيومترية وهذا يتعلّق بالتعرّف على الوجه ومسح بصمات الأصابع بغية تحديد هوية العملاء[26]. وتمثّل هذه القضية واحدة من أكبر التسويات ذات الصلة بدعوى الخصوصية الرقمية. وفي إطار الاستجابة لهذه الدعوى، كان فيسبوك قد قام بتحديث إعدادات "اقتراحات الإشارة" (Tag Suggestions) الخاصة به، لعدم السماح بشكلٍ تلقائي بتطبيق تقنية التعرف على الوجه في الصور أو مقاطع الفيديو. وتجدر الإشارة إلى أنّ فيسبوك لديه العديد من براءات الاختراع المرتبطة باستخدام تقنية التعرف على الوجه للإعلان الموجّه ولأغراضٍ أخرى. ويرى المناهضون لهذه التقنية في أنّ البيانات البيومترية هي معلومات شخصية حساسة بسبب تقييدها الفطري، على عكس كلمة المرور أو اسم المستخدم، إذ لا يمكن تغيير ميزات الوجه بسهولة[27]. كذلك، قد تعمد شركات أخرى لاستخدام التعرف على الوجه للتمييز على نحوٍ غير عادلٍ أو غير قانوني. وعلى سبيل المثال، يمكن لسلسلة متاجر البيع بالتجزئة أن تنشئ مجموعة بياناتٍ خاصة بها من المجرمين "المعروفين" أو "ذوي السوابق" دون أيّ معايير واضحة لمن يتمّ استهدافهم. علاوةً على ذلك، قد تشارك سلسلة متاجر البيع بالتجزئة هذه القوائم مع شركاتٍ أخرى، ما قد يؤدي إلى حرمان الأفراد من الخدمة على نطاقٍ واسعٍ دون أيّ إجراءاتٍ قانونية سليمة وواضحة. وبالتالي، فالكيانات التجارية تُظهِر أنّ ممارساتها في مجال الخصوصية قد لا تكون أفضل حالًا، حيث تقوم بجمع واستغلال البيانات الشخصية للأفراد والجماعات وحتى البلدان[28]. وغالبًا ما يكون الخط الفاصل بين الوصول التجاري والحكومي للبيانات وبين الاستخدام غير واضحة. ما يضع المخاوف والمخاطر التي تنجم عن أنظمة التعرف على الوجه تستند إلى أسسٍ منطقية. وفي حين أنّ هناك بعض الأمثلة على وضع الأطر القانونية، للردّ على تحديات الخصوصية مثل قانون الخصوصية في الاتحاد الأوروبي (GDPR)، إلّا أن هذه الجهود تعدّ محدودة بل شبه معدومة في العالم العربي، ما يستوجب التفكير جديّا في العمل على مزيد من التنظيم وحماية البيانات لدى المستخدمين بالمنطقة.

7. الخاتمة

إنّ استخدام أنظمة التعرّف على الوجه ليست بالطبع وحدها المسؤولة عن المشاكل المرتبطة بالخصوصية في العالم. لكن، منذ نشأة هذه التقنية في منتصف الستينيات من القرن الماضي، كثر الحديث عن احتمال إمكانية إساءة الاستخدام، وهذا ما قد يزداد خلال العقد المقبل، مع توقّعات بتوسّع استخدام أنظمة التعرّف بشكلٍ كبير[29]. وعليه، فإدخال هذه الأنظمة إلى العمل يتطلّب الأخذ بعين الاعتبار عدد من المسائل: كفاءة التطبيقات لتدخل حيّز التنفيذ لا سيما في مجال التعرّف على الوجه، وكذلك تفنيد عناصر الخصوصية الضرورية التي ينبغي حمايتها، بالإضافة إلى ضرورة تحديد مستوى الأمان الذي يمكن أن يرافق إدخال هذه التقنية وتطويرها خاصةً مع أولئك المبرمجين الذين يعملون على تطوير الأنظمة، والذين قد يصبّون تركيزهم على الجانب التقني والبرمجي فقط دون الجوانب الأخرى، لذلك من المهمّ أن يتمّ فهم إمكانات أنظمة التعرّف بشكلٍ صحيح من حيث زيادة الأمان والخصوصية ومن حيث إساءة الاستخدام المحتملة. وفي هذا الإطار، أصبح هناك أكثر من 80 دولة حول العالم أنشأت قوانين مرتبطة بخصوصية البيانات لحماية البيانات الشخصية لمواطنيها[30].

وفي المقابل، يرى بعض المنتقدين لأنظمة التعرّف على الوجه أنها تشكّل أداةً إضافية في دائرة التكنولوجيا للحكومات القادرة بالفعل على تحديد واستهداف وتعقّب الأفراد إلى ما هو أبعد من أيّ شيء يمكن تصوّره في الماضي. وهذه ليست المرة الأولى التي يجري فيها الاعتراض على تقنيات ذات صلة. ففي الولايات المتحدة مثلًا خيضت الكثير من المناقشات حول بطاقات الهوية الوطنية التي تدور رحاها حول هذه الأنظمة، وحول ما إذا كان ينبغي للحكومات الحصول على الهويات الشخصية للمواطنين من أجل الحصول على الخدمات أو السلع أو البحث عن عمل وغيرها بحجة "مكافحة الإرهاب" الذي لا يوجد تعريف موحّد حوله[31]. وعليه فإشكاليات الخصوصية، لا تنحصر فقط في المناقشات المتعلّقة باستخدام نظم التعرّف على الوجه. وسواء كانت هذه التحديات في الماضي أو الحاضر، فإنها تستند جميعها إلى مسألة كيفية تحقيق التوازن بين الأمن وبين حماية خصوصية الأفراد وبياناتهم الشخصية. وفي هذا السياق، فإنّ هذه الورقة البحثية هي بمثابة دعوة لتسليط الضوء أكثر على مفهوم الخصوصية حيال التقنيات الذكية المستخدمة في العالم العربي بشكلٍ عام، وكذلك تقنية التعرّف على الوجه بشكلٍ خاص.

المصادر:

1. Cullum, J. (2018). “Facial Recognition at Border Nets More Impostors than at Airports. Available from: https://www.hstoday.us/subject-matter-areas/airport-aviation-security/facial-recognition-at-border-nets-more-impostors-than-at-airports/
2. Zhang, L. (2021). Facial recognition ID: how safe is your face? Deakin University. Available from: https://this.deakin.edu.au/innovation/ready-set-boom-is-the-wait-for-renewable-energy-finally-over
3. Garvais, J. (2018): How facial recognition works? Available from: https://us.norton.com/internetsecurity-iot-how-facial-recognition-software-works.html
4. US Government Accountability Office. (2015). Facial Recognition Technology: Commercial Uses, Privacy Issues, and Applicable Federal Law, GAO-15-621. Available from: https://www.gao.gov/products/gao-15-621
5. Moraes, T.G., Almeida, E.C., & Pereira, J.R. (2020). Smile, you are being identified! Risks and measures for the use of facial recognition in (semi-)public spaces. Available from: https://link.springer.com/content/pdf/10.1007/s43681-020-00014-3.pdf
6. Lynch, J. (2020).Face Off: Law Enforcement Use of Face Recognition Technology. Available from: https://www.eff.org/wp/law-enforcement-use-face-recognition
7. Future of Privacy Forum. (2018). Understanding Facial Detection, Characterization and Recognition Technologies. Available from: https://fpf.org/wp-content/uploads/2018/09/FPF_FaceRecognitionPoster_R5.pdf
8. Dwivedi, D. (2018). Face Detection for Beginners. Available from: https://towardsdatascience.com/face-detection-for-beginners-e58e8f21aad9
9. Jain, C., Sawant, K., Rehman, M., & Kumar, R. (2018). Emotion Detection and Characterization using Facial Features. 2018 3rd International Conference and Workshops on Recent Advances and Innovations in Engineering (ICRAIE), 1-6. Available from: https://ieeexplore.ieee.org/document/8710406
10. Clark, E.A., Kessinger, J., Duncan, S., Bell, M., Lahne, J., Gallagher, D.L., & O'keefe, S. (2020). The Facial Action Coding System for Characterization of Human Affective Response to Consumer Product-Based Stimuli: A Systematic Review. Frontiers in

Psychology, 11. Available from: https://www.frontiersin.org/articles/10.3389/fpsyg.2020.00920/full

11. Agarwal, A., Biswas, I. (2021). Facial Recognition Fundamentals. Available from: https://www.eetasia.com/facial-recognition-fundamentals/

12. آبل (2020). حول تقنية "Face ID" المتقدمة. متاح في: https://support.apple.com/ar-ae/HT208108

13. La, L. (2018). 10 Best Phones with Facial Recognition: IPhone X, Note 9, LG G7, and More. Available from: https://www.cnet.com/news/10-best-phones-with-facial-recognition-iphone-x-note-9-galaxy-s9-lg-g7/

14. Haley Fox, H. (2020). 3 Privacy Concerns around Facial Recognition Technology. Available from: https://www.swiftlane.com/blog/facial-recognition-privacy-concerns/#:~:text=As%20mentioned%2C%20facial%20recognition%20technologies,does%20not%20make%20a%20difference.

15. إم آي تي. (2020). آي بي إم تنسحب من تطوير تقنية التعرف على الوجوه بسبب استخدامها في التصنيف العنصري. متاح في: https://cutt.ly/Vc76SQ5/

16. تجمّع مشرفي المعلوماتية العرب. (2020). ما هو الهجوم الأعمى وكيف تكون في أمانٍ منه؟ متاح في : https://cutt.ly/1c761xM

17. Rec Faces. (2021). What Is Biometric Security and Why Does It Matter Today? Available from: https://recfaces.com/articles/biometric-security

18. National Cyber Security Centre. (2019).Biometric recognition and authentication systems. Available from: https://www.ncsc.gov.uk/collection/biometrics/how-biometrics-are-attacked

19. US Homeland Security. (2017). DHS Privacy Policy Guidance Memorandum 2017-01. Available from: https://www.dhs.gov/publication/dhs-privacy-policy-guidance-memorandum-2017-01

20. National Institute of Standards and Technology. (2019).Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects. Available from: https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf

21. Zhao, C. (2018). Jaywalking in China: Facial Recognition Surveillance Will Soon Fine Citizens via Text Message. Available from: https://www.newsweek.com/jaywalking-china-facial-recognition-surveillance-will-soon-fine-citizens-text-861401

22. Grenoble, R. (2017). Welcome To The Surveillance State: China's AI Cameras See All. Available from: https://www.huffpost.com/entry/china-surveillance-camera-big-brother_n_5a2ff4dfe4b01598ac484acc

23. Dudley, L. (2020). China's Ubiquitous Facial Recognition Tech Sparks Privacy Backlash. Available from: https://thediplomat.com/2020/03/chinas-ubiquitous-facial-recognition-tech-sparks-privacy-backlash/#:~:text=As%20the%20number%20of%20facial,the%20security%20of%20sensitive%20data.

24. البوابة العربية للأخبار التقنية. (2021). تقنية التعرّف على الوجه تجبر فيسبوك على دفع 650 مليون دولار. متاح في : https://cutt.ly/ac5qww1/

25. Georgtown Law.(2017).The Color of Surveillance. Available from: https://www.law.georgetown.edu/privacy-technology-center/events/color-of-surveillance-2017/

26. Free Privacy Policy. (2021). Guide to the Illinois Biometric Information Privacy Act. Available from: https://www.freeprivacypolicy.com/blog/bipa/

27. Germain, T. (2020). Facebook Settles $550 Million Facial Recognition Lawsuit. Available from: https://www.consumerreports.org/lawsuits-settlements/facebook-settles-facial-recognition-lawsuit/

28. The Guardian. (2018). the Cambridge Analytica Files. Available from: https://www.theguardian.com/news/series/cambridge-analytica-files

29. Mordor Intelligence. (2020). Facial Recognition Market – Growth, Trends, Covid-19 Impact, and Forecasts (2021 - 2026). Available from: https://www.mordorintelligence.com/industry-reports/facial-recognition-market

30. National Conference of State Legislatures. (2019). 2019 Consumer Data Privacy Legislation. Available from: https://www.ncsl.org/research/telecommunications-and-information-technology/consumer-data-privacy.aspx

31. American Civil Liberties Union. (2021). 5 Problems with National ID Cards. Available from: https://www.aclu.org/other/5-problems-national-id-cards