Security Policy Papers أوراق السياسات الأمنية
https://spp.nauss.edu.sa/index.php/spp

المفاهيم الأمنية

# مفهوم القياسات الحيوية: بين الأبعاد الأمنية والإشكاليات الأخلاقية

# The Concept of Biometrics: Between Security Considerations and Ethical Issues

## المقدمة

أدركت الدول والمنظَّمات والشركات الرائدة في جميع أنحاء العالم أهميَّة التحوُّل من البطاقات وكلمات المرور وأنظمة المصادقة التقليديَّة، وضرورة استبدال تكنولوجيا القياسات الحيويَّة بها، بعد أن أضحت وسيلة محايدة لحماية الهُويَّة في العالم الرقمي (Norval & Prasopoulou, 2018)، وذلك على شاكلة: بصمات الأصابع، وقزحيَّة العين، وملامح الوجه، والصوت، والحمض النووي، وغير ذلك. وهو ما يرجع إلى جملة من العوامل، منها: صعوبة تزوير تلك القياسات، وتنوُّع مجالات استخداماتها، مدفوعًا بالتطوُّرات التكنولوجيَّة المُطَّردة، وزيادة معدَّلات الهجمات السيبرانيَّة، وسهولة اختراق كلمات المرور التقليديَّة، ورقمنة الخدمات المصرفيَّة التقليديَّة، وظهور المَحافظ الإلكترونيَّة، وتواتُر جهود الشمول المالي، وغير ذلك.

ونتيجةً لذلك، تعدَّدت استخدامات القياسات الحيويَّة في مجالات: الأمن السيبراني، وحماية البيانات، والتحقُّق والتوثيق (Authentication & Authorization) من الهُويَّة في المطارات والمعابر الحدوديَّة والمنشآت الحسَّاسة، والمراقبة والتتبُّع، وأمن الهواتف والأجهزة الإلكترونيَّة، وتسجيل الدخول إلى الحواسيب والشبكات، وتأمين قواعد البيانات، وإنفاذ القانون، والمعاملات الإلكترونيَّة والرقميَّة، وغير ذلك.

وفي اتجاه مضاد لأهميَّة تلك التقنيَّات وتنوُّع استخداماتها، فقد تعدَّدت الأبعاد الأمنيَّة للقياسات الحيويَّة (Biometric Security Dimensions) من جهة، وتعالت الأصوات الناقدة لها والمشكِّكة فيها من جهة أخرى. وبعبارة ثانية، فإن هناك مخاوفَ حقيقيَّةً تنتج عن توظيف تلك التقنيَّات بسبب إمكانيَّة خداع الأنظمة المشغِّلة لها، كما أن إدارة الهُويَّة وتخزينها أمرٌ يظل موضعًا للشك لدى عدد واسع من المدافعين عن الخصوصيَّة، بالنظر إلى ممارسات تخزين البيانات غير الآمنة حال استضافتها على خوادم محليَّة، ما قد يؤدِّي إلى ثغرات أمنيَّة، ولذا تزداد أهميَّة تأمين تلك البيانات من خلال تدابير أمنيَّة محكمة.

## ماهيَّة القياسات الحيويَّة

ظهرت القياسات الحيويَّة بوصفها إجراءً بديلًا للتعرُّف إلى البشر بالاعتماد على عددٍ من الطرق، منها: بصمة الإصبع، وقزحيَّة العين، وبصمة الكف، والأذن، وأوردة الإصبع، والصوت، والتوقيع، وغير ذلك. وقد أضحت جميعها من طرق القياس الحيوي الأكثر شيوعًا واستخدامًا للتعرُّف إلى الهُويَّة الفرديَّة بفعل مزاياها المتعدِّدة، مثل: التفرُّد

العالي حتى في حالة التوائم، والشكل والمظهر المستقر والمتسق نسبيًّا لفترات زمنيَّة ممتدَّة، وغير ذلك (Vukobrat & Gnjatović, 2023).

وتتعدَّد تقنيَّات تحديد الهُويَّة باستخدام القياسات الحيويَّة، التي تضفي سمات فريدة على الأفراد، وذلك على شاكلة ما يلي:

- **التحقُّق من بصمات الأصابع:** وذلك للتحقُّق من هُويَّة الفرد عبر مقارنة بصمة إصبع الشخص المُقدَّمة مع أخرى مسجَّلة سلفًا.
- **التعرُّف إلى العين:** وهي تقنيَّة بيومتريَّة تعتمد على تحليل السمات الفريدة لقزحيَّة العين أو أنماط الأوعية الدمويَّة في شبكيَّة العين، بهدف التحقُّق من هُويَّة الفرد تحقُّقًا دقيقًا وموثوقًا.
- **التعرُّف إلى شكل اليد:** من خلال سماتها الظاهرة على شاكلة طولها وعرضها وغير ذلك، عن طريق الاستعانة بالكاميرا التي تلتقط صورة ظليَّة لليد وتقارنها بتلك المخزَّنة في قواعد البيانات.
- **التعرُّف إلى الصوت:** فلكل صوت بصمة صوتيَّة تُميِّزه يمكن التعرُّف إليها ومطابقتها مع الأصوات المسجَّلة في قواعد البيانات.
- **التعرُّف إلى التوقيع:** إذ يمكن التفرقة بين خطوط الأيدي ومقارنة التوقيعات الإلكترونيَّة الممسوحة ضوئيًّا (أمازون، 2024).
- **التعرُّف إلى الوجه:** تتعرَّف تلك التقنيَّة إلى الوجه المطلوب في ثوانٍ معدودة، وإن اختلف هذا التوقيت من نظام إلى آخر. وتتطلَّب تلك التقنيَّة دراسة أبعاد الأنف وشكل العينين والأذنين والشفتين وغير ذلك.

وبطبيعة الحال، يتباين انتشار التقنيَّات السابقة باختلاف خصائصها وإمكاناتها التقنيَّة، وقد حظيت تقنيَّة التعرُّف إلى الوجه بانتشار أوسع مقارنةً بغيرها، نظرًا لقدرتها العالية على التقاط ملامح الوجه وتحليلها عن بُعد، بخلاف تقنيَّات التعرُّف إلى بصمة الإصبع أو الصوت التي تواجه تحديات فنيَّة وميدانيَّة. فلا يسهل التعرُّف إلى الصوت عند الازدحام أو عند الإصابة بنزلات البرد، كما أن بصمة الإصبع قد تتعرَّض للتلف أو التشوُّه نتيجة الحروق أو الإصابات، بينما يمكن أن تتغيَّر بصمة العين نتيجة أمراض مثل الرمد. ونتيجة لهذه المزايا النسبيَّة، شهد سوق تقنيَّات التعرُّف إلى الوجه نموًّا ملحوظًا خلال السنوات الأخيرة، مدفوعًا بازدياد مبادرات حماية البيانات، وتنامي الحاجة إلى نُظم متقدِّمة لمكافحة الاحتيال، فضلًا عن الطلب المتزايد على أدوات فعَّالة لمراقبة الفضاءات العامَّة وتأمينها (البهي، 2020).

وقد أصبحت القياسات الحيويَّة خيارًا واعدًا لجميع المنظَّمات التي تستخدم البطاقات الماديَّة والوثائق وكلمات المرور أو أرقام التعريف لتأمين البيانات المخزَّنة في أشكال إلكترونيَّة على جهاز كمبيوتر أو على ماكينة صرف آلي (ATM). ويتمثَّل الغرض العام منها في التقاط المعلومات وتخزينها في مرحلة التسجيل، ثم مقارنتها لاحقًا في مرحلة التحقُّق. وفي إطار عملية الالتقاط، يُحدِّد البرنامج قيمًا معيَّنة لصورة القياس الحيوي، ويُخزِّن تلك القيم في قالب يحتاج إلى مساحة تخزين أقل كثيرًا من الصورة نفسها. وفي أثناء عملية التحقُّق، وعندما يبدأ العميل تعاملًا ما، يمسح النظام مقاييسه

الحيويَّة، ثم يضاهي هذا المسح مع القالب المخزَّن، ومن ثَمَّ يقبله أو يرفضه. كما يجري أيضًا استحداث تسجيل مُؤمَّن مُحدَّث لكل محاولة مضاهاة يقوم بها النظام (ويلان، 2024).

## مجالات الاستخدام وتطبيقاته

إن كيفيَّة جلوس الأفراد ومشيتهم وروائحهم وأوردتهم في أيديهم وبصمات أصابعهم وشكل آذانهم وغير ذلك هي مُعرّفات مميّزة؛ لذا تُستخدم القياسات الحيويَّة المتقدِّمة لحماية المستندات والحسابات الحسَّاسة. ومن الأمثلة البارزة على ذلك: توظيف مصرفَي «Citibank» و«Halifax» تقنيَّة التعرُّف إلى الأصوات وأخرى لمراقبة نبض العملاء بهدف التحقُّق من هُويَّاتهم على الترتيب. كما أُدمجت القياسات الحيويَّة في جوازات السفر الإلكترونيَّة من قِبل عدة دول عالميًّا. ففي الولايات المتحدة، حوت جوازات السفر الإلكترونيَّة شريحة تشمل صورًا رقميَّة لأوجه الأشخاص وبصمات أصابعهم وقزحياتهم، مع الاستعانة بتقنيَّة تحول دون قراءة تلك الشريحة بواسطة أجهزة غير مصرَّح لها (كاسبرسكي، د.ت).

وتتعدَّد مزايا القياسات الحيويَّة واستخداماتها بوصفها وسيلة لتحديد الهُويَّة، ومنها: انخفاض التكاليف من ناحية، وانعدام الحاجة إلى استخراج بطاقات تعريفيَّة حال ضياعها من ناحية ثانية، وعدم الحاجة إلى تغيير كلمات المرور من ناحية ثالثة. ولا تتعرَّض البيانات الحيويَّة للفقد أو النسيان لطابعها الفريد غير القابل للتغيير؛ لذا، فقد ازداد استخدام القياسات الحيويَّة جرَّاء المزايا السابقة، بجانب تراجُع تكلفة الأجهزة اللازمة لها نسبيًّا. فلا يتطلَّب فحص شبكيَّة الأعين للوصول إلى الخدمات المصرفيَّة، أو فحص أوردة المرضى في المستشفيات، أجهزة ضخمة (جمعة، 2022).

ويتزايد الاعتماد على تقنيَّة التعرُّف إلى الوجه من قِبل الأجهزة الأمنيَّة؛ فتجمع الشرطة صور المشبوهين وتقارنها وتضيفها إلى قواعد البيانات لتُمسَح ضوئيًّا عندما تُجري الشرطة بحثًا جنائيًّا آخرَ. كما يسمح التعرُّف إلى الوجه للأجهزة الشرطيَّة باستخدام الهواتف الذكيَّة أو الأجهزة اللوحيَّة لتصوير السائقين والمشاة ومقارنة الصور فورًا بقواعد بيانات التعرُّف إلى الوجه لمحاولة تحديد الهُويَّة (كاسبرسكي، د. ت).

وتستخدم وكالات إنفاذ القانون تلك التقنيَّات استخدامًا متزايدًا في أعمالها الروتينيَّة. ويمكن لها في سبيل إنشاء قواعد بيانات ضخمة أن تستعين بوسائل التواصل الاجتماعي والدوائر التلفزيونيَّة المغلقة وكاميرات المرور، بل والصور التي التقطتها بنفسها في الميدان. ويمكن أيضًا مقارنة الوجوه في الوقت الفعلي مع «القوائم الساخنة» للأشخاص المشتبه في قيامهم بنشاط غير قانوني. وبناءً عليه، استُخدِمت تقنيَّة التعرُّف إلى الوجه على نطاق واسع في المطارات وعند المعابر الحدوديَّة وفي الأحداث الضخمة على شاكلة الألعاب الأولمبيَّة، كما تُستخدم أيضًا لدواعٍ أمنيَّة في المتاجر والملاعب الرياضيَّة، وإن اختلفت القواعد المنظِّمة لتلك التقنيَّة في الحالتين (Electronic Frontier Foundation, 2023).

ويحتوي نظام الإنتربول للتعرُّف إلى الوجوه (INTERPOL Facial Recognition System, IFRS) على صور لوجوه واردة من أكثر من 179 دولة، ما يجعله قاعدة بيانات جنائيَّة عالميَّة فريدة من نوعها. فإلى جانب تطبيق برمجي بيومتري آلي، يمكن لهذا النظام أن يُحدِّد هُويَّة الشخص ويتحقَّق منه من خلال مقارنة وتحليل الأنماط والأشكال والنسب الملامح

وجهه. وقد حُدِّدت هُويَّة حوالي 1500 إرهابي أو مجرم أو هارب أو شخص موضع اهتمام أو مفقود منذ إطلاق نظام الإنتربول للتعرُّف إلى الوجه في عام 2016 فحسب. فعند إدخال صورة الوجه في النظام، يجري تشفيرها تلقائيًّا بواسطة إحدى الخوارزميَّات ومقارنتها بالملفات الشخصيَّة المخزَّنة بالفعل في النظام، وينتج عن هذا قائمة «المرشحين» بالمطابقات الأكثر احتمالًا.

وينفِّذ الإنتربول عملية «التعرُّف إلى الوجه» للتحقُّق من نتائج النظام الآلي. ويفحص موظفو الإنتربول المؤهلون وذوو الخبرة الصور بعناية للعثور على الخصائص الفريدة التي يمكن أن تؤدِّي إلى إحدى النتائج التالية: «مرشح محتمل» أو «لا يوجد مرشح» أو «غير حاسمة». وبعد ذلك تُمرَّر تلك المعلومات إلى البلدان التي قدَّمت الصور، والبلدان التي قد تكون مهتمَّة بالملف الشخصي أو المطابقة. ويجري التعامل مع جميع المعلومات بما يتماشى مع قواعد الإنتربول بشأن معالجة البيانات. ويجري البحث عن جميع صور الوجوه الموجودة في الإشعارات والتعميمات التي تطلبها البلدان الأعضاء ويجري تخزينها في نظام التعرُّف إلى الوجه، بشرط أن تستوفي معايير الجودة الصارمة اللازمة للتعرُّف إليها. ويمكن للدول الأعضاء أيضًا أن تطلب «البحث فقط» في نظام التعرُّف إلى الوجه، لإجراء فحص لشخص محل اهتمام في المطارات أو المعابر الحدوديَّة الأخرى (Interpol, 2023).

ومما سبق، يمكن القول: إن وكالات إنفاذ القانون والوكالات الحكوميَّة ومختلف الشركات والدول في جميع أنحاء العالم تواصل التعاقد مع كثير من الشركات المختصَّة بالقياسات الحيويَّة (الحرة، 2023)، واستخدمتها في مجال تصنيع الهواتف المحمولة (مثل شركة أبل)، وفي المطارات (عبر الأجهزة الأمنيَّة لتحديد الأفراد الذين قد يتجاوزون مدة تأشيراتهم)، وفي مجال إنفاذ القانون (من خلال جمع الصور الفوتوغرافيَّة ومقارنتها بقواعد البيانات المتاحة)، ومن قِبل وسائل التواصل الاجتماعي (مثل «فيسبوك» لوضع علامة على الأفراد في الصور الفوتوغرافيَّة)، وفي مجال أمن الأعمال (حيث يمكن للشركات استخدام التعرُّف إلى الوجه للدخول إلى مبانيها)، وكذا في مجال التسويق (حيث يمكن للمسوِّقين استخدام التعرُّف إلى الوجه لتحديد العمر والجنس والعرق للجماهير المستهدَفة) (Gillis, 2022).

وفي ضوء هذا، فإن هناك استخدامات عدَّة للقياسات الحيويَّة على الرغم من حداثتها، وهي الاستخدامات التي يمكن الوقوف عليها تفصيلًا من خلال النقاط التالية:

- **الطب الشرعي:** تسهم القياسات الحيويَّة في التحقيقات الجنائيَّة للتعرُّف إلى الجثث والقتلى وهُويَّة الأفراد في الفيديوهات والتعرُّف إلى الأطفال المفقودين بمقارنة صور المفقودين والتعرُّف إليهم بمجرد ظهورهم في الأماكن العامَّة. فإن جرت إضافة الأفراد المفقودين إلى قواعد البيانات، أمكن تنبيه جهات إنفاذ القانون بمجرد التعرُّف إليهم في أي مكان.
- **الخدمات المصرفيَّة:** يمكن استبدال كلمات المرور التقليديَّة بالنظر إلى هواتف المستخدمين الذكيَّة أو أجهزتهم المحمولة، فمع ميزة التعرُّف إلى الوجه، لا توجد كلمات مرور يمكن للمتسللين اختراقها. وهي التقنيَّة التي قد تُستخدم أيضًا لإجراء عمليات السحب أو الإيداع (سيبر وان، 2022).

- **المطارات ومراقبة الحدود الدوليَّة:** تعتمد كثير من الدول على القياسات الحيويَّة لمطابقة هُويَّة المسافر مع البيانات المخزَّنة في قواعد بيانات الجوازات الإلكترونيَّة أو أنظمة الهجرة، بهدف الحدِّ من استخدام الوثائق المزوَّرة أو المسروقة. كما تُمكِّن أنظمة الجوازات الإلكترونيَّة (e-Gates) المسافرين من عبور نقاط التفتيش دون تدخُّل بشري مباشر، ممَّا يُسرِّع عملية العبور ويقلِّل الازدحام. ويمكن أيضًا مقارنة البيانات الحيويَّة للمسافرين مع قواعد بيانات دوليَّة، مثل: قاعدة بيانات الإنتربول، أو قواعد بيانات الإرهاب أو الأشخاص الخاضعين للعقوبات، لرصد أي تطابُق محتمَل، ناهيك عن استخدام البيانات الحيويَّة لتتبُّع تحرُّكات الأفراد عبر الحدود وتحليل سلوكهم لاكتشاف أنماط مشبوهة قد تدلُّ على الاتجار بالبشر أو التهريب أو الأنشطة غير المشروعة الأخرى .(Polito & Alaimo, 2023)
- **دعم أنظمة اللجوء والهجرة:** تُستخدم القياسات الحيويَّة لتسجيل طالبي اللجوء والتأكُّد من عدم تقديم طلبات متكرِّرة بهُويَّات مختلفة في دول عدَّة، كما هو الحال في نظام «يوروداك» التابع للاتحاد الأوروبي، الذي يُخزِّن بصمات الأصابع من جميع طالبي اللجوء ويحتفظ بها لمقارنتها مع طلبات لاحقة في دول الاتحاد الأخرى، وهو ما يُمكِّن من تطبيق اتفاقيَّات الهجرة بصرامة، ولا سيَّما اتفاقيَّة دبلن التي تُحمِّل مسؤوليَّة دراسة طلب اللجوء لأول دولة أوروبيَّة دخلها المتقدِّم، ما يسهم في تحسين الكفاءة التشغيليَّة لأنظمة الهجرة واللجوء، ويعزِّز ثقة الدول المضيفة بمعايير الأمان والشفافية. بينما تستخدم الولايات المتحدة برنامج «TISIV-SU» الذي يجمع بصمات أصابع وصورًا رقميَّة من معظم الزائرين القادمين إلى الولايات المتحدة، بمن فيهم طالبو اللجوء، لمقارنة هُويَّات المتقدِّمين مع قواعد بيانات وزارة الأمن الداخلي ومكتب التحقيقات الفيدرالي، بهدف الكشف عن سجلات جنائيَّة أو تهديدات أمنيَّة محتمَلة (Farraj, 2010).
- **مكافحة الإرهاب:** تتيح القياسات الحيويَّة للدول تبادل المعلومات الحيويَّة بدقة وكفاءة أكثر، ممَّا يدعم التحقيقات الجنائيَّة ومكافحة الإرهاب عبر الحدود، حيث أسهم هذا التعاون في الكشف عن تحرُّكات أشخاص ضمن خلايا نائمة كانت تتنقَّل بين عدة دول أوروبيَّة وآسيويَّة. ولعلَّ المثال الأبرز في هذا الصدد هو التعاون بين الولايات المتحدة ودول الاتحاد الأوروبي من خلال برامج تبادُل بيانات القياسات الحيويَّة، وهو ما مكَّن السلطات من تعقُّب عناصر متطرِّفة عبر عدة دول قبل تنفيذ عملياتهم. كما تُستخدم تلك القياسات في مراقبة الإنترنت ومنصات التواصل الاجتماعي؛ إذ تسمح خوارزميَّات التعرُّف إلى الوجه بتحليل الصور ومقاطع الفيديو المنشورة للتعرُّف إلى وجوه أشخاص مطلوبين أو مشتبه بهم، خصوصًا حينما ينشر الإرهابيون دعايتهم أو يظهرون في مقاطع تهديد (Amoore, 2006).
- **الأمن السيبراني:** يصعب الوصول غير المصرَّح به إلى أنظمة التعرُّف إلى الوجه، ما يجعلها أداة أمان مريحة ودقيقة للغاية لفتح الهواتف الذكيَّة والأجهزة الشخصيَّة الأخرى. وبعبارة ثانية، تَستخدم كثيرٌ من الهواتف تقنيَّة التعرُّف إلى الوجه لفتحها لحماية المعلومات الشخصيَّة وتأمين البيانات الحسَّاسة إن تعرضت الهواتف للسرقة. وعليه، تدفع شركة «أبل» بأن فرصة فتح الهاتف عشوائيًّا عن طريق الوجه تبلغ واحدًا في المليون.

## الإشكاليَّات والتحديات

يمكن القول: إن القياسات الحيويَّة قد شهدت تطورات لافتة مؤخرًا، كما تعدَّدت استخداماتها من قِبَل مختلف البنى التحتيَّة والأجهزة الأمنيَّة والشرطيَّة والمؤسَّسات المدنيَّة وغير ذلك. فلم تعُد القياسات الحيويَّة مجرد أدوات تقنيَّة تُستخدم لدفع وتيرة المعاملات أو لتعزيز الأمن، بل أصبحت مكونًا بنيويًّا في نظم الحوكمة المعاصرة. فمع انتشارها السريع في مختلف المجالات، يُثار التساؤل عن إمكانيَّة تحوُّل تلك التقنيَّات إلى ركيزة في نظام عالمي بيومتري تتحكَّم فيه الدول في حركة الأفراد وتُحكم به رقابتها عليهم. ومن شأن الإجابة عن هذا السؤال أن تثير إشكاليَّات سياسيَّة في قلب النقاشات المعاصرة ذات الصلة بالهُويَّة والمواطنة والحريَّة، جنبًا إلى جنب مع جملة من الإشكاليَّات التي يمكن الوقوف على أبرزها من خلال النقاط التالية:

- إحكام الرقابة الأمنيَّة: تسمح القياسات الحيويَّة للدول بإحكام رقابتها الجماعيَّة والمباشرة على مواطنيها وتعقُّب تحركاتهم؛ إذ تنتشر أنظمة المراقبة (CCTV) عالميًّا، وقد طوَّرت بعض الدول -وفي مقدمتها الصين- كاميرات مراقبة بدقَّة بلغت 500 ميجابكسل، ما يعني قدرتها على التقاط صور دقيقة تُحدِّد هُويَّة المستهدَفين بين عشرات الآلاف (البوَّابة العربيَّة للأخبار التقنيَّة، 2019).
- تفاوُت الأطر التشريعيَّة: تختلف الأطر التشريعيَّة المقنِّنة للقياسات الحيويَّة في صرامتها من دولة إلى أخرى، ولا يوجد إطار قانوني عالمي موحَّد ينظِّم استخداماتها، كما تتعدَّد الفجوات التشريعيَّة المقنِّنة لتلك التقنيَّات في الدول النامية، وبخاصَّةٍ مع تطوُّرها بوتائر مُطَّردة تتجاوز التطوُّر المماثل في الأطر القانونيَّة، ما يعني بالضرورة فجوة بين الاستخدامات الفعليَّة على أرض الواقع والأطر التنظيميَّة، ما يهيِّئ الفرصة لإساءة الاستخدام، خصوصًا عند الحصول على صور المواطنين دون إذنهم المسبق (البهي، 2020).
- انتهاك الخصوصيَّة: تثير القياسات الحيويَّة إشكاليَّات أخلاقيَّة في ظل تراجع الضوابط المقنِّنة لها وتغوُّلها على الحق في الخصوصيَّة وإساءة استخدامها المحتمَل وإحكام عمليَّات الرقابة الجماعيَّة وغياب الإشراف المدني عليها. وما يدلل على ذلك -على سبيل المثال- حالة كوريا الجنوبيَّة؛ ففي إطار مجابهتها لجائحة فيروس كورونا المستجد (كوفيد-19)، تتبَّعت الحكومة الحالات المصابة بالفيروس من خلال تقنيَّة التعرُّف إلى الوجه، مع استخدام واسع للذكاء الاصطناعي وكاميرات المراقبة، بيد أن ذلك تسبَّب في غضب المعارضة التي رأت أن تلك الخطوة تعني أن الحكومة ستتجسَّس على مواطنيها (حمدون، 2023).
- احتماليَّة خداع التقنيَّة: على عكس بصمات الأصابع والحمض النووي وغير ذلك من سمات لا تتغيَّر خلال حياة الشخص، يجب أن يأخذ التعرُّف إلى الوجه في الاعتبار عددًا من العوامل المختلفة، مثل: الشيخوخة، وجراحات التجميل، ومستحضرات التجميل، وآثار تعاطي المخدِّرات، والتدخين. كما تُعدُّ جودة الصور أمرًا شديد الأهميَّة، وقد لا تكون الصور ذات الجودة المنخفضة أو المتوسطة -بفعل مساحيق التجميل أو الأقنعة المصنَّعة بالطابعات ثلاثيَّة الأبعاد- قابلة للبحث، ما يؤثِّر في دقَّة النتائج. وبعبارة ثانية، يسهل خداع الخوارزميَّات وتعديل الصور دون

الكشف عن ذلك. وحتى في ظل انعدام آليَّات الخداع، فإن دقة النتائج تظل محلًّا للشك. ففي عام 2018، اختبرت «منظمة الاتحاد الأمريكي للحريات المدنيَّة» نظام «Amazon Rekognition» الذي طوَّرته شركة «أمازون»، وقد أشارت نتائجه إلى وجود 82 عضوًا من أعضاء الكونجرس الأمريكي من مرتكبي جرائم سابقة. وأثارت تلك النتائج تساؤلات بشأن تداعيات التعويل على تقنيَّات التعرُّف إلى الوجه التي قد تُسفر عن عمليَّات اعتقال غير قانونيَّة (البوَّابة العربيَّة للأخبار التقنيَّة، 2019).

- التحيُّز العرقي: لا تخلو البيانات المستخدَمة بواسطة تقنيَّات التعرُّف إلى الوجه وما يتصل بها من تقنيَّات القياس الحيوي من أخطاء، ما قد يورِّط أشخاصًا في جرائم لم يرتكبوها. كما تتراجع فعاليَّتها في التعرُّف إلى الأمريكيين من أصل أفريقي والأقليات العرقيَّة الأخرى والنساء والشباب، وغالبًا ما تخطئ أو تفشل في التعرُّف إليهم، ما يؤثر تأثيرًا متباينًا في مجموعات بعينها (Electronic Frontier Foundation, 2023). فقد تخطئ أنظمة التعرُّف إلى الوجه التابعة لكبريات الشركات التكنولوجيَّة -على شاكلة «أمازون» و«مايكروسوفت»- عند التعرُّف إلى الأمريكيين من أصل أفريقي مقارنةً بغيرهم. واتصالًا بذلك، أجرى «المعهد الوطني للمعايير والتكنولوجيا» (TSIN) مؤخرًا اختبارًا واسع النطاق بهدف تحديد التحيُّزات المحتمَلة في تقنيَّات التعرُّف إلى الوجه وما يتصل بها من تقنيَّات القياس الحيوي. وقد اكتشف أنه حتى أفضل الخوارزميَّات لا تزال تعرض معدلًا إيجابيًّا كاذبًا أعلى بين أفراد غرب أفريقيا وشرقها وشرق آسيا، في حين كان لدى الأوروبيين الشرقيين أدنى معدل إيجابي كاذب، والسبب هو الخلل الديموغرافي في بيانات التدريب المستخدَمة لتدريب تلك المحرِّكات (scirtavonnI).
- احتماليَّة سرقة البيانات البيومتريَّة: قد تتحوَّل البيانات الحيويَّة إلى أهداف محتمَلة للقراصنة والهواة لسرقتها وتوظيفها في عمليات التزييف والابتزاز وغير ذلك من جرائم غير مشروعة. فقد حذرت شركة «كليرفيو» عملاءها من سرقة بياناتها في أعقاب اختراق الشركة ووصول القراصنة إلى بياناتها. وإن نفت الشركة حدوث أي خرق أمني لخوادمها، بينما أكَّدت تعزيز تدابيرها الأمنيَّة (البهي، 0202).

وتتمثَّل المشكلة الأكثر إلحاحًا في أن قواعد البيانات الخاصَّة بالمعلومات الشخصيَّة هي أهداف للقراصنة والمتسللين. ففي عام 2015، عند اختراق مكتب إدارة شؤون الموظفين بالولايات المتحدة، أمكن لمجرمي الإنترنت سرقة بصمات أصابع 5.6 مليون عامل، ما جعلهم عرضة لسرقة هُويَّاتهم؛ لذا، يُعتبر تخزين البيانات الحيويَّة على جهاز مثل «TouchID» أو «Face ID» أكثر أمانًا من تخزينها مع مزوِّد الخدمة وإن شُفِّرت البيانات. وعليه، يتماثل ذلك مع المخاطر التي قد تتعرَّض لها قواعد بيانات كلمات المرور، حيث قد يخترق المتسللون النظام، ويسرقون البيانات غير المؤمَّنة بفعاليَّة. ومع ذلك، فإن التداعيات تختلف إلى حدٍّ بعيد؛ فإن اخترقت كلمات المرور، أمكن تغييرها، أما البيانات الحيويَّة فلن تتغيَّر طول الأمد (القيادي، 2023).

## الخاتمة

على الرغم من حداثة القياسات الحيويَّة، فإن كفاءتها تزداد مع مرور الوقت، ولا سيَّما في ظل إتاحتها وتعدُّد الشركات التكنولوجيَّة الرائدة والناشئة التي تعمل في مجال تطويرها من ناحية، وقدرتها على إحداث تحوُّلات كبرى تُنذر بتزايُد استخداماتها في المستقبل ولا سيَّما في: مختلف الأعمال التجارية، وعمليات المراقبة، وكشف الكذب، والتحقُّق من العمر، وتمييز تعبيرات الأفراد، والتحقيق مع المشتبه بهم من ناحية ثانية. وقد تتمكَّن تلك التقنيَّات مستقبلًا من اكتشاف المشاعر، فتصبح أنظمة التشغيل التي تتحكَّم في تلك التقنيَّة أكثر مرونة وذكاءً في المستقبل القريب مع تحسُّن دقة أنظمة القياسات الحيويَّة وسرعتها؛ فمن شأن التقدُّم في التعلُّم الآلي والذكاء الاصطناعي أن يزيد من تعزيز قدرات المصادقة البيومتريَّة، ما يزيد من قوتها وانتشارها.

وفي الوقت الذي تهدف فيه القياسات الحيويَّة إلى تعزيز الأمان وتسهيل الوصول إلى الخدمات، فإنها تثير في الوقت ذاته تساؤلات عن الخصوصيَّة والسيطرة الحكوميَّة والعدالة الاجتماعيَّة والحوكمة الديمقراطيَّة، وتتطلَّب النظر في طبيعة العلاقة بين السلطة والمواطن في العصر الرقمي، ما يستوجب الحيلولة دون تحوُّل تلك التقنيَّات إلى أدوات للرقابة والتهميش.

# المراجع

## المراجع العربيَّة


أمازون (2024). ما المقصود بتقنية التعرُّف على الوجه؟ أمازون، متاح على: https://aws.amazon.com/ar/what-is/facial-recognition/.

البهي، رغدة (2020). «التعرُّف على الوجه»: تكنولوجيا جديدة للمراقبة العالميَّة، المركز المصري للفكر والدراسات الإستراتيجيَّة، متاح على: https://ecss.com.eg/8433/.

البوَّابة العربيَّة للأخبار التقنيَّة (أكتوبر 2019). 5 أسباب تثير القلق من تقنية التعرُّف على الوجه، العربيَّة، متاح على: https://rb.gy/h52itc.

الحرة (2023). رغم «أخطائها العنصرية».. هل تصلح تقنية «التعرُّف على الوجوه» في مكافحة الجريمة؟ الحرة، متاح على: https://rb.gy/u4dg69.

القيادي (2023). القياسات الحيوية.. ما هي؟ وكيف يتم استخدامها في الأمن؟ القيادي، متاح على: https://t.ly/7UQ7o.

جمعة، الشاذلي (2022). تعرَّف على مزايا استخدام القياسات الحيويَّة كبديل لبطاقة الهُويَّة لعملاء التأمين، جريدة المال، متاح على: https://t.ly/2G9hE.

حمدون، فاطمة (2023). هل تنتهك تكنولوجيا «التعرُّف على الوجه» خصوصيَّتنا؟ بي بي سي، متاح على: https://www.bbc.com/arabic/business-59747242.

سيبر وان (2022). ما هو نظام التعرُّف على الوجه؟ سيبر وان، متاح على: https://rb.gy/c864vg.

كاسبرسكي. ما المقصود بالمقاييس الحيويَّة؟ Kaspersky، متاح على: https://me.kaspersky.com/resource-center/definitions/biometrics.

ويلان، ستيف (2024). تكنولوجيا القياسات الحيويَّة، سلسلة ابتكارات تكنولوجيا المعلومات، المجموعة الاستشاريَّة لمساعدة الفقراء، متاح على: https://www.findevgateway.org/sites/default/files/publications/files/mfg-ar-biometrics-technology-22649_0.pdf.


## المراجع الأجنبيَّة


Amoore, L. (2006). Biometric borders: Governing mobilities in the war on terror. Political geography, 25(3), 336-351.

Electronic Frontier Foundation (2023), Face Recognition, Electronic Frontier Foundation, Available online: https://www.eff.org/ar/pages/face-recognition.

Farraj, A. (2010). Refugees and the biometric future: the impact of biometrics on refugees and asylum seekers. Colum. Hum. Rts. L. Rev., 42, 891.

Innovatrics, Facial Recognition Technology, Innovatrics, Available online: https://www.innovatrics.com/facial-recognition-technology/, Assessed on: November 25, 2023.

Interpol, Facial Recognition (2023), Interpol, Available online: https://www.interpol.int/How-we-work/Forensics/Facial-Recognition.

Norval, A., & Prasopoulou, E. (2018). Seeing Like a Citizen: Exploring Public Views of Biometrics. Political Studies, 67(2), pp. 367-387.

Polito, C. & Alaimo, C. (2023). The Politics of Biometric Technologies: Borders control and the making of data citizens in Africa. ECIS 2023 Research-in-Progress.

Vukobrat, N. & Gnjatović, M. (2023). Implementation of two factor authentication using face and iris biometrics, Science Direct, In: Blockchain Technology Solutions for the Security of IoT-Based Healthcare Systems. Available online: https://www.sciencedirect.com/topics/computer-science/multimodal-biometric.

May 2026 مايو 2026

**Security Research Center** **مركز البحوث الأمنية**

*Naif Arab University for Security Sciences*
*Riyadh, Saudi Arabia*

جامعة نايف العربية للعلوم الأمنية
الرياض، المملكة العربية السعودية

**Keywords:** digital identity, facial recognition, privacy, cybersecurity, government surveillance, algorithmic bias

**الكلمات المفتاحية:** الهوية الرقمية، التعرف إلى الوجه، الخصوصية، الأمن السيبراني، الرقابة الحكومية، التحيز الخوارزمي

Production and hosting by NAUSS

Email:SRCenter @nauss.edu.sa
doi:10.26735/UWVE7900