المراقبة البيومترية وحماية البيانات الشخصية قلق متصاعد بشأن حقوق الإنسان

ألقت منظمة أميركيون من أجل الديمقراطية وحقوق الإنسان في البحرين الضوء على ملف المراقبة البيومترية في ما يسمى "بدول الخليج"، واعتبرت أنه على مدار العقد الماضي، شهدت "دول الخليج" إنفاذِا واسعًا لنظام حماية البيانات الشخصية (PDPLs)، في خطوة تُبرز سعيها لتنظيم جمع معلومات الأفراد ومعالجتها. ورغم أن هذه الأنظمة تبدو ظاهريًا إنجازًا مهمًا لتعزيز الخصوصية في مجتمعات تسير بخطى متسارعة نحو الرقمنة، إلا أنها تثير في الوقت ذاته تساؤلات جوهرية حول فعالية حماية البيانات، وحدود سلطة الدولة، وتأثير ذلك على حقوق الإنسان. وقد توسّعت حكومات المنطقة فعليًا في استخدام التقنيات البيومترية، مثل التعرف على الوجه ومسح بصمات الأصابع، خصوصًا في الإمارات العربية المتحدة التي استثمرت بقوة في تطوير تقنيات الذكاء الاصطناعي. هذا التوسع أثار مخاوف متزايدة بين المواطنين بشأن إمكانية توظيف تلك التقنيات لأغراض المراقبة غير المصرح بها أو التضييق السياسي. مخاوف، يصعب تجاهلها عند تحليل منظومات حماية البيانات الشخصية السارية في دول الخليج.

ووفقا للمنظمة الحقوقية فقد تصدّرت قطر المشهد الخليجي عام 2016 باعتبارها أول دولة تسنّ نظام حماية البيانات الشخصية. ومع ذلك، ما زالت تواجه حتى اليوم تحديات كبيرة في تطبيق هذا النظام على أرض الواقع، خصوصًا فيما يتعلّق بضعف حماية حقوق أصحاب البيانات، وغياب التعريفات الواضحة لما يُصنّف ضمن البيانات الحساسة (مثل البيانات البيومترية والوراثية)، إضافةً إلى نقص التفاصيل بشأن التزامات معالجي البيانات ومراقبيها تجاه الأفراد. والأبرز أن النظام يجيز معالجة البيانات الشخصية في حالات عدّة دون الحاجة إلى موافقة صاحبها، من بينها المعالجة لأسباب تتعلق بـ"المصلحة العامة"، وهو مصطلح فضفاض يفتح الباب أمام تفسيرات واسعة ومتباينة.

وعلى صعيد "السعودية"، أكدت المنظمة أنه يبدو للوهلة الأولى أن "السعودية" أرست إطارًا أكثر شمولًا لحماية البيانات تحت إشراف ما يسمى "الهيئة السعودية للبيانات والذكاء الاصطناعي" (SDAIA)، زاعمة سعيها إلى مواءمة نظام حماية البيانات الشخصية لعام 2024 مع اللائحة العامة لحماية البيانات الأوروبية (GDPR). ورغم أنّ النظام يعترف صراحةً بالبيانات البيومترية ويفرض عقوبات صارمة على الانتهاكات، إلا أنه يتضمّن استثناءات مشابهة لما هو معمول به في قطر، إذ لا يُشترط الحصول على موافقة صاحب البيانات قبل جمعها إذا كان ذلك لأغراض "المصلحة العامة" أو "الأمن العام". غير أنّ هذه الأحكام، في كيان يُعرف بتشدّده تجاه المعارضة والنقد، تفتح الباب فعليًا أمام جمع البيانات على نطاق واسع وتُكرّس ذلك تحت ذريعة "الأمن القومي".

في المقابل، تُقدّم الإمارات العربية المتحدة مشهدًا أكثر تعقيدًا فيما يتعلق بحماية البيانات الشخصية. فوفقًا لنظام حماية البيانات الشخصية لعام 2022، تُصنَّف البيانات البيومترية ضمن فئة "البيانات الشخصية الحساسة"، ويُلزم النظام بمعالجتها بشفافية ومسؤولية. ومع ذلك، لا يزال تطبيق هذا النظام محدودًا، إذ لم يُنشأ بعد مكتب البيانات المسؤول عن تنفيذه، ولم تُحدّد أي عقوبات واضحة على حالات الانتهاك. إلى جانب ذلك، يؤدّي وجود أطر تشريعية موازية—مثل قانون رقم (26) لسنة 2015 بشأن تنظيم نشر وتبادل البيانات في إمارة دبي ونظام حماية البيانات لمركز دبي المالي العالمي (DIFC) لعام 2020—إلى تجزئة المساءلة وخلق ثغرات محتملة يمكن أن تُستغل من قبل الجهات الحكومية.

ومع الانتشار الواسع لتقنيات المراقبة البيومترية في الأماكن العامة وعلى غرار ما يحدث في

"السعودية"، تتزايد المخاوف من اتساع نطاق المراقبة وضعف الضوابط المنظمة لها. هذا الغياب الفعلي للتطبيق يثير تساؤلات عميقة حول حدود الرقابة على المراقبة البيومترية، واحتمال تآكل الخصوصية في الدولة.

وعلى صعيد باقي دول الخليج، أبرزت المنظمة حالة سلطنة عمان، إذ يتضمن نظام حماية البيانات الشخصية لعام 2022 أحكامًا تُعدّ أكثر تقدّمًا نسبيًا، حيث يعترف بالبيانات البيومترية كـ"بيانات شخصية حساسة"، ويشترط الحصول على موافقة صريحة من صاحب البيانات، ويضع قيودًا على معالجة هذه البيانات دون تفويض من الوزارة المختصة. أما البحرين، فبالرغم من سنّها للقانون رقم (30) لعام 2018 (الذي دخل حيّز التنفيذ عام 2019)، إذ يفرض عقوبات جنائية تصل إلى السجن لمدة عام وغرامات مالية كبيرة على المعالجة غير المصرّح بها. كما يُلزم بالحصول على تفويض خطي من الجهة المختصة لمعالجة البيانات البيومترية أو الوراثية، وإلا يُعدّ ذلك محظورًا. ومع ذلك، يتضمّن كلا النظامين، كما هو الحال في بقية "دول الخليج"، استثناءات واسعة تحت ذريعة "الأمن القومي" و"المصلحة العامة"، مصطلحات فضفاضة تُوفّر غطاءً قانونيًا لممارسات يُفترض أن الأنظمة وُجدت أساسًا لتنظيمها. ومن اللافت أيضًا أن البحرين، ضمن قائمتها للدول التي تعتبرها تتمتع بحماية كافية للبيانات الشخصية لنقلها عبر الحدود، أدرجت الكويت، رغم أنها لا تمتلك حتى الآن نظامًا محددًا لحماية البيانات.
وتعكس هذه التناقضات واقعًا يشير إلى أن حماية البيانات في الخليج لا تزال، في كثير من الأحيان، واجهة قانونية أكثر منها التزامًا فعليًا بصون خصوصية الأفراد.

أكدت المنظمة أميركيون من أجل الديمقراطية وحقوق الإنسان في البحرين أن الفجوة في تطبيق أطر حماية البيانات في "دول الخليج" تُبرز التوتر الواضح بين حماية الخصوصية وتعزيز سيطرة الدولة. فرغم أن هذه الأنظمة تبدو متوافقة مع المعايير الدولية، مثل اللائحة العامة لحماية البيانات، تُضعف الاستثناءات الواسعة التي تتضمنها، إلى جانب قلة التركيز على البيانات البيومترية، قدرتها الفعلية على توفير الحماية المنشودة. وفي ظلّ غياب هيئات رقابية مستقلة وآليات شفافة قابلة للتنفيذ، يتحوّل استخدام المراقبة البيومترية إلى أداة سياسية محتملة بيد السلطة. لذلك، فإن تحقيق تقدم حقيقي يتطلب تجاوز التشريعات الشكلية وضمان أن تصبح حماية البيانات أداة فعالة لصون حقوق الأفراد وكرامتهم الإنسانية.