

منظمات حقوقية تحذر من إلزام مستخدمي المحمول بالبيانات البيومترية



الثلاثاء 25 أغسطس 2026 03:30 م

أثارت دعوة 19 منظمة حقوقية مصرية ودولية جدلاً واسعاً بشأن توجهات استخدام البيانات البيومترية في خدمات الاتصالات بمصر، بعدما طالبت هذه المنظمات الجهاز القومي لتنظيم الاتصالات بالتراجع عن أي إجراءات تجعل تقديم صورة الوجه أو بصمة الإصبع أو غيرها من القياسات الحيوية شرطاً لتسجيل خطوط الهاتف المحمول أو إدارتها أو استعادتها، وكذلك لاستخدام خدمة «أرقامى» أو الاعتراض على تسجيل خطوط بأسماء أشخاص دون علمهم

وجاء الموقف الحقوقي على خلفية وقائع تتعلق باكتشاف مواطنين تسجيل خطوط هواتف محمول، وفي بعض الحالات محافظ مالية مرتبطة بهذه الخطوط، باستخدام بياناتهم الشخصية دون علمهم، وهي الوقائع التي دفعت الجهاز القومي لتنظيم الاتصالات إلى اتخاذ إجراءات بحق شركات الاتصالات العاملة في السوق المصرية

وترى المنظمات الموقعة على البيان أن معالجة هذه الوقائع يجب أن تبدأ بتحديد مصدر الخلل داخل منظومة تسجيل وتفعيل خطوط المحمول، ومحاسبة المسؤولين عنه، بدلاً من التوسع في جمع بيانات شخصية أكثر حساسية من ملايين المستخدمين

أزمة تسجيل خطوط المحمول دون علم أصحابها

تعود خلفية الأزمة إلى تلقي الجهاز القومي لتنظيم الاتصالات شكاوى من أشخاص اكتشفوا وجود خطوط محمول مسجلة بأسمائهم دون علمهم، وفي بعض الحالات ارتبطت هذه الخطوط بمحافظ مالية، الأمر الذي أثار تساؤلات حول سلامة إجراءات التحقق من هوية المشتركين وآليات تسجيل الخطوط وتفعيلها داخل شركات الاتصالات ومنافذ البيع التابعة لها

وفي 10 أغسطس 2026، أعلن الجهاز القومي لتنظيم الاتصالات إحالة شركات الاتصالات الأربع العاملة في مصر إلى النيابة العامة، بعد إجراءات فحص وتحقيق بشأن وقائع تسجيل خطوط باستخدام بيانات أشخاص دون علمهم

وبالتزامن مع ذلك، ودّج الجهاز شركات الاتصالات إلى الإسراع في إتاحة آليات للتحقق من هوية أصحاب الخطوط باستخدام القياسات الحيوية عبر تطبيقاتها الإلكترونية

وهنا تحديداً تتركز المخاوف التي عبرت عنها المنظمات الحقوقية، إذ ترى أن الانتقال من مشكلة تسجيل خطوط بصورة غير مصرح بها إلى جمع صور الوجوه أو بصمات الأصابع لملايين المستخدمين يحتاج إلى مبررات قانونية وتقنية واضحة، وإلى إثبات أن هذا الإجراء هو بالفعل الوسيلة الضرورية لمعالجة الخلل

لماذا تعترض المنظمات على التحقق البيومتري؟

بحسب البيان، فإن المشكلة الأساسية لا تزال تتمثل في عدم الإعلان بصورة واضحة عن الكيفية التي تمكن من خلالها أشخاص أو جهات من تسجيل خطوط هواتف محمول باستخدام بيانات مواطنين دون علمهم

وتطرح المنظمات عدة احتمالات لمصدر الخل، من بينها انتحال الهوية باستخدام بطاقة رقم قومي تخص شخصًا آخر عند نقطة البيع، أو إساءة استخدام صلاحيات الموظفين والوكلاء، أو التلاعب بأجهزة التفعيل والحسابات والسجلات الداخلية لشركات الاتصالات[]

وتؤكد أن تحديد مصدر المشكلة يمثل خطوة أساسية قبل اعتماد أي حل جديد، لأن التحقق البيومتري، بحسب رؤيتها، قد يثبت أن الشخص الذي يجري معاملة معينة يطابق هوية مرجعية، لكنه لا يمنع بالضرورة إساءة استخدام صلاحيات العاملين أو الوكلاء، ولا يمنع التلاعب الداخلي بالسجلات أو إضافة خطوط إلى حسابات المستخدمين بطرق غير مشروعة[]

كما أن المطابقة البيومترية لا تعني بالضرورة أن جميع صور إساءة استخدام البيانات ستختفي، خصوصًا إذا كانت المشكلة مرتبطة بصلاحيات الوصول إلى أنظمة الشركات أو آليات التحكم في سجلات المشتركين[]

البيانات البيومترية[] معلومات لا يمكن تغييرها

أحد أبرز أسباب اعتراض المنظمات يتعلق بطبيعة البيانات البيومترية نفسها[]

فكلمة مرور يمكن تغييرها، وبطاقة هوية يمكن استبدالها، وحساب يمكن إغلاقه، لكن الأمر مختلف عندما يتعلق الأمر بصورة الوجه أو بصمة الإصبع[]

وتشير المنظمات إلى أن تسرب هذه البيانات أو استخدامها بصورة غير مشروعة يطرح مخاطر طويلة الأمد، لأن الشخص لا يستطيع ببساطة تغيير بصماته أو ملامح وجهه كما يغير كلمة مرور أو وثيقة إثبات شخصية[]

ولا تقتصر المخاطر، بحسب البيان، على الاحتفاظ بالصورة الأصلية للوجه أو البصمة، وإنما تمتد إلى القوالب الرقمية التي يمكن استخراجها من البيانات البيومترية واستخدامها في عمليات المطابقة، وربطها ببيانات أخرى مرتبطة بهوية الشخص[]

وترى المنظمات أن الجمع بين البيانات البيومترية وبيانات الاشتراك في خدمات الاتصالات قد يؤدي إلى إنشاء بنية تقنية تسمح بربط مجموعات متعددة من المعلومات المتعلقة بالشخص نفسه[]

وتحذر من أن هذه البنية قد تفتح مستقبلًا الباب أمام استخدامات أخرى للبيانات، بما في ذلك المراقبة أو التنميط، إذا لم تكن هناك قيود قانونية وتقنية صارمة على الوصول إلى البيانات وربطها والاحتفاظ بها ومشاركتها[]

من يتحمل مسؤولية الخل؟

من النقاط المركزية في البيان الحقوقي تحميل شركات الاتصالات والجهات المنظمة مسؤولية معالجة الخل داخل منظومة تسجيل الخطوط، بدلاً من نقل العبء إلى المواطنين[]

وترى المنظمات أن الشخص الذي اكتشف استخدام بياناته في تسجيل خط دون علمه لا ينبغي أن يصبح مطالئًا بتقديم بيانات أكثر حساسية حتى يتمكن من معرفة الخطوط المسجلة باسمه أو الاعتراض عليها[]

وبحسب هذا التصور، فإن وجود خط مسجل دون علم صاحبه يمثل خللاً في منظومة التسجيل والتحقق، وبالتالي يجب أن يكون إصلاح هذا الخل مسؤولية الجهات التي تدير المنظومة وتشرف عليها[]

وتطالب المنظمات بإتاحة وسائل فعالة وسريعة للاعتراض على الخطوط غير المصرح بها، مع تصحيح البيانات وتحمل الجهات المسؤولية تبعات الأخطاء التي تقع داخل منافذ البيع أو أنظمة الشركات[]

مخاوف من توسيع نطاق جمع البيانات

تقول المنظمات إن فرض معالجة بيانات شديدة الحساسية على جميع المستخدمين قبل تحديد مصدر المشكلة قد يؤدي إلى نقل الأزمة من محاولة إصلاح أوجه القصور في منظومة التسجيل إلى جمع مزيد من المعلومات الشخصية عن المواطنين[]

وتزداد هذه المخاوف، وفق البيان، لأن الشركات التي قد تتولى جمع أو معالجة البيانات البيومترية هي نفسها الشركات التي وقعت داخل منظومة البيع والتسجيل والتفعيل التابعة لها وقائع تسجيل غير مصرح بها، والتي أحييت إلى النيابة العامة[]

وتطالب المنظمات السلطات بنشر تقييم واضح لقدرة الشركات ومقدمي الخدمات والتقنيات الذين قد يعملون لصالحها على حماية البيانات البيومترية، إلى جانب تحديد المسؤوليات القانونية في حال تعرض هذه البيانات للتسريب أو الوصول غير المصرح به أو استخدامها في أغراض أخرى[]

الخصوصية في مواجهة متطلبات الأمن والتحقق

لا ترفض المنظمات، بحسب البيان، فكرة التحقق من هوية مستخدمي خدمات الاتصالات من حيث المبدأ، لكنها تعترض على جعل البيانات البيومترية الحل الافتراضي أو الإلزامي دون إثبات ضرورته وتناسبه

وتؤكد أن أي تدخل في خصوصية الأفراد يجب أن يستند إلى أساس قانوني واضح، وأن يكون مرتبطًا بهدف محدد ومشروع، وأن يكون ضروريًا لتحقيق هذا الهدف، مع عدم تجاوز حجم البيانات التي تتم معالجتها القدر اللازم لتحقيق الغرض

وتشير المنظمات إلى أن قانون حماية البيانات الشخصية رقم 151 لسنة 2020 يصنف القياسات الحيوية ضمن البيانات الشخصية الحساسة، وهو ما يفرض متطلبات مشددة فيما يتعلق بجمعها ومعالجتها وحمايتها

كما تستند إلى المادة 57 من الدستور المصري، التي تحمي حرمة الاتصالات وخصوصيتها، لتأكيد أهمية وجود ضوابط واضحة عند التعامل مع بيانات مرتبطة بخدمات الاتصالات

خطر الإقصاء الرقمي

وتحذر المنظمات من أن فرض التحقق البيومتري قد تكون له آثار تتجاوز مسألة الخصوصية وحماية البيانات

فالهاتف المحمول أصبح جزءًا أساسيًا من الحياة اليومية، ولم يعد استخدامه مقتصرًا على المكالمات والرسائل، بل يرتبط بمجموعة واسعة من الخدمات الحكومية والمصرفية والتعليمية والصحية، فضلًا عن فرص العمل والتعاملات المالية

ومن ثم، فإن ربط القدرة على الوصول إلى خدمات الاتصالات بعملية تحقق إلكترونية أو بيومترية قد يخلق صعوبات أمام فئات من المستخدمين، خصوصًا كبار السن والأشخاص ذوي الإعاقة والأشخاص الذين لا يمتلكون هواتف ذكية مناسبة أو يواجهون مشكلات في الاتصال بالإنترنت

وتطالب المنظمات بإتاحة وسائل بديلة وغير بيومترية تكون متكافئة وفعالة، بما في ذلك التحقق الحصري باستخدام أصل مستند الهوية، مع توفير التسهيلات اللازمة للفئات التي تواجه صعوبات في الوصول إلى الخدمات الرقمية

مطالب بإجراءات أكثر استهدافًا

بدلًا من فرض التحقق البيومتري على جميع المستخدمين، تقترح المنظمات مجموعة واسعة من الإجراءات التي تستهدف الخل داخل منظومة شركات الاتصالات

وتتصدر هذه المطالب سحب أي توجيه يجعل صورة الوجه أو بصمة الإصبع أو أي معرف بيومتري شرطًا لتسجيل خطوط الهاتف المحمول أو تجديد التعاقد أو إعادة التعاقد أو استعادة الخط، أو استخدام خدمة «أرقامى»، أو الاعتراض على خط مسجل باسم شخص دون علمه

كما تطالب بعدم جمع أو معالجة أو الاحتفاظ بالبيانات البيومترية لهذه الأغراض ما لم يوجد أساس قانوني محدد يجيز ذلك، مع إثبات ضرورة الإجراء وتناسبه وعدم وجود وسيلة أقل تدخلًا يمكن أن تحقق الهدف نفسه

وتدعو كذلك إلى توفير إجراءات غير بيومترية فعالة لجميع المستخدمين، وإتاحة التحقق الحصري، وتوفير الدعم اللازم لكبار السن والأشخاص ذوي الإعاقة وغير القادرين على التعامل مع الوسائل الرقمية

نشر نتائج التحقيقات في وقائع التسجيل غير المصرح به

ومن بين المطالب التي طرحتها المنظمات نشر نتائج التحقيقات المتعلقة بتسجيل الخطوط دون علم أصحابها، في صورة مجمعة تحافظ على خصوصية المتضررين

وتريد المنظمات أن تتضمن النتائج عدد الحالات التي ثبتت صحتها، والمراحل التي وقع فيها الخل، والأدوار التي لعبتها منافذ البيع والموظفون والوكلاء وحسابات وأجهزة التفعيل، فضلًا عن الإجراءات الرقابية التي جرى اتخاذها لمنع تكرار هذه الوقائع

وترى أن الكشف عن طبيعة الخل يمثل عنصرًا أساسيًا لتقييم مدى الحاجة إلى إجراءات إضافية، بدلًا من اعتماد حلول واسعة النطاق دون نشر تشخيص واضح للمشكلة

سجلات تدقيق ومراقبة داخل شركات الاتصالات

وتقترح المنظمات إلزام شركات الاتصالات بإنشاء سجلات تدقيق محمية من التعديل أو الحذف لكل عملية تسجيل أو نقل ملكية أو استبدال لخطوط المحمول

ويجب، وفق المطالب، أن تسمح هذه السجلات بتتبع كل معاملة، وربطها بنقطة البيع وحساب الموظف أو الوكيل وجهاز التفعيل المستخدم وتوقيت تنفيذ العملية وأي تعديلات لاحقة عليها

كما تطالب بمراجعة صلاحيات الوصول داخل أنظمة الشركات، وقصرها على الموظفين الذين تقتضي طبيعة عملهم ذلك، مع تسجيل عمليات الدخول والتعديل بما يسمح بتحديد المسؤولية عن أي استخدام غير مشروع لبيانات المشتركين أو سجلات الخطوط

وتدعو أيضًا إلى استخدام أنظمة لرصد الأنماط غير المعتادة في تسجيل الخطوط، بما يسمح باكتشاف العمليات التي قد تشير إلى إساءة استخدام حسابات الموظفين أو الوكلاء أو أجهزة التفعيل

إخطار فوري عند تسجيل خط جديد

ومن بين المقترحات المطروحة أن يتم إخطار المواطن فور استخدام بياناته في تسجيل خط جديد أو نقل ملكية خط أو استبداله

وترى المنظمات أن الإخطار المباشر يمكن أن يمنح صاحب البيانات فرصة لاكتشاف أي معاملة لم يجرها، ووقفها أو الاعتراض عليها في أسرع وقت ممكن

كما تطالب بإنشاء آلية مجانية وسريعة وموثقة للاعتراض على الخطوط المسجلة دون علم أصحاب البيانات، مع إلزام شركات الاتصالات بتصحيح السجلات غير الدقيقة وتوفير سبل انتصاف فعالة للمتضررين

وفي الحالات التي يثبت فيها وقوع ضرر، تطالب المنظمات بإتاحة التعويض للمتضررين، وعدم الاكتفاء بمجرد إزالة الخط غير المصرح به من بيانات المواطن

دعوة للشفافية قبل إطلاق أي نظام بيومتری

طالبت المنظمات كذلك بنشر البنية القانونية والتقنية الكاملة لأي نظام للتحقق البيومتری تعتزم السلطات المصرية اعتماده قبل تشغيله

وتشمل هذه المعلومات، وفق البيان، تحديد نوع البيانات التي ستتم معالجتها، ومصدر البيانات المرجعية المستخدمة في المطابقة، ومكان إجراء عمليات المعالجة والتخزين، والجهات التي يمكنها الوصول إلى البيانات، ومدد الاحتفاظ بها وإجراءات حذفها

كما تشمل تحديد ضوابط مشاركة البيانات وربطها بقواعد بيانات أخرى، وآليات المراجعة البشرية، ووسائل التظلم والطعن في الحالات التي تفشل فيها عملية المطابقة البيومترية

وترى المنظمات أن هذه التفاصيل ليست مسائل تقنية هامشية، وإنما تمثل جزءًا أساسيًا من تقييم المخاطر المترتبة على أي نظام جديد لجمع البيانات الشخصية الحساسة

المنظمات الموقعة:

1. أكسس ناو
2. أنسم للحقوق الرقمية
3. إيجيب وايد لحقوق الإنسان
4. الأصوات العالمية
5. الجبهة المصرية لحقوق الإنسان
6. المبادرة المصرية للحقوق الشخصية (EIPR)
7. المركز الإقليمي للحقوق والحريات
8. المفوضية المصرية للحقوق والحريات
9. المنتدى المصري لحقوق الإنسان

10. ديجيتال أكشن

11. سمكس

12. سيناء لحقوق الإنسان

13. شبكة المنظمات غير الحكومية العربية للتنمية

14. مؤسسة دعم القانون والديمقراطية

15. مؤسسة مسار

16. مركز النديم لإعادة تأهيل ضحايا العنف والتعذيب

17. مشروع التنظيم والتنمية والتعليم والبحث (PODER)

18. معهد القاهرة لدراسات حقوق الإنسان

19. منصة اللاجئين في مصر