

دون علم أصحابها عصابات توّط مواطنين في جرائم مخدرات ونصب بخطوط محمول مسجلة بأسمائهم



السبت 8 أغسطس 2026 12:00 م

رصدت تقارير صحفية وبيانات أمنية 3 وقائع في الشرقية وبورسعيد والقاهرة، استغل خلالها متهمون خطوطًا مسجلة ببيانات آخرين في المخدرات والنصب والاتجار بالشرائح، فانتهى أبرياء مفترضون أمام الاتهامات والأحكام والملاحقات

وتكشف الوقائع أن خلل تسجيل الخطوط لم يعد خطأ فنيًا عابرًا، بل بوابة تدفع مواطنين إلى ساحات المحاكم بينما يتحرك الجناة خلف هويات مستعارة، في مشهد يحمل الشركات والجهات الرقابية مسؤولية التقاعس عن حماية الناس

وبحسب بيان الجهاز القومي لتنظيم الاتصالات، فإن ظهور خط باسم مواطن لا يجعله مسؤولًا تلقائيًا عن استخدامه غير المشروع، ما دامت التحقيقات تثبت أن الرقم لم يكن في حيازته الفعلية وقت ارتكاب الجريمة

وفي المقابل، دعا الجهاز المواطنين إلى مراجعة الأرقام المسجلة بأسمائهم عبر تطبيقه الرسمي، وتقديم شكوى عند اكتشاف رقم مجهول، مؤكدًا فحص إجراءات التسجيل ومحاسبة الشركة عند ثبوت مخالفتها للضوابط المقررة

خط قاد إلى المؤبد

بدأت الواقعة الأولى في الشرقية عندما قال طالب بكلية الحاسبات والمعلومات إنه استخرج خطأ باسمه لمساعدة معرفة تعمل في المبيعات، ثم تركه دون استخدام، قبل أن يظهر الرقم لاحقًا في تحقيقات قضية مخدرات

ووفقًا لرواية الطالب وأسرته، ارتبط الخط بشحنة مواد مخدرة ضبطت داخل سيارة نقل محملة بالبصل قرب نفق الشهيد أحمد حمدي، وصدر ضده حكم غيابي بالسجن 25 عامًا رغم نفيه أي صلة بالواقعة

وعقب علمه بالحكم، سلم الطالب نفسه لجهات التحقيق طالبًا إعادة إجراءات المحاكمة، وقال إنه يمتلك مستندات تثبت وجوده بعيدًا عن مكان الضبط، بينما تبقى براءته أو إدانته مسألة تفصل فيها المحكمة بعد فحص الأدلة

وفي هذا الإطار، حذر خبير أمن المعلومات محمود فرج من السماح للآخرين باستخدام البيانات الشخصية أو استخراج خطوط بأسماء الغير، موضّحًا أن المجاملة قد تتحول إلى أزمة قانونية وأمنية يصعب الخروج منها

وبالتالي، لا تعفي موافقة المواطن على استخراج الشريحة الشركة من التحقق من تسليمها إليه أو توثيق انتقال حيازتها، لأن التسجيل الورقي المنفصل عن المستخدم الفعلي يسمح للجناة باستعارة هوية قانونية جاهزة

كما أن الحكم الغيابي الذي لاحق الطالب يوضح حجم الضرر الممكن قبل اكتمال التحقق من الحيازة، إذ قد يفقد المتضرر دراسته وسمعته وحريته، ثم يتحمل وحده عبء إثبات أنه لم يستخدم الرقم

لذلك، يصبح الاحتفاظ بسجلات التفعيل وموقع التسليم وهوية الموظف والجهاز المستخدم ضرورة قضائية، وليس مجرد إجراء تجاري، لأن هذه البيانات قد تفصل بين صاحب بطاقة سجل الخط باسمه وبين الجاني الذي استعمله فعليًا

أما الواقعة الثانية، فبدأت عندما اكتشف محمد صلاح الشاذلي في بورسعيد وجود 8 خطوط مسجلة باسمه لدى شركة لم يكن عميلاً لديها، وقال إن الخطوط استُخدمت في عمليات احتيال بلغت اتهاماتها نحو 40 مليون جنيه

وإضافة إلى ذلك، ذكر الشاذلي أن 3 من الخطوط ارتبطت بمحافظ مالية إلكترونية، واستُخدمت الأرقام في إنشاء حسابات وهمية وإجراء مراسلات لاستدراج الضحايا، قبل أن تتجه الشكاوى والالتزامات نحوه باعتباره المالك المسجل

ومن جراء ذلك، صدر ضده في إحدى القضايا حكم بالحبس 3 أشهر، وظهرت السابقة في صحيفته الجنائية، وفق روايته، بينما قال إنه تعرض لمضايقات من متضررين توجهوا إلى منزله مطالبين بأموالهم

وفيما بعد، أقرت الشركة بأن الخطوط مسجلة باسمه من دون وجود عقود موثقة، وأغلقتها وبدأ قسمها القانوني فحص الواقعة، لكن الإغلاق المتأخر لم يمنح الأحكام والبلاغات والضرر الذي لحق باسمه وأسرته

ومن جانبه، حذر خبير التكنولوجيا وأمن المعلومات محمد عزام من أن الخطوط مجهولة المستخدم قد تورط أصحاب البيانات في جرائم لا يعلمون عنها شيئاً، ودعا إلى تقديم شكوى فورية بمجرد اكتشاف أي رقم غريب

ومن ثم، تكشف واقعة بورسعيد أن مسؤولية الحماية لا يجوز نقلها كاملة إلى المواطن، لأن الشركة التي قبلت 8 عمليات تسجيل بلا عقود موثقة كانت تملك القدرة التقنية والإدارية على اكتشاف النمط قبل وقوع الكارثة

غير أن بيان الجهاز يعيد ضبط المسألة قانونياً بالتأكيد أن بيانات التسجيل ليست وحدها دليل الإدانة، وأن المسؤولية تحددها جهات التحقيق والقضاء وفق الحياة الفعلية والاتصالات والتحويلات ومواقع الاستخدام وبقية الأدلة المرتبطة بالجريمة

238 شريحة هويات الغير

وفي الواقعة الثالثة، ضبطت أجهزة الأمن في منطقة الموسكي بالقاهرة مالك منفذ هواتف يبيع خطوطاً مفعلة ببيانات أشخاص آخرين، وعثرت بحوزته على 238 شريحة ومبالغ قالت إنها من متحصلات نشاطه غير المشروع

وبعد مواجهته، أقر المتهم وفق بيان الضبط بالحصول على الشرائح من موظف بإحدى شركات الاتصالات ومالك محل هواتف، ثم أُلقت الأجهزة الأمنية القبض عليهما، وقالت إنهما اعترفا بالمشاركة في الواقعة محل التحقيق

وفوق ذلك، تكشف مشاركة موظف من داخل المنظومة، بحسب التحريات، أن الخطر لا يقتصر على سرقة صورة بطاقة، بل يمتد إلى إساءة استخدام صلاحيات العمل وقواعد بيانات المشتركين لتحقيق أرباح من بيع هويات المواطنين

وفي ضوء ذلك، قال خبير التكنولوجيا شاكر الجمل إن التحقق البيومتري يوفر طبقة أساسية لمطابقة الهوية ويقلل فرص التزوير وسرقة البيانات، عبر تصوير البطاقة ومضاهاة وجه طالب الخدمة بالهوية المسجلة

وبناءً عليه، أعلن الجهاز استمرار تطوير ضوابط تسجيل وتفعيل الخطوط وتشديد الرقابة على الشركات وتطبيق أدوات التحقق البيومتري، لكن نجاح المنظومة يظل مرهوناً بمنع تجاوز الموظفين ومراجعة العمليات غير المعتادة لحظياً

وعلى صعيد المسألة، يجب ألا يتوقف التعامل مع المخالفة عند إغلاق الأرقام، بل يتطلب تدقيقاً شاملاً في كل خط باعه المتهمون، وتحديد الجرائم المرتبطة به، وإبلاغ أصحاب البيانات وتصحيح سجلاتهم وتعويض من تضرر منهم

أخيراً، تثبت الوقائع الثلاث أن مطالبة المواطن بالفحص الدوري إجراء وقائي ضروري لكنه ليس بديلاً عن الرقابة، فحماية الهوية واجب أصيل على الشركات والجهاز، وأي تسجيل بلا تحقق صارم قد يصنع متهماً بريئاً ويمنح مجرماً غطاءً مجانياً