25 ألف فيديو و10 آلاف صورة.. تحقيق يكشف فضائح جنسية تهز أركان جيش الاحتلال

الاثنين 8 يونيو 2026 04:00 م

كشف تحقيق استقصائي نشرته صحيفة يديعوت أحرنوت العبرية، عن ثغرة أمنية واسعة داخل جيش الاحتلال الإسرائيلي، بعد وقوع آلاف الجنود والضباط ضحية حسابات وهمية استدرجتهم إلى تصوير مقاطع ذات طابع جنسي، ثم نشرتها عبر منصات الإنترنت وتطبيق تليجرام.

وتتجاوز خطورة القضية حدود الفضيحة الشخصية، لأن المواد المنشورة تضمنت صورًا ومقاطع لجنود بزيهم العسكري وداخل مواقع خدمة، بما يفتح الباب أمام الابتزاز، وتسريب المعلومات، واحتمال استغلال الجنود في عمليات تجنيد أو ضغط أمني من جهات معادية للاحتلال.

حسابات وهمية تصطاد الجنود من داخل الخدمة

يرصد التحقيق نمطًا منظمًا يقوم على إنشاء حسابات مزيفة لشابات عبر مواقع التواصل وتطبيقات المحادثة، ثم تبدأ هذه الحسابات في بناء تواصل تدريجي مع الجنود، قبل دفعهم إلى محادثات وصور ومقاطع يجري تسجيلها دون علمهم.

وبحسب ما ورد في التحقيق، لم تقتصر المقاطع على جنود صغار أو محادثات خاصة، بل شملت ضباطًا وجنودًا في أماكن حساسة، بينها مواقع حراسة وغرف عمليات وداخل دبابات، وهو ما حوّل السلوك الفردي إلى تهديد أمني مباشر.

وتظهر خطورة الأسلوب في أن الحسابات الوهمية لا تطلب أسرارًا عسكرية في البداية، بل تبدأ بخداع اجتماعي بسيط، ثم تنتقل إلى جمع مواد شخصية يمكن استخدامها لاحقًا للضغط على أصحابها أو كشف هوياتهم.

كما يشير التحقيق إلى أن بعض القنوات نشرت المواد مرفقة بصور شخصية ومعلومات عن الخدمة العسكرية، وهو ما يضاعف الضرر، لأن الجندي لا يصبح معرضًا للفضيحة فقط، بل يتحول إلى هدف معروف يمكن تتبعه.

وفي هذا السياق، تبدو الأزمة أكبر من إخفاق أخلاقي داخل الجيش، لأنها تكشف ضعفًا في وعي الجنود الرقمي، وفشلًا في حماية العناصر المنتشرة في مواقع حساسة من عمليات خداع إلكتروني بدائية لكنها مؤثرة.

آلاف المقاطع وقنوات تليجرام تكشف حجم الاختراق

يكشف التحقيق أن مجموعة واحدة نشطة منذ نحو 3 سنوات احتوت على أكثر من 16 ألف مقطع ونحو 10 آلاف صورة، بينما ضمت مجموعة أخرى أكثر من 4 آلاف مقطع، ونشرت مجموعة إضافية نحو 5 آلاف مقطع وألفي صورة.

وتوضح هذه الأرقام أن القضية لا تتعلق بحالات فردية معزولة، بل بسوق رقمي كامل يعيد تدوير المواد ونشرها لجمهور واسع، حيث تتحول مقاطع الجنود إلى محتوى قابل للبيع والمشاهدة والمساومة.

وتشير المعطيات إلى وجود طريقتين أساسيتين للإيقاع بالجنود، الأولى تعتمد على حسابات مزيفة عبر إنستغرام وتطبيقات مشابهة، والثانية تعتمد على مواقع محادثات فيديو مع غرباء، تبدأ بواجهة تعارف ثم تتحول إلى تسجيل واستغلال.

وتبرز أسماء حسابات وهمية مثل مايا بوصفها نموذجًا لطريقة الخداع، إذ تستخدم صورًا مسروقة وتفاعلًا مصطنعًا يمنح الجندي شعورًا بأن الطرف الآخر حقيقي، رغم أن الحساب لا يملك نشاطًا طبيعيًا.

ولأن بعض المقاطع جرى تصويرها داخل قواعد ومرافق عسكرية، فإن الضرر لا يقتصر على صاحب المقطع، بل يشمل كل ما يظهر في الخلفية من معدات وممرات وأنظمة حراسة ومكاتب ومواعيد وجود الأفراد.

وحذر خبير في الأمن السيبراني والأمن القومي، بحسب التحقيق، من أن ظهور منظومات داخل دبابة أو عدد الجنود في مناوبة واحدة قد يوفر معلومات استخباراتية مهمة تساعد في التخطيط لهجمات أو جمع بيانات تشغيلية.

ابتزاز أمني يطارد جيشًا اعتاد الحرب الرقمية

ينص القانون الإسرائيلي على أن نشر هذه المواد قد يشكل جريمة جنسية تصل عقوبتها إلى السجن 5 سنوات، لكن الخطر الأشد في حالة الجنود يرتبط بإمكانية تحويل الفضيحة إلى أداة ابتزاز أمني.

وبحسب التحقيق، يمكن لجهات معادية الحصول على المقاطع ثم التواصل مع الجنود وطلب معلومات مقابل عدم النشر، أو دفعهم تدريجيًا إلى التعاون، بما يجعل قاعدة البيانات الضخمة قنبلة مؤجلة داخل المؤسسة العسكرية.

وتعيد هذه القضية إلى الواجهة تحذيرات قديمة داخل جيش الاحتلال من الحسابات الوهمية، إذ أعلن الجيش في نوفمبر 2023 أنه كشف شبكة حسابات مزيفة استهدفت جنوده عبر إنستغرام بهدف جمع معلومات عن الوحدات والتحركات.

كما نشرت تقارير إسرائيلية في ديسمبر 2023 تفاصيل عن شبكة صور رمزية استخدمت حسابات لشابات وهميات تتحدث العبرية، وتواصلت مع جنود عبر رسائل ومكالمات نصية ومرئية، واتهم الجيش جهات مرتبطة بحماس ودول مدعومة من إيران بتشغيلها.

وتكشف المقارنة بين تلك الشبكات والتحقيق الجديد أن التحذيرات لم توقف الظاهرة، بل تطورت الأدوات من محاولة استخراج معلومات مباشرة إلى إنتاج مواد شخصية قابلة للتخزين والابتزاز وإعادة الاستخدام.

ومن جانبه، قال جيش الاحتلال إن النتائج التي أثيرت في التحقيق قيد الفحص، وإنه ينظر بخطورة بالغة إلى أي اعتداء على خلفية جنسية، لكن الرد الرسمي لا يجيب عن سؤال أوسع يتعلق بفشل منظومة أمن المعلومات.

وفي النهاية، تكشف الفضيحة أن جيش الاحتلال لا يواجه فقط تهديد الصواريخ والجبهات المفتوحة، بل يواجه اختراقًا داخليًا ناعمًا يبدأ من شاشة هاتف وينتهي بملفات ابتزاز قد تكشف مواقع، وتربك ضباطًا، وتضع المؤسسة العسكرية أمام عجزها الرقمي.