الحيز المدني

موجز

الاختراق وبرامج التجسس

بينما يزعم أن برامج التجسس تُستخدم لمكافحة الإرهاب والجريمة، إلا أنها غالبًا ما تُستعمل لأسباب غير مشروعة، من بينها قمع الآراء الناقدة أو المعارضة، واستهداف من يعبرون عنها، بمن فيهم الصحفيون والمعارضون السياسيون والمدافعون عن حقوق الإنسان.

HC report on the right to privacy in the digital age (A/HRC/51/17, 2022)

الاختراق هو نوع من التدخل السري في الأجهزة الرقمية، مثل الحواسيب المحمولة والهواتف الذكية، يتيح الوصول إلى المعلومات الشخصية والسرية دون تفويض من المستخدمين أو علمهم أو علم مالك الجهاز أو الشركة المصنعة. وعلى الرغم من أن الاختراق قد يكون قانونيًا في بعض الحالات، إلا أنه غالبًا ما يُستخدم **لأغراض المراقبة غير القانونية** من خلال أدوات التجسس. ورغم عدم توفر بيانات دقيقة، **يبدو أن حوادث استخدام برامج التجسس من قبل جهات حكومية أو مرتبطة بالدول آخذة في الازدياد.**

يتيح الاختراق لأغراض المراقبة للمتسلل **الحصول على تفاصيل تتعلق بآراء الهدف، وأنشطته، وصحته، وغيرها من المعلومات الحساسة المحتملة**. ويمكن لأدوات التجسس تشغيل الكاميرات والميكروفونات الخاصة بالأجهزة أو حذف البيانات المخزنة أو التلاعب بها بطرق أخرى.

تتوفر برامج التجسس عالية الاختراق على نطاق واسع في السوق العالمية. وتمنح هذه الأدوات السلطات وغيرهم صلاحيات واسعة للتعدي على خصوصية الأفراد والوصول إلى بياناتهم السرية. ويمكن استخدامها للوصول الكامل إلى جميع أجزاء الجهاز، بما في ذلك الكاميرا، والميكروفون، وبيانات الموقع، والرسائل، والصور، والتطبيقات، ويمكن تثبيتها دون علم الهدف.



كيف يمكن لاستخدام برامج التجسس أن يقوض حقوق الإنسان؟

• يمكن أن يؤدي إلى كشف معلومات شديدة الخصوصية عن الأهداف، **مما يشكل انتهاكًا جسيمًا للخصوصية.** كما قد يؤدي إلى الرقابة الذاتية نتيجة التأثير المرهب على حرية التعبير الناجم عن التهديد بالإضرار بالسمعة أو التسبب بأذى آخر.

• يؤثر استخدام برامج التجسس على مجموعات وسكان مختلفين بطرق متفاوتة، وقد يؤدي إلى **نتائج تمييزية.** فعلى سبيل المثال، أُثبت أن كشف المعلومات الشخصية قد يقوض فرص النساء المرشحات للمناصب السياسية. كما أن مستوى التطفل الشديد يمكن أن يسبب صدمات نفسية ويؤثر على الصحة العقلية للضحايا، وعائلاتهم، ومعارفهم.

• تم ربط برامج التجسس بحالات **اعتقال واحتجاز تعسفي، وتعذيب، وقتل خارج نطاق القانون**، بما في ذلك استهداف مدافعين عن حقوق الإنسان، وصحفيين، وفاعلين سياسيين. وقد تُستخدم لانتهاك حقوق المحاكمة العادلة والإجراءات القانونية الواجبة، من خلال تمكين المتسللين من التلاعب بالأجهزة المستهدفة وتلفيق الأدلة.

• **الأشخاص الذين يتواصلون مع الفرد المستهدف أو يتواجدون بالقرب منه ماديًا يكونون أيضًا عرضة للخطر.**

STAND UP FOR HUMAN RIGHTS
#STANDUP4HUMANRIGHTS

UNITED NATIONS HUMAN RIGHTS
OFFICE OF THE HIGH COMMISSIONER

الحيز المدني

موجز

> مع الإعراب عن بالغ القلق بشأن استخدام الأدوات التكنولوجية التي طورتها صناعة المراقبة الخاصة، واختراق الأجهزة والأنظمة، واعتراض وتعطيل الاتصالات، وجمع البيانات، بما يؤدي إلى التدخل في الحياة المهنية والخاصة للأفراد، بما في ذلك أولئك المنخرطين في تعزيز والدفاع عن حقوق الإنسان والحريات الأساسية، من صحفيين وعاملين في وسائل الإعلام، وذلك في انتهاك أو إساءة لاستخدام حقوقهم الإنسانية، وبشكل خاص الحق في الخصوصية.
>
> GA Resolution on the right to privacy in the digital age (A/RES/77/211, 2022)

لقد اعترفت الأمم المتحدة والعديد من المنظمات الإقليمية بأن الطبيعة التطفلية والعشوائية لأدوات التجسس تمثل تهديدات فريدة وخطيرة للخصوصية وغيرها من حقوق الإنسان. وبناءً على ذلك، يوجب قانون حقوق الإنسان على الدول أن تضمن ما يلي:

• يجب أن يكون أي اختراق تقوم به الدولة مصرحا به قانونيًا من قبل محاكم مستقلة، وأن يستوفي متطلبات قانون حقوق الإنسان الدولي، **ويشمل ذلك أن يكون مبنيًا على القانون، ويهدف إلى غرض مشروع، وأن يكون ضروريًا** ومتناسقًا مع مبدأ عدم التمييز وبنسبة معقولة.

• **عدم تقويض جوهر الحق في الخصوصية.**

الإجراءات الأساسية لإنهاء الانتهاكات:

يجب على الشركات التي تقدم أدوات المراقبة أن:

• **تجري العناية الواجبة في مجال حقوق الإنسان** وتضمن المساءلة وتقديم التعويضات، وفقًا لمبادئ الأمم المتحدة التوجيهية للأعمال وحقوق الإنسان؛

• **تمتنع عن بيع برامج التجسس للدول التي لديها سجل في المراقبة غير القانونية؛**

• **وضع إجراءات تصعيدية** عندما يكون هناك خطر نشوب صراع عنيف.

For more details, see our report A/HRC/51/17 on the right to privacy in the digital age.

يجب على الدول:

• **الحد من توفر تكنولوجيا المراقبة التدخلية** من خلال فرض وقف مؤقت على بيع ونقل واستخدام أدوات الاختراق حتى يمكن ضمان الامتثال لحقوق الإنسان؛

• **إدراج الحق في الخصوصية في التشريعات** وضمان تنظيم القانون الوطني لاستخدام الاختراق بشكل صارم، مع إدخال ضمانات لحماية سرية المستخدمين؛

• **تعزيز وحماية** التشفير الشامل (end-to-end encryption) والتشريع ضد مسح البيانات على جانب العميل (client-side scanning)؛

• **استخدام الاختراق فقط كملاذ أخير**، بعد الحصول على موافقة مسبقة من جهة قضائية ومراقبة مستقلة صارمة، وتقييد الاستخدام لمنع أو التحقيق في أعمال محددة تشكل تهديدات خطيرة للأمن الوطني أو جرائم خطيرة، مع توجيه الاستخدام بشكل ضيق نحو الشخص المشتبه بارتكاب تلك الأفعال. يجب توضيح من هي الجهات المسموح لها باستخدام الاختراق والشفافية حول من يستخدمه، وحصر الوصول إلى البيانات على الأشخاص المسئولين بالاستجابة للتهديد المطروح.

• إجراء **تقييمات منتظمة وشاملة لتأثيرات حقوق الإنسان**، وتقييم المخاطر المحتملة والأضرار الأمنية وسلامة الجهاز المستهدف والبيانات بشكل منهجي.