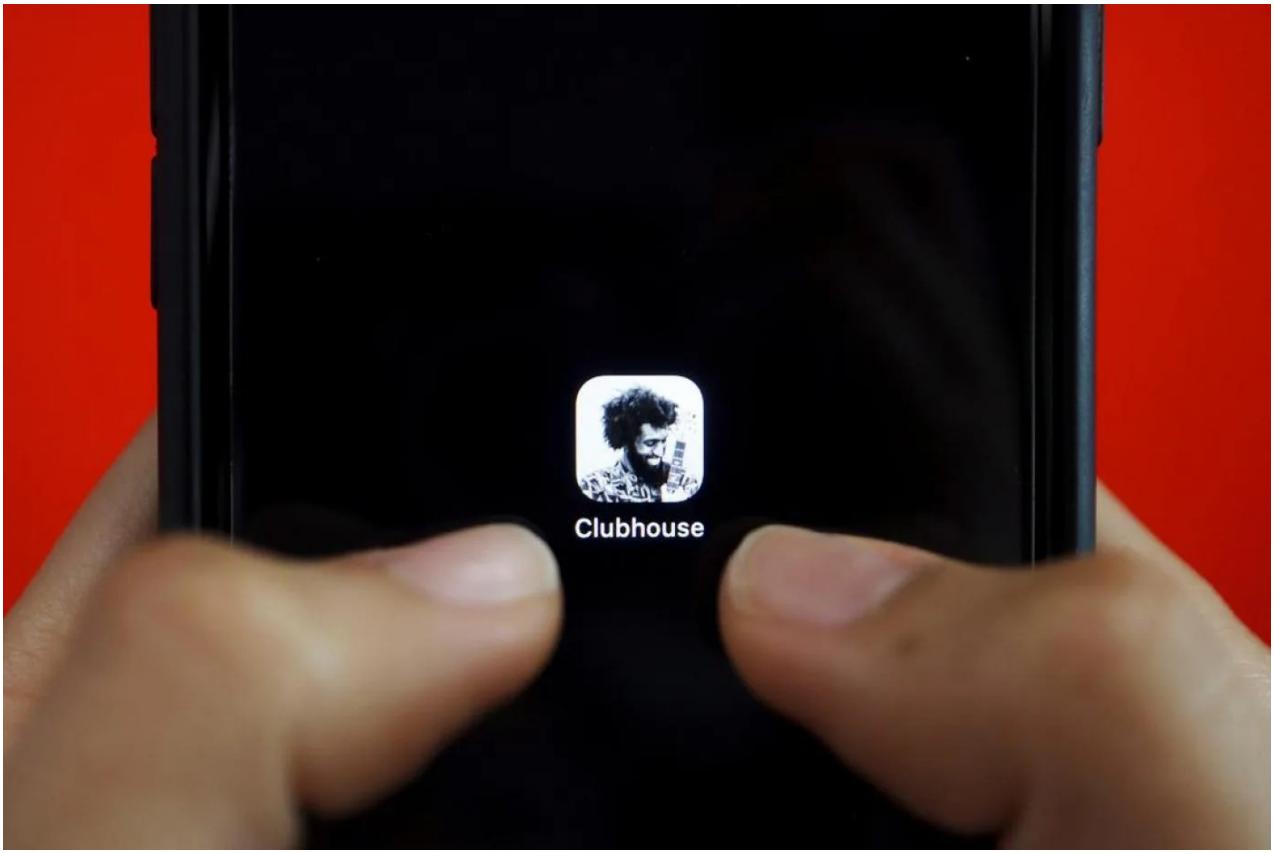
فرانك أندروز | نشر في ١٢ مارس ٢٠٢١,

"كلوب هاوس".. هل المستخدمون في مأمن من الاستبداد الرقمي؟



ترجمة وتحرير: نون بوست

لما يوفره من وعود التحرر، يبدو أن تطبيق "كلوب هاوس" استفاد من توق الكثيرين في منطقة الشرق الأوسط إلى منفذ للتعبير عن مواقفهم السياسية وآرائهم الشخصية. في شباط/ فبراير، بلغ عدد مستخدمي التطبيق للدردشة الصوتية، الذي يسمح للمستخدمين بإنشاء أو الانضمام إلى غرف الدردشة بناء على مواضيع من اختيارهم، حوالي عشرة ملايين مستخدم من جميع أنحاء العالم – مسجلًا زيادةً بنحو خمسة أضعاف مقارنة بالشهر السابق، وذلك في فترة قصيرة منذ إطلاقه في نيسان/ أبريل 2020.

لجأ العديد من سكان منطقة الشرق الأوسط إلى تطبيق "كلوب هاوس"، هربا من الاستبداد الرقمي الذي جعل الكثيرين يعيشون في حالة من الخوف الدائم من المراقبة المستمرة. وهو متاح للأجهزة التي تعمل بنظام التشغيل "آي أو إس" فقط، وقد تصدّر العديد من قوائم التحميل الوطنية.

من مصر إلى عُمان، ومن تركيا إلى السعودية، بدأ المستخدمون بإناء غرف الدردشة لمناقشة مواضيع مختلفة من السياسة والهوية والجنس والنظام الذكوري والدين والعنصرية وحتى تنسيق الاحتجاجات. وقد أُشيدَ بهذا التطبيق باعتباره ملاذًا لحرية التعبير. ومؤخرًا، قال أحد الكتّاب في تقرير نشره "بلومبرغ" إن "كلوب هاوس قد يساعد أخيرا في تحقيق تطلعات مظاهرات الربيع العربي التي مضى عليها عقد".

رغم الحماس الذي أبداه المستخدمون، اتضح أن "كلوب هاوس" ليس آمنا حقًا. يجمع التطبيق كميات كبيرة من بيانات المستخدمين، الذين يمكن التعرف عليهم بسهولة، ولا يوجد ما يمنع الجهات الأخرى – بما في ذلك المخبرين الموالين للحكومة أو الشرطة السرية – من مراقبة واستقاء المستخدمين الذين

يتحدثون عن مواضيع محظورة وحساسة. والأسوأ من ذلك، قد تضطر الشركة إلى مشاركة البيانات التي تجمعها مع سلطات إنفاذ القانون.

في حديثه مع موقع "ميدل إيست آي"، قال الباحث في منظمة العفو الدولية للتكنولوجيا جو ويستبي: "أعتقد أن سكان المنطقة بحاجة إلى توخي الحذر الشديد عند استخدام التطبيق. فمن شأن وعود المنصات الأولى لفتح المجال للتواصل بين الناس وإتاحة قدر أكبر من حرية التعبير أن تخرج عن السيطرة بسرعة".

بيانات لا حصر لها

يحتفظ تطبيق "كلوب هاوس" بقدر هائل من المعلومات حول مستخدميه. إلى جانب الاسم والرقم، تتضمن البيانات التي يتم جمعها معلومات حول الجهاز المستخدم والموقع وعنوان بروتوكول الإنترنت، وما يستمع إليه المستخدمون، ووقت دخولهم للتطبيق والمدة التي يقضونها عليه، و"الإجراءات التي يتخذها" المستخدمون، وذلك حسب ما تبينه سياسة خصوصية التطبيق. عمليًا، يعني ذلك أنه بإمكان الشركة جمع بيانات بخصوص أي شيء يفعله المستخدمون على منصة "كلوب هاوس".

يسجل التطبيق المحادثات الصوتية أيضا، مدعيًا أن السجلات الصوتية تحفظ فقط في حالة قيام أحد المستخدمين بالإبلاغ عن حادث، ويتم حذفها إن لم يتم ذلك. ومؤخرا، نشر مرصد ستانفورد المختص في أبحاث الإنترنت منشورا أشار فيه إلى أنه "من المستبعد جدًا" أن تكون السجلات الصوتية في "كلوب هاوس" قائمة على التشفير الطرفي، مما يجعلها في متناول الآخرين خارج المحادثة.

يستخدم كلوب هاوس ملفات تعريف الارتباط وتقنيات أخرى لتتبع نشاطات المستخدم في أي مكان آخر على الإنترنت – حتى عندما يكون التطبيق مغلقًا

علاوة على ذلك، إذا قام شخص ما بتسجيل الدخول إلى التطبيق باستخدام منصة أخرى مثل "تويتر" أو "فيسبوك"، يجوز أن "يجمع كلوب هاوس المعلومات المرتبطة بهذا الحساب وتخزينها وتحديثها بشكل دوري"، وذلك حسب مرصد ستانفورد.

إن ما يفعله التطبيق – أو ما قد يفعله في المستقبل – بهذا الكمّ من البيانات غير واضح، حيث لم يصرح مالكوه بمخططاتهم حول كيفية كسب المال منه بعد. يُقال إن منصة التطبيق تريد كسب الإيرادات من خلال الإكراميات والاشتراكات وتذاكر الفعاليات المختلفة، بدلاً من الإعلانات، لكن سياسة الخصوصية تنص على أنها قد تشارك البيانات مع قائمة طويلة من شركات الطرف الثالث، بما في ذلك أصحاب الإعلانات، وذلك "دون إشعار المستخدم".

يستخدم "كلوب هاوس" ملفات تعريف الارتباط وتقنيات أخرى لتتبع نشاطات المستخدم في أي مكان آخر على الإنترنت – حتى عندما يكون التطبيق مغلقًا – لإرسال الإعلانات.

سريّة محدودة

إن إمكانية اقتناء أي شركة لهذا الكم من المعلومات حول المستخدمين أمر يبعث على القلق. قد يكون اختراق بيانات "كلوب هاوس" أو بيانات أي طرف ثالث يشاركه التطبيق معلومات المستخدمين كارثيًا. كتب "كلوب هاوس" في سياسة الخصوصية الخاصة به: "إننا نتخذ تدابير معقولة تجاريًا لضمان التزام مزودي الخدمة لدينا بمعايير الأمان التي نطبقها على بياناتك الشخصية".

يحتوي "كلوب هاوس" على برنامج مكافآت العثور على الأخطاء، حيث تتم مكافأة المتسللين على الكشف عن الثغرات الأمنية، دون الحاجة إلى اللجوء لاختراق البيانات على غرار تسريبات موقع "أشلي ماديسون"، بيد أنه يمكن التعرف على المستخدمين بسهولة لأن التطبيق يلزم المستخدم باعتماد

الاسم والهوية الحقيقيين.

يحتفظ "كلوب هاوس" بحق "إلزام المستخدمين بتقديم إثبات للهوية" في حالة إبلاغ أحدهم عن اعتماد مستخدم آخر اسمًا مزيفًا. يساهم الحد من سريّة الهوية إلى التقليل من عدد روبوتات الإنترنت والمتصيدين، ولكنه قد يتسبب في امتناع المستخدمين عن قول أي شيء قد يعتبر تحديًا للمعايير الاجتماعية. كما أنه يجعل المستخدمين عرضة للمراقبة من قبل عملاء الدولة.

ذكرت مديرة الحقوق الرقمية في الشرق الأوسط وشمال إفريقيا في مؤسسة "أكسس ناو"، مروة فطافطة، أنه "من الشائع جدًا أن تقوم الحكومات بمراقبة مواقع التواصل الاجتماعي والاستماع إلى محادثات الناس. أظن أن الحكومات وعملاءها متواجدون بالفعل على التطبيق، ويستمعون لما يقال عليه". وتابعت: "حسب رأيي، لن يطول الأمر حتى نسمع أن شخصًا ما تم اعتقاله بسبب ما تفوه به عبر المنصة".

ويرى ويستبي أنه "بمجرد أن تكتسب المنصات التقنية بعض الشعبية، فإنها قد تصبح ضحية لنجاحها، نظرا لأن السلطات تستهدف بسرعة على كل ما يُنظر إليه كقناة جديدة وسريّة للاتصالات".

يكمن الخطر الآخر في استقاء المعلومات من قبل المستخدمين المحتالين. فقد ظهرت حالات، كما حدث في السعودية على سبيل المثال، تم فيها تسجيل المحادثات الحساسة ونشرها عبر الإنترنت. وفي مصر، زعم برنامج تلفزيوني موالي للحكومة أنه اكتشف – وسجل – شبكة "إرهابية" في "كلوب هاوس".

لا يسمح "كلوب هاوس" للمستخدمين بتفعيل خاصية تسجيل لقطات الشاشة في شكل مقطع فيديو. وبعد اكتشاف بث مستخدم في الصين المحادثات في مكان آخر عبر الإنترنت، قام التطبيق بإضافة "إجراءات وقائية" للتصدي لحوادث مماثلة. لكن التطبيق يعترف بأنه "لا يمكن التحكم في تصرفات المستخدمين على المنصة الذين قد يلجؤون لاستخدام تطبيقات أو أجهزة تابعة لجهات خارجية لتسجيل أو تخزين أو مشاركة المحتوى أو الاتصالات دون موافقة مسبقة من المستخدمين الآخرين".

يوضح منشور مرصد ستانفورد طرقًا أخرى يمكن من خلالها التعرف على هوية مستخدمي التطبيق، بما في ذلك كيفية تتوافق المقاطع الصوتية الفردية مع معرفات مستخدم محددة. وقد علق "كلوب هاوس" على التقرير بالقول إنه يراجع ممارساته الأمنية وأن التطبيق "ملتزم بشدة بحماية البيانات وخصوصية المستخدم".

جهات الاتصال

قد تكون عائلات وأصدقاء مستخدمي "كلوب هاوس" معرضين لخطر الكشف عن الهوية أيضا. في الوقت الراهن، إن الطريقة الوحيدة للولوج إلى التطبيق هي من خلال تلقي دعوة. ولكن حتى يحظى المستخدم بشرف دعوة الآخرين، يطلب تطبيق "كلوب هاوس" النفاذ إلى جهات الاتصال الخاصة به – وهو ما يعدّ بمثابة مخاطرة كبيرة.

قالت مروة فطافطة إنه "من الشائع جدا أن تقوم الحكومات بمراقبة أقارب وأصدقاء النشطاء. ومهما كان حجم البيانات التي يمكنهم الوصول إليها، فسوف يأخذونها". وأضافت أنه في العديد من دول المنطقة، يتعيّن على المواطنين الاستظهار برقم الهوية الشخصية أو نسخة من جواز السفر عند شراء شريحة هاتف. لذلك، إن ربط الأسماء بأرقام على التطبيق يسهل على السلطات عملية تعقب.

إن تبادل جهات الاتصال بالدعوات يعني أنه في حال قام شخص ما بتنزيل تطبيق "كلوب هاوس" وسمح له بالنفاذ إلى قائمة جهات الاتصال الخاصة به، فإن التطبيق يستحوذ على كل بيانات الاتصال هذه، دون علم هؤلاء الأشخاص – الذين ربما لم يسمعوا عن التطبيق مطلقًا. قد تكون هذه الممارسة انتهاكا للوائح حماية البيانات العامة للاتحاد الأوروبي، ولكن هذا القانون لا يُطبّق في الشرق الأوسط.

تقول فطافطة إنه "لسوء الحظ، لا تعتبر حماية البيانات أولوية قصوى بالنسبة (للعديد من حكومات المنطقة). فإذا كنت تراقب مواطنيك وتتعقبهم بنشاط، فلن تكون مهتمًا بحماية بياناتهم. أينما كنت في أي بلد من بلدان الشرق الأوسط وشمال إفريقيا، فإنه ليس لديك أدنى فكرة كمواطن عمن لديه حق الوصول إلى بياناتك ومن يتشاركها. لذلك حتى إذا كنت تريد معالجة الوضع ورفض ذلك، فإن النتيجة تظل غير مضمونة".

تطبيق القانون

لعل أحد أكثر الأجزاء المقلقة في سياسة خصوصية تطبيق "كلوب هاوس" هو أن التطبيق قد يشارك بيانات المستخدم مع السلطات "في حال طُلب منه ذلك بموجب القانون، بما في ذلك الوفاء بمقتضيات الأمن القومي أو إنفاذ القانون". وقد يحدث هذا أيضا دون علم المستخدمين. وتنص سياسة الخصوصية على أنه "اعترافًا بالطابع العالمي للإنترنت، فإنك توافق على الامتثال لجميع القواعد والقوانين المحلية المتعلقة باستخدامك للشبكة، بما في ذلك ما يتعلق بالسلوك الإلكتروني والمحتوى

المقبول".

لكن فطافطة قالت إن المشكلة في ذلك تكمن في حقيقة أن "القوانين في المنطقة قمعية ومبهمة ومُصاغة بشكل عام، بطريقة يمكن من خلالها للحكومات أن تقوم بتأويل أي نوع من الخطاب والأنشطة على الإنترنت لمقاضاة النشطاء والصحفيين والمدافعين عن حقوق الإنسان أو أي مواطن عادي لديه وجهة نظر غير موالية للنظام".

في قضية مثيرة للجدل خلال السنة الماضية، حكمت مصر على خمسة مؤثرات على تطبيق "تيك توك" بالسجن ودفع غرامات مالية بتهمة التعدي على قيم المجتمع في مقاطع الفيديو التي تتضمن الغناء والرقص. وقد أُلغيت أحكام السجن الصادرة في حقهن في شهر كانون الثاني/ يناير.

تمتلك العديد من الشركات بنودا تشترط الموافقة على مشاركة البيانات مع السلطات في ظروف معينة. وفي سنة 2019، قامت شبكة "نتفليكس" بحذف حلقة من برنامج كوميدي أمريكي بعد أن اشتكت السعودية من انتقاده الحرب في اليمن وقتل خاشقجي.

ولكن من غير الواضح ما إذا كان تطبيق "كلوب هاوس" سيتحدى طلبات جهات إنفاذ القوانين، هذا إن وُجدت. وتتساءل فطافطة بشأن "ما سيفعله تطبيق كلوب هاوس في حال طلبت حكومة المملكة العربية السعودية أو الحكومة المصرية، وفقا لقوانينها ولوائحها الخاصة، من شركات التكنولوجيا تسليمها البيانات الشخصية للأفراد المتورطين في ما يسمى بالجرائم الإلكترونية؟".

التحكم في البيانات من خلال منع حذف الحسابات

قالت فطافطة إن النشطاء في الشرق الأوسط غالبًا ما يواجهون خطر مصادرة قوات الأمن لأجهزتهم والبحث في حساباتهم على مواقع التواصل الاجتماعي "للاستيلاء على ما يعتبرونه دليلا ضدك". لذلك، من الضروري أن تكون قادرا على حذف حسابك وبسرعة. ولكن لا يوجد خيار لحذف الحساب في تطبيق كلوب هاوس. بدلا من ذلك، يتعين على المستخدمين إرسال بريد إلكتروني في الغرض، ولم يقع تحديد المدة التي يستغرقها كلوب هاوس للرد.

تقول سياسة خصوصية التطبيق: "يرجى ملاحظة أننا سنحتاج إلى التحقق من أن لديك السلطة لحذف الحساب"، كما تنص أيضًا، وعلى نحو مثير للقلق، على أنه حتى إذا تمكنت من حذف الحساب، "فقد تظل بعض الأنشطة التي قام بها المستخدم قبل الحذف مخزنة من قبلنا ويمكن مشاركتها مع أطراف ثالثة".

يقول تطبيق "كلوب هاوس" إنه يحتفظ بالبيانات الشخصية بعد حذف الحساب "طالما أن ذلك ضروري ومعقول" وطالما أن "لدينا أعمالا تجارية نحتاج إلى القيام بذلك"، من بين أسباب أخرى. من الناحية العملية، يعني ذلك أنه يمكنه الاحتفاظ ببيانات المستخدم الشخصية طالما أراد ذلك.

في قسم الأمان التابع لسياسة الخصوصية الخاصة به، كتب تطبيق "كلوب هاوس" أنه ينفذ تدابير "معقولة تجاريا" لحماية البيانات الشخصية للمستخدمين، ولكنك "تستخدم الخدمة على مسؤوليتك الخاصة ... وأنه لا توجد عملية إرسال للبيانات عبر الإنترنت أو البريد الإلكتروني آمنة تمامًا". ويضيف: "نحن لسنا مسؤولين عن التحايل على أي إعدادات خصوصية أو إجراءات أمنية متضمنة في الخدمة أو مواقع الطرف الثالث".

قال ويستباي من أمنيستي تيك: "نتوقع أن تتخذ الشركة خطوات لتحديد المخاطر التي تتعرض لها حرية التعبير وحرية التنظيم، أو انتهاكات حقوق الإنسان المحتملة التي يمكن ربطها بعملياتها، ثم اتخاذ إجراءات مناسبة لمنع تلك الأضرار، بما في ذلك من خلال استخدام التشفير". في المقابل، لم ترد شركة "كلوب هاوس" على طلب التعليق على النتائج الواردة في هذا المقال.

بعد سنة من القيود المفروضة بسبب فيروس كورونا، وفر التطبيق فضاءً للأشخاص الذين يتوقون إلى التفاعل غير المباشر. وقالت فطافطة إن ذلك قد لبى أيضا حاجة أخرى، وهي "أن يعبر الناس عن آرائهم لإيجاد روابط أيديولوجية وسياسية واجتماعية". وأضافت: "بالنسبة لمجتمع الميم، على سبيل المثال، لا يمكنك التعبير عن نفسك، سواء كان ذلك بصريا أو لفظيا أو جسديا في مكان عام – أو حتى في بعض الأحيان في دوائر خاصة – في المنطقة. إنها حقيقة مؤسفة ومحزنة".

يبدو أن الكثيرين يتمتعون بإحساس جديد بالحرية على تطبيق كلوب هاوس، لكن لا ترى فطافطة أن "هذه الحرية ستستمر لفترة طويلة". وأضافت: "تنظر الحكومات في المنطقة إلى الإنترنت على أنه تهديد ... إنهم مبتكرون للغاية في إيجاد طرق للسيطرة عليه. وكلوب هاوس ليس استثناء".

المصدر: ميدل إيست آي

رابط المقال: https://www.noonpost.com/40074/