اختيار
ikhtyar

بناء الإنترنت النسوي

دراسة حالة: أسطورة التحكم بالأجهزة في ظل واقع إستغلال البيانات

نُشر النص الأصلي باللغة الإنجليزية على موقع Privacy International.

كتابة: المنظمة الدولية لحماية الخصوصية

ترجمة: ريبيكا صعب سعادة

تقوم أجهزتنا المتصلة (بالشبكة) بحمل ونقل كمّاً هائلاً من المعلومات الشخصية، الظاهرة منها والمخفية.

في حال نشوب حريق، ما هي الأغراض الثلاثة التي تنقذونها معكم/ن على عجل؟ من شبه المؤكد أنّ هواتفكم/ن المحمولة من أكثر الأغراض المذكورة. هاتفنا هويتنا، يكشف عنّا أكثر ممّا ندركه، يحوي صورنا وروزنامتنا وتاريخ تصفح الشبكة الخاص بنا والمواقع الجغرافية التي زرناها ونزورها ورسائلنا الإلكترونية وملفاتنا على مواقع التواصل الإجتماعي، كما تحمل حساباتنا المصرفية الإلكترونية وخواطر لم ننه كتابتها وقوائم التسوق، تكشف أذواقنا الموسيقية وبودكاستاتنا (محطات البث السمعي الرقمي) والبيانات المتعلقة بصحتنا ولياقتنا البدنية. لا تكتفي هذه الأجهزة بالكشف عن هوية من نقوم بالتواصل معه/ا، بل تحفظ بيانات ومحتوى التواصل، من رسائل وصور، وذلك سواء كنّا نتواصل مع العائلة أو الأصدقاء أو المعارف المهنية.

حتّى لو قمنا بتفتيش الشخص أو منزله، لن نعثر على ما يضاهي المعلومات التي نجدها على الجهاز الواحد. لو فقدنا أو تعطّل الجهاز تملّكنا شعور بالإحباط والإنزعاج عند التفكير تكرار عملية الإعداد على جهاز جديد. لكن ما الذي سنشعر به لو إكتشفنا أنّ جهة ما قادرة على وضع يدها على كافة بياناتنا من دون علمنا؟ من دون موافقتنا؟ وإن كانت قادرة على الوصول لما لا ندرك أنّه مخزّن على هاتفنا؟ وإن كانت هذه الجهة هي الشرطة؟

مصدر القلق

في شهر يناير ٢٠١٧، كتبت المنظمة الدولية لحماية الخصوصية (Privacy International) عن تحقيق نشرته البريستول كايبل (Bristol Cable) حول إستخدام الشرطة غير المأذون لأدوات معاينة الهواتف المحمولة، ممّا قوّض التحقيق في عدد من الجرائم الخطيرة. قمنا بمتابعة طلبات الوصول إلى المعلومات الموجهة إلى كافة مراكز الشرطة في المملكة المتحدة لمعرفة ما إذا كانت هذه المراكز تستخدم أدوات إستخراج البيانات من الهواتف المحمولة في حالات الجرائم المنخفضة الخطورة، بالإضافة إلى هوية الشركات التي توفّر هذه الأدوات.

إليكم/ن ما توصلنا إليه: تستخدم الشرطة البريطانية تكنولوجيات متطوّرة لإستخراج البيانات من الهواتف، وذلك بالتعاقد مع الشركات التالية، سيليبرايت (Cellebrite) وأسيسو (Aceso) وراديو تاكتيكس (Radio Tactics) وأكس أر واي (XRY وهو منتج طوّرته أم أس آي بي) وأم أس آي بي (MSAB) ومايكروسيستمايشن (Microsystemation وهو منتج طوّرته أكس أر واي).

تتباهى هذه الشركات بالخدمات التي تؤمنها منتجاتها، ففي زمن "باتت فيه البيانات المحفوظة [على الهواتف المحمولة] أكبر من أي وقت مضى" فأنك قادر على ولوج حياة الفرد كاملةً بمجرد وضع اليد على هاتفه/ا المحمول".

يشمل ذلك الوصول إلى معلومات متعلّقة بنا وبقوائم المعارف الخاصة بنا، كما تمّت الإشارة إليه أعلاه. تتيح هذه المنتجات الوصول إلى بيانات تفوق إدراكنا وتتجاوز قدرتنا على السيطرة، نذكر منها:

- "المواقع التي تم إدخالها، وموقع الجهاز وفقاً للجي بي أس (جهاز تحديد المواقع GPS)، والمواقع التي تمّ تحديدها كمفضلة، ومعلومات الجي بي أس"؛

- "بيانات النظام والبيانات المحذوفة"؛

- "تقسيمات الجهاز التي لا يمكننا الوصول إليها..."؛

- "الإستحواذ على بيانات دون تعديل، بالإضافة إلى البيانات المخفية أو المحذوفة"؛

- "بيانات مخزنة "أبعد من الهاتف"، أي التخزين على السحابة (storage Cloud)"؛

- "نسخة عن كامل محتوى الفلاشة..."؛

ماهية المشكلة

- نعتقد أننا نمتلك هواتفنا، ولكن ما معنى هذه الملكية بوجود بيانات على أجهزتنا لا يمكننا الوصول إليها، ولا يمكننا حذفها، ولا يمكننا التحقق من دقتها، ولا يمكن الوصول إليها إلا من خلال أدوات تقنية متطورة وغير متاحة لعامة الشعب؟

- إنّنا في وضع يمكن لأجهزتنا فيه أن تخوننا إلا أنّ فهمنا لكيفية حدوث ذلك وكيفية التعامل معه محدودين. لم نكتشف إلا مؤخراً أنّ شركة أوبر (Uber) تقوم بوسم أجهزة الآيفون (iPhone) بهويات دائمة كي تتمكّن من تحديد الجهاز حتّى بعد مسحه وإعادة تهيئته من الصفر.

في المنظمة الدولية لحماية الخصوصية نطلق على البيانات المخفية، أو تلك التي لا نراها، إسم "البيانات على الأجنحة"، ولا يقتصر القلق من البيانات على الأجنحة على تلك المخزنة في الهواتف المحمولة. كما أشرنا في العرض الذي قدمناه في العام ٢٠١٧ في ري:بوبليكا (Re:Publica)، وفي إطار تحقيق جنائي في الولايات المتحدة الأمريكية تمّ فيه إستخدام خدمة أمازون إيكو (Amazon Echo)، في أول التحقيق أصرت أمازون على أن الإيكو لا يقوم بتخزين أي تسجيل صوتي عند

الإستخدام، إلا أن السلطات أصرّت على معاينة الجهاز حيث تمّ العثور على بيانات وإستخراجها.

في عالم تستطيع القوى الأمنية - وهي المخولة إعتقالنا، وتوجيه الإتهام ضدنا، ومنعنا من حرياتنا - فيه شراء وإستخدام برمجيات إستخراج متطورة تخولها قراءة البيانات من هواتفنا وأجهزتنا المتصلة (بالشبكة) المتواجدة في منازلنا ومن شبكة إنترنت الأشياء الآخذة بالنمو، وعندما يتمّ إعتبار موافقة صاحب/ة ومنتج/ة هذه البيانات غير ضرورية، في عالم من هذا النوع يصبح فيه غياب النقاش والتشاور العامين والتدقيق القانوني أمراً غير مقبول.

لا تنحصر المشكلة بحصول الشرطة على كميات هائلة من البيانات من دون موافقة أصحاب العلاقة ولأجل غير محدد ومن دون رقابة أو توجيه أو تشريعات واضحة، بل أيضاً بأن هذه السلطات أثبتت مراراً وتكراراً عدم أهليتها للتعامل مع بياناتنا.

في المملكة المتحدة على سبيل المثال، نتبيّن ذلك من خلال عدم الجدية في تشفير بيانات الهواتف المحمولة وإستخدام قواعد البينات من أجل "أهداف لا علاقة لها بالعمل"، لكن أيضاً في فشل السلطات الجسيم في حماية معلومات شديدة الحساسية والموقف اللامبالي في ما يتعلّق بالبيانات، وقد تمّ الإبلاغ عن هذه الحوادث مراراً وتكراراً على مرّ السنين.

ففي العام ٢٠١٧ على سبيل المثال، تمّ تغريم شرطة دائرة مانشستر الكبرى (Greater Manchester Police) ١٥٠ ألف جنيه إسترليني بعدما فُقدت تسجيلات غير مشفرة ومحفوظة على قرص دي في دي (DVD) لشهادات في قضايا جرائم عنيفة وجنسية عند إرسالها عبر البريد. وقد صرّح/ت مسؤول/ة المعلومات بأنّ "موقف شرطة مانشستر أتى متعجرفاً في التعامل مع هذه البيانات، وينمّ عن لامبالاة بالعواقب المحتملة في حال عدم الحفاظ على أمان هذه البيانات».

ماهية الحل

تقوم القوى الأمنية حول العالم بشراء تكنولوجيات حديثة لتعزيز قدرتها على المراقبة، وذلك على مستوى قلّما يفهمه أولئك الذين/اللواتي من المفترض بهذه القوى خدمتهم/ن. أمّا القانون فمتخلّف عن مجاراة تطوّر الأحداث. ومع تزايد الأجهزة المتصلة من حولنا، من مجسات وكاميرات، باتت سبل التحقيق التقليدية - كتلك التي لا تستلزم إستصدار مذكرات - غير قادرة على تحقيق الأهداف المرجوة منها في حين أنّ أجهزتنا الإلكترونية، بقدرتها الهائلة على التخزين، تحفظ حتّى أكثر تفاصيل حيواتنا حميمية.

وفي حين أنّ إستخدام الشرطة غير المقيّد لتكنولوجيات الإستخراج مقلق، إلّا أنّ فكرة وجود بيانات مخفية محفوظة على أجهزتنا - وهي قادرة على الوشي بنا - يطرح عدداً من الأسئلة على شركات التكنولوجيا الكبرى المنتجة للبرمجيات والهواتف الذكية، وهي الشركات التي تريد لنا إعتناق إنترنت الأشياء، كما تنادي بمساحات عامة متصلة تكون "أكثر ذكاءً".

أقل ما يمكن المطالبة به هو الشفافية والمحاسبة من الشرطة، من جهة، والمزيد من التدقيق من السلطات التشريعية.

في الماضي كنّا نقصد التكنولوجيا، أي أنّ إنتاج البيانات كان يتمّ عبر تفاعلات واضحة ومباشرة، أمّا الآن، باتت التكنولوجيا تصلنا، سواء أردنا ذلك أم لا، سواء أدركنا ذلك أم لا. في المنظمة الدولية لحماية الخصوصية، نرى أنّ تحقيق هذه النقلة يستلزم تغييراً في القوانين وشروط الحوار. نريد إعترافاً كاملاً بأنّ التلاعب بالخصوصية يبدأ من لحظة إنتاج البيانات، من اللحظة التي تقوم فيها شركة أو مؤسسة ما بجمع البيانات نفقد أحد عناصر التحكم بها، وبالتالي بعضاً من خصوصيتنا. تقع على الأجهزة والشبكات الخدمات المحيطة بنا مسؤولية عدم إنتاج وجمع والتعامل وبيع البيانات بإفراط. لا بدّ لقوانيننا ضمان قدرة المعني/ة بالبيانات على التحكم بمصير هذه البيانات، وبالرغم من إستحالة تحقيق ذلك، يجب أن نسعى لخلق عالم يمكن للفرد فيه الكينونة من دون إنتاج البيانات، في حال رغبته/ا بذلك.