أوسما بيرنوت | نشر في ٢٠ ديسمبر ٢٠٢٢,

كيف نتعرّض جميعًا للمراقبة طوال الوقت؟

ترجمة: حفصة جودة

درست مجموعة من الباحثين بيانات 15 شهرًا من حركة التنقل البشري لـ 1.5 مليون شخص، وقد اتضح أن 4 نقاط في المكان والزمان كانت كافية للتعرّف إلى 95% منهم، حتى عندما لم تكن البيانات بالجودة المثالية، كان ذلك عام 2013.

الآن بعد 10 سنوات، تغلغلت تكنولوجيا المراقبة في جميع مظاهر حياتنا، فهم يجمعون حُزم البيانات منا بأشكال مختلفة وكثيرًا دون علمنا.

أعمل كباحثة مراقبة وأركز على حوكمة التكنولوجيا، وهذا ما جمعته حول أنظمة المراقبة واسعة النطاق، وأعتقد أن جميع الناس يجب أن يكونوا على دراية به.

أنظمة المراقبة بالفيديو (CCTV) وكاميرات الدخول المفتوح

رغم أن الصين تملك أكثر من 50% من جميع كاميرات المراقبة المثبّتة في العالم (حوالي 34 كاميرا لكل 1000 شخص)، إلا أن المدن الأسترالية تلحقها في ذلك، ففي عام 2021 كان لدى سيدني 4.67 كاميرات لكل 1000 شخص.

وبينما قد تُستخدم الكاميرات لأغراض قانونية كتعزيز الأمان في المدن ومساعدة الشرطة في التحقيقات الجنائية، إلا أن استخدامها أيضًا يثير الكثير من القلق.

في عام 2021 أُثيرت اشتباهات حول استخدام شرطة نيو ساوث ويلز للقطات كاميرا المراقبة بالفيديو مقترنة بخاصية التعرّف إلى الوجوه، للعثور على أفراد شاركوا في احتجاجات مناهضة للإغلاق، عند سؤال الشرطة لم تؤكّد أو تنفي إذا ما كانت قد قامت بذلك فعلًا، أو تنوي القيام بذلك في المستقبل.

في أغسطس/ آب 2022، أكّدت الأمم المتحدة استخدام أنظمة المراقبة بالفيديو في انتهاكات خطيرة لحقوق الإنسان ضد الإيغور وغيرهم من الأقليات المسلمة في شينجيانغ شمال غرب الصين، حيث لا

تسجّل كاميرات أنظمة المراقبة بالفيديو في الصين لقطات مباشرة فقط، فبعضها مزوّد بخاصية التعرّف إلى الوجوه للاستمرار في مراقبة تحركات الأقليات، وقيل إن بعضها خاضع لتجارب الكشف عن المشاعر.

المشكلة الأخرى المتعلقة بأنظمة المراقبة بالفيديو هي الأمن، فالكثير من تلك الكاميرات ذات وصول مفتوح، ما يعني أنها لا تحتوي على كلمة سرّ للحماية ويمكن الوصول إليها بسهولة عبر الإنترنت.

للولايات المتحدة أيضًا تاريخ طويل في استخدام كاميرات المراقبة بالفيديو لدعم ممارسات الشرطة العنصرية، ففي عام 2021 أصدرت منظمة العفو الدولية تقريرًا يقول إن المناطق ذات النّسَب الأعلى من السكان الملوّنين، يوجد فيها كاميرات مراقبة بالفيديو أكثر من غيرها.

المشكلة الأخرى المتعلقة بأنظمة المراقبة بالفيديو هي الأمن، فالكثير من تلك الكاميرات ذات وصول مفتوح، ما يعني أنها لا تحتوي على كلمة سرّ للحماية ويمكن الوصول إليها بسهولة عبر الإنترنت، لذا يمكنني أن أقضي اليوم كله في مراقبة شرفة أحدهم طالما أن هناك كاميرا مفتوحة في المكان.

يعرض المشروع الأخير لفنان المراقبة درايس ديبورتر "Follower The" نقاط ضعف الكاميرات المفتوحة بكفاءة، وذلك بالجمع بين لقطات للكاميرات المفتوحة مع الذكاء الاصطناعي وصور إنستغرام، تمكّن ديبورتر من مطابقة صور الناس مع لقطات لمكان ووقت التقاط الصور.

تعتمد قانونية الأمر من عدمه على ظروف محددة وأين تعيش، وبكل حال المشكلة هنا أن ديبورتر تمكّن من القيام بذلك في المقام الأول.

أجهزة "إنترنت الأشياء"

جهاز إنترنت الأشياء هو أي جهاز يتصل بشبكة لا سلكية ليعمل، لذا فكّر في الأجهزة الذكية بالمنزل مثل "أمازون إيكو" أو "جوجل دوت" أو جهاز مراقبة الطفل أو حتى الأضواء الذكية.

من المتوقع أن يصل الإنفاق العالمي على أجهزة إنترنت الأشياء إلى 1.2 تريليون دولار أمريكي هذا العام، وتشكّل شبكة إنترنت الأشياء حوالي 18 مليار جهاز متصل، ومثل كاميرات أنظمة المراقبة بالفيديو، من السهل اختراق أجهزة إنترنت الأشياء إذا كانت تستخدم كلمات المرور الافتراضية أو كلمات مرور تعرّضت للتسريب.

في بعض الأمثلة، يسرق القراصنة كاميرات مراقبة الأطفال لمراقبة الأمهات أثناء الرضاعة الطبيعية لأطفالهم، أو تهديد الوالدين بأن طفلهم اختُطف، أو قول أشياء مخيفة للأطفال مثل "أحبك".

إضافة إلى القرصنة، يمكن للشركات أيضًا أن تستخدم تلك البيانات التي جمعتها من خلال إنترنت الأشياء لاستهداف العملاء بالمنتجات والخدمات.

أثار خبراء الخصوصية مخاوفهم في سبتمبر/ أيلول بشأن اتفاقية اندماج أمازون مع شركة المكانس الكهربائية الروبوتية iRobot، حيث قال خطاب موجّه للجنة التجارة الفيدرالية في الولايات المتحدة، موقع من قبل 26 جماعة للدفاع عن الخصوصية والحقوق المدنية:

"إن ربط أجهزة iRobot بنظام أمازون المنزلي المتطفّل بالفعل، يحفّز لجمع المزيد من البيانات من المزيد من أجهزة المنزل المتصلة بالإنترنت، ومن المحتمل أن يتضمن ذلك تفاصيل خاصة حول عاداتنا وصحّتنا، ما يعرّض حقوقنا الإنسانية وأمننا للخطر".

يمكن للبيانات التي يجمعها إنترنت الأشياء أيضًا أن تنتقل إلى أطراف ثالثة من خلال شراكات البيانات (وهو أمر شائع جدًا)، ودون موافقة صريحة من العملاء.

تكنولوجيا وبيانات كبيرة

عام 2017، تجاوزت قيمة البيانات الكبرى قيمة النفط، وتقود الشركات الخاصة غالبية هذا النمو، بالنسبة إلى منصات التكنولوجيا فالجمع الواسع للمعلومات الشخصية للمستخدمين يمثل تجارة أيضًا حرفيًا، لأن المزيد من البيانات يعني المزيد من التحليل الدقيق وإعلانات مستهدفة أكثر فعالية، ما يعني المزيد من العائدات.

هذا المنطق في تحقيق الربح من خلال الإعلانات المستهدفة يسمّى "رأسمالية المراقبة"، وكما يقول المثل القديم: "إذا لم تكن تدفع المقابل، فأنت المنتج".

تعتمد منصات التواصل الاجتماعي على نقاط ضعفنا النفسي لنبقى على الإنترنت أطول وقت ممكن، وقياس ردود أفعالنا في كل ثانية نقضيها بالتجول بين الإعلانات.

جنت شركة ميتا (المالكة لفيسبوك وإنستغرام) حوالي 23 مليار دولار كعائدات الإعلانات في الربع الثالث لهذا العام، وقد شُرحت الآلية الضخمة التي تقف وراء ذلك جيدًا في الفيلم الوثائقي عام The 2021 Social Dilemma ولو بطريقة درامية.

فقد أظهر لنا كيف تعتمد منصات التواصل الاجتماعي على نقاط ضعفنا النفسي لنبقى على الإنترنت أطول وقت ممكن، وقياس ردود أفعالنا في كل ثانية نقضيها بالتجول بين الإعلانات.

برامج الولاء

رغم أن الكثيرين لا يدركون ذلك، إلا أن برامج الولاء واحدة من أكبر طرق جمع البيانات الشخصية، أحد الأمثلة على ذلك أنه في عام 2021 أرسل بائع تجزئة كتالوغًا مليئًا بصور لأطفال رضّع مبتسمين وأثاث للأطفال إلى فتاة مراهقة، حيث ذهب والد الفتاة الغاضب لمواجهة مديري المتجر المحلي، ثم اكتشف أن التحليل التنبؤي يعلم عن ابنته أكثر ممّا يعلمه هو.

يستخدم الكثير من الشباب برامج الولاء، هذه المخططات تبني ملفًا خاصًا لاستهلاكك لتبيع لك المزيد من الأشياء، بعضها حتى يأخذ منك رسومًا مخادعة، ويجذبك بالامتيازات المستقبلية ليبيعك أشياء باهظة.

يقول صحفي التكنولوجيا روس بيج: "إن البيانات التي تسلّمها عند الدفع، يمكن مشاركتها وبيعها لشركات لم تتعامل معها مطلقًا".

كخطوة مخادعة، يمكنك أن تجد صديقًا تتبادل معه بطاقات الولاء الخاصة بك، فالتحليل التنبؤي يكون قويًا فقط عندما يتعرّف إلى أنماط السلوك، عندما يفسد النمط تتحول البيانات إلى فوضى.

المصدر: ذي كونفرسيشن

رابط المقال: https://www.noonpost.com/46102/