في المدن الذكية: كل خطوة مسجلة!

المدن الحديثة اليوم مليئة بأشياء تستقبل وتجمع وترسل البيانات كالهواتف النقالة مثلاً إضافة إلى أجسام مدمجة فعليًا في مدننا، كإشارات المرور ومحطات تلوث الهواء وحتى أشياء بسيطة مثل سلة المهملات يمكن أن تكون متصلةً بالإنترنت، مما يعني إنها تشكل جزءًا مما يُسمى إنترنت الأشياء **Internet of things** أو اختصارًا **IOT**. تجمع المدن الذكية البيانات من هذه الأجهزة الرقمية وتستخدمها لإنشاء منتجات جديدة تجعل المدن صالحةً أكثر للعيش.

على الرغم من أن هذه المدن لديها إمكانيات هائلة لتحسين مستوى الحياة إلا أن إمكانية زيادة ذكاء تلك المدن تثير مخاوف كثيرة حول موضوع الخصوصية، فمن خلال أجهزة الاستشعار **Sensors** المدمجة في مدننا والهواتف الذكية في جيوبنا، ستمتلك المدن الذكية القدرة باستمرار على تحديد مكان الناس ومن يقابلون بل وربما حتى ما الذي يفعلونه.

مدينة شرق أسيوية. حقوق الصورة: The Conservation

أصبح مهما أكثر من أي وقت مضى أن نمعن النظر بدقة في وجهة بياناتنا وكيف تُستخدم، وذلك بعد الكشف عن تسريب بيانات الفيس بوك **Facebook** لـ 87 مليون مستخدم واستخدمت للتأثير على سلوك التصويت الانتخابي. وبالمثل، تقع المزيد من البنية التحتية الحيوية ضحية للهجمات السيبرانية **cyber-attacks** لذا نحن بحاجة إلى الأخذ بعين الاعتبار أن مدننا كلما أصبحت أكثر ذكاءً أصبحت أكثر عرضةً للهجمات الإلكترونية.

مدن أذكى

تصبح المدن أكثر ذكاء بسرعة حول العالم، فمدن مثل سنغافورة ولندن وسان فرانسيسكو تستخدم تقنيات مثل الاستشعار المدني **Urban sensing** (الذي يلتقط كيفية تفاعل الناس مع بعضهم البعض ومع محيطهم) والتتبع الجغرافي **geo-tracking** (الذي يسجل حركة الناس) والتحليلات الفورية **real-time analytics** (التي تعالج كميات هائلة من البيانات المُجمعة) تستخدم المدن الذكية هذه التقنيات لتحسين إدارة الطاقة وإمدادات المياه وتقليل التلوث والاختناقات المرورية، وكذلك لتحسين طرق جمع القمامة أو مساعدة الناس في ركن سياراتهم، وخير مثال على ذلك هو مشروع تنظيم الأشياء **Array of Things** في مدينة شيكاغو الأمريكية.

لا تقتصر مبادرات المدن الذكية على المساعدة في جعل الحياة أكثر قابلية للعيش وحسب، بل ويمكنها أن تساعدنا في تحسين العالم. ففي عام 2013 قدّم الأكاديمي اليوناني فاسيليس كوستاكوس **Vassilis Kostakos** شاشات **LCD** تفاعلية شجعت الناس على الانتظار في موقف الباص للمساعدة في تحديد خلايا الدم المصابة بالملاريا **Malaria**.

مخاوف البيانات الكبيرة والخصوصية

في الأشهر القليلة الماضية التي تلت اكتشافات شركة **Cambridge Analytica** وفيس بوك تزايدت المخاوف بصورة كبيرة بشأن كيفية استخدام الشركات للبيانات المتراكمة.

بالرجوع إلى عام 2009، كان الخبراء مدركين بالفعل إن بإمكان أصحاب المصالح جمع معلومات شخصية من المستخدمين. وقد سمحت سياسات الخصوصية الغامضة والاتفاقيات المُعقدة لمشاركة البيانات للشركات بتخطي قانون حماية البيانات باستخدام البيانات المُجمعة لأغراض غير مُعلنة.

يمكن أن تؤدي مشاريع المدن الذكية إلى مخاوف مماثلة بسبب المعلومات الضخمة والمُفصلة التي جُمعت من خلال أجهزة إنترنت الأشياء **IOT**. خذ على سبيل المثال مشروع **Cityware** الذي أظهر إمكانية عرض بيانات اللقاءات الفعلية بين أصدقاء الفيس بوك وليست الرقمية وحسب، فقد تمكن مشروع **Cityware** من تعقب حركة 30 ألف شخص باستخدام الملف الشخصي لهم على الفيس بوك وإشارات بلوتوث الهواتف الذكية.

يميل معظم الناس إلى الاستخفاف بفكرة إن الهاتف الذكي الذي يحملونه هو عبارة عن أداة استشعار قوية جدًا. لكي يعمل هاتفك، فإنه يقوم بمشاركة بيانات خاصة عن موقعك وتفاعلك الرقمي والجسدي وربما أكثر من ذلك وبشكل مستمر، وعندما تتطابق هذه البيانات مع معلومات إضافية مُجمعة من أجهزة إنترنت الأشياء والشبكات الذكية **smart grids** كشبكات إمداد الكهرباء التي تكشف وتتفاعل بسرعة مع التغيرات المحلية في الاستخدام، فإنها تثير تداعيات خطيرة على مستوى خصوصية الأشخاص وحرية إرادتهم.

كما تُعطي فيس بوك الحق في امتلاك كل ما تنشره على حسابك الشخصي، فالبيانات المُجمعة عن طريق أجهزة الاستشعار عبر الإنترنت ستكون مملوكةً لمجموعة متنوعة من الشركات، بما في ذلك مزودي خدمة الإنترنت **internet service providers** أو اختصارًا **ISPs**. قام الكونجرس الأمريكي في العام الماضي بإلغاء حماية خصوصية الإنترنت ومنح مزودي خدمات الإنترنت الحق في بيع معلومات المستخدمين كسجل التصفح مثلًا لطرف ثالث.

بمجرد اتصال معظم أجهزتك بالإنترنت، يمكن لهذه الأشياء إبلاغ الشركات عن العلامات التجارية والمنتجات التي تفضلها وكيف ومتى تستخدمها، مما يعني إن كل البيانات التي ستجمعها أدوات إنترنت الأشياء، سواء في منزلك أو مدينتك، يُمكن أن تُباع إلى طرفٍ ثالث.

المخاوف الأمنية السيبرانية

كلما أصبحت مدننا أكثر ذكاءً أصبحت معلوماتنا الرقمية أكثر عرضةً للهجمات السيبرانية، فعلى سبيل المثال برنامج **ransomware** المعروف ببرنامج الفدية الذي يقوم بتشفير المعلومات ثم يطلب فدية لفك تشفيرها، يمكن أن يُصيب أكبر مالكي البيانات، مثل خدمة الصحة الوطنية في المملكة المتحدة **UK National Health Service** أو اختصارًا **NHS**.

تكون الرهانات عالية جدًا عندما تصيب الفيروسات السلطات المحلية. وقد شَلَت الهجمات السيبرانية الأخيرة على مدينة أتلانتا العديد من الأنظمة الحساسة في المدينة بما في ذلك قسم الشرطة. إن وكالة تطبيق القانون الأوروبية **Europol** تقوم حاليًا بتطبيق مبادرة (لا مزيد من الفدية) **No More Ransom** وهي مبادرة تقوم بإعطاء نصائح جيدة عن كيفية التعامل مع هذا النوع من التهديد.

يستطيع القراصنة التحكم في مبانٍ و أنظمةٍ بأكملها. وما انقطاع التيار الكهربائي الذي ترك أكثر من 225 ألف شخص بدون ضوء في ديسمبر/كانون الأول عام 2015 إلا مثال على ذلك. وتظل معرفة المسؤول عن الهجمات السيبرانية تحديًا دائمًا على الرغم من اعتبار روسيا من المشتبه بهم.

في نهاية المطاف، وبالرغم من هذه المخاوف، فإن دمج إنترنت الأشياء في المدن هو توجه يتزايد يومًا بعد آخر. وللتحكم فيما يعنيه هذا، يحتاج الناس أن يصبحوا أكثر اطلاعًا ومشاركةً، وينبغي كذلك فحص نماذج الأعمال لأصحاب المصالح إضافةً إلى عملية استخدامهم لبيانات يجب أن تكون عرضة للمحاسبة، والأهم من ذلك أن يتم إعطاء أذن صاغية للمواطنين حول الكيفية التي يريدون بها لمدنهم أن تتطور.

- التاريخ: 2018-08-27
- التصنيف: تكنولوجيا

#تكنولوجيا #الحضارة التكنولوجية #المدن الذكية

المصادر

- phys
- الصورة

المساهمون

- ترجمة
  - محمد شريف
- مُراجعة
  - كرار زيني
- تحرير
  - رأفت فياض
  - روان زيدان
- تصميم
  - أحمد أزميزم
- نشر
  - يقين الدبعي