إنترنت بلا مراقبة.. كيف يمكن للحكومة المصرية إنهاء سياسة المراقبة الجماعية؟

تاريخ النشر: الخميس, 3 يونيو, 2021

الحقوق الرقمية

Twitter Facebook

إعداد وتحرير وحدة الأبحاث بمؤسسة حرية الفكر والتعبير

ملخص تنفيذي

مع بداية انعقاد مجلس النواب المنتخب عام 2015، أولت لجنة الاتصالات اهتمامًا بالغًا بإصدار قوانين تنظم استخدام الفضاء الإلكتروني. لاحقًا، صدر قانون الجريمة الإلكترونية رقم 175 لسنة 2018، ثم قانون حماية البيانات الشخصية رقم 151 لسنة 2020 وهي القوانين التي ساهمت في تعزيز ممارسات المراقبة، وعلى الرغم من حداثة القوانين السابق ذكرها، فإن مراقبة جميع الأنشطة الإلكترونية، مثل: البريد الإلكتروني، تصفح الإنترنت، المحادثات الهاتفية، ووسائل التواصل الاجتماعي، هي ممارسات تمتد لسنوات طويلة، وهو ما يعطينا مؤشرًا عامًا لفهم السياق الذي صدرت فيه وكمثال على تبني الحكومة المصرية سياسة للمراقبة الجماعية والعشوائية، فإن الأجهزة الأمنية تتوسع في القبض على مستخدمي الإنترنت، على إثر القيام بمراقبة المستخدمين. لذا، فإن السلطات المصرية يمكنها وقف هذه الممارسات عبر إحداث تعديلات تشريعية، ووقف الممارسات غير القانونية لأجهزة الأمن، بما يشمل التوقف عن شراء برمجيات تجسس.

مقدمة

بعد مرور عشر سنوات على ثورة الخامس والعشرين من يناير، التي انقطعت خلالها خدمات الإنترنت في جميع أنحاء مصر، بموجب المادة (67) من قانون تنظيم الاتصالات رقم 10 لسنة 2003، فلا تزال الحكومة وعلى الأخص أجهزتها الأمنية تفرض مزيدًا من المراقبة الموسعة والجماعية على الإنترنت، فيما يعتبر انتهاكًا للخصوصية في المجالين العام والخاص الرقميين. وتمتد هذه الممارسات عبر سنوات، من خلال الاستناد إلى نصوص قانونية بعينها، أو خارج إطار القانون تمامًا. ويتم ذلك في إطار التوسع في استخدام الإنترنت كمساحة أخيرة للتعبير عن الرأي والتواصل، فيما يتعلق بالشأن العام. وبحسب التقرير الموجز عن مؤشرات الاتصالات وتكنولوجيا المعلومات الصادر عن وزارة الاتصالات، بلغ عدد مستخدمي الإنترنت في مصر 62.3 مليون مستخدم بنهاية سبتمبر 2020.

في هذا السياق، تناقش الورقة السياسة التي تتبعها الحكومة المصرية في مراقبة المستخدمين، في ظل قوانين تهيمن بها جهات الأمن القومي/ الأجهزة الأمنية على بيانات المستخدمين. ومع صدور قانون حماية البيانات الشخصية رقم 151 لسنة 2020، عاد الجدل حول كيفية حماية خصوصية المواطنين الرقمية، خاصة مع كون الغرض الأساسي من القانون هو حماية بيانات المستخدمين. واستندت الورقة إلى تحليل ممارسات الحكومة المصرية، ومدى ارتباطها بسياسة عامة تعتمد على استخدام المراقبة لحماية الأمن وتعزيز الاستقرار، وتبعات ذلك على مستخدمي الإنترنت في مصر، فضلًا عن التأثيرات السلبية لذلك على مناخ الاستثمار.

ويمكن الاستعاضة عن تلك السياسة عبر وقف ممارسات المراقبة وتعزيز حكم القانون، ومن ثم تمهيد الطريق أمام مزيد من الاستثمارات وتمكين المواطنين من النقاش العام، وفي الأولوية الكبيرة لحماية البيانات في عمل الشركات وتقديم الخدمات للجمهور.

خلفية.. كيف أصبحت المراقبة للجميع؟

تعتمد سياسة المراقبة الجماعية على شراء برمجيات التجسس، بالإضافة إلى إصدار تشريعات تسمح لأجهزة الأمن بمراقبة المستخدمين. ما يؤدي إلى القبض على بعضهم. ففي عام 2013، اشترت السلطات المصرية برمجية proxySG من شركة blue coat systems الأمريكية، التي تمكن من استخدام تقنية "الفحص العميق للحزم" deep packet inspection، وهي تعطي مقدمي خدمات الاتصالات القدرة على معرفة الكثير حول سلوك المستخدمين، مثل: تحديد الموقع الجغرافي، والتتبع ومراقبة وتصفية محتويات الإنترنت بشكل جماعي[1]. وفي نفس العام، أعلنت وزارة الداخلية عن قرار للممارسة المحدودة، رقم 22 لسنة 2013/2014، تحت مسمى "منظومة قياس الرأي العام"، والتي من خلالها تم إجراء مناقصة لتوريد وتشغيل برمجيات تهدف إلى مراقبة الفضاء الإلكتروني.

وكرد فعل على ذلك، تقدمت عدة منظمات حقوقية بدعوى، في عام 2014، أمام محكمة القضاء الإداري لوقف تنفيذ وإلغاء قرار وزارة الداخلية فيما يخص الممارسة المحدودة[2]. وتم الحكم برفض الدعوى في عام 2017، لأسباب تتعلق بعدم وجود صلة لمقيمي الدعوى، بالعقد المطعون عليه، وبالتالي رفضت المحكمة الدعوى شكلًا، دون التطرق إلى أهمية موضوع القضية المرتبط بخصوصية المواطنين[3].

وفي 2017، اشترت دولة الإمارات العربية المتحدة برمجية التجسس Cerebro وقدمتها إلى الحكومة المصرية، وهذه البرمجية تُتيح للسلطات المصرية مراقبة شاملة للاتصالات عبر تقنيةDeep Packet Inspection بما في ذلك المكالمات الصوتية والرسائل النصية ورسائل البريد الإلكتروني والرسائل الفورية، وشبكات التواصل الاجتماعي المختلفة وعمليات البحث على محركات البحث[4].

ويلاحظ قيام الأجهزة التابعة لوزارة الداخلية، مثل الإدارة العامة لتكنولوجيا المعلومات[5] بالتنسيق مع جهاز الأمن الوطني بفرض المراقبة على مستخدمي وسائل التواصل الاجتماعي، حيث حدث تصاعد في أعداد المقبوض عليهم لأسباب تتعلق بمشاركة محتوى أو كتابة تعليق أو إبداء إعجاب بمحتوى، أو إدارة صفحة على إحدى وسائل التواصل الاجتماعي، فوفقًا لما تم رصده وتوثيقه من قبل مؤسسة حرية الفكر والتعبير منذ النصف الثاني من عام 2013، حتى الربع الأول من عام 2021، تم القبض على 300 شخص على الأقل لهذا السبب. ليس ذلك فقط، بل استحدثت النيابة العامة وهي جزء من السلطة القضائية وحدة لرصد وسائل التواصل الاجتماعي تقوم بمراقبة المستخدمين.

وتخلق المراقبة الجماعية على وسائل التواصل الاجتماعي خوفًا لدى المستخدمين من زيارة مواقع بعينها، أو التعبير عن آرائهم، وهو ما يخلق حالة من الرقابة الذاتية على ما يمكن كتابته أو إبداء الإعجاب بشأنه، ويمتد إلى المنشور على حسابات المستخدمين في وسائل التواصل الاجتماعي (فيسبوك/ تويتر/ إنستجرام/ تيك توك)، بعد أن كان مقتصرًا على الرسائل الخاصة.

وكنتيجة للمراقبة، وغياب الضمانات القانونية لحماية الحق في الخصوصية، يلجأ المستخدمون في بعض الأحيان إلى حلول تقنية تمكنهم من التمتع بالخصوصية والاتصال بشكل آمن عبر شبكة الإنترنت، بينما يمكن إحالتهم إلى محاكمات بسبب ذلك، إذ ينص قانون تنظيم الاتصالات على تجريم استخدام "أدوات تشفير خدمات الاتصالات، سواء من قبل مقدمي الخدمة، أو من قبل المستخدمين".[6]

وتجدر الإشارة هنا إلى أن كافة الوسائل الإلكترونية، بداية من البريد الإلكتروني، وصولًا إلى شبكات التواصل الاجتماعي تستخدم بروتوكولات مشفرة لنقل البيانات[7]، وهو ما يعني التباس المفاهيم لدى المشرع، إلا أنه يمكن فهم المقصود من تلك المادة في سياق سعي السلطات إلى حجب مواقع تقدم خدمات VPN، إذ قامت بحجب موقع i2p وموقع مشروع free internet اللذين يقدمان المجهولية لمستخدمي الإنترنت.

بالإضافة إلى محاولات حجب تطبيقات محادثات شخصية مشفرة/ معماة كتطبيق سيجنال. ففي السادس عشر من ديسمبر 2016 حاولت السلطات المصرية حجب سيجنال، ونشر التطبيق عبر حسابه الرسمي على تويتر: "لقد قمنا بالتحقق خلال الأيام الماضية مؤكدين أن مصر تقوم بتصفية الوصول الى سيجنال."[8]

بالتطبيق لكل الأنظمة الشمولية وخاصة أن الشعار يقوم بتصنيف الموجودين إلى تصنيفات .

وترجع هذه الممارسات إلى سياسة عامة انتهجتها السلطات المصرية لاعتبار المراقبة أداة لحماية الأمن القومي، دون التقيد باحترام حقوق الإنسان وحكم القانون. وتساهم تلك السياسة في التأثير على علاقات مصر الدولية. وعلى سبيل المثال أنفت الشرطة الألمانية تدريبًا للشرطة المصرية بخصوص مراقبة المواقع الإلكترونية المتطرفة تخوفًا من استخدامه لمراقبة المصريين، في عام 2017[9]. إضافة إلى تأثير ذلك على الشركات الدولية العاملة في مصر، والتي قد تتعرض لضغوط لمشاركة بيانات مستخدميها مع السلطات المصرية.

بين بدائل عدة.. إنهاء سياسة المراقبة الجماعية هو الحل الأمثل

تفضل الحكومة المصرية حتى وقتنا هذا الاستمرار في المراقبة الجماعية واستخدام التكنولوجيا والتشريع وأجهزة الأمن في سبيل تحقيق ذلك. وقد عزز تطور تقنيات المراقبة من قدرات الحكومة على مراقبة الاتصالات والإنترنت بشكل جماعي. وبحسب خبير في الأمان الرقمي، يتم من خلال استخدام برامج ذكاء اصطناعي شديدة التعقيد تحليل الأنماط واللغة، وهو ما يعني جمع بيانات ضخمة عن الحياة اليومية لمستخدمي الإنترنت، وتحليل تلك البيانات، والتي تساعد على تحديد اهتمامات المستخدمين وتوجهاتهم السياسية بناء على الصفحات التي يستخدمونها[10].

وإذ كانت تلك الممارسات هي الحاكمة للقوانين التي تلتها، فقد نص قانون الجريمة الإلكترونية على إمكانية الحصول على حفظ وتخزين بيانات المستخدمين من خلال شركات الاتصالات لمدة ستة أشهر، وبالتالي استخدمت الحكومة التشريع للاستمرار في المراقبة الجماعية[11]، بما يعزز قدراتها على فرض تدابير المراقبة الشاملة[12]. ويساعد على ذلك سيطرة الدولة على ملكية البنية التحتية للاتصالات والإدارة المركزية لهذا القطاع الحيوي[13]. وجاء في تقرير الشفافية الخاص بشركة فودافون مصر في المملكة المتحدة، قبل أن يتم بيعها إلى STC السعودية، أن الشركة لا تستطيع أن تفصح بأي معلومات تخص أعمالها في مصر، وإلا تعرضت رخصتها للإلغاء[14].

وقد يدافع بعض المشرعين والخبراء عن تبني سياسة مختلفة بعض الشيء، بحيث يتم التجاوز عن ممارسات مراقبة المستخدمين، والتركيز فقط على إعلان تبني تشريع لحماية البيانات الشخصية بهدف توفير مناخ جاذب للاستثمار. وقد ظهر هذا التوجه في إصدار قانون حماية البيانات الشخصية، وأعلنت الحكومة أن أحد أهم أهداف القانون هو تهيئة مناخ تشريعي يشجع المستثمرين، في مجال صناعة مراكز البيانات العملاقة[15]، ورفع تصنيف مصر في مؤشر حقوق الإنسان[16]، دون اتخاذ أي إجراءات بشأن ممارسات المراقبة التي تقوم بها جهات تنفيذية وأجهزة أمنية.

وكان من المنتظر أن يقوم القانون بتنظيم عملية استخدام ومشاركة البيانات، وحماية المستخدمين من انتهاك خصوصيتهم من قبل الأطراف المتعددة، إلا أن القانون استثنى جهات الأمن القومي، والجهات الخاضعة للبنك المركزي من أحكام القانون[17]، وهو ما ينفي عن القانون هدفه الأساسي في حماية خصوصية البيانات. وإلى جانب ذلك لم تصدر اللائحة التنفيذية للقانون حتى وقتنا الحالي، وهو ما يثير القلق حيال مناخ الاستثمار، خاصة مع إبداء عدد من الشركات العالمية، مثل، جوجل ومايكروسوفت، مخاوف حيال القانون وقت مناقشته[18]. كما لا يظهر هذا النهج سببًا للتعامل مع ممارسات شراء برمجيات التجسس ومراقبة مستخدمي الإنترنت من قبل الأجهزة الحكومية.

نقترح أن تتبنى الحكومة المصرية سياسة تعتمد على الإنهاء الفوري للمراقبة والالتزام بحماية الخصوصية. بدءًا من وقف استخدام برمجيات التجسس أو شرائها، وحتى تعديل نصوص تشريعية، من خلال فتح نقاش موسع مع خبراء في مجالات الاتصالات، شركات الاتصالات، ومنظمات مجتمع مدني، لتحديد الوجهة والهدف من تلك القوانين. ووضع ضمانات أقوى لحماية حقوق المستخدمين في التمتع بالخصوصية، بما يضمن وقف الهيمنة على مزودي خدمات الإنترنت والاتصالات، والتزام الأجهزة الأمنية بالقانون.

هذه السياسة من شأنها أن توفر طرقًا قانونية للتعامل مع أي تهديدات للأمن الوطني وتكبح جماح الأجهزة الأمنية التي تخترق خصوصية المواطنين، ما يؤدي إلى تعزيز الاستقرار السياسي والاجتماعي. من جانب آخر، يساعد إدخال التعديلات التشريعية التي تمنع ممارسات المراقبة على تشجيع المستثمرين والشركات الكبرى على العمل في مصر، وهناك فرصة أمام الحكومة المصرية بعد تبني هذه السياسة في تعزيز علاقاتها الدولية بالإشارة إلى تعزيز التزاماتها في حماية الخصوصية، ما يمنح مزيدًا من فرص التعاون والتدريب مع الدول الديمقراطية.

توصيات

ترى مؤسسة حرية الفكر والتعبير أن الحكومة المصرية يمكنها إنهاء سياسة المراقبة من خلال عدة توصيات، يمكن تلخيصها كما يلي:

- يجب على رئيس مجلس الوزراء أن يصدر قرارًا ينص على الوقف الفوري لاستخدام برمجيات التجسس في عمل الأجهزة الحكومية والأمنية، ومنع الوزارات من شراء برمجيات جديدة.
- يجب أن تراجع وزارة الداخلية الإجراءات الأمنية في مراقبة مستخدمي وسائل التواصل الاجتماعي، بما يشمل وقف إحالة مستخدمي الإنترنت إلى نيابة أمن الدولة العليا.
- على مجلس النواب إلغاء العمل بقانون الجريمة الإلكترونية رقم 175 لسنة 2018، لما يحمله القانون من نصوص تسمح للأجهزة الأمنية بالقيام بالمراقبة الجماعية، على أن يتم استخدام قوانين العقوبات والجنايات في الجرائم المرتكبة عبر الإنترنت.
- على الحكومة المصرية التقدم إلى مجلس النواب بتعديل للفقرة الخامسة من المادة (3) من قانون حماية البيانات الشخصية، بحيث تخضع كل الجهات والأجهزة لسلطة القانون، وأن يقتصر استثناء بعض الجهات على صدور أوامر قضائية في حالات محددة.

- على الحكومة المصرية التقدم إلى مجلس النواب بتعديل المادة (20) من قانون حماية البيانات الشخصية، لاستبعاد الجهات الأمنية من تشكيل مركز حماية البيانات.
- يجب أن تتقدم الحكومة المصرية إلى مجلس النواب بتعديلات للمواد (64) و(67) من قانون تنظيم الاتصالات، بحيث تمنع الأجهزة الأمنية من مواصلة المراقبة الجماعية، وفرض الهيمنة على شركات الاتصالات.

خاتمة

تزداد أهمية إنهاء سياسة المراقبة مع توسع استخدام التكنولوجيا والإنترنت في كافة نواحي الحياة، ويمكن للحكومة المصرية الاهتمام بحماية الخصوصية وتعزيز حكم القانون بدلًا من التورط في ممارسات المراقبة، التي تشكل انتهاكًا لحقوق الإنسان. من شأن تبني سياسة جديدة أن يعزز من حماية الخصوصية ومن ثم يتم تعزيز فرص الاستقرار على المستويين السياسي والاجتماعي، كما أن ذلك يسهم في جذب الاستثمارات والشركات الكبرى. كما يمكن لذلك تعزيز مشاركة المواطنين في النقاش العام، بما يخدم خطط التنمية التي أعلنتها الحكومة المصرية للسنوات العشر المقبلة. ويمكن للحكومة المصرية أن تقترح تعديلات تشريعية تخدم هذه الأهداف.

مراجع

[1] Access now ، "مصر: تاريخ طويل من مراقبة الإنترنت"، أكتوبر 2020، متاح على الرابط التالي: 8%A7

[2] مؤسسة حرية الفكر والتعبير، "دعوى أمام القضاء الإداري ضد وزارة الداخلية لإيقاف نظام مراقبة ال

[3] حكم محكمة القضاء الإداري بخصوص الدعوى رقم 63055 لسنة 68 قضائية، 2017، متاح على الرابط التال

[4] Access now ، مرجع سبق ذكره.

[5] الوطن، "منبع شخص أدمن صفحة على فيسبول تحرض على قتل أفراد الجيش والشرطة في المنيا"، 2016، مت

[6] تم المادة 64 من قانون تنظيم الاتصالات رقم 64 لسنة 2003 "يلتزم مقدمو ومعدمو خدمات الاتصالات وا
ومع مراعاة حرمة الحياة الخاصة للمواطنين التي يحميها القانون يلتزم كل مشغل أو مقدم خدمة أو موف

[7] :~:text=The%20briefing%2C%20Encryption%3A%20A%20Matter,to%20privacy%20and%20free%20speech

[8] مسار، "أحداث الرقابة على الإنترنت في مصر"، ديسمبر 2020، متاح على الرابط التالي: 8%B5%D8%B1

[9] مركز هردو للتعبير الرقمي، "موجز سياسات مراقبة الاتصالات والإنترنت"، 2020، متاح على الرابط ال

[10] محادثة هاتفية مع خبير في الأمان الرقمي، إبريل 2021.

[11] مؤسسة حرية الفكر والتعبير، "الحريات الرقمية.. مفاهيم أساسية"، 2013، متاح على الرابط التا

[12] تقرير مفوضية الأمم المتحدة السامية لحقوق الإنسان، "الحق في الخصوصية في العصر الرقمي"، يونيو

[13] ps://afteegypt.org/wp-content/uploads/Egypt-Internet-Censorship-AFTE-OONI-2018-07.AR_.pdf

[14] مدى مصر، "مراقبة الاتصالات.. كيف مكنتهن محاولات الدولة للسيطرة على الفضاء الإلكتروني"، مايو 5

[15] المذكرة الإيضاحية لقانون حماية البيانات الشخصية رقم 151 لسنة 2020.

[16] مسار، "قانون حماية البيانات الشخصية.. تعزيز للحق في الخصوصية، أم إبهام يتحصن البيئة التنظ

[17] تم المادة (3) من قانون حماية البيانات الشخصية رقم 151 لسنة 2020 "لا تسري أحكام القانون الص

١ - البيانات الشخصية التي يحتفظ بها الأشخاص الطبيعيون للغير، ويتم معالجتها للاستخدام الشخصي. ا

٢ - البيانات الشخصية التي تتم معالجتها بغرض الحصول على البيانات الإحصائية الرسمية أو تطبيقًا لنص

٣ - البيانات الشخصية التي تتم معالجتها حصرًا للأغراض الإعلامية بشرط أن تكون صحيحة ودقيقة، وألا تستخ

٤ - البيانات الشخصية المتعلقة بمحاضر الضبط القضائي والتحقيقات والدعاوى القضائية.

٥ - البيانات الشخصية لدى جهات الأمن القومي، وما تقدره لاعتبارات أخرى، ويجب على المركز، بناءً على

٦ - البيانات الشخصية لدى البنك المركزي المصري والجهات الخاضعة لرقابته وإشرافه، عدا شركات تحويل

[18] العربي الجديد، "مصر، قانون حماية البيانات الشخصية يقلق جوجل ومايكروسوفت"، 2019، متاح على

تابعونا على :

آخر التحديثات

حرية الفكر والتعبير تدعو نقابة الأطباء إلى احترام حرية التعبير

النقد الممنوع.. هل يستحق مبدو المحاسبة والعقاب؟

النشرة الأسبوعية للأخبار القانونية (7 : 14 أغسطس 2022) | تجديد الحبس الاحتياطي لخمسة متهمين

الدعوة إلى الحوار لا توقف آلة القمع

النشرة الأسبوعية للأخبار القانونية (31 يوليو: 7 أغسطس 2022)

محكمة الجنايات تُجدد حبس الصحفي مدحت رمضان لمدة 45 يومًا

محتوى الموقع منشور برخصة المشاع الإبداعي نَسب المُصنَّف 4.0