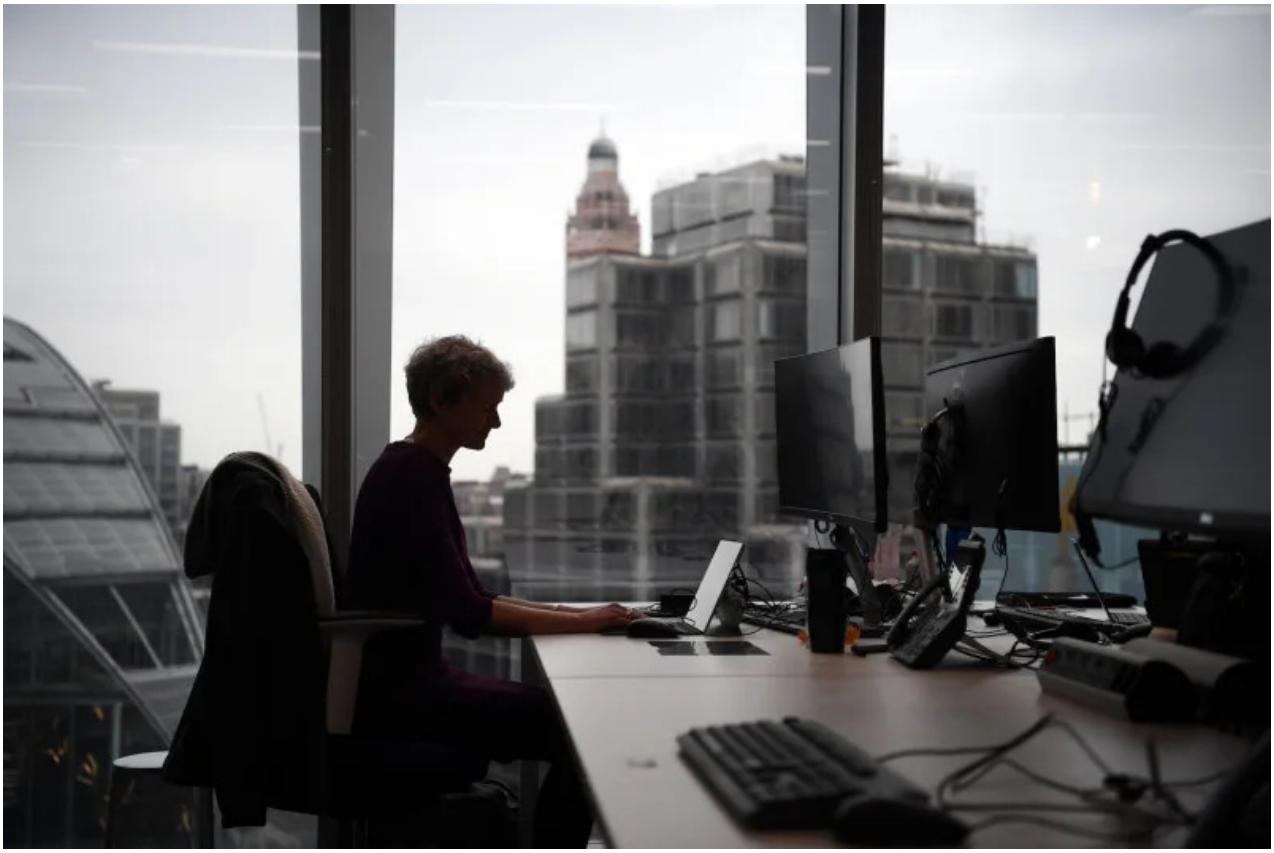
هل يمكن تقنين الإنترنت دون السقوط في فخ الدكتاتورية؟



ترجمة وتحرير: نون بوست

يوم 16 تشرين الثاني/ نوفمبر 2018، وقع الرئيس الأمريكي دونالد ترامب مشروع قانون لإنشاء وكالة جديدة للأمن الإلكتروني وأمن البنى التحتية ليغيّر بموجبه "إدارة الحماية القومية والبرامج" في وزارة الأمن الوطني إلى وكالة الأمن الإلكتروني وأمن البنى التحتية.

يهدف هذا التغيير إلى تعزيز دفاعات الولايات المتحدة ضد المخاطر المادية والرقمية التي تهدد البنية التحتية الحيوية. ولا تُعد أسباب إنشاء هذه الوكالة غامضة، حيث تدرك الديمقراطيات بشكل متزايد أنها لا تستطيع الاعتماد بشكل تام على السوق غير الخاضعة للقوانين لحماية المواطنين أو حتى الشركات من المخاطر السيبرانية. وفي الوقت الراهن، تكمن المشكلة الأساسية في كيفية مواجهة التهديدات الحالية مع الحفاظ على شبكة إنترنت مجانية ومفتوحة لجميع الأمريكيين.

تكافح الديمقراطيات في التعامل مع الاختلافات القائمة بين ضرورة الحفاظ على المبادئ التي ترتكز عليها الإنترنت على غرار الحرية والانفتاح التي تدعو إليها سياسة هذه البلدان، وحقيقة الإنترنت في الواقع التي تتصف بكونها شبكة غير آمنة ومركزية وتخضع لقيود متزايدة. وتواجه استراتيجيات الإنترنت الديموقراطية العديد من المشاكل التي ينبغي حلها، بما في ذلك الحاجة إلى إيجاد توازن بين الانفتاح الكلي لهذه الشبكة (وهو الأمر الذي يشكل خطرا كبيرا) والتحكم الكامل فيها (وهو نموذج استبدادي للإنترنت).

خلال الأشهر الستة الماضية، جرى إقرار أو اقتراح العديد من القوانين الصارمة والشاملة بذريعة مكافحة الجريمة الإلكترونية في كل من الفيتنام وتايلاند وتنزانيا والإمارات العربية المتحدة ومصر

خلال سنة 2016، عانت الانتخابات الرئاسية الأمريكية والانتخابات في جميع أنحاء أوروبا من التدخل الخارجي في العمليات الانتخابية، كما أدت الهجمات الإلكترونية المدمرة للبرمجيات الخبيثة بيتيا على أوكرانيا في خلق فوضى عارمة في جميع أنحاء العالم. وفي الواقع، يدفع الأمن السيبراني العديد من البلدان لاعتماد نهج أكثر استبدادية فيما يتعلق بالإنترنت.

في شهر تشرين الثاني/ نوفمبر من سنة 2018، صدر قرار يُعنى بالجريمة الإلكترونية دعمته روسيا وتبنته الجمعية العامة للأمم المتحدة. وقد صوتت ثلاث دول من أكبر الديمقراطيات في العالم وهي الهند والبرازيل ونيجيريا إلى جانب كل من روسيا والصين، لتتصادم مع بعض الدول التي تعتبر أكثر انفتاحا على غرار أستراليا وكندا وإستونيا وفرنسا واليونان وإسرائيل والولايات المتحدة وبريطانيا.

في هذا الإطار، اختارت بعض الدول الاتجاه الذي يقضي بضرورة زيادة المراقبة على شبكة الإنترنت. وخلال الأشهر الستة الماضية، جرى إقرار أو اقتراح العديد من القوانين الصارمة والشاملة بذريعة مكافحة الجريمة الإلكترونية في كل من الفيتنام وتايلاند وتنزانيا والإمارات العربية المتحدة ومصر. وحتى الهند، التي تعتبر أكبر ديمقراطية في العالم، لجأت إلى تبني بعض السياسات التكنولوجية المثيرة للقلق في الآونة الأخيرة.

لابد من اعتماد خيارات جديدة للتصدي للمخاطر التي تهدد الأمن السيبراني بدلا من تبني نهج عدم التدخل النسبي، حتى لا تتحكم بعض الحكومات في الإنترنت بشكل استبدادي، وتفرض رقابة مشدّدة على هذه الشبكة ضمن حدودها. وقد دعا بعض خبراء الأمن الإلكتروني إلى اعتماد النموذج البريطاني. فقد ارتأت المملكة المتحدة أن مواطنيها والشركات الصغيرة غير معنيين بمعالجة المخاطر التي تهدد الأمن السيبراني بشكل شخصي. وعلى هذا النحو، يقدم النهج الذي تعتمده بريطانيا مقاربة فلسفية مثيرة للاهتمام حول أدوار ومسؤوليات الحكومات إزاء حماية الأمن السيبراني داخل حدودها.

عززت الحكومة البريطانية بروتوكول البوابة الحدودية (الذي يدير حركة الإنترنت في جميع أنحاء العالم) ونظام التشوير رقم 7 (بروتوكول تنظيم الاتصالات الدولية) لجعل عملية إعادة توجيه حركة الإنترنت أو تدفق المعطيات الخبيثة أكثر صعوبة

يمكن للحكومات ممارسة هامش من النفوذ على شبكة الإنترنت داخل حدودها دون أن تكون استبدادية؛ في حال كانت تسعى إلى حماية المواطنين من المخاطر التي تهدد الأمن السيبراني، على غرار سرقة الهوية أو قرصنة جهاز الحاسوب، وكانت هذه التدابير مدعومة بالقوانين والإجراءات الديمقراطية التي تمنع إساءة استخدام السلطة (مثل استخدام الأمن الإلكتروني كذريعة للرقابة على الإنترنت). وتكتسي هذه الفكرة قدرا من الأهمية في وقت يبدو فيه أن البلدان في جميع أنحاء العالم تتجه نحو تبني نموذج استبدادي لتنظيم الإنترنت بتعلة الحفاظ على الأمن السيبراني.

يتبنى "المركز الوطني للأمن الإلكتروني" في المملكة المتحدة مجموعة من الإجراءات الجديدة للدفاع عن الأمن السيبراني. فعلى سبيل المثال، طبق المركز مؤخرًا بروتوكولا لأمن البريد الإلكتروني الحكومي إلى جانب اعتماد آليات جديدة لتصفية أسماء النطاقات المخصصة، لوقف الهجمات قبل أن تصل إلى المستخدمين النهائيين.

يكمن الهدف الحقيقي من هذه الخطوة في حظر النطاقات الخبيثة وعناوين بروتوكولات الإنترنت، التي جرى إرسال الرمزين 0 و1 عبر الويب إليها، قبل أن تصل تلك البيانات إلى مواطني المملكة المتحدة. ومن خلال أتمتة عملية الكشف عن التهديدات البسيطة وتخفيفها على الشبكات العامة، يمكن تركيز المزيد من الموارد على مخاطر أكبر (على غرار التهديدات المستمرة المتقدمة).

عززت الحكومة البريطانية بروتوكول البوابة الحدودية (الذي يدير حركة الإنترنت في جميع أنحاء العالم)

ونظام التشوير رقم 7 (بروتوكول تنظيم الاتصالات الدولية) لجعل عملية إعادة توجيه حركة الإنترنت أو تدفق المعطيات الخبيثة أكثر صعوبة. تساهم هذه الخطوة، التي اتخذتها كل من الصين وروسيا وغيرها من الدول الاستبدادية، في نقل حركة الإنترنت في بلد ما عبر حدود دولة أخرى مما يتيح إمكانية الوصول بسهولة إلى المعلومات الحساسة.

وفقًا للتحديث الذي أجرته بريطانيا سنة 2018 حول هذه الاستراتيجية، خفضت الحكومة من متوسط وقت ظهور مواقع التصيّد الاحتيالي والمواقع المخترقة فعليًا في المملكة المتحدة قبل إزالتها

تعتبر هذه السياسات جزءا من نظام أكبر للدفاع السيبراني في بريطانيا عبر شبكات المملكة المتحدة العامة، الذي يهدف بالتحديد إلى "تقليل أكثر أشكال هجمات التصيّد الاحتيالي أو الخداع الإلكتروني شيوعًا، وتصفية العناوين السيئة لبروتوكول الإنترنت، ومنع النشاطات الخبيثة عبر الإنترنت"، وذلك وفقًا لما أكدته الإستراتيجية الوطنية للأمن السيبراني 2016-2021.

يبدو أن تصفية التهديدات على المستوى الوطني قد آتت أكلها، فوفقًا للتحديث الذي أجرته بريطانيا سنة 2018 حول هذه الاستراتيجية، خفضت الحكومة من متوسط وقت ظهور مواقع التصيّد الاحتيالي والمواقع المخترقة فعليًا في المملكة المتحدة قبل إزالتها. وعلى الرغم من أن الحجم العالمي لعمليات التصيّد الاحتيالي حقق زيادة بنسبة 50 بالمئة منذ منتصف سنة 2016 إلى الوقت الحاضر، إلا أن نصيب هذه المواقع في المملكة المتحدة انخفض إلى حدود النصف بفضل هذه الاستراتيجية التي ساهمت في التقليل من الهجمات السيبرانية التي تؤثر على المواطنين.

خلال السنة الماضية، أشار فيليب ريتينر، رئيس "التحالف السيبراني العالمي" والمدير السابق "لمركز الأمن الإلكتروني الوطني" في الولايات المتحدة، إلى أنه "علينا التوقف عن محاولة تعليم الناس كيفية إنشاء نظام أمن سيبراني. بعبارة أخرى، تحتاج الحكومات إلى تخفيف العبء الملقى على عاتق الفرد لضمان أمنه السيبراني".

بالنسبة للخمسين دولة التي لم تتخذ موقفا حاسما فيما يتعلق بنماذج الإنترنت الخاصة بها، والتي وصفتها أنا وزملائي "بالمقررين الرقميين"، قد يكون من غير الواضح ما هو الفرق بين دفاع الحكومة عن الهجمات السيبرانية في المملكة المتحدة والتحكم في شبكة الإنترنت في دول مثل الصين. ومن الضروري كسر هذا التمييز لفهم السبب الذي يجعل النموذج البريطاني يوفر وسيلة لحماية المواطنين دون ممارسة نفوذ استبدادي على الإنترنت.

تدعم بريطانيا خدمة الإنترنت المفتوحة التي تكرس مجموعة من المبادئ على غرار حرية التعبير والنفاذ الحر إلى المعلومات وتوسع التجارة العالمية، مما يجعلها تتمسك بموقفها المناهض لنموذج الإنترنت السيادي الخاضع للقيود كما هو الحال في العديد من الدول مثل الصين وروسيا وإيران. ويخلق الإنترنت السيادي مناخا مواتيا لممارسات قمعية ضد حركات المعارضة، ويبيح عملية حجب المواقع الإخبارية الأجنبية.

تقوم استراتيجية المملكة المتحدة على تصفية البيانات عوضا عن المحتوى والتي تمثل إحدى النقاط الحاسمة في مبدأ التمايز

لقد عملت هذه الدول على تصفية المعطيات المتدفقة داخل حدودها عبر شبكة الإنترنت وتنظيمها منذ فترة طويلة، حيث تتحكم في مكان تخزين البيانات والمعلومات وفي مستخدمي الشبكة العنكبوتية وما ينشرونه، بتعلة انعدام الأمن داخل شبكة الإنترنت. ونظرا لأن الشبكة العالمية تفتح المجال أمام ظهور مخاطر عديدة، ترى السلطات أنه من الضروري فرض رقابة مشدّدة على حركة المرور على الإنترنت.

تقوم استراتيجية المملكة المتحدة على تصفية البيانات عوضا عن المحتوى والتي تمثل إحدى النقاط

الحاسمة في مبدأ التمايز. في هذه الحالة، تشير البيانات إلى الشفرة الثنائية (لغة الآلات) حيث تتكون من رمزين 1 و0، في حين تتمثل المعلومات فيما تعنيه هذه البيانات بالنسبة للمستخدم.

تهدف استراتيجية المملكة المتحدة بالأساس إلى الإطاحة بمواقع التصيد الاحتيالي، التي تسعى لإلحاق الضرر بالنظم الرقمية أو النفاذ بطريقة غير شرعية إلى بيانات معينة. في المقابل، تحاول الصين، من خلال مراقبة المحتوى، إعاقة الوصول إلى المواقع الإخبارية الأجنبية التي تنشر ما تصفه السلطات الصينية بالبرمجيات الخبيثة والمحتوى الذي يتعارض مع أهداف الحكومة. وهذا يعني أن استراتيجية بريطانيا تهدف إلى الحد من التهديدات الإلكترونية، على غرار سرقة الهوية وعمليات القرصنة، بدلا من فرض الرقابة وعزل شبكة الإنترنت في البلاد، مثلما يحدث في الصين.

قد تلجأ بعض الدول الديمقراطية إلى تصفية المحتوى، في بعض الأحيان، إلا أن هذه الممارسات تختلف عن عمليات تصفية المحتوى المعتمدة من قبل الأنظمة الاستبدادية. من جهتها، تراقب الصين المحتوى الذي يتعارض مع مبادئ قادتها وأهدافهم، وتستخدم روسيا نظام المراقبة المحلي 3-SORM للكشف عن نشاط حركات المعارضة السياسية.

من خلال تنفيذ استراتيجيات جديدة تعزز نظام الدفاع السيبراني، وضعت دول ديمقراطية على غرار المملكة المتحدة معايير مهمة تبيّن كيف تضطلع الدول الأخرى بمهامها في الوقت الذي تعزز فيه استخدام إنترنت عالمية ومفتوحة

عادة ما تعتمد الأنظمة الديمقراطية عملية تصفية المحتوى من أجل الحفاظ على رفاه الطفل والملكية الفكرية، على غرار قانون حماية الأطفال على الإنترنت بالولايات المتحدة الأمريكية وقانون حقوق الطبع والنشر بأستراليا، الذي يهدف إلى حماية المواطنين والشركات من المخاطر الإلكترونية الناجمة عن سرقة عنوان بروتوكول الإنترنت الخاص أو نفاذ الأطفال إلى المواقع الإباحية.

من خلال تنفيذ استراتيجيات جديدة تعزز نظام الدفاع السيبراني، وضعت دول ديمقراطية على غرار المملكة المتحدة معايير مهمة تبيّن كيف تضطلع الدول الأخرى بمهامها في الوقت الذي تعزز فيه استخدام إنترنت عالمية ومفتوحة. وقد حظي اقتراح فرنسا الدولي بشأن القوانين السيبرانية بتأييد واسع النطاق في إطار موافقتها على تعزيز الأمن داخل الفضاء الإلكتروني، كما تلقت مقترحات مماثلة في الجمعية العامة للأمم المتحدة القدر ذاته من الدعم. وتلعب السياسات المتبعة من قبل مؤيدي شبكة الإنترنت المفتوحة دورا مهما في التأثير على الدول التي تبدي اهتماما بمجال التكنولوجيا، والتي تصارع مع النهج الذي تتبعه فيما يتعلق بالإنترنت على غرار سنغافورة وإندونيسيا والبرازيل والمكسيك وجنوب أفريقيا.

يبقى السؤال مطروحا حول إذا كان تطبيق الاستراتيجية البريطانية حول العالم أمرا فعالا أم لا. من المؤكد أن التنفيذ سيختلف باختلاف عوامل عديدة على غرار مدى مركزية البنية التحتية للإنترنت لدى كل بلد وقوانينه الحالية. وفي حال لم ينجح تطبيق هذه الاستراتيجية على نطاق واسع، قد تستفيد بلدان مثل الصين من دفاعات الإنترنت التي تستخدمها المملكة المتحدة لتثبت أنها كانت "على حق منذ البداية" وبالتالي ستتمكن من قلب موازين الحوارات المستقبلية حول إدارة شبكة الإنترنت لصالحها.

فعلى سبيل المثال، تملك الولايات المتحدة الأمريكية عددا أكبر من عناوين آي بي الفريدة مقارنة بالمملكة المتحدة، حيث تقل فرص توحيد فضاء بروتوكول الإنترنت. لكن هذا الأمر يزيد من صعوبة تنفيذ الآليات الموجهة لتصفية البيانات المتنوعة في بريطانيا، نظرًا لوجود نطاق أوسع من عناوين الويب التي يتعين على الحكومة تصفيتها وتصنيفها ضمن المخاطر السيبرانية. ويمكن للتعديل الأول لدستور الولايات المتحدة الذي أقرته المحكمة العليا في تسعينيات القرن الماضي على خلفية قضية برنستاين ضد وزارة العدل، أن يستخدم لحماية "لغة الآلة" باعتبارها خطابا.

يعتبر تبرير الأنظمة السلطوية الذي يتمثل في تشديد الرقابة على شبكة الإنترنت من أجل مواجهة انعدام الأمن السيبراني حجة مقنعة، وهو ما يتسبب في انتشار نموذج استبدادي للإنترنت في شتى أنحاء العالم

يعد هذا الأمر بمثابة السؤال المركزي فيما يتعلق بالجهود الأمريكية لمحاكاة استراتيجية المملكة المتحدة. وحيال هذا الشأن، تقول جين بامباور إن "البيانات لا تعني بالضرورة خطابا تلقائيا ينطبق على جميع السياقات" ولكن "تقوم الدولة بتنظيم المعلومات بشكل دقيق نظرا لأنها وسيلة لإعلام الناس". ومن المحتمل أن تصفية الشيفرة الثنائية 1 و0 للبحث عن المخاطر التي تهدد الأمن السيبراني يمثل انتهاكا للمبدأ الذي يقوم عليه التعديل الأول من الدستور.

في حال كانت المملكة المتحدة على حقا لاعتقادها أن أفضل طريقة لحماية الشركات والمواطنين من التهديدات السيبرانية تكمن في إشراك الخصوم داخل شبكة الإنترنت، فإنه ينبغي على ديمقراطيات أخرى اعتماد هذا المسار أيضا. ويعتبر تبرير الأنظمة السلطوية الذي يتمثل في تشديد الرقابة على شبكة الإنترنت من أجل مواجهة انعدام الأمن السيبراني حجة مقنعة، وهو ما يتسبب في انتشار نموذج استبدادي للإنترنت في شتى أنحاء العالم.

من أجل الدفاع عن شبكة إنترنت عالمية ومفتوحة وحماية كل من الحكومات والأنظمة الاقتصادية والمواطنين على أكمل وجه ضد المخاطر السيبرانية، فإنه يجدر بالدول أن تنسج على منوال المملكة المتحدة. ويتمثل التحدي الرئيسي للأنظمة الديمقراطية في معرفة كيفية تطبيق هذه الاستراتيجية واعتمادها، فضلا عن تحقيق التوازن بين الانفتاح الكلي للشبكة ومراقبتها بطريقة تحمي المستخدمين من جهة وتضمن فوائد شبكة إنترنت عالمية وحرة من جهة ثانية.

المصدر: فورين بوليسي

رابط المقال: https://www.noonpost.com/26655/