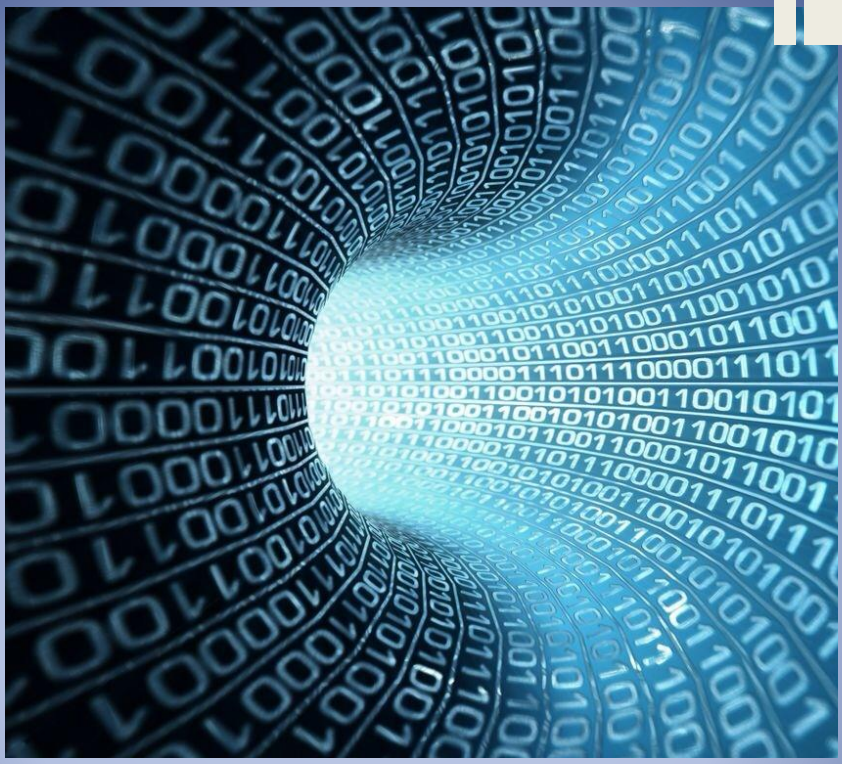


التصدي للاستبداد الرقمي

مرزوق الحلالي

منشورات فضاء الحوار الإلكترونية

شكر وامتنان

الشكر الجزيل الموصول والتقدير الوفير

لمن ألهموني إعادة إحياء

الإصرار على المضي

في الدرب إلى منتهاه

جبريل وخولة وياسمينة ونزيهة



محتويات

- المقاربة الهندية في إدارة البيانات
- اقتصاد البيانات في الهند
- البنية التحتية الرقمية
- حاجة الهند لإدارة البيانات
- الجيوسياسة والفضاء السيبراني
- الرهانات الاستراتيجية للثورة الرقمية؟

ملحق:

الدعم الدولي للدفاع السيبراني الأوكراني

الهجمات الإلكترونية الروسية

الإطار العام

المجتمع المدني العالمي في عصر جيوسياسي:

ملاحظات أولية

يتصارع الفاعلون في المجتمع المدني حول العالم مع المنافسة بين أنظمة القيم. وتؤثر التوترات الجيوسياسية المتصاعدة على المجتمع المدني الدولي ودوره في هذا النظام العالمي المتغير.

على مدى العشرية الماضية ، أصبح اشتداد الخصومات والتوترات الجيوسياسية يهيمن على الاهتمام السياسي والدبلوماسي والتحليلي. لقد رسم العديد من المحللين خريطة لمنافسة القوى العظمى للعصر الناشئ. إن التنافس المتصاعد بين الولايات المتحدة والصين هو مجال رئيسي للقلق ، في حين أن الاحتكاك بين روسيا والغرب قد انفجر الآن من قلق متصاعد إلى حرب مستعرة. ولا تزال الخلافات العامة والخلافات الجيوسياسية الأخرى ، التي تشمل قوى مثل الهند وباكستان وتركيا ودول الخليج وإيران وغيرها ، حاضرة بجلاء على نطاق واسع عبر المشهد الدولي.

هناك اليوم اتفاق واسع النطاق على أن المنافسة الجيوسياسية المتزايدة هي السمة المميزة للعلاقات الدولية المعاصرة. بينما تختلف التفسيرات حول أنواع الجغرافيا السياسية التي تعتبر الآن أكثر تحديدًا وحول كيفيات عملها

في ديناميكيات بين الدول. ومع ذلك ، فإن أحد الجوانب التي لم تحظ باهتمام مستمر هو ما يعنيه هذا الاتجاه على المستوى غير الحكومي أو المجتمعي.

فكيف يؤثر العصر الجيوسياسي على المجتمع المدني العالمي؟
إن التماشي مع روح العصر الجيوسياسي جعل التحليل يرتكز على الإجراءات والتكتيكات الحكومية ، و الكثير من تحليلات العلاقات الدولية اتجهت نحو المفاهيم ر الموجهة نحو الدولة. بينما يولي المحللون القليل من الاهتمام لدور الجهات الفاعلة غير الحكومية في الصراعات الجيوسياسية ، فإن الدور الأوسع للفاعلين المدنيين في الجغرافيا السياسية المعاصرة ما يزال يعاني من نقص التحليل. عمومًا الجميع أضحى اليوم يفهم أن الديناميكيات الناشئة لنظام عالمي مُعاد تشكيله تحركها بشكل أساسي الدول والجهات الفاعلة الأمنية ، حيث تضيف الكيانات التجارية منطقًا جغرافيًا اقتصاديًا أكثر حدة. فإلى أي مدى يجب أن يُنظر إلى الفاعلين المدنيين على أنهم جزء من المشهد الجيوسياسي المتغير؟ وما هو بُعد المجتمع المدني في الجغرافيا السياسية؟ وما المقصود بالجغرافيا السياسية الناشئة للمجتمع المدني؟

هناك جملة من التساؤلات تستوجب المزيد من الفهم والتوضيح، مثل التعاون الصيني مع جزء من المجتمع المدني في تايوان والتقارب بين الصين والمجتمع المدني المحافظ في تايلاند، والدعم غير الغربي للمجتمع المدني في جميع أنحاء إفريقيا وكيف تتفاعل الجماعات المدنية الأفريقية مع هذا الاتجاه، ومحاولة الحكومة التركية استخدام الفاعلين المدنيين لتحقيق أهداف استراتيجية، و استخدام الجماعات غير الحكومية في صراعات الشرق الأوسط، و الأنشطة الدولية المتزايدة للجماعات المحافظة الأمريكية والتصدير الفعلي للاستقطاب السياسي الأمريكي إلى

دول أخرى، و دور ديناميكيات المجتمع المدني في الحرب على أوكرانيا، واستخدام الحكومات للمجتمع المدني لأسباب استراتيجية وردود فعل المجتمع المدني على الجغرافيا السياسية للدولة.

من خلال التطورات العالمية الأخيرة يبدو أن هناك "جيوسياسة للمجتمع المدني" - geopolitic civil society - في طور التبلور. فهناك أنواع ودرجات مختلفة من التغيير جعلت المجتمع المدني العالمي جيوسياسيًا.

من الواضح أن جملة من الحكومات أضحت تستخدم الجهات الفاعلة في المجتمع المدني. وأن الحكومات الغربية تعمل منذ فترة طويلة مع المجتمع المدني لتعزيز مصالحها الخاصة ، وبدأت القوى غير الغربية الآن تحذو حذوها، وذلك لدعم مبادرات المجتمع المدني والجهات الفاعلة للأغراض الجيوسياسية. لسنوات عديدة ، كان دعم المجتمع المدني يكاد يكون حصريًا حول قيام المانحين الغربيين بتمويل الجماعات المدنية كجزء من الجهود المبذولة لتعزيز الديمقراطية والحقوق والتنمية، أما اليوم ، تشارك الحكومات الأخرى – غير الغربية - في مثل هذا الدعم لمجموعة مختلفة عن القيم الغربية. مثلا تسعى الحكومات المتورطة في التوترات الجيوسياسية والتنافس العالمي إلى توظيف الفاعلين المدنيين كأدوات لتعزيز أهدافها الاستراتيجية. كما تسعى الحكومات أحيانًا كثيرة إلى دعم المجتمع المدني الخاص بها نحو المساهمة في تحقيق أهدافها في النزاعات أو الأزمات. وفي أوقات أخرى ، تعتمد أشكالًا أكثر انتشارًا للتأثير من خلال الجهود التعليمية والثقافية.

بالإضافة إلى الإجراءات الحكومية فيما يتعلق بالمجتمع المدني ، هناك

ديناميكية مختلفة تتعلق بالطريقة التي يتعامل بها الفاعلون المدنيون مع بعضهم البعض استجابة للتوترات والتحديات الجيوسياسية. تتوفر اليوم الروابط الجديدة عبر الحدود بين الجهات المدنية ذات الصلة بالديناميكيات الجيوسياسية. وغالبًا ما تدعم الحكومات شركائها الوطنيين من المجتمع المدني بشكل صريح لبناء روابطهم الخاصة مع المجتمع المدني في البلدان الأخرى. وفي حالات أخرى ، تكون شبكات المجتمع المدني مستقلة نسبيًا عن المشاركة الحكومية المباشرة ومع ذلك لها تداعيات واضحة على المصالح الجيوسياسية.

يبدو اليوم كأن هناك إعادة تموضع المجتمع المدني، ويتضح هذا من خلال الطريقة التي تغير بها منظمات المجتمع المدني وجهات نظرها واستراتيجياتها تجاه الأجندات الجيوسياسية للدول والحكومات، تبديل التحالفات والشركاء. بينما يصبح المجتمع المدني جزءًا من ساحة المعركة الجيوسياسية ، يغير الفاعلون المدنيون استراتيجياتهم وحتى أجنداتهم الأساسية، وتختلف طبيعة هذه التحولات بشكل كبير عبر المناطق. وأصبح العديد من الفاعلين في المجتمع المدني أكثر حذراً في عملهم الطويل الأمد الموجه نحو الحقوق بسبب الاعتبارات الجيوسياسية. الجيوسياسية كطريقة لترسيخ وإبراز تركيزهم على القيم الليبرالية والديمقراطية. في حالات أخرى ، يحاولون التخفيف أو ببساطة الابتعاد عن المجالات الجيوسياسية.

إن المنافسة الاستراتيجية بين الحكومات تترك بصماتها على المستوى المجتمعي. لا يظهر عصر السياسات الدولية التنافسية والمقسمة فقط في العلاقات بين الحكومات ولكن أيضًا في المجال المدني. كانت القوى غير الديمقراطية وغير الغربية تقتصر تقليديًا على بناء علاقات مع الحكومات ، لكنها بدأت في البحث عن تحالفات مع المجتمع المدني. إذ يتم جذب العديد

من الفاعلين المدنيين إلى المنافسة الجيوسياسية. في الوقت نفسه ، يقوم البعض منهم بتعديل تركيزهم وأنشطتهم في محاولة للتخفيف من الآثار السلبية لتنافس القوى العظمى.

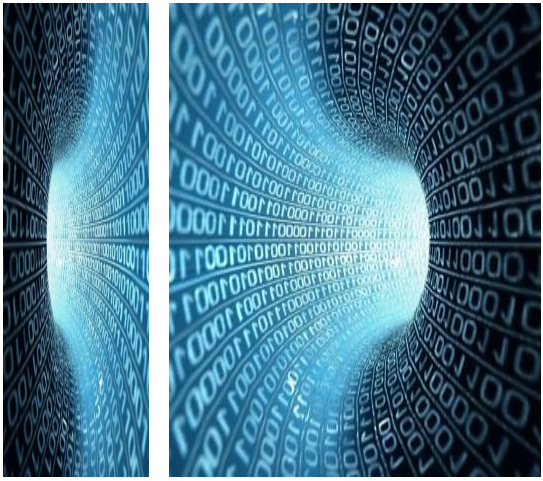
قد يبدو هذا الاتجاه في العديد من الأماكن جنيني وجزئي. لكن تتجه القوى الرئيسية إلى زيادة وجودها في المجتمع المدني وتأثيرها عليه. وفي كثير من الحالات ، أصبح المجتمع المدني جيوسياسيًا ولكن بطرق غير مباشرة نسبيًا.

ومع ذلك ، هناك إشارات وقرائن تدل على أن المجتمع المدني يتجه في اتجاه جيوسياسي أكثر. وهذا يعني أن المجتمع المدني قد يصبح فاعلا في الجيوسياسية العالمية في المستقبل. التناقض الناشئ هو أن الأنظمة غير الديمقراطية المنخرطة في سحق المجتمع المدني داخليًا وتضييق الخناق عليه تستخدم فاعلين مدنيين في الخارج. فهل المجتمع المدني العالمي يتجه نحو عدم الحد من الدولة بقدر ما يتعلق الأمر بالعمل معها شمن أهداف جيوسياسية.

نشأ المجتمع المدني العالمي في أعقاب الحرب الباردة مباشرة ، عندما كانت الديمقراطية تتوسع بسرعة ، وكانت المنافسة بين القوى العظمى على مستوى العالم في أدنى مستوياتها بعد عدة عقود من التنافس بين القوى العظمى ثنائية القطب. وقد ميزت هذه السمات بقوة كلاً من مجموعات المجتمع المدني الوطنية والمحلية أثناء انتشارها في جميع أنحاء العالم. نظرًا لأن هذه السمات الشاملة قد أفسحت المجال لعلاقات دولية

أكثر تصادمية وصراعات حول القيم ، فقد بدأت ملامح المجتمع المدني العالمي في التحول.

ومع ذلك ، فإن هذه المعطيات الجديدة لحياة المجتمع المدني في ظل المنافسة الجيوسياسية المتزايدة لم يتم رسمها بشكل منهجي بعد، ولم يتم تحديد الاتجاهات بعد بدقة ، ولكن الأكيد، هو أنه سيكون هناك المزيد من التقاطع مستقبلا بين التطورات الجيوسياسية والمجتمعية. وستشكل الجيوسياسة المجتمع المدني ، وسيؤثر المجتمع المدني على الجيوسياسة، و سيكون المجتمع المدني العالمي موضوعًا لمنافسة القوى العظمى وموضوعًا منخرطًا بشكل أعمق في الجيوسياسة.



تقديم

برزت مؤخرا مخاوف بشأن الاستبداد الرقمي الغربي، وقد ذهب العديد من المراقبين إلى اعتبار أن التنافس بين الديمقراطية والاستبداد من شأنه التأثير في مسار حوكمة التكنولوجيا والبيانات (1)

Governance of technology and data

في هذا السياق ، يقال إن الديمقراطيات في العالم لديها مقاربات مفتوحة تعتمد على آليات السوق، على النقيض من ذلك ، تتميز الأنظمة الاستبدادية في العالم بدور الدولة الكبير ورغبتها الحثيثة لتعزيز قدرتها على تسخير جميع البيانات ، العامة والخاصة على حد سواء لفائدتها.

(1) - حوكمة البيانات هي مجموعة من المبادئ والمعايير والممارسات التي تضمن أن بياناتك موثوقة ومتسقة ، ويمكن الوثوق بها لاتخاذ القرارات المناسبة والوقت المناسب واستغلال كل الفرص لدعم الاختيارات المعتمدة وعرقلة أو إفشال ما يناهضها ويعاكسها و وتعزيز التحولات الرقمية. يمكنك برنامج إدارة البيانات الناجح من القيام بهذه الأشياء بطريقة قابلة للتكرار ، والتي يمكن أن تتوسع وتتكيف مع نمو أحجام البيانات - والمصادر - وتطور التقنيات. باختصار ، تعني الإدارة الجيدة للبيانات أنه يمكنك استخدام بياناتك بثقة ، الآن وفي المستقبل وتوظيفها لتحقيق أهدافك.

لكن هذا التأطير الثنائي من شأنه حجب ما طورته بعض الديمقراطيات من مناهج متنوعة للتخلص من الاستبداد الرقمي الغربي. فقد قامت بعض الديمقراطيات ، خاصة في آسيا ، بتكييف إجراءات سياسية وتنظيمية توسع

نطاق تدخل الدولة. إذ طورت أنظمة حوكمة البيانات تعكس السمات الخاصة و الفريدة لمؤسساتها وثقافاتها السياسية. وقد يكون هذا المسار مجديا للعديد من الدول للتعايش مع "الاستبداد الرقمي الغربي" بشكل يخدم مصالحها، خاصة في الوقت الذي يتزايد فيه التركيز على سياسة البيانات على المستويين الدولي و القاري والإقليمي والوطني.

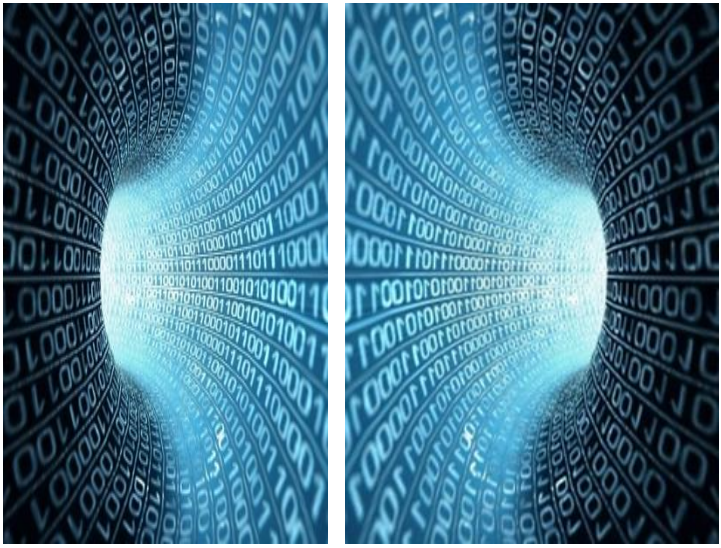
إن التأطير الثنائي الذي يصور العالم منقسما إلى مجالين فقط - مجال "سينوسفير" (2) - Sinosphere - استبدادية" تهيمن عليها الصين ومجال مفتوح وديمقراطي يتركز في الغرب عبر الأطلسي، وهذا تصور غير دقيق . فهناك دول ثالثة ، وكثير منها تحسب على الديمقراطيات الموحدة ، تؤثر، بشكل أو بآخر، مجال الجدال حول سياسة البيانات ، ونماذج الأعمال، والأطر التنظيمية. وإن هي تمكنت (أي هذه البلدان) من التعاون ، والاستفادة من قوة المعايير المفتوحة والبرمجيات مفتوحة المصدر ، وإبتكار مناهج جديدة للتنمية الرقمية ، فيمكنها أن تصبح رائدة في حد ذاتها مع تطور المرحلة القادمة من اقتصاد البيانات (3)

data economy unfolds-

(2) - يشير إلى مجموعة من البلدان والمناطق التي يسكنها حاليا غالبية السكان الصينيين أو كانت تاريخيا تحت التأثير الثقافي الصيني. صاغ عالم اللسانيات "جيمس ماتيسوف - James Matisoff - "هذا المصطلح في 1990 ، على عكس مصطلح - Indosphere - الذي يشير إلى المناطق الصينية والهندية ذات التأثير اللغوي / الثقافي في جنوب شرق آسيا باسم" سينوسفير "و" إندوسفير ". وتم تلميع المصطلح على أنه: مجال اجتماعي وسياسي يشمل تلك البلدان والثقافات واللغات التي تأثرت تاريخيًا بالسياسة والثقافة والدين واللغات في الصين.

(3) - أحدث التحول الرقمي نوعا جديدا من الاقتصاد يعتمد على "تحويل البيانات" فعليا إلى أي جانب من جوانب النشاط الاجتماعي والسياسي والاقتصادي البشري نتيجة للمعلومات التي تم إنشاؤها بواسطة الروتين اليومي الذي لا يعد ولا يحصى للأفراد والآلات المتصلة رقميا. هذا الاقتصاد الناشئ قائم على البيانات في النماذج النظرية للنمو الداخلي ، والتي تقدم البحث والتطوير ، وتكوين رأس المال البشري والتدمير الإبداعي من خلال سرقة الابتكارات كمحركات للنمو الاقتصادي ، إلى جانب العوامل الخارجية المتعلقة بتداعيات المعرفة المحلية. و يسمح هذا الاقتصاد للابتكار بتوليد قوة سوقية وإيجارات احتكارية لأنه على الرغم من أن المعرفة ليست منافسة (أي يمكن استخدامها في وقت واحد من قبل العديد من الوكلاء دون الانتقاص من

فائدتها) ، إلا أنها على الأقل مستبعدة جزئيا إذ يمكن للشركات المبتكرة تقييد الوصول إلى اختراعاتها). علاوة على ذلك ، نظرًا لأن البيانات هي معلومات في حد ذاتها ، فليس لها قيمة جوهرية ، لأن استخدامها (أو إعادة استخدامها) هو الذي يحدد قيمتها.



البدائل الآسيوية لإدارة البيانات الآسيوية:

الهند وكوريا الجنوبية تنشئان نماذج وسياسات جديدة

ولعل أبرز مثال لبديل إدارة البيانات يخص الهند وكوريا الجنوبية. وهو مثال يبين محدودية التأطير الثنائي الذي يصور العالم منقسما إلى مجالين -

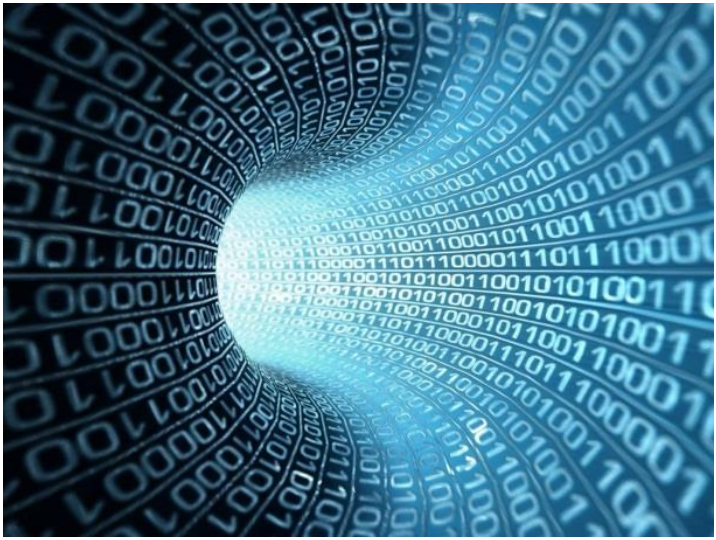
السالف الذكر- ويكشف مدى تعقيد العالم بدرجة أكبر من التنبؤ الشائع بمعركة بين النهج المتمحور حول الولايات المتحدة والصين.

فالطريقة الكورية الجنوبية في التعاطي مع البيانات تتميز في ثلاثة جوانب مهمة: مرونة البيانات ، وتوطين البيانات والخصوصية ، والمصادقة عبر الإنترنت والتحكم في الوصول إلى البيانات. كما تمثل البيانات المفتوحة وحوكمة البيانات عبر الحدود - مع الهند ، شركة رائدة في خدمات البرمجيات وتكنولوجيا المعلومات.

بالنسبة لأولئك الذين يعتقدون أن العالم يواجه خيارا صارخا أو ثنائيا – لا ثلث له- فقد أظهر مثال كوريا الجنوبية والهند بين النماذج الديمقراطية التي تتمحور حول المحيط الأطلسي أو النماذج الاستبدادية المتمركزة حول الصين ، فقد أظهر مثال كوريا الجنوبية والهند أن لاعبين إضافيين يمكنهم أن يقودوا المسار في عدة جوانب رئيسية. فالهند وكوريا الجنوبية محسوبتان على الأنظمة الديمقراطية ، ولا تقوم أي منهما بمحاكاة التجارب الأمريكية أو الأوروبية، بل بدلاً من ذلك ، فإنهما قادتا مناهجهما الخاصة ، وتموجان وتطابقان عناصر التأطير المؤسساتي للديمقراطية المتعارف عليها مع المتطلبات والسياسات الوطنية المستمدة من ثقافات سياسية خاصة بهما.

إن الديمقراطيات الآسيوية الكبرى مثل الهند وكوريا الجنوبية لا تحاكي وتتبع ببساطة الولايات المتحدة وأوروبا في إدارة البيانات. بدلاً من ذلك ، وفي العديد من المجالات المتصلة بكل من البيانات المفتوحة والبيانات العابرة للحدود ، فإنهما يبتكران مناهجهما الفريدة الخاصة بهما ، والتي

ترتكز بقوة على مؤسساتهم الديمقراطية. ويمكن للكثير من بلدان العالم التي تعاني من الاستبداد الرقمي الغربي أن تتعلم منهما الكثير، بل ويمكنها محاكاة كل أو بعض من تجارب هاتين الديمقراطيتين الأسيويتين.



كيف يمكن للهند وكوريا قيادة تفكير جديد حول البيانات؟

أدت المخاوف بشأن الاستبداد الرقمي إلى جعل العديد من المراقبين يفترضون أن تنافس صارخ بين الديمقراطية والاستبداد سيشكل حوكمة التكنولوجيا والبيانات . وفي هذا النطاق، اعتبروا أن الديمقراطيات في العالم لديها مقاربات مفتوحة تعتمد على آليات السوق. وعلى النقيض من

ذلك ، فإن الأنظمة الاستبدادية في العالم ، تمنح امتيازًا لدور الدولة التي تهدف إلى تعزيز قدرتها على تسخير جميع البيانات ، العامة والخاصة على حد سواء لفائدتها.

لكن هذا التأطير الثنائي يظل ضيقا، إذ يلغي المدى الذي طورت فيه الديمقراطيات مناهج متنوعة. قامت بعض الديمقراطيات ، خاصة في آسيا ، بتكييف ميزات سياسية وتنظيمية تعمق وتوسع نطاق تدخل الدولة. لقد طورت بعض الديمقراطيات ، وخاصة في آسيا ، أنظمة حوكمة البيانات التي تعكس السمات الفريدة لمؤسساتها وثقافاتها السياسية.

لذلك، من المهم الخروج من دائرة الثنائية للبحث في هذا التنوع ، لا سيما في وقت يتزايد فيه التركيز على سياسة البيانات على المستويين الدولي والقاري والإقليمي والوطني والمحلي. إن هذا التركيز المكثف على البيانات مدفوع بعدة عوامل، بما في ذلك :

- القوة المتزايدة لشركات "الخدمات السحابية"(4) متعددة الجنسيات ، مثل Amazon Web Services -؛

(4) - الحوسبة السحابية هي توفير خدمات الحوسبة (بما في ذلك الخوادم والتخزين وقواعد البيانات وإدارة الشبكات والبرمجيات والأدوات التحليلية والذكاء الاصطناعي) عبر الإنترنت (السحابة) بغرض تقديم ابتكار أسرع وموارد مرنة واقتصاديات الحجم. عادةً ما تدفع فقط مقابل الخدمات السحابية التي تستخدمها (تقليل تكاليف التشغيل) ، وإدارة البنية التحتية الخاصة بك بشكل أكثر كفاءة ، وتوسيع نطاق الخدمات بناءً على احتياجات عملك.

-الكميات الهائلة من البيانات التي يتم جمعها بواسطة منصات التواصل الاجتماعي ؛

-الأهمية المتزايدة لـ "إنترنت الأشياء" (5) في العديد من قطاعات الاقتصاد العالمي ؛

(5) - إنترنت الأشياء هي "بنية تحتية عالمية لمجتمع المعلومات ، والتي تجعل من الممكن الحصول على خدمات متقدمة من خلال ربط الأشياء (المادية أو الافتراضية) بفضل المعلومات الحالية القابلة للتشغيل البيني وتقنيات الاتصال. من وجهة نظر مفاهيمية ، يميز إنترنت الأشياء، الأشياء المادية المتصلة والتي لها هويتها الرقمية الخاصة وقادرة على التواصل مع بعضها البعض. تخلق هذه الشبكة بطريقة ما جسراً بين العالم المادي والعالم الافتراضي.

-مخاوف واسعة النطاق حول العالم من سرقة بيانات المواطنين لصالح الشركات الأجنبية ؛

-الإثارة حول التطبيقات الجديدة للذكاء الاصطناعي (6)، وخاصة التعلم الآلي ، والتي ستفيد الشركات والبلدان القادرة على إنشاء وإدارة وإعادة دمج مخزون ضخم من البيانات بجودة عالية.

(6) - الذكاء الاصطناعي هو في الواقع تخصص حديث يمتد لنحو ستين عامًا فقط ، والذي يجمع بين العلوم والنظريات والتقنيات (على وجه الخصوص المنطق الرياضي والإحصاء والاحتمالات وعلم الأعصاب الحسابي وعلوم الكمبيوتر) والذي يتمثل هدفه في التوصل إلى تمكين آلة تقليد القدرات المعرفية للكائن البشري.

وسط هذا الزخم والتركيز المتزايد على البيانات ، لم يعد العالم ينقسم إلى مجالين فقط - مجال "سينوسفير" استبدادي تهيمن عليه الصين ومجال مفتوح وديمقراطي يتركز حول الغرب عبر الأطلسي. وبدلاً من ذلك ، فإن دولاً ثالثة ، وكثير منها ديمقراطيات موحدة ، تؤثر على المناقشات حول سياسة البيانات ، ونماذج الأعمال لشركات التكنولوجيا ، والأطر التنظيمية. إذا تمكنت هذه البلدان من التعاون ، والاستفادة من قوة المعايير المفتوحة والبرمجيات مفتوحة المصدر ، وإظهار مناهج جديدة للتنمية الرقمية ، فيمكنها أن تصبح رائدة في حد ذاتها مع تطور المرحلة التالية من اقتصاد البيانات (7).

(7) - يُنشئ التحول الرقمي نوعًا جديدًا من الاقتصاد يعتمد على "تحويل البيانات" فعليًا إلى أي جانب من جوانب النشاط الاجتماعي والسياسي والاقتصادي البشري نتيجة للمعلومات التي تم إنشاؤها بواسطة الروتين

اليومي الذي لا يعد ولا يحصى للأفراد والآلات المتصلة رقمياً. إنه اقتصاد ناشئ قائم على البيانات، ويمكن وضعه في النماذج النظرية للنمو الداخلي ، والتي تقدم البحث والتطوير، وتكوين رأس المال البشري و"التدمير الإبداعي" من خلال سرقة الابتكارات، كمحركات للنمو الاقتصادي ، إلى جانب العوامل الخارجية الإيجابية المتعلقة بتداعيات المعرفة المحلية. يسمح هذا الإطار النظري بمعدلات نمو متفاوتة في مختلف البلدان بناءً على سياساتها لدعم الابتكار، ولكن أيضًا الانفتاح على التجارة للوصول إلى التطورات التكنولوجية المتولدة في أماكن أخرى. كما أنه يسمح للابتكار بتوليد قوة سوقية وإيجارات احتكارية لأنه على الرغم من أن المعرفة ليست منافسة (أي يمكن استخدامها في وقت واحد من قبل العديد من الوكلاء دون الانتقاص من فائدتها) ، إلا أنها على الأقل مستبعدة جزئيًا (أي أن الشركات المبتكرة يمكن تقييد الوصول إلى الميزات الجديدة لاختراعاتها).

ولعل النماذج البديلة التي نشأت في ديمقراطيتين آسيويتين رئيسيتين ، الهند وكوريا الجنوبية من شأنها تبيان مدى تعقيد العالم أكثر من التنبؤ الشائع بصراع بين النهج المتمحور حول الولايات المتحدة و النهج المتمحور حول الصين.

بالنسبة لأولئك الذين يعتقدون أن العالم يواجه خيارًا صارخًا أو ثنائيًا بين النماذج الديمقراطية التي تتمحور حول المحيط الأطلسي أو النماذج الاستبدادية المتمركزة حول الصين ، تناسوا أن هناك لاعبين إضافيين قد يقودون المسار في عدة جوانب عوض الثنائية المزعومة. فتعتبر كل من الهند وكوريا الجنوبية محسوبة على الأنظمة الديمقراطية في عالم اليوم، ولا يقوم أي منهما بمحاكاة واتباع التجارب الأمريكية أو الأوروبية. وبدلاً من ذلك ، فإنهما تقودان مناهجهما الخاصة ، حيث تمزجان وتطابقان عناصر من الأطر المؤسسية الديمقراطية مع المتطلبات والسياسات الوطنية المستمدة من ثقافات سياسية مختلفة.

من المؤكد أن التقدم في حوكمة البيانات في كل من الهند وكوريا الجنوبية كان متفاوتًا. فقصتهما ليست بسيطة بأي حال من الأحوال. على سبيل

المثال ، إن المؤسسات والوكالات المختلفة في حكومات كل من هذين البلدين لديها أهداف سياسية متضاربة ، وعندما تصطدم سياساتهما ، يكون من المستحيل تقريبًا تطوير رؤية واستراتيجية واضحة ومتسقة. وغالبا ما كانت النتيجة عدم كفاية الاستثمار ومشاريع متعثرة؛ والفرص الضائعة لمشاركة البيانات ودمجها واستخدامها لحل المشكلات في القطاعين العام والخاص الهندي والكوري الجنوبي. فالوكالات والمؤسسات المتباينة في بيروقراطية مجزأة يمكن أن تؤدي إلى أهداف سياسية متباينة.

1 - عندما تتعارض السياسات

في المحافل الدولية مثل مجموعة العشرين - G20 - (8) عملت وزارة الخارجية الكورية الجنوبية بجد لإبرام اتفاقيات لتسهيل تدفق البيانات عبر الحدود. وتم دعم جهود الوزارة من قبل وزارة الاقتصاد والمالية الكورية ، التي تسعى جاهدة لتعظيم الفرص للشركات الكورية التي ترغب في تقديم خدمات تعتمد على البيانات للعملاء والشركات في جميع أنحاء العالم.
ولكن في الوقت نفسه ، منعت وكالات الأمن القومي في كوريا الجنوبية تصدير أنواع معينة من بيانات الخرائط وغيرها من البيانات التي يرون أنها يمكن أن تستخدمها كوريا الشمالية أو خصوم آخرون لمهاجمة البلاد. هذه الوكالات التي تركز على الأمن لا تخشى الهجمات المادية فحسب ،

بل تهتم أيضًا بالقرصنة الخبيثة وحرب المعلومات (بما في ذلك المعلومات المضللة). وفي الوقت نفسه ، فإن المنظمين الماليين في كوريا ومختلف الوكالات الحكومية المكلفة بحماية خصوصية البيانات الشخصية للمواطنين الكوريين متخوفون من السماح للشركات الأجنبية بتخزين ومعالجة البيانات الكورية الجنوبية في بلدان أخرى ، لا سيما في البلدان التي لديها لوائح حماية بيانات غير كافية أو غير واضحة أو ضعيفة التنفيذ .

(8) - تم إنشاء مجموعة العشرين في 1999. وهي تضم دول مجموعة الثمانية (ألمانيا وكندا والولايات المتحدة وفرنسا والمملكة المتحدة وإيطاليا واليابان وروسيا) ، بالإضافة إلى الاتحاد الأوروبي والمملكة العربية السعودية والأرجنتين وأستراليا والبرازيل والصين وجنوب كوريا والهند وإندونيسيا والمكسيك وجنوب إفريقيا وتركيا. وبالتالي فهي تمثل 90 في المائة من الناتج القومي الإجمالي للعالم ، و 80 في المائة من التجارة العالمية وثلثي سكان الكوكب .

الوضع مشابه تمامًا في الهند. دافعت وزارة الإلكترونيات وتكنولوجيا المعلومات في البلاد عن قضية عالم رقمي "بلا حدود" حتى تتمكن الشركات الهندية من نقل البيانات بسهولة عبر الحدود وخدمة عملائها بشكل أفضل، بغض النظر عن مكان تواجدهم. ولكن هناك العديد من العوائق التي تحول دون تحقيق هذه الرؤية الهندية للبيانات عبر الحدود. كما في حالة كوريا الجنوبية. تتضمن هذه العقبات اعتراضات من منظمي الخصوصية في الهند ، الذين يطورون قواعد حماية البيانات الهندية التي يمكن أن تمنع تصدير البيانات الشخصية للمواطنين الهنود إلى بلدان أخرى. والأكثر صعوبة هي مطالب مؤسسات وإدارة إنفاذ القانون الهندية ، التي تريد الوصول إلى البيانات لإجراء تحقيقات جنائية وضمان الامتثال التنظيمي، وتخشى في حالة ما إذا تم تخزين بيانات الهنود في الخارج ، سواء في قواعد بيانات الشركات أو منصات وسائل التواصل الاجتماعي أو مراكز الحوسبة السحابية ، فإنهم قد يصادفون صعوبات وعراقيل للوصول إلى البيانات التي تحتاجها. لكن الهند وكوريا الجنوبية تختلفان في أحد الجوانب بهذا الخصوص: في الهند ، غالبًا ما يبدو أن هذه الحجج من سلطات إنفاذ القانون هي التي تربح اليوم. في المقابل ، في كوريا ، كان

للمخاوف المتعلقة بالأمن القومي تأثير أكبر بكثير على النتائج والسياسات من مخاوف أجهزة إنفاذ القانون.

2 - الحاجة للقيادة الرقمية

ومن المثير للاهتمام ، في كل من الهند وكوريا الجنوبية ، أن السياسة الرقمية تأتي على رأس قائمة الأولويات الوطنية. لهذا السبب تعالج حكومتا البلدين القضايا الرقمية والمتعلقة بالبيانات على أعلى مستوى ممكن. جعل رئيس الوزراء الهندي "ناريندرا مودي" من مشروع Aadhaar (9)

للهوية البيوميتيرية ، والذي أعطى مئات الملايين من الهنود شكلاً من أشكال التعريف الرقمي ، كأولوية شخصية. وبالمثل ، في الانتخابات الرئاسية الكورية الجنوبية لعام 2022 ، ناقش مرشحو الأحزاب الرئيسية موضوع الهوية الرقمية.

(9) - عندما تم إطلاق البرنامج في 2009 ، شرعت الهند في تحقيق المرتبة الأولى على مستوى العالم: إعطاء كل مواطن رقم تعريف فريد يمكن التحقق منه باستخدام القياسات البيوميتيرية. قالت الحكومة إن هذه القياسات الحيوية (مسح قزحية العين وسجلات بصمات الأصابع) سيتم ربطها برقم Aadhaar الخاص بشخص ما ، والذي سيتم استخدامه بدوره في جميع التفاعلات مع الدولة - للتخلص من الاحتيال ، وجعل الضرائب أكثر كفاءة ، وفي النهاية توفير المال .

غالبًا ما تجبر البلدان التي يتولى رؤساؤها ورؤساء وزرائها زمام القيادة في القرارات السياسية المتعلقة بالاقتصاد الرقمي وتفرض على الوزارات المتنافسة التوصل إلى توافق في الآراء. هذه البلدان تتمتع بميزة كبيرة في مساعدة الصناعات كثيفة البيانات على المنافسة. في النهاية ، تميل هذه البلدان إلى تصميم حلول حكومية إلكترونية جديدة ، وتعزيز التعلم الآلي ، وتمكين نماذج أعمال جديدة قائمة على البيانات.

إستونيا ، وهي اقتصاد أصغر بكثير من أي من الهند أو كوريا الجنوبية، قد استفادت بشكل كبير من القيادة الرقمية التي أظهرها الرئيس السابق "توماس هندريك إلفيس" ، الذي أصبح نصيرًا يحظى باحترام دولي للحكومة الإلكترونية وسياسة الأمن السيبراني . وفي المملكة المتحدة ، ساعدت المشاركة الشخصية لرئيس الوزراء السابق "توني بلير" في تعزيز الحكومة الإلكترونية في اختراق الحواجز البيروقراطية التي أعاقت

الوكالات عبر الإنترنت ، وعمل "معهد توني بلير للتغيير العالمي" على مساعدة القادة على التحول إلى عالم رقمي . وفي الولايات المتحدة ، جادل البعض بأن النجاحات المبكرة لإدارة الرئيس "بيل كلينتون" في الترويج للإنترنت التجاري ، مما جعل الحكومة الأمريكية رائدة في استخدام شبكة الويب العالمية وفي تعزيز التجارة الإلكترونية ، تدين بالكثير للدور القوي الذي لعبه البيت الأبيض (وخاصة نائب الرئيس "آل جور). تواصل البيت الأبيض والخطب رفيعة المستوى وحملات العلاقات العامة والمشاريع الإيضاحية (مثل الموقع الإلكتروني الأول للبيت الأبيض) ساعدت أيضًا في تسليط الضوء على الحاجة إلى سياسات رقمية استباقية . كما أن المشاركة الشخصية للرئيس السابق "باراك أوباما" في المبادرات الرقمية جعله يلقب بـ "رئيس جهاز التحويل الرقمي."

اليوم ، في معظم البلدان ، هناك إمكانات أكبر للابتكار الرقمي ولكن هناك القليل من القيادات الرقمية. وكانت النتيجة سياسات متضاربة أصدرتها وكالات مختلفة يمكن أن تثبط المبتكرين والمجازفين في كل من القطاع الخاص والبيروقراطيات الحكومية. يرغب هؤلاء الفاعلون الجدد في تقديم أدوات وخدمات جديدة عبر الإنترنت ، لكنهم يخشون الخروج من اللوائح الحكومية المتعلقة بحماية البيانات وضوابط التصدير ومتطلبات المراقبة والأمن السيبراني إلخ... لكم من منظور عالمي ، فإن التجارب الهندية والكورية الجنوبية تجارب بارزة.

قد تؤدي الاستعارات الخاطئة إلى سياسات خاطئة ، لكن ، بالطبع ، لا تعني القيادة أنه يجب على الرؤساء ورؤساء الوزراء التعمق في أسرار إدارة البيانات والمعايير الفنية والإلمام بها كليا لبلورة السياسة الرقمية. ففي كثير من الحالات ، يمكن أن تكون أهم مساهماتهم ببساطة، هي المشاركة

في بلورة رؤية حول كيف يمكن لتكنولوجيا المعلومات والبيانات، التي تولدها وتجمعها وتنسقها وتحللها، أن تعود بالفائدة على المواطنين الذين يحكمونهم والبلدان التي يقودونها. وبعبارات بسيطة ، يمكن للقادة الوطنيين الأذكياء شرح كيفية التفكير في المستقبل الرقمي.

لكن لسوء الحظ ، تبنى الكثير من صانعي السياسات استعارات ونماذج خاطئة لا تؤدي إلا إلى إرباك تفكير بلدانهم بشأن البيانات. المثال الأكثر وضوحًا هو التصريح المتكرر بأن "البيانات هي النفط الجديد"، والذي تم تعميمه بشكل واسع ، وهو وصف ليس مفيدًا ولكنه مؤذٍ تمامًا. ومن ناحية أخرى ، تشير مقارنة البيانات بالنفط إلى أن البيانات هي سلعة يتم بيعها واستهلاكها، لكن البيانات ، في الواقع ، ليست سلعة محدودة ، مثل النفط ، يتم تداولها وشحنها ذهابًا وإيابًا ويجف منبعها يوما ما. في الواقع ، على عكس النفط والمواد الخام الأخرى ، من السهل تكرار البيانات ومشاركتها ، مما يزيد من استخدامها وقيمتها. تدفع فكرة أن البيانات "وقود" للاقتصاد الرقمي الكثير من صانعي السياسات إلى افتراض أن البلدان يجب أن تخزن البيانات المنتجة داخل حدودها، والتحكم فيها أو تبادلها بإحكام ، مثل العملة الوطنية ، بدلاً من تشاركها مع الغير.

فما هو النموذج الأفضل إذن؟ إنه نموذج بسيط للغاية، إن البيانات تشبه، في الواقع، الهواء الذي نتنفسه أو الماء أكثر من كونها مثل النفط أو العملة . مثل الهواء ، على سبيل المثال ، يمكن النظر إلى البيانات على أنها شيء يجب السماح له بالتدفق بحرية ، متجاوزًا الحدود الوطنية. وذلك لأن الهواء ، مثل البيانات ، يمكن استخدامه وإعادة استخدامه لأغراض مختلفة من قبل العديد من الأشخاص المختلفين. ويمكن أن يكون ملوثًا ولكن يمكن أيضًا تنظيفه، شأنه شأن البيانات. هذا النهج في التفكير في البيانات - مثل

الهواء بدلاً من النفط أو العملة - يعمل بشكل جيد، وبشكل خاص عند معالجة البيانات العلمية ، مثل البيانات البيئية ، حيث يحتاجها الباحثون في جميع أنحاء العالم.

كما أن الماء هو استعارة أخرى مفيدة ، وذلك لأنه بالنسبة لمعظم البيانات ، هناك أسباب لوضع بعض القيود على استخدامها وتدفقها. يمكن أن تشمل أسباب القيام بذلك حماية البيانات والخصوصية والأمن القومي وإنفاذ حقوق النشر وضمان الميزة التجارية وغيرها. في هذه الحالات ، يمكن استخدام تشبيه مختلف. بدلاً من التدفق بحرية مثل الهواء ، يجب معالجة هذه البيانات مثل المياه . بعد كل شيء ، تدور جميع مياه العالم تقريبًا بحرية في المحيطات والأنهار والبحيرات والسحب الجوية أو يتم تخزينها في مخازن باردة في ألواح الجليد والأنهار الجليدية. لكن بعض مياه العالم يتم التقاطها في الخزانات وتصفيتها وتوصيلها بالأنابيب إلى العملاء. كما أن بعض المياه الجوفية يتم تعبئتها وتوسيمها وبيعها.

بالنسبة لصناع القرار وواضعي السياسات الذين يرغبون في وضع بعض القيود على البيانات ، فإن هذا التشبيه بالمياه يعمل جيدًا. إنه يبين بشكل فعال مدى أهمية البيانات للحياة في العصر الرقمي وكيف يحتاج القادة إلى العمل لضمان توفير المزيد من البيانات النظيفة لمزيد من الناس. وتوضح معالجة البيانات مثل المياه أنه ليست كل البيانات متطابقة أو لها نفس القيمة ، والأهم من ذلك ، أن البيانات شيء - مثل الماء - يمكن إعادة استخدامه وإعادة مزجه.

ما هي الخيارات الرئيسية لصناع القرار وواضعي السياسات ؟

إن أهم قضية ذات المستوى الأعلى بالنسبة لصناع القرار وواضعي السياسات - الذين يتصارعون مع سياسة البيانات - هي ما إذا كان ينبغي محاولة إنشاء نهج شامل واحد لإدارة البيانات أو بدلاً من ذلك اتباع نهج تشاركي موسع. بالرجوع إلى استعارة المياه، يمكن القول أن هناك خيارين، إما أن يكون مرفق مياه وطني موحد يخدم كل الساكنة ، أو بدلاً من ذلك تشجيع تشكيل العديد من شركات المياه المحلية والآبار المنزلية التي تعمل ضمن إطار تنظيمي واسع.

الهند تروج لـ "هندسة حماية تمكين البيانات" **(10)**

-(DEPA) Data Empowerment Protection Architecture-

لتوحيد مجموعات البيانات في جميع أنحاء البلاد وخارجها. في حين شجعت كوريا الجنوبية مئات الشركات على العمل مع وزارات مختلفة لإيجاد طرق جديدة ومفيدة لتطبيق البيانات التي تجمعها. وهكذا توصلتا إلى نهجين مختلفين للغاية.

(10) - يهدف إطار عمل DEPA إلى السماح للأشخاص بالوصول إلى بياناتهم بسلاسة وأمان ، ومشاركتها مع مؤسسات خارجية. إنه نموذج هندي لحوكمة البيانات يتطور ويستهدف تمكين الأفراد ، والانتعاش الاقتصادي والنمو ، وديمقراطية البيانات التنافسية.

قد يبدو ، أن النهج الكوري الجنوبي أسهل كثيرًا في التنفيذ عندما يُسمح للشركات بالاستفادة الكاملة من العديد من مزودي الخدمات السحابية الذين يمكنهم منح الشركات الصغيرة أو المتوسطة الحجم إمكانية الوصول إلى أدوات تخزين البيانات القوية وأدوات التعلم الآلي وخدمات الأمن السيبراني. إذ كانت في السابق متاحة فقط لشركات تكنولوجيا المعلومات الكبيرة. ولكن نظرًا لأن العديد من هذه الخدمات يتم توفيرها الآن من قبل شركات أمريكية أو صينية ، فإن الدول التي تفتقر إلى مزودي خدمات سحابية محلية تخشى أن الدول الأجنبية لن توفر الحماية الكافية للبيانات التي تعالجها. في الحالة الصينية على وجه الخصوص، هناك مخاوف تتعلق بالأمن القومي تدخل حيز التنفيذ لأن بكين لديها نهج تدخلي في البيانات بشكل عام.

بشكل عام ، إن مؤسسات ووكالات إنفاذ القانون - بما في ذلك تلك الموجودة في الهند - تشعر بالقلق بشكل خاص من أنها لن تكون قادرة على الوصول إلى البيانات التي تحتاجها للقبض على المجرمين ومقاضاتهم إذا تم تخزين هذه البيانات في مراكز البيانات التي تسيطر عليها الشركات في الخارج. ففي الولايات المتحدة ، أدت مخاوف مماثلة إلى قانون توضيح "الاستخدام القانوني الخارجي للبيانات" أو - CLOUD Act- **(11)**، والذي يحدد كيف يمكن للحكومات الأجنبية طلب البيانات من مزودي الخدمات السحابية من الشركات المستوطنة في الولايات المتحدة . لكن دولًا مثل كوريا الجنوبية والهند ليست قادرة على الاستفادة من هذا التشريع الأمريكي.

(11) - قانون اتحادي للولايات المتحدة تم تبنيه في 2018 بشأن الوصول إلى بيانات الاتصال (البيانات الشخصية) ، ولا سيما التي تعمل في السحابة. يدل بشكل أساسي قانون الاتصالات المخزنة (SCA) لعام 1986 من خلال السماح لسلطات العدل (الفيدرالية أو المحلية) بإجبار مقدمي الخدمات المنشأة على أراضي الولايات المتحدة ، بموجب أمر أو استدعاء ، على تقديم البيانات المتعلقة بالاتصالات الإلكترونية ، المخزنة على الخوادم ، سواء كانت موجودة في

الولايات المتحدة أو في دول أجنبية. تم انتقاد هذا القانون من قبل بعض الجمعيات للدفاع عن الخصوصية ، إذ يسمح هذا القانون بشكل خاص للمحاكم الأمريكية بالتماس من مقدمي الخدمات العاملين في الولايات المتحدة الاتصالات الشخصية للفرد دون إبلاغ هذا الأخير، وأيضا بلد إقامته ، أوالدولة التي يتم فيها تخزين هذه البيانات. وهذا باسم حماية السلامة العامة في الولايات المتحدة ومكافحة الأفعال الخطيرة بما في ذلك الجرائم والإرهاب.

لذلك ، كانت هناك دعوات في كوريا الجنوبية والهند لمزيد من توطين البيانات ، وذلك بدافع رغبة الحكومتين في حماية خصوصية المواطنين وتطلعات الهند لتمكين الوصول الأيسر والأسرع إلى البيانات لمراقبة إنفاذ القانون.

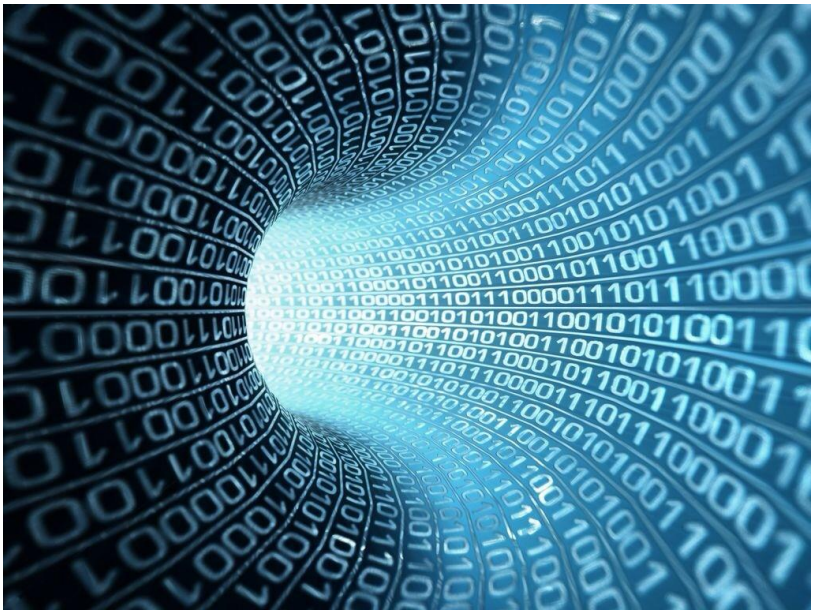
استفادت الهند على وجه الخصوص من شركات تكنولوجيا المعلومات الهندية التي تعالج البيانات للشركات في جميع أنحاء العالم. ففي الماضي ، سمحت الهند بحرية نقل البيانات عبر حدودها ، لكن التشريعات المحلية التي في طور الإعداد قد تعاكس هذه الممارسات المفتوحة. وبالمثل ، في كوريا الجنوبية، أصبحت الحجج المؤيدة والمعارضة للتوطين أكثر وضوحًا. وجدت الدراسات القليلة التي قيمت التأثير الاقتصادي لمتطلبات توطين البيانات أن الحد من تدفقات البيانات عبر الحدود يمكن أن يبطئ بشكل كبير نمو الناتج المحلي الإجمالي. ويقدم البعض حجة مهمة مفادها أن التدفق الحر للبيانات يجب أن يُنظر إليه أيضًا على أنه قضية من قضايا حقوق الإنسان لأن المواطنين يريدون أن يكونوا قادرين على اختيار الشركات التي تتحكم وتحمي البيانات المتعلقة بهم وأي الحكومات قد تكون قادرة على الوصول إلى تلك البيانات.

لكن هذا سيتطلب منهم التفكير بشكل مختلف واعتماد بعض الأساليب الجديدة. ويتضمن أحد النماذج الجديدة المثيرة لحوكمة البيانات اتحادات البيانات أو تعاونيات البيانات ، وهي فكرة يروج لها عالم الكمبيوتر الأمريكي "ساندي بنتلاند" (12) - Sandy Pentland - وزملاؤه في معهد "ماساتشوستس" للتكنولوجيا من بين آخرين. ويعمل تعاون البيانات مثل بنك أو اتحاد ائتماني ، ولكن بدلاً من معالجة الأموال وتوزيعها ، يقوم بتخزين البيانات ومشاركتها حول المستخدمين الفرديين. والمفتاح لإنجاح هذا النموذج هو أن التعاونية ملزمة تعاقديًا أمام المستخدمين أو المؤسسات بحماية استخدام البيانات حول فرد أو مجموعة لفائدته ولمصلحته فقط.

يتمثل التأثير الأكثر أهمية لهذا النهج في أنه سيمكن من إنشاء بنية بيانات عالية التوزيع، حيث لا يلزم تجميع البيانات في عدد قليل من "محيطات البيانات" التي تتحكم فيها مجموعة صغيرة من الشركات.

(12) - يدير البروفيسور أليكس "ساندي" بنتلاند MIT Connection Science ، وهي مبادرة على مستوى معهد ماساتشوستس للتكنولوجيا ، وساعد سابقًا في إنشاء وتوجيه MIT Media Lab وMedia Lab Asia في الهند. إنه أحد أكثر علماء الحوسبة شهرة في العالم ، وقد أعلنته مجلة Forbes أنه أحد "أقوى 7 علماء بيانات في العالم" جنبًا إلى جنب مع مؤسسي Google والمسؤول الفني الأول في الولايات المتحدة.

لكن يجب تسليط الضوء على تحديات السياسة الرقمية التي تواجهها الحكومات ، ولماذا أصبحت هذه التحديات معقدة بشكل متزايد وأكثر أهمية من أي وقت مضى؟



الآثار المترتبة على إدارة الإنترنت

ماذا يحدث في الهند وكوريا الجنوبية على المستوى الوطني وما يمكن أن يتعلمه صانعو السياسات الوطنية من تجاربهما ؟ وكيف يمكن لهذين النموذجين التأثير على الجدال في المنتديات الدولية حول مستقبل الإنترنت؟

إن حوكمة الإنترنت **(13)** مصطلح واسع يشمل مجموعة متكاملة من القرارات ، الكبيرة والصغيرة ، التي تتخذها الحكومات والشركات وهيئات وضع المعايير والمستخدمون والتي تؤثر على كيفية عمل الإنترنت وتطورها. لسنوات ، ناقش الدبلوماسيون وصانعو السياسات التكنولوجية وممثلو الشركات وغيرهم كيفية اتخاذ هذه القرارات وما إذا كانت هناك حاجة إلى مزيد من التنسيق الدولي. وتم عقد الآلاف من الاجتماعات الدولية ، وتم تطوير كتابات واسعة حول هذه الخيارات.

(13) - حوكمة البيانات هي مجموعة من المبادئ والمعايير والممارسات التي تضمن أن بياناتك موثوقة ومتسقة ، ويمكن الوثوق بها لاتخاذ القرارات المناسبة والوقت المناسب واستغلال كل الفرص لدعم الاختيارات المعتمدة وعرقلة أو إفشال ما يناهضها ويعاكسها و وتعزيز التحولات الرقمية. يمكّنك برنامج إدارة البيانات الناجح من القيام بهذه الأشياء بطريقة قابلة للتكرار ، والتي يمكن أن تتوسع وتتكيف مع نمو أحجام البيانات - والمصادر - وتطور التقنيات. باختصار ، تعني الإدارة الجيدة للبيانات أنه يمكنك استخدام بياناتك بثقة ، الآن وفي المستقبل وتوظيفها لتحقيق أهدافك.

اليوم ، أصبحت هذه المناقشات حول حوكمة الإنترنت أكثر أهمية من أي وقت مضى. والسؤال الرئيسي هو ما إذا كانت الإنترنت ستستمر شبكة عالمية مفتوحة تربط المستخدمين في كل مكان أو أنها ستتفتت إلى شبكات

وطنية وإقليمية حيث تمارس الحكومات تأثيرًا أكبر على كيفية تصميمها وكيفية استخدامها. كما برز الجدل حول السياسة الرقمية. بدلاً من مجرد التركيز على الشبكات التي تربط مستخدمي الإنترنت بالتطبيقات التي يرغبون في استخدامها ، فإن البيانات والمعدات المتصلة بالإنترنت ، مثل الهواتف الذكية وأجهزة "إنترنت الأشياء" (14) ومراكز البيانات ومرافق الحوسبة السحابية تجذب الانتباه أيضًا.

(14) - إنترنت الأشياء هي "بنية تحتية عالمية لمجتمع المعلومات ، والتي تجعل من الممكن الحصول على خدمات متقدمة من خلال ربط الأشياء (المادية أو الافتراضية) بفضل المعلومات الحالية القابلة للتشغيل البيني وتقنيات الاتصال. من وجهة نظر مفاهيمية ، يميز إنترنت الأشياء، الأشياء المادية المتصلة والتي لها هويتها الرقمية الخاصة وقادرة على التواصل مع بعضها البعض. تخلق هذه الشبكة بطريقة ما جسراً بين العالم المادي والعالم الافتراضي.

ينعكس هذا الاهتمام المتزايد في المناقشات حول إدارة البيانات الدولية ، وسيادة البيانات ، و "مجال البيانات"(15) - the datasphere - قام الأمين العام للأمم المتحدة ، "أنطونيو غوتيريس" ، بالترويج لـ "التعاون الرقمي" ، المبني على عمل منتدى إدارة الإنترنت ومختلف وكالات ومكاتب الأمم المتحدة ، ولكنه يمتد إلى ما هو أبعد من مجرد تشكيل الإنترنت وكيفية عملها. . فالكثير من الأعمال المتعلقة بالأمم المتحدة التي شجعها "غوتيريش" تركز على سياسة البيانات والحاجة إلى جعل البيانات عالية الجودة متاحة أكثر لعدد أكبر من الناس لمزيد من الأغراض (مع التركيز بشكل خاص على تحقيق أهداف التنمية المستدامة للأمم المتحدة).

(15) - يمكن تصور مجال البيانات على أنه تمثل لفضاء جديد يتكون من جميع البيانات الرقمية والتقنيات التي تكمن وراءها ، بالإضافة إلى تفاعلاتها مع العالم المادي والإنساني والسياسي الذي ترتكز عليه. إنه مجموعة من المفاهيم والآثار المترتبة على مجالات بيانات الحاسوب وتقنية المعلومات والأمن السيبراني.

إن زيادة التركيز على البيانات وكيفية تطبيقها يمكن أن يساعد في إزالة الحواجز التي تمنع المبتكرين في البلدان حول العالم من تطوير وتجريب خدمات جديدة عبر الإنترنت. يتضمن ذلك مجموعة واسعة من الأنشطة التي تتراوح من إجراء أبحاث لتغيير الحياة أو إنقاذها، إلى مساعدة العمال على أن يكونوا أكثر إنتاجية وكفاءة في استخدام الطاقة وجعل الحياة المهنية أكثر أمنًا وأمانًا. ولكن في معظم البلدان ، كانت سياسة البيانات بمثابة مياه راكدة مهملة، على عكس القضايا المشحونة سياسياً مثل الخصوصية عبر الإنترنت ، أو خطاب الكراهية على الإنترنت ، أو المعلومات المضللة والاستقطاب الذي تسببه . إن الجدال حول إتاحة البيانات الحكومية بشكل أكبر أو حول تدفقات البيانات عبر الحدود لا تحظى بالاهتمام الذى من الواجب أن تحظى به. والأسوأ من ذلك ، لا توجد إجابات سهلة لهذه الأسئلة المتعلقة بالسياسة لأن الأنواع المختلفة من البيانات تتطلب أنواعًا مختلفة جدًا من المعالجة.

لا يوجد لدى معظم الحكومات (بما في ذلك حكومتي الهند وكوريا الجنوبية) نقطة محورية واضحة وحيدة لقرارات سياسة البيانات. وعلى الصعيد الدولي ، لا توجد هيئة مماثلة مثل "منظمة البيانات العالمية") - World Data Organization- وقد يجادل الجميع ضد أي فكرة من هذا القبيل). لكن بدلاً من ذلك ، هناك العديد من المنظمات الحكومية الدولية والمنظمات العلمية المختلفة التي تعالج أجزاء مختلفة من لغز البيانات هذا. على أعلى مستوى ، على سبيل المثال ، أضافت مجموعة العشرين (16) - G20 - تدفقات البيانات عبر الحدود إلى أجندتها ، من خلال جهود رئيس الوزراء الياباني الراحل "آبي شينزو"- Abe Shinzo- في قمة مجموعة العشرين في أوساكا عام 2019 من أجل "التدفق الحر للبيانات بثقة". وأدت مبادرة "آبي" إلى ظهور مبادئ التجارة الرقمية لمجموعة السبعة (17) - G7 - في 2021 ، والتي تهدف إلى

إزالة الحواجز أمام مشاركة البيانات عبر الحدود الوطنية . ولكن رفضت أحد الهند التوقيع مبادرة "آبي" في "أوساكا."

(16)- تم إنشاء مجموعة العشرين في 1999. وهي تضم دول مجموعة الثمانية (ألمانيا وكندا والولايات المتحدة وفرنسا والمملكة المتحدة وإيطاليا واليابان وروسيا) ، بالإضافة إلى الاتحاد الأوروبي والمملكة العربية السعودية والأرجنتين وأستراليا والبرازيل والصين وجنوب كوريا والهند وإندونيسيا والمكسيك وجنوب إفريقيا وتركيا. وبالتالي فهي تمثل 90 في المائة من الناتج القومي الإجمالي للعالم ، و 80 في المائة من التجارة العالمية وثلثي سكان الكوكب.

(17) - مجموعة السبعة أو G7 هي مجموعة الحوار والتشاور والشراكة الاقتصادية، تجمع كل عام الدول السبع الأكثر تصنيعًا في العالم وهي ألمانيا وكندا والولايات المتحدة وفرنسا وإيطاليا واليابان والمملكة المتحدة. وتمثل هذه البلدان 40 في المائة من الناتج المحلي الإجمالي العالمي و 10 في المائة من سكان العالم. في البداية تم إنشاء G5 بمبادرة من فرنسا في أعقاب الصدمة النفطية الأولى ، وهي إطار غير رسمي جمع الولايات المتحدة واليابان وفرنسا وألمانيا الغربية (آنذاك) والمملكة المتحدة ، وكانت النشأة في عام 1974. في 1975 انضافت إيطاليا إلى المجموعة. وأصبحت G6 في عام 1976 ، مع إضافة كندا بناءً على طلب ألماني أمريكي. وستدرج روسيا في عمل المجموعة اعتبارًا من عام 1998 ، قبل تعليقها في مارس 2014 ، بعد ضمها لشبه جزيرة القرم في انتهاك للمبادئ التي يقوم عليها النظام الدولي. كما ارتبط الاتحاد الأوروبي بقمم مجموعة السبع منذ عام 1977 ويمثله رئيس المفوضية الأوروبية الذي يرافقه منذ عام 2009 رئيس المجلس الأوروبي.

طبعا، يجب أن تستمر هذه الجهود الدولية لتركيز المزيد من الاهتمام على سياسة البيانات ويجب أن تحفز البلدان المتقدمة والنامية على حد سواء لتوضيح مزيج السياسات الوطنية التي تؤثر على كيفية معالجة البيانات ومشاركتها واستخدامها. وتلعب المنظمات الدولية دورًا حاسمًا في إظهار كيف تتخذ البلدان الفردية ، مثل الهند وكوريا الجنوبية ، خطوات لتمكين مواطنيها وشركاتها من إطلاق العنان لقوة البيانات. يمكن لهذه المجموعات المتعددة الجنسيات والمتعددة الأطراف ، الرسمية منها والمتخصصة ، أن تقاوم السياسات والنماذج التي من شأنها أن تكبح تلك المجهودات.

وماذا عن البيانات المفتوحة؟

إن الإشكالية هي الوصول إلى البيانات الحكومية، وهذه أولوية قصوى. ولدا كل من الهند وكوريا الجنوبية تشريعات تضمن مشاركة الوكالات الحكومية للبيانات التي يمكن نشرها بأمان. ولكن كيفية تنفيذ هذه التشريعات، على وجه الخصوص، ستحدد المسار الذي يتم من خلاله تطوير العديد من التطبيقات المبتكرة والجديدة لتلك البيانات .

والأهم في نهاية المطاف هو أن السياسات الخاصة بالبيانات الحكومية (والبنية التحتية التي تم إنشاؤها لتوفير الوصول إلى هذه المعلومات) تقدم نماذج للوصول إلى أنواع أخرى من البيانات التجارية وبيانات المستهلك بطرق آمنة وموثوقة. ولكن لسوء الحظ ، قد تؤدي بعض اللوائح الحكومية لحماية البيانات وتوطينها البيانات إلى إعاقة – بشدة - تطوير هذه الأساليب الجديدة عن غير قصد.

تم تصميم بنية - DEPA - **(18)** في الهند لتحسين الشمولية والسماح لمن هم في أمس الحاجة إلى الوصول إلى الخدمات عبر الإنترنت ولكن لديهم أيضًا إشراف أوسع على الموافقة. فنظرًا لأن تخزين البيانات رخيص وغير مكلف ، يمكن للكيانات الهندية والأجنبية تجميع كميات هائلة منها. لكن هذه البيانات معزولة وعادة ما تكون متاحة فقط لأولئك الذين حصدوها ، في حين أن المواطنين الهنود الذين تتعلق بهم البيانات ليس لديهم أي رأي تقريبًا في استخدامها. وتهدف سياسات البيانات الهندية إلى التعامل مع كلا التحديين ، ليس فقط من خلال تقليل مخاطر عدم احترام الخصوصية وإساءة الاستخدام المحتملة للبيانات ولكن من خلال منح الأفراد وسائل عملية للوصول إلى بياناتهم والتحكم فيها ومشاركتها لمصلحتهم الخاصة .

(18) - هندسة تمكين وحماية البيانات (DEPA) - يمكن للتدفق الحر في البيانات أن يطلق العنان لقيمة اجتماعية واقتصادية ضخمة في بيانات المستخدم التي عادة ما تكون مقفلة في صوامع. مع

هذا الدافع ، يتم تطوير هندسة تمكين وحماية البيانات (DEPA) ، وهو مسعى بين القطاعين العام والخاص ، في الهند كنموذج للمستخدمين للوصول إلى بياناتهم ومشاركتها وفقًا لشروطهم. لا يعزز هذا الشكل من مشاركة البيانات المنافسة فحسب ، بل يعزز الابتكار أيضًا.

في كوريا الجنوبية، رغم تحقيق تقدم في إدارة سياسة البيانات المفتوحة الكورية في ثلاث مجالات (المؤسسات والسياسات والقدرات التنظيمية) ، لاتزال هناك بعض النواقص في النهج الحالي المعتمد. أحد الأمثلة على ذلك هو الإطار التنظيمي الذي يقسم المسؤولية بين وزارات متنوعة ذات مناهج مختلفة. ويتعقد الأمر أكثر بمجرد دخول "الحكومات المحلية" في هذا المزيج. إذ لا يمكن دمج البيانات العامة والخاصة بسهولة لأنها تندرج تحت ولايات قضائية وبيروقراطية مختلفة تتداخل وظيفيًا ولكنها تظل منقسمة مؤساساتيًا.

بخصوص البيانات عبر الحدود، سعت كل من الهند وكوريا الجنوبية لإدارة التوازن الدقيق بين الأقلمة والتدويل.

يمكن لبعض مقترحات توطين البيانات ، التي غالبًا ما تكون مدفوعة برغبة الحكومات في حماية خصوصية المواطنين أو تمكين مراقبة إنفاذ القانون ، أن تعرقل التدفق الحر للبيانات. على سبيل المثال ، سمحت الهند ، في معظم الحالات ، بحرية نقل البيانات عبر حدودها ، لكن التشريعات المحلية المعلقة قد تعيق هذه الممارسات الأكثر انفتاحًا. وبالمثل ، في كوريا الجنوبية ، أصبحت الحجج المؤيدة والمعارضة للتوطين أكثر وضوحًا. لقد وجدت الدراسات القليلة التي قيمت التأثير الاقتصادي لمتطلبات توطين البيانات أن الحد من تدفقات البيانات عبر الحدود يمكن أن يبطئ بشكل

كبير نمو الناتج المحلي الإجمالي - وهو تحد صعب للهند وكوريا في وقت يواجه فيه كلا البلدين رياحًا اقتصادية معاكسة محلية وعالمية متزايدة.

إن التناقض المركزي الذي تواجهه الهند يتمثل كالتالي: لقد جنت البلاد فوائد كبيرة من اتصالها الرقمي وسياسة السوق المفتوحة ، لكن الدولة تتصارع أيضًا مع التحديات التي يفرضها احتكار البيانات ، والعوائق أمام الوصول القانوني إليها والقيود المفروضة على الفعالية والقيود المفروضة على الإنفاذ الفعال للقوانين والقواعد واللوائح في المجال الرقمي. تهدف الهند إلى الانتقال من مستخدم إلى متحكم في الأسواق الرقمية ، وتحقيقا لهذه الغاية ، اعتمدت على الاستقلالية التكنولوجية جنبًا إلى جنب مع التأكيدات المتكررة على "السيادة الرقمية ."

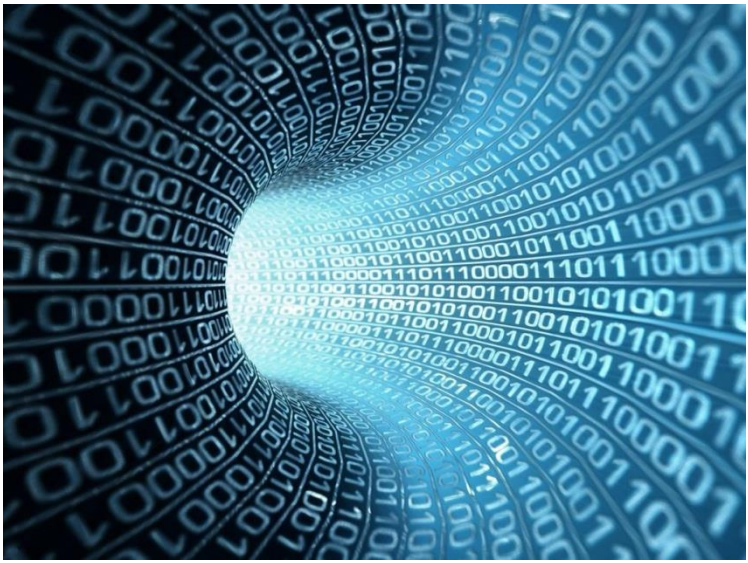
و خارج النطاق الوطني ، هناك الصكوك الدولية مثل "اتفاقية بودابست"(19) Convention de Budapest- - فالهند ليست من الدول الموقعة على الاتفاقية ، وهي معاهدة ملزمة متعددة الجنسيات تتعامل بشكل شامل مع جرائم الإنترنت وجمع الأدلة الإلكترونية للأنشطة غير المتعلقة بجرائم الإنترنت.

(19) - اتفاقية جرائم الإنترنت (اتفاقية بودابست) هي أول معاهدة دولية تحاول معالجة جرائم الكمبيوتر والإنترنت بما في ذلك استغلال الأطفال في المواد الإباحية وانتهاك حقوق الطبع والنشر وخطاب الكراهية من خلال تنسيق بعض القوانين الوطنية وتحسين تقنيات التحقيق وزيادة التعاون بين الدول. بالإضافة إلى ذلك ، فإنه يعزز حماية حقوق الإنسان والحريات من خلال حث الموقعين على تطبيق اتفاقية حماية حقوق الإنسان والحريات ، والعهد الدولي الخاص بالحقوق المدنية والسياسية وغيرها من الصكوك الدولية لحقوق الإنسان. منذ صيف 2011 ، كانت عدة دول أوروبية قد وقعت على المعاهدة. واعتبارًا من نوفمبر 2021 ، صادقت عليها 66 دولة.

إن كوريا الجنوبية أيضا لم تصادق على "نظام بودابست" الذي يوفر بديلاً لعمليات معاهدة المساعدة القانونية المتبادلة التي تستغرق وقتًا طويلاً والتي تتطلب من وكالات إنفاذ القانون طلب المساعدة من نظيراتها الأجنبية.
وبالمثل ، مع الاعتراف بالمخاوف المتعلقة بخصوصية المواطنين كهدف هام من أهداف السياسة ، فعملية ملاءمة اللائحة العامة لحماية البيانات في الاتحاد الأوروبي أو عملية التصديق الخاصة بقواعد الخصوصية عبر الحدود الخاصة بمنتدى التعاون الاقتصادي لآسيا والمحيط الهادئ قد توفر المتطلبات اللازمة مستوى الحماية ، بغض النظر عن مكان تخزين البيانات ومعالجتها.

إن الديمقراطيات الآسيوية مثل الهند وكوريا الجنوبية لا تتبع ببساطة نموذج الولايات المتحدة أو أوروبا في إدارة البيانات. بدلاً من ذلك ، وفي العديد من المجالات المتصلة بكل من البيانات المفتوحة والبيانات العابرة للحدود ، فإنهما يبتكران مناهجهما الفريدة الخاصة بهما ، والتي ترتكز بقوة على مؤسساتهما الديمقراطية.

يمكن القول إن عالم اليوم - بخصوص التعامل مع البيانات – يعاين النهج المتمحور حول الولايات المتحدة والمتمحور حول الصين ، و النهج الديمقراطي و النهج السلطوي، في هذا الإطار العام تشكل تجربة كل من الهند وكوريا الجنوبية تجربتين فريدتين .



المقاربة الهندية في إدارة البيانات

تسعى الهند إلى ابتكارات مؤسسية وتكنولوجية طموحة لأنها تسعى إلى التحول من مجرد استخدام الخدمات الرقمية القائمة على البيانات إلى التحكم في هذه البيانات والاستفادة منها لتحقيق غاياتها الاستراتيجية والاقتصادية.

شهدت الهند نموًا رقميًا سريعًا في فترة زمنية قصيرة. وقد أدى ذلك إلى تطورات تكنولوجية وأنظمة حوكمة جديدة وسياسات رقمية مخصصة للهند فقط. مجتمعة ، أصبحت هذه التغييرات تحدد النموذج الهندي لحوكمة البيانات. ويهدف هذا النموذج بدوره ، من منظور هندي ، إلى تمكين المواطنين.

مع تسارع وتيرة تبني الحكومة للتقنيات والخدمات الجديدة ، تسارعت المناقشات العامة في الهند حول الحاجة إلى الموازنة بين حقوق البيانات والابتكار الرقمي مع الضرر المحتمل الذي قد ينشأ عن إساءة استخدام البيانات. على الرغم من هذه المخاوف ، لم يكن لدى الهند ، إلى حدود غشت 2022 ، قانونًا موحدًا وشاملًا لحماية البيانات ، على الرغم من أن البيانات أصبحت مركزية لمعظم الشركات الخاصة والمبادرات العامة.

نظرًا لأن تخزين البيانات رخيص ، يمكن للكيانات الهندية والأجنبية أن تجمع ، يومًا بعد يوم ، وعامًا بعد عام ، كميات هائلة من المعلومات في حالة عدم استخدامها يومًا ما ، بدلاً من المخاطرة بعدم توفرها عند الحاجة إليها. ومع ذلك ، نظرًا لأن هذه البيانات معزولة وعادة ما تكون متاحة فقط لأولئك الذين حصدوها ، فلا يتم عمل الكثير لإلغاء تأمين القيمة الكاملة للبيانات. والأسوأ من ذلك ، أن المواطنين الهنود الذين تتعلق بهم البيانات ليس لديهم أي رأي تقريبًا في طرق استخدامها.

ركزت سياسات البيانات الهندية على معالجة هذين التحديين. بالإضافة إلى الأساليب التقليدية لتقليل مخاطر الخصوصية وإساءة الاستخدام المحتملة للبيانات ، تهدف هذه السياسات الهندية أيضًا إلى تزويد الأفراد بوسائل عملية يمكنهم من خلالها الوصول إلى بياناتهم والتحكم فيها ومشاركتها لمصلحتهم الخاصة.

لقد تطور نهج الهند في إدارة البيانات في ضوء أولويات الهند المحلية والموقع الدولي .

اقتصاد البيانات في الهند

في ثمانينيات القرن الماضي ، كان قطاع تكنولوجيا المعلومات (IT) في الهند يركز بشكل أساسي على صادرات البرمجيات والخدمات وكانت قيمتها 25 مليون دولار فقط ، وتشكل حوالي 0.01 في المائة فقط من الناتج المحلي الإجمالي للهند في ذلك الوقت - ويرجع ذلك أساسًا إلى أن هذا القطاع كان مغلقًا أمام العالم وخاضعًا لرسوم الاستيراد المرتفعة. لم تكن البرمجيات صناعة معترف بها من قبل الحكومة ، ولم يكن المصدرون الهنود قادرين على إقناع البنوك بتمويل أنشطتهم. وقد ازدهرت صناعة تكنولوجيا المعلومات المبكرة في البلاد على الرغم من الحكومة - وليس بسببها.

على النقيض من ذلك ، فإن صناعة تكنولوجيا المعلومات في الهند والقطاعات ذات الصلة لديها حاليًا عائدات سنوية تبلغ 200 مليار دولار

وتمثل 13 في المائة من الناتج المحلي الإجمالي للبلاد . لطالما عُرفت الهند بأنها قوة عالمية في تصدير خدمات تكنولوجيا المعلومات ، لكن قطاع تكنولوجيا المعلومات في البلاد لم يعد فقط يعتمد على الصادرات من أجل النمو. على مدار العقد الماضي ، نما الطلب المحلي على خدمات تكنولوجيا المعلومات بسرعة ، مع تجاوز القيمة الإجمالية للطلب المحلي على الخدمات الرقمية في الهند القيمة الإجمالية للصادرات . واليوم ، تُستخدم الخدمات الرقمية على نطاق واسع أكثر من أي وقت مضى في الهند. وكان هذا التغيير ممكنًا بفضل الاختراق العميق للوصول إلى الإنترنت عبر الهاتف المحمول من طرف جميع طبقات المجتمع الهندي - بما في ذلك المناطق الريفية النائية في البلاد. يستخدم أكثر من 750 مليون هندي الهواتف الذكية ، أو ما يقرب من 54 في المائة من إجمالي ساكنة البلاد ، مما يسمح لهم بالوصول إلى الترفيه والمعلومات والخدمات العامة أثناء التنقلات.

بالإضافة إلى ذلك ، على مدى السنوات العشر الماضية ، أطلقت الهند بنية تحتية رقمية على نطاق متناسب ، مما مكن السكان من اتخاذ خطوات سريعة نحو وجود افتراضي بلا أوراق ، مما يسمح لهم بالوصول إلى الخدمات الرقمية من أي مكان في البلاد دون الحاجة إلى حمل المال أو القيام بزيارة مواقع محددة لتقديم الخدمة. اليوم ، يتم إجراء أكثر من 5.4 مليار عملية دفع رقمية شهريًا عبر واجهة الدفع الموحدة في الهند (UPI) ، وهو نظام دفع رقمي يسهل تحويل الأموال بين الحسابات المصرفية وحسابات الأموال عبر الهاتف المحمول والمحافظ الرقمية. يمكن شراء الشاي والبسكويت من الباعة المتجولين بعربات وتدفع أثمنتها إلكترونيا ناهيك عن مدفوعات التجارة الإلكترونية الكبيرة للسلع والخدمات. كما أتاحت الواجهة أيضًا لأصحاب المشاريع الصغيرة والشركات الصغيرة

على حد سواء تحديد الفرص التجارية التي لم تكن متاحة لهم في السابق والاستفادة منها.

من المتوقع أن تتكشف ثورة مماثلة في خدمات البيانات الجديدة ، التي تم تمكينها من خلال إطار رقمي جديد في قطاع الخدمات المالية. ومن المتوقع بالمثل أن تستفيد القطاعات الأخرى (مثل الرعاية الصحية والتعليم) من هذا الإطار .

أخيرًا ، يجري العمل على تفكيك التجارة الرقمية القائمة على الموقع ، مما يسمح للعناصر المختلفة عبر النظام البيئي التجاري بالتفاعل بشكل أكثر كفاءة وفتح الباب أمام منافسة أكبر. وعند نشرها ، من المرجح أن تقلل هذه الشبكة المفتوحة للتجارة الرقمية من اعتماد المستهلكين وصغار تجار التجزئة على منصات متكاملة رأسياً لصالح نهج أكثر تفصيلاً ولا مركزية.

فكيف تطور قطاع تكنولوجيا المعلومات ونما بهذه السرعة في الهند، وكيف تم الترويج لتكنولوجيا المعلومات ؟

مكنت ثلاثة عوامل حاسمة من تطوير صناعة تكنولوجيا المعلومات في الهند بدءًا من تسعينيات القرن الماضي:

- التحرير الاقتصادي لعام 1991 ، والتدابير الخاصة بالصناعة مثل إنشاء مجمعات تكنولوجيا البرمجيات في عام 1989 ،

- المشتريات الحكومية المكثفة لمعدات وخدمات تكنولوجيا المعلومات،

- شجعت هذه البيئة الترحيبية العديد من الشركات متعددة الجنسيات على إنشاء متاجر في الهند ، وهو تطور أدى بدوره إلى ازدهار تصدير خدمات تكنولوجيا المعلومات ، بحلول 2000-2001 ، بلغ إجمالي صادرات الهند من البرمجيات 6.4 مليار دولار.

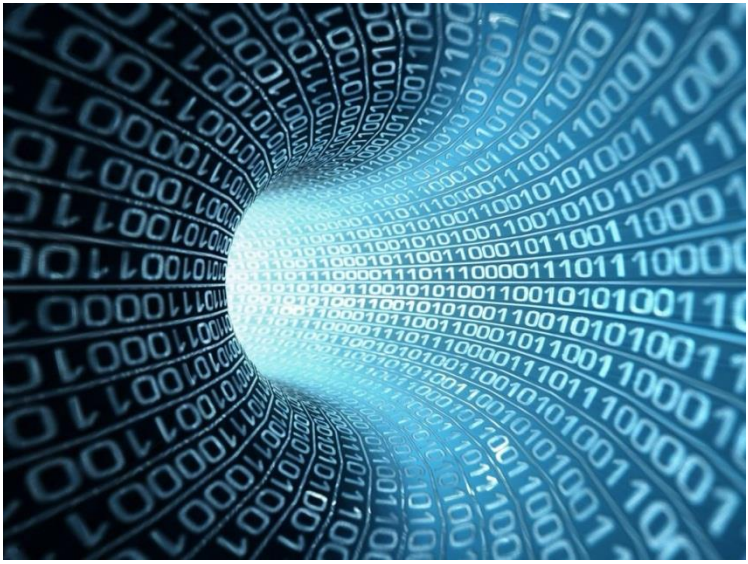
أدت الإصلاحات الاقتصادية ، وتحرير الاقتصاد ، والوجود المتزايد باطراد للشركات الأجنبية متعددة الجنسيات في الهند إلى العديد من التطورات الإضافية ، بما في ذلك إطلاق الإنترنت عبر الكابل وإصدار أول تشريع متعلق بتكنولوجيا المعلومات في الهند . في 2015 ، تم إطلاق مبادرة الهند الرقمية. و يهدف هذا البرنامج الطموح متعدد الأوجه إلى تحويل البنية التحتية الرقمية للبلد إلى مرفق عام وتسهيل الحوكمة الرقمية وتمكين المواطنين. وتم إطلاق العديد من البرامج الإضافية تحت مظلة - Digital India - بما في ذلك - BharatNet - وهو برنامج لتوفير الوصول إلى الإنترنت لجميع القرى في البلاد ، والوصول الشامل إلى الهاتف المحمول، برنامج مصمم لتوفير الاتصال المحمول لأكثر من 55000 قرية في الهند والتي كانت تفتقر سابقًا إلى إمكانية الوصول عبر الهاتف المحمول ، و - Smart Cities Mission - **(20)** وهو برنامج لتحويل جميع المدن الهندية إلى مدن ذكية **(21)**.

(20) - المهمة الوطنية للمدن الذكية هي برنامج للتجديد والتعديل الحضري من قبل حكومة الهند مع مهمة تطوير المدن الذكية في جميع أنحاء البلاد. وزارة الاتحاد للتنمية الحضرية هي المسؤولة عن تنفيذ المهمة بالتعاون مع حكومات الولايات في المدن المعنية. تضمنت المهمة في البداية 100 مدينة، مع الموعد النهائي لإنجاز المشاريع المحدد بين 2019 و 2023. وبلغت

نسبة الإنجاز المشترك الفعلي لجميع المشاريع اعتبارًا من 2019 ، 11 في المائة. واعتبارًا من مارس 2022 ، تم الانتهاء من 3577 مشروعا من إجمالي 6939 مشروعًا تم طرحها.

(21) - المدينة الذكية - Smart city - هي منطقة حضرية حديثة تقنيًا تستخدم أنواعًا مختلفة من الأساليب الإلكترونية وطرق تنشيط الصوت وأجهزة الاستشعار لجمع بيانات محددة. تُستخدم المعلومات المكتسبة من تلك البيانات لإدارة الأصول والموارد والخدمات بكفاءة؛ في المقابل، يتم استخدام هذه البيانات لتحسين العمليات في جميع أنحاء المدينة. يتضمن ذلك البيانات التي تم جمعها من المواطنين والأجهزة والمباني والأصول التي تتم معالجتها وتحليلها لمراقبة وإدارة أنظمة المرور والنقل ومحطات الطاقة والمرافق وشبكات إمدادات المياه والنفايات وكشف الجرائم وأنظمة المعلومات والمدارس والمكتبات، المستشفيات والخدمات المجتمعية الأخرى .

أدت زيادة الرقمنة ، وانتشار الخدمات عبر الإنترنت التي تستهدف العملاء الهنود ، واستخدام التقنيات الجديدة، إلى زيادة حجم البيانات المتداولة بشكل كبير. وفقًا لتوقعات الحكومة ، يمكن أن تولد التقنيات الناشئة في الهند ما يصل إلى تريليون دولار من القيمة الاقتصادية ؛ يمكن تسخير ثروة البيانات لتحقيق طموحات البلاد في أن تصبح اقتصادًا بقيمة 5 تريليون دولار من حيث القيمة الإجمالية بحلول 2025.



البنية التحتية الرقمية

على مدى العقد الماضي ، تم تسريع جهود الرقمنة في الهند بشكل كبير من خلال نشر البنية التحتية الرقمية على نطاق السكان. تشكل هذه الأطر القائمة على البروتوكولات المفتوحة ، والمرتبة فوق بعضها البعض ، مكدسًا رقميًا. في الأساس توجد عناصر أساسية مثل علامات الهوية الرقمية ، بينما يتم وضع تطبيقات محددة (بما في ذلك الأداءات

والمدفوعات ومشاركة البيانات المتفق عليها والتجارة غير المجمعة). يشار إلى هذه الطبقات التكميلية للبنية التحتية الرقمية عادةً باسم

India Stack – (22).

(22) - هو اسم يطلق على مجموعة من واجهات برمجة التطبيقات المفتوحة والسلع العامة الرقمية التي تهدف إلى إطلاق العنان للأولويات الاقتصادية للهوية والبيانات والمدفوعات على نطاق السكان.

الوسائل الرقمية لتحديد الهوية

بدأت India Stack في 2010 بإصدار أرقام تعريف فريدة لجميع المواطنين الهنود كجزء من برنامج تحديد الهوية الوطني المعروف باسم Aadhaar(23).

(23) - عندما تم إطلاق البرنامج في 2009 ، شرعت الهند في تحقيق المرتبة الأولى على مستوى العالم: إعطاء كل مواطن رقم تعريف فريد يمكن التحقق منه باستخدام القياسات البيوميتيرية. قالت الحكومة إن هذه القياسات الحيوية (مسح قزحية العين وسجلات بصمات الأصابع) سيتم ربطها برقم Aadhaar الخاص بشخص ما ، والذي سيتم استخدامه بدوره في جميع التفاعلات مع الدولة - للتخلص من الاحتيال ، وجعل الضرائب أكثر كفاءة ، وفي النهاية توفير المال.

قبل إنشاء البرنامج ، لم يكن لدى ما يقدر بنحو 400 مليون مواطن هندي أي شكل من أشكال تحديد الهوية . ونتيجة لذلك ، كافح المواطنون ، ولا سيما في الطبقات الاجتماعية والاقتصادية الدنيا في البلاد ، للوصول إلى الأموال والإعانات الحكومية التي يحق لهم الحصول عليها. وقد تفاقمت هذه المشكلة بسبب سهولة تحويل الأموال من قبل الجهات الخبيثة. وإجمالاً

، بناءً على البرنامج ، فإن ما بين 10 في المائة و 60 في المائة من الأموال المخصصة للإعانات وخدمات الرعاية الاجتماعية وقعت فريسة للتسرب أو سوء الاستخدام ، وفقًا لإحدى الدراسات.

كان من المفترض أن يزود Aadhaar جميع السكان الهنود بمعرف فريد ، مما يجعل من الممكن تقديم خدمات أكثر دقة للأشخاص المناسبين. نظرًا لأن المعرّف رقمي ، يمكن ربطه بالحلول التقنية التي استفادت من التحقق الرقمي لتقديم خدمات غير ورقية وأكثر كفاءة.

أدى التبني الواسع النطاق لـ Aadhaar إلى تحسينات في تقديم الخدمات الرقمية في جميع أنحاء الهند. أصدرت الحكومة الهندية حوالي 1.3 مليار بطاقة Aadhaar منذ 2016 ، تغطي ما يقرب من 96.4 في المائة من سكان البلاد . وقد سمح ذلك للحكومة بإجراء تحويلات الثروة على نطاق واسع بطريقة فعالة. على سبيل المثال ، خلال وباء كورونا ، تم صرف ما يقرب من 44 مليار دولار للمزارعين والفئات المهمشة الأخرى باستخدام India Stack.ويقدر أن الحكومة قد وفرت ما يقرب من 30 مليار دولار اعتبارًا من مارس 2021 من خلال القضاء على الاستفادة المكررة. كما قام Aadhaar بتعريف ملايين الهنود الريفيين على المعاملات الرقمية وأدى إلى زيادة في محو الأمية الرقمية والتغلغل الرقمي في جميع أنحاء البلاد.

أدى Aadhaar إلى إنشاء العديد من وسائل المصادقة ، بما في ذلك عملية المصادقة الإلكترونية التي يستخدم فيها مزود الخدمة رقم Aadhaar

للاستعلام عن قاعدة بيانات Aadhaar ، التي تديرها سلطة التعريف الفريدة في الهند. يستجيب مسؤولو الهيئة لمثل هذه الطلبات بالإشارة إلى ما إذا كانت قاعدة البيانات تحتوي على سجل يطابق رقم Aadhaar والتفاصيل الواردة في الطلب ، وبالتالي توفير وسيلة دقيقة للتحقق من الهوية. إن خدمة Aadhaar الإلكترونية ، التي تستعمل طريقة المصادقة هذه ، قد أجريت بالفعل على ما يقرب من 75 مليار عملية تحقق من الهوية ، استجابة لطلبات من الحكومة وغيرها من المؤسسات المالية والاتصالات السلكية واللاسلكية وغيرها من الخدمات العامة الأخرى. وتسمح إمكانية التوقيع لأي حامل رقم Aadhaar بإنشاء توقيع رقمي صالح قانونيًا ويمكن التحقق منه.

مع نضوج برنامج Aadhar والخدمات ذات الصلة ، قفزت نسبة سكان الهند الذين لديهم حساب مصرفي من 35 بالمائة في عام 2011 إلى 80 بالمائة في عام 2017 . وقدر البنك الدولي أن خدمة "اعرف عميلك" من Aadhaarخفضت تكاليف انضمام العملاء إلى أحد البنوك الهندية من 23 دولارًا أمريكيًا إلى 0.15 دولار أمريكي فقط. زود التحقق من العملاء المستند إلى Aadhaar شركات الاتصالات بدفعة كبيرة من حيث اكتساب العملاء ، وتحديداً في الأسواق الريفية حيث كانت هناك إمكانات هائلة غير مستغلة. أدى الإعداد الأسرع والأرخص والأبسط لشركة واحدة - Reliance Jio، أحد المشاركين المتأخرين إلى سوق الاتصالات الهندية - إلى اتخاذ قرار بجعل Aadhar الطريقة الوحيدة للمشتركين الجدد للحصول على بطاقة .SIM فازت هذه الشركة بـ 16 مليون مشترك في الشهر الأول بعد افتتاحها للعمل و 50 مليونًا في أقل من تسعين يومًا.

الأداءات والمدفوعات الرقمية

مع انتشار اتصالات الهاتف المحمول والحسابات المصرفية في جميع أنحاء الهند ، كان على صانعي السياسات جعل استخدام البنوك أرخص وأكثر سهولة. دفعت هذه الحاجة إلى تصميم الطبقة التالية من India - Stack، (UPI)وبعبارات بسيطة هي لغة ترميز للدفع تعمل على مفتاح مركزي تديره شركة المدفوعات الوطنية في الهند. ونظرًا لأن جميع البنوك المرخصة متصلة بخادم National Payments Corporation - of India - يمكن إرسال رسائل الدفع من وإلى هذه الكيانات ، مما يسمح بإجراء معاملات الدفع على الفور تقريبًا.

UPIهي نفسها تكدس للنيانات من ثلاثة مستويات. تم إنشاء الطبقة الأساسية وتشغيلها بواسطة National Payments Corporation في الهند ، وتتكون من المحول الذي يتعامل مع توجيه رسائل الدفع. تشمل الطبقة التالية البنوك والكيانات المالية المنظمة الأخرى المسموح لها بموجب القانون بحفظ أموال المستخدمين ودفع المبالغ واستلامها في هذه الحسابات. وتتكون الطبقة الثالثة والأعلى من تطبيقات الدفع التي يديرها لاعبو التكنولوجيا المالية المنظمون بشكل خفيف والتي تنشئ واجهات العملاء التي تسمح للمستخدمين العاديين بالوصول إلى نظام الدفع البيني. نظرًا لقابلية التشغيل البيني الأساسية لهذه البروتوكولات ، يمكن لكل مشارك في حزمة الدفع، التفاعل مع كل مشارك آخر باستخدام نفس المجموعة العالمية من واجهات برمجة التطبيقات. ونتيجة لذلك ، تجنب

نظام الدفع الهندي الاضطرار إلى إقامة علاقات فردية بين البنوك بشق الأنفس لتمكين العملاء من تحويل الأموال إلى بعضهم البعض.

ابتكار آخر من UPI هو استخدامه لعنوان دفع افتراضي (VPA) ، وهو معرف فريد يربط الحساب المصرفي لمستخدم معين بسلسلة يسهل تذكرها من الأسماء والحروف والأرقام التي يمكن مشاركتها لغرض تلقي المدفوعات. بينما توفر هذه الطريقة مزايا الخصوصية والأمان (لأن المعرفة بـ VPA لا تقدم أي معلومات حول التفاصيل المصرفية المرتبطة) ، نظرًا لأن VPA منتشر في كل مكان في جميع أنحاء النظام ، فإن VPA غير محايد لتطبيقات الدفع ، مما يسمح بتبادل الأموال حتى بين المستخدمين على تطبيقات الدفع المختلفة.

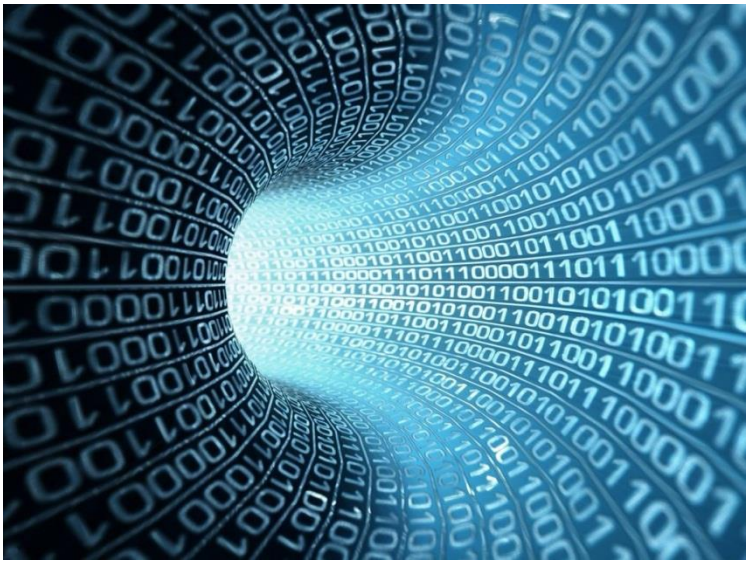
في يونيو 2022 ، تم إجراء ما يقدر بنحو 5.9 مليار معاملة ، بقيمة حوالي 127 مليار دولار ، باستخدام UPI ، وقد حقق نجاحًا معترفًا به في الهند وخارجها . وتم دمج مجموعة واسعة من عروض الإنترنت والهاتف المحمول في نظام UPI البيئي ، مع وجود لاعبين أجانب مثل Amazon و Googleو Meta و Walmart الذين يعتمدون عليها في الهند ، كما أن 31 دولة منها الولايات المتحدة تفكر أيضًا في اعتماد ميزات UPI ضمن أنظمة الدفع المحلية الخاصة بها . برز UPI كنظام دفع محلي رائد مع إمكانية منح الهند بدائل مكتفية ذاتيًا للاعتماد على حلول الدفع العالمية.

تبادل البيانات

بعد أن قامت الهند ببناء أنظمة تعريف ودفع موثوقة على نطاق واسع ، بدأت في إنشاء وتجميع كميات هائلة من بيانات المعاملات. كانت الخطوة المنطقية التالية هي استخدام هذه البيانات لتمكين المواطنين المتحمسين لاستخدام التجارة الإلكترونية وخدمات الحكومة الإلكترونية ، وخاصة أولئك الذين ليس لديهم وسائل أخرى للوصول إلى النظام المالي الرسمي.

تم تصميم الطبقة الثالثة من India Stack ، والتي تسمى بنية تمكين وحماية البيانات (DEPA) ، لتسهيل مشاركة البيانات التي تمت الموافقة عليها. على عكس الطبقات السابقة التي كانت في الغالب تكنولوجية ، فإن DEPA، من خلال تصميمها ، هي بنية تقنية قانونية يمكن للأفراد استخدامها لممارسة قدر أكبر من الاستقلالية حول كيفية استخدام بياناتهم الشخصية. توفر هذه البنية أدوات تكنولوجية للأشخاص لاستدعاء الحقوق المتاحة لهم بموجب قوانين الخصوصية المعمول بها. في إطار مختلف ، إنه نظام تقني يضمن أن جميع عمليات نقل بيانات الشخص من وكالة بيانات إلى أخرى تتم من خلال سير عمل رقمي مشفر يتم تشغيله فقط بعد الحصول على موافقة هذا الشخص إلكترونيًا.

لقد تم بالفعل نشر DEPA في قطاع الخدمات المالية ، والعمل جار لتنفيذه في نظام الرعاية الصحية. ليس من الصعب تصور كيف يمكن تطبيق هذا الإطار عبر مجموعة من القطاعات مثل التعليم والاتصالات السلكية واللاسلكية وغيرها .



حاجة الهند لإدارة البيانات

مع إطلاق- Digital India - (24) (و India Stack- (25) - نما انتشار الهواتف الذكية في المناطق الريفية بالهند من 9 في المائة إلى 25 في

المائة بحلول 2018 ، وقفز عدد الهنود الذين يستخدمون وسائل التواصل الاجتماعي من 142 مليونًا في 2015 إلى 326 مليونًا بحلول نفس 2018 ، وبين عامي 2015 و 2018 ، زاد متوسط استخدام البيانات شهريًا بنسبة 129 بالمائة. كان التأثير المباشر للرقمنة الشديدة للاقتصاد الهندي يتمثل في الأحجام غير المسبوقة من البيانات التي تم إنشاؤها وما زال يتم إنشاؤها . من المتوقع أن يزداد عدد مستخدمي الإنترنت في الهند بنحو 45 في المائة في السنوات القليلة المقبلة ، حيث سينمو من حوالي 622 مليونًا في 2020 إلى 900 مليون في عام 2025. زادت كمية البيانات اللاسلكية التي يستخدمها المستهلكون الهنود بسرعة فائقة لتصل إلى أكثر من 30 ألف بيتابايت (26) - petabytes - في الربع الأول من 2021-2022. في الوقت نفسه ، انتقل المستهلك العادي من استخدام 1.2 غيغابايت (27) - gigabytes - من البيانات اللاسلكية في 2017-2018 شهريًا إلى 14.1 غيغابايت في 2021-2022. ومن المتوقع أيضًا أن يرتفع الاستهلاك الشهري للبيانات إلى 50 غيغابايت لكل هاتف ذكي بحلول عام 2027.

(24) - برنامج رائد لحكومة الهند مع رؤية لتحويل الهند إلى مجتمع مُتمكّن رقميًا وذو اقتصاد المعرفة - knowledge economy .

(25) - هو اسم يطلق على مجموعة من واجهات برمجة التطبيقات المفتوحة والسلع العامة الرقمية التي تهدف إلى إطلاق العنان للأولويات الاقتصادية للهوية والبيانات والمدفوعات على نطاق ساكنة الهند.

(26)- وحدة قياس تخزين في الحوسبة تعادل 10 أس 15 بايت.

(27) - الجيجابايت هي وحدة قياس تخزين في الحوسبة تعادل مليار بايت أي (10 أس 9) .

تقوم الهند الآن بالرقمنة بشكل أسرع من معظم الاقتصادات الأخرى ، مما يخلق قاعدة استهلاكية سريعة النمو تستهدفها الشركات المحلية والأجنبية

على حد سواء. وغني عن البيان أنه بدون نظام مناسب للحكم ، فإن الفوائد التي يتم الحصول عليها من كل هذه البيانات قد لا يتمتع بها جميع المواطنين الهنود. تتطلع الهند إلى سد الفجوة التنظيمية بين إنشاء البيانات المزدهر والحاجة إلى تنظيم البيانات المتاحة والاستفادة منها. وبذلك ، طورت الهند أطرًا لحماية البيانات ومشاركتها، وهي تدابير تهدف إلى تعزيز استخدام كل من الحكومة والقطاع الخاص للبيانات لتحقيق منافع اجتماعية واقتصادية.

الأطر القانونية لإدارة البيانات في الهند

فمن المعلوم أن هناك عدة أنواع من البيانات المتداولة والقضايا المختلفة المتعلقة بالحوكمة من كل نوع ، إلا أنه نظرا لأن تحليلنا يتعامل حصريًا مع أنواع البيانات التي تبحث الحكومة الهندية بنشاط عن تنظيمها ، مثل البيانات الشخصية الناتجة عن الأفراد والبيانات غير الشخصية ، والتي في قد يتم أيضًا اشتقاق منها بعض الحالات من البيانات الشخصية ولكنها تتضمن أيضًا بيانات ليس لها علاقة بالأفراد. لا نعنى في هذه المحاولة البحثية البسيطة والمحدودة بكيفية مشاركة الأنواع الأخرى من البيانات - بما في ذلك البيانات العلمية والبيانات التجارية وما شابه - ، على الرغم من أن هذه الأنواع من البيانات لها نفس الأهمية في الخطاب الأوسع حول إدارة البيانات. سيتم الاقتصار على تحليل ممارسات حوكمة البيانات الهندية في المقام الأول من حيث مشاركة البيانات بين الكيانات الحكومية والشركات والمجتمعات والأشخاص العاديين للأغراض العامة والتجارية فقط.

من المهم أيضًا تحديد أصحاب المصلحة المختلفين في نظام البيانات الهندي من أجل فهم التفاعل بينهم بشكل أفضل. إن أولوية الحكومة الهندية هي استخدام التقنيات الرقمية للتنمية المحلية ، والاستفادة من البيانات لصالح مواطنيها وحمايتهم. واعتاد القطاع الخاص - الذي يركز بشكل كبير على المكاسب التجارية - على النظر إلى حوكمة البيانات على أنها عائق ، ولكن في الآونة الأخيرة ، أصبحت الشركات تدرك أن العملاء ينظرون إلى ممارسات حوكمة البيانات الجيدة بشكل إيجابي خلافا للسابق. وللمواطنين الأفراد مصلحة في ضمان قدرتهم على ممارسة سيطرة ذات مغزى على بياناتهم لحماية أنفسهم من الأضرار المحتملة.

في جميع أنحاء العالم ، يتم تنفيذ حوكمة البيانات من خلال تنظيم جمع واستخدام البيانات الشخصية. في معظم البلدان ، اتخذت هذه اللوائح شكل تشريعات حماية البيانات التي تحدد ما يمكن وما لا يمكن فعله بالبيانات الشخصية. وتسعى هذه اللوائح جاهدة لضمان أن يكون للمواطنين دور أكبر في كيفية استخدام بياناتهم. في الآونة الأخيرة ، تم التركيز أيضًا على جوانب أخرى من إدارة البيانات. تحاول الإستراتيجية الرقمية للاتحاد الأوروبي ، على سبيل المثال ، تنظيم الأسواق الرقمية في السلع والخدمات لتشجيع المزيد من المنافسة مع تسهيل إنشاء ما يسمى بـ "مساحات البيانات" (28) - data spaces- وهي المساحات التي يمكن من خلالها مشاركة البيانات . تُبذل جهود مماثلة لتنظيم استخدام البيانات لتطوير أنظمة الذكاء الاصطناعي والتخفيف من آثار هذه الأنظمة على الخصوصية الشخصية.

(28) - يشير مصطلح "مساحة البيانات" إلى نوع من علاقة البيانات بين الشركاء الموثوق بهم الذين يلتزمون بنفس المعايير والإرشادات عالية المستوى فيما يتعلق بتخزين البيانات ومشاركتها داخل واحد أو أكثر من الأنظمة البيئية العمودية. يتمثل أحد الجوانب المهمة لمفهوم مساحة البيانات في أن البيانات لا يتم تخزينها مركزيًا ، بل يتم تخزينها في المصدر. وبالتالي ، يتم نقلها فقط من خلال قابلية التشغيل البيني الدلالي عند الضرورة .

على الرغم من أن الهند قد خطت خطوات كبيرة في رقمنة اقتصادها ، إلا أن الأطر القانونية الهندية لم تواكب هذا النمو السريع. لا يوجد لدى الهند حتى الآن إطار قانوني شامل لإدارة البيانات. تم تقديم مشروع قانون حماية البيانات إلى البرلمان ، لكن تم سحبه . من المرجح أن يتم تقديم نسخة مبسطة وأكثر شمولاً من مشروع القانون، لكن الجدول الزمني غير واضح.

يمكن للتأخير في إنشاء إطار قانوني شامل لإدارة البيانات أن يخدم مصلحة الهند إذا كان بإمكانها التعلم من تجارب البلدان الأخرى واستخدام تلك المعرفة لتنفيذ إطار عمل حديث لإدارة البيانات. ويمكن أن يشمل ذلك بعض المقترحات التي تتم مناقشتها في أوروبا بالإضافة إلى حلول جديدة أخرى تهدف إلى معالجة هذه القضايا .

إدارة البيانات في الهند

في الوقت الحاضر ، تنظم الهند البيانات الشخصية من خلال قواعد تكنولوجيا المعلومات (ممارسات وإجراءات الأمان المعقولة والبيانات الشخصية الحساسة أو المعلومات) ، وهي قواعد تعمل كإطار أساسي لتنظيم البيانات الشخصية الحساسة. لا توفر هذه القواعد إطارًا شاملاً لحماية البيانات على غرار معظم قوانين حماية البيانات في الولايات القضائية الأخرى. (فهي ، على سبيل المثال ، لا تنظم حقوق بيانات

الأطفال أو عمليات نقل البيانات عبر الحدود ، كما أنها لم تنشئ حتى منظمًا لحماية البيانات.) وبدلاً من ذلك ، تقتصر هذه القواعد في المقام الأول على جمع وحيازة وتخزين ومعالجة والاحتفاظ ونقل البيانات. ، والإفصاح عن البيانات الشخصية الحساسة من قبل الشركات من خلال إدخال شرط الموافقة على جميع هذه الأنشطة. كما ينص القانون على بعض "الممارسات والإجراءات الأمنية" للتعامل مع البيانات الحساسة.

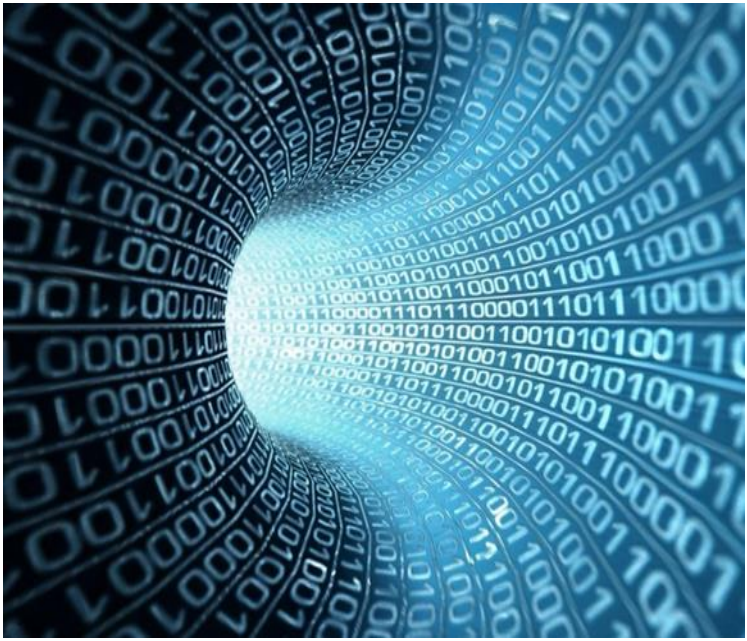
على الرغم من دخول هذه القواعد حيز التنفيذ منذ أكثر من عقد من الزمان ، إلا أن التأخير وعدم كفاية الآليات الإدارية والقضائية أعاقت تنفيذها . منذ عام 2011 ، كان هناك القليل من اللوائح أو لم يتم تنفيذها بموجب أحكامها. تمتثل الشركات لأحكامها ولكنها تلقت القليل من التوجيه أو لم تتلق أي إرشادات حول كيفية التعامل مع العديد من الالتباسات التي نشأت.

ومع ذلك ، فقد ازداد وعي المواطنين الهنود والمجتمع المدني بالأضرار الكامنة في جمع البيانات الشخصية وتوليدها ومعالجتها. في 2018 ، كان حكم تاريخي للمحكمة العليا ، والذي أيد استخدام أرقام تعريف Aadhaar الرقمية الهندية ، معالجة المخاوف المتعلقة بالتنميط الحكومي والمراقبة. وقضت المحكمة العليا في حكم آخر في 2017 بأن الحق في الخصوصية هو حق أساسي - على الرغم من عدم تحديده في الدستور الهندي - مشتق من الحق في الحياة والحرية الشخصية . ركزت هذه الأحكام اهتمام الجمهور على حق تمتع الأفراد باستقلالية فيما يتم عمله ببياناتهم.

يسير نهج الهند في إدارة البيانات على ثلاثة مسارات مختلفة. الأول هو تنظيم البيانات الشخصية بطرق تعتمد بشكل كبير على المبادئ المنصوص

عليها في اللائحة العامة لحماية البيانات (GDPR) (29) للاتحاد الأوروبي بالإضافة إلى اللوائح الدولية الأخرى المتعلقة بمعلومات التعريف الشخصية. ثانيًا ، الهند بصدد إنشاء إطار بيانات غير شخصي - وهو مسار لم يشرع فيه أي بلد آخر بعد. ويتعلق الجانب الثالث من هذا العمل بحوكمة البيانات الحكومية ، والتي يتم تغطيتها في إطار مشاركة البيانات الوطنية و نهج الوصول إليها.

(29)- هي اللائحة الأوروبية لحماية البيانات. دخلت حيز التنفيذ في 2018 وتؤثر على جميع الشركات العاملة في معالجة البيانات الشخصية للمقيمين في أوروبا. وتسعى اللائحة إلى عدة أهداف طموحة : توحيد لوائح حماية البيانات على المستوى الأوروبي، جعل الشركات أكثر مسؤولية من خلال تطوير المراقبة الذاتية، و تعزيز حق الأفراد (الحق في الوصول ، والحق في النسيان أي الحذف ، والحق في النقل ، وما إلى ذلك.



الجيوسياسة والفضاء السيبراني

إن النهج الجيوسياسي، جنبًا إلى جنب، مع التعامل مع المعلومات التقنية للغاية وكميات كبيرة من البيانات في المصادر المفتوحة يجعل من الممكن ، من خلال عبور كميات هائلة من البيانات المكانية وغير المكانية ، لفهم العلاقات بين الجهات الفاعلة ، واستراتيجيات التأثير ، ومخاطر صراع جيوسياسي أو سوق حساسة. وهذا يتطلب نهجًا متعدد التخصصات

جوهريًا بين العلوم الإنسانية والاجتماعية (الجغرافيا والقانون والعلوم السياسية والفلسفة) وعلوم الكمبيوتر والرياضيات.

القضايا الرقمية والمناخية

ترتبط القضايا الرقمية والمناخ ارتباطًا وثيقًا ، حيث تتقدم الثورة الرقمية في سياق التدهور البيئي الذي يجبر مجتمعاتنا على التطور لتقليل أثر الأنشطة البشرية على هذا الكوكب. تعكس البيانات الرقمية كلاً من العالم المادي والأنشطة البشرية. إلى جانب الخوارزميات القوية ، فإن هذا الحجم المذهل من البيانات يجعل من الممكن مراقبة وفهم النظم البيئية وكذلك التنبؤ بتغير المناخ. كما أنها تتيح إمكانية التحليل بأدق التفاصيل لتحركاتنا ومهننا وتبادلاتنا الاجتماعية وسلوكنا التجاري ، وبالتالي وضع أشكال من الحوكمة الرقمية التي بدأت تظهر في بعض البلدان الآسيوية ، ولا سيما الصين. يوضح تنفيذه في سياق وباء الفيروس التاجي الفوائد المحتملة التي يقدمها وكذلك المخاطر الأخلاقية وحقوق الإنسان التي ينطوي عليها. تواجه هذه المبادرات التمثيلات الغربية للحريات الفردية مع التمثيلات الأصلية للطبيعة والمصلحة الجماعية ، المتجذرة في الفلسفة الصينية القديمة ، وتطرح لتجربة أشكال جديدة من الحوكمة الرقمية من أجل فهم التحديات المتزايدة القضايا الأكثر تعقيدًا التي تواجه مجتمعاتنا. يتمثل التحدي السياسي الرئيسي في وضع التكنولوجيا الرقمية في خدمة التنمية المتناسقة والاستدامة لمجتمعاتنا. ومع ذلك ، فإن التحولات التي أحدثتها التكنولوجيا الرقمية ، إذا كان من الممكن أن تكون مصدرًا للحل ، هي أيضًا عامل زعزعة الاستقرار السياسي وتفاقم الانقسامات الحزبية والاجتماعية في ديمقراطياتنا.

التلاعب بالمعلومة

فاجأ قرصنة رسائل البريد الإلكتروني للحزب الديمقراطي وإصدارها من قبل "ويكيليكس" خلال الحملة الرئاسية لعام 2016 الإدارة الأمريكية على حين غرة .أدركت الإدارة فجأة نقاط الضعف في نظام يعتمد على سجلات الناخبين وآلات التصويت غير الآمنة ، وخشيت من أن تؤدي العملية الإلكترونية إلى تقويض نزاهة العملية الانتخابية. ومع ذلك ، فقد تم تنفيذ عملية التدخل على المستوى المعلوماتي ، مستغلة ضعفًا رئيسيًا - وهو ليس ضعفا إلكترونيا أو تقنيا - وإنما للمجتمع الأمريكي ، وهو الاستقطاب السياسي القوي للمجتمع الأمريكي واستياء أولئك الذين تخلفوا عن ركب العولمة من النخب. ومع ذلك ، تواجه الديمقراطيات الغربية الآن خطر التلاعب على نطاق واسع بالرأي العام في سياق أزمة الثقة في المؤسسات ، وصعود الشعبوية ، وحتى التطرف ، والذي زاد بمقدار عشرة أضعاف عن طريق الويب والشبكات الاجتماعية. يمكن بعد ذلك استغلال حرية التعبير كأداة لزعزعة الاستقرار خلال الشأن السياسي أو النقاش العام أو الحركة الاجتماعية أو العملية الانتخابية. في الهند ، يأتي هذا الاستغلال من الحزب الحاكم نفسه. وتشجع الحكومة تطوير الاتصال والتحول الرقمي للدولة مع استغلال الشبكات الاجتماعية للأغراض الانتخابية ، لا سيما من خلال تأجيج التوترات بين المجموعات العرقية والاجتماعية ذات العواقب الوخيمة.

في أوروبا ، يتمثل التهديد على الصعيدين، الخارجي والداخلي. لاسيما بفعل الأساليب والأهداف -الخاصة بالجماعات اليمينية المتطرفة القريبة من روسيا - على الشبكات الاجتماعية للتواصل أثناء الحملات الانتخابية في أوروبا. على وجه الخصوص ، يوضح تأثير الابتكارات المرتبطة بتقنيات هندسة التأثير التي تستخدمها هذه المجموعات. يمكن أن تؤثر عمليات المعلومات أيضًا على مجالات الاهتمام الاستراتيجي أو التوسع فيها بشكل انتهازي. يوضح انتشار المحتوى الذي أنتجته الوكالات الروسية والصينية في إفريقيا الناطقة بالفرنسية التأثير المتزايد لروايات هذه القوى

، التي تتبناها طواعية المواقع الإخبارية في جميع أنحاء القارة. ويثير هذا الموضوع مخاوف جدية ولكنه أيضًا يثير الكثير من الارتباك. إن تكاثر المصطلحات لوصف هذه الظاهرة (الأخبار الكاذبة ، التضليل ، التلاعب بالمعلومات) يكشف عن صعوبة استيعابها وتوصيفها ، ومن هنا تأتي أهمية إجراء دراسات دقيقة لفهمها .

تزداد مكافحة هذه الظاهرة تعقيدًا حيث يعتمد الفاعلون ، من ناحية ، على حرية التعبير ، وهي قيمة أساسية للديمقراطيات ، ومن ناحية أخرى ، على منصات ذات أنشطة عابرة الحدود، والتي ليس لمعظم الدول أي سلطة عليها. وهكذا تفرض هذه المنصات نفسها على الساحة الدولية باعتبارها تحديًا لسيادة الدول ولكن أيضًا كشريك أساسي في ممارسة سلطاتها السيادية. قضية السلطة والسيادة هي أيضًا في صميم "التسييس" المتزايد لقضايا التكنولوجيا الرقمية.

القضايا الاستراتيجية للتقنيات الرقمية

تعتبر قضية "الحوسبة السحابية - cloud computing - "التي تسمح بالتخزين عن بعد واستخدام البيانات والخدمات الرقمية - مثالاً واضحًا على ذلك. ومازالت تبدو هذه "الحوسبة السحابية" كأسطورة بسبب الترابط التكنولوجي ولكن أيضًا بسبب واقع السوق ووسائله. ومع ذلك ، أصبحت تكنولوجيا "الحوسبة السحابية" ضرورية للتحول الرقمي للشركات والمؤسسات وحتى الجيوش حاليا. وتعد البيانات الرقمية في صميم تحديات التحول الرقمي لوزارات الدفاع اليوم ، والتي تسعى إلى امتلاك التقنيات الناشئة بسرعة من خلال استخداماتها الجديدة ، لتجنب اضطرابات في ممارسات ومنظومات العمل للجيش. لذلك وجب توخي البراعة في كيفية معالجتها وتشاركها بشكل أفضل، و أيضًا تخزينها وتأمينها. الطموح

الرقمي لوزارات الدفاع اليوم هو أيضًا طموح للسيادة الرقمية ، والتي يتم التعبير عنها بلغة عسكرية ب " الاستقلال الذاتي الاستراتيجي."

في واقع الأمر، تقدم مختلف هذه المفاهيم وجهين لعملة واحدة ، أي قدرة الدولة على ممارسة سلطاتها السيادية والاحتفاظ بالسيطرة على مصيرها في العصر الرقمي .فرض مفهوم السيادة الرقمية نفسه في الجدال العام بعد ما كشف عنه "إدوارد سنودن" بشأن المراقبة الواسعة المدى التي مارستها الولايات المتحدة ، بينما أصبحت أوروبا تدرك فجأة مخاطر اعتمادها على التقنيات الرقمية الأمريكية .علما أنه مازالت هناك صعوبات في تحديد ملامح مفهوم "الاستقلال الذاتي الاستراتيجي" – المنتشر كثيرا في وسائل الإعلام - والذي يغطي عددًا كبيرًا من القضايا من أنواع مختلفة . كما أن تنفيذه لايزال معقدًا للغاية، على المستويين الوطني والأوروبي ، من حيث بُعده السياسي والصناعي. ولعل النقلة من تقنية الهاتف المحمول 4 Gإلى 5 Gمثالاً ممتازًا بهذا الخصوص.

لقد برزت عدة رهانات وتحديات بخصوص نشر تقنية الهاتف المحمول 5 - Gمنها الاقتصادية والتكنولوجية والجيوسياسية – فقد ضغط "دونالد ترامب" على حلفائه لحظر شركة "Huawei" الصينية ، التي تتفوق بفارق كبير على الشركات الأخرى ، بما في ذلك في الأسواق الأوروبية. وقد ظهر بجلاء، من خلال تركيز كل الاهتمام على الشركة الصينية ، أراد الرئيس الأمريكي إرجاع جميع المشكلات الأمنية والمخاطر الكامنة في أي تقنية رقمية إلى مصدر بعينه - ضمن القائمة السوداء لشركات التكنولوجيا الصينية - وهي استراتيجية كشفت الكثير عن القدرة التنافسية للصين و عن سياق المنافسة الإستراتيجية العامة المتزايدة بين البلدين أكثر من المنافسة حول التكنولوجيا نفسها. فلم يتردد "دونالد ترامب" في تسييس القضايا التكنولوجية. في حين أن إدارة "أوباما" كانت قد تشاورت مع الخبراء لفترة طويلة على حيادية الإنترنت قبل أن تقرر لصالحها ، إلا أن "دونالد ترامب"، فور وصل إلى السلطة اختار عدم اعتبار هذه الحيادية .ويضمن

هذا المبدأ التأسيسي للإنترنت المعاملة المتساوية لجميع تدفقات الإنترنت ، وبالتالي يمنع مزودي خدمة الإنترنت من تفضيل أو إبطاء محتوى معين. وهو مبدأ يحظى بشعبية لدى الرأي العام والذي تدافع عنه بحماس شركات "وادي السيليكون - Silicon Valley - "المصممة على الكفاح من أجل استعادته .

وبالنسبة لروسيا، إن السيادة الرقمية ليست مفهومًا أو طموحًا ، ولكنها سياسة عامة تهدف إلى ضمان الاستقلال الاستراتيجي والاستقلال الرقمي لروسيا ضد الاعتماد على الكيانات الخارجية. ويبدو أن اكتشافات "سنودن" كانت بمثابة حافز لطموحات التطوير الرقمي التي تعتمد بشكل أساسي على البرامج المجانية ومفتوحة المصدر ، والتي تجمع بين مزايا تكاليف التشغيل المنخفضة وإمكانية تعزيز سيطرة سلطات الدولة على البنى التحتية الرقمية ، وهي ممارسة تتعارض مع الروح التي أدت إلى ظهورها للسماح للمستخدمين باختيار والتحكم في تشغيل برامجهم بأنفسهم. وتتضمن الاستراتيجية الروسية أيضًا تطوير مناطق رقمية استراتيجية. لاسيما ة في سيبيريا ، وهي منطقة تحظى بوفرة الكهرباء بأسعار جذابة والمناخ البارد ومراكز استضافة البيانات العديدة سياقًا ملائمًا لتطوير هذا النشاط الذي يساهم بدوره في تشكيل الإقليم.

استراتيجيات القوة في الفضاء السيبراني

من الأمثلة البارزة حالة "إستونيا"، التي اعتمدت على التكنولوجيا الرقمية لتطوير أراضيها وتحرير نفسها من القوة الروسية لبناء هوية وطنية قوية ، بعد سقوط الاتحاد السوفيتي. من خلال تبني الابتكار التكنولوجي والأمن السيبراني والدفاع السيبراني في إستراتيجية "العلامة التجارية القومية " الخاصة بها ، تمكنت "إستونيا" من تولي زمام القيادة بشكل كبير على البلدان الأخرى من حيث التنمية الرقمية وضمان تأثيرها الدولي. وتمكنت

الدولة ، التي أصيبت بالشلل - بسبب الهجمات الإلكترونية في عام 2007 (30) والتي رفعت الوعي الحقيقي على نطاق دولي - من الاستفادة من ظهورها الإعلامي للحفاظ على مكانتها كرائدة عالمية في مجال الابتكار الرقمي ، حتى لو بدأت هذه الاستراتيجية في إظهار حدودها.

(30) - اجتاحت هجمات WannaCry - و - NotPetya لعام 2017 أكثر من 150 دولة دون حسيب ولا رقيب ، مما تسبب في أضرار بمئات الملايين من الدولارات للشركات والمؤسسات من جميع الأحجام.

وهناك مثال الدولة العبرية- فيبدو أن إسرائيل لا تعرف حدودًا في ازدهار الابتكار إذ يشكل جزءًا من استراتيجية شاملة للقوة وتحتل فيها التكنولوجيا الرقمية مكانة بارزة. لقد نجحت إسرائيل في تقعيد صناعة متطورة في المجال الرقمي واستثمرت بالكامل في تطوير القدرات الإلكترونية في خدمة نفوذها وقوتها. ففي الفضاء الرقمي كما هو الحال في المجالات العسكرية الأخرى ، تفضل إسرائيل سرعة العمل وخفة حركتها وقوتها الضاربة لإقامة توازن ملائم للقوى في صالحها ضد أعدائها ، مهما كانت التكلفة السياسية أو القانونية ، وبالتالي الانخراط الكامل في عسكرة الفضاء السيبراني الذي تم استنكاره من طرف الصين.

ومع ذلك ، تطمح الصين لأن تصبح "القوة الإلكترونية الكبرى" ، وهو هدف رفعته السلطات الصينية إلى مرتبة الأولوية المطلقة. إن استراتيجية القوة هذه هي جزء من الهدف الأوسع للرئيس "شي جين بينغ Xi - " Jinping - لتحقيق "الحلم الصيني" وتستجيب بشكل أساسي للأهداف السياسية المحلية ، حتى لو تضمنت عنصرًا دبلوماسيًا إضافيًا ، وهو الأهم. يجب أولاً استخدام الاستثمارات الضخمة المخصصة للتعليم والبحث والتطوير للنهوض بالاقتصاد الرقمي والذكاء الاصطناعي من أجل تطوير الدولة وحكمها بشكل أفضل ، وتمكينها من تحقيق برنامجها السياسي مع

ضمان استقرارها السياسي. ومن ثم فإن صعود الرقمنة مصحوب بسياسة للأمن السيبراني لا تنفصم ، والتي تشمل أيضًا التحكم في المحتوى المعلوماتي المتداول على الويب والشبكات .

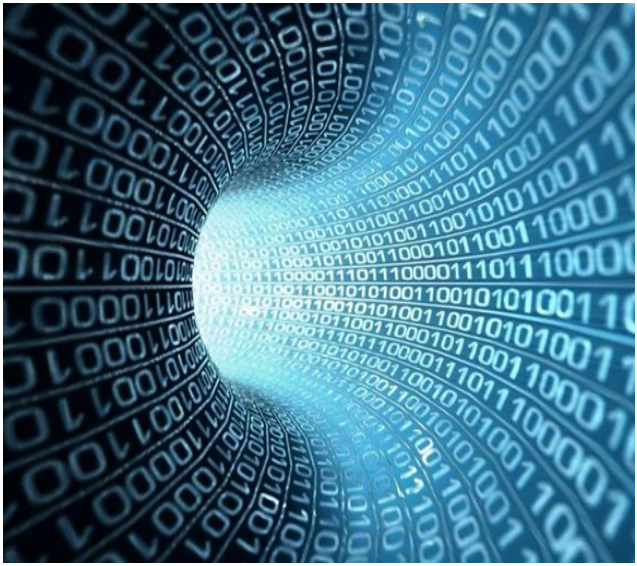
إن القوة الأمريكية أمر واقع لا مفر منه في الفضاء الإلكتروني. ومع ذلك ، اتخذت استراتيجية إدارة "ترامب" في هذا المجال منعطفًا هجوميًا بشكل خاص أثار الكثير من الجدل والتساؤل عبر المحيط الأطلسي. إنها عقيدة "الاشتباك المستمر" ومفهوم "الدفاع عن المستقبل" الخاص برؤية القيادة الإلكترونية والتي تعزز التعرف على العمليات السيبرانية الهجومية وبالتالي تشكل تحولًا في التمثلات والأجهزة في هذا المجال العسكري الجديد. ويتمثل هذا الموقف في إبراز القوة بلهجات رادعة لتحقيق أهداف أمن الولايات المتحدة والاستقرار الدولي في الفضاء الإلكتروني. ومن خلال إضفاء الشرعية على استخدام العمل الهجومي في الفضاء الرقمي ، تساهم هذه الاستراتيجية بشكل مباشر في تسريع وتضخيم " سباق التسلح السيبراني."

استخدام الفضاء الإلكتروني لشن الحرب

منذ خريف عام 2019 برزت جدالات في الأمم المتحدة بهدف ضمان أمن واستقرار الفضاء السيبراني. ويرتبط مفهوم الفضاء السيبراني هنا ارتباطًا وثيقًا بإضفاء الطابع الإقليمي عليه وعسكرة الفضاء. تجد الدول نفسها عالقة بين ضرورتين أمنيتين تخلقان توتراً متناقضاً: من ناحية ، ضمان قوتها "الرقمية "للحفاظ على استقلاليتها الاستراتيجية وتفوقها التشغيلي على أعدائها وخصومها ؛ ومن ناحية أخرى ، للحد من المخاطر

المنظومية المرتبطة بانتشار الأدوات الهجومية التي يمكن أن تأتي بنتائج عكسية ، وتنتشر دون حسيب ولا رقيب ، وتتسبب في أضرار جسيمة وتزعزع استقرار الفضاء الإلكتروني والمجتمعات.

في نهاية المطاف ، ينضم هذا الجدال إلى المخاوف التي أثيرت منذ أكثر من خمسين عامًا في الجدال حول الردع النووي. باستثناء أن "الرقمنة" أضحت موجودة في كل مكان ، والأدوات الهجومية في متناول الجميع ، والترابط والتفاعلات بين مجالات متعددة ، غير معروفة جيدًا وبالتالي يصعب التحكم فيها. وهكذا تجد الدول نفسها عند مفترق طرق. وحتى في مجال البيانات ، هناك مسارات تؤدي إلى حيث لا نريد أن ينتهي بنا الأمر.



الرهانات الاستراتيجية للثورة الرقمية

شهدت الثورة الرقمية، التي أحدثها التبني الجماعي لتكنولوجيا المعلومات والترابط العالمي لأنظمة المعلومات والاتصالات، تسارعًا شديدًا خلال العقدين الماضيين. لقد أدت إلى اضطراب عميق في الممارسات الاجتماعية والاقتصادية والسياسية للمجتمعات البشرية ، أكثر أهمية من القطيعة الناتجة عن اختراع الكتابة والطباعة.

يتم الآن تحويل أقسام المعرفة والنشاط البشري بالكامل إلى بيانات رقمية ، يتزايد حجمها أضعافًا مضاعفة - إن لم نقل انفجارًا حقيقيًا - مما يفرض تطوير أنواع جديدة من الإحصائيات. ومن ثم ، فإن العالم المادي مليء بأجهزة استشعار منتشرة في الأماكن العامة والخاصة ، والهواتف الذكية ، والأدوات المتصلة وأيضًا معدات الحياة اليومية (السيارات ، والتلفزيونات ، والأجهزة المنزلية) ، وفي الصناعة ، وفي القوات المسلحة ، بل تم إدخالها مباشرة في جسم الإنسان (أجهزة تنظيم ضربات القلب). تتيح الآثار الرقمية التي يتركها المستخدمون بعد ذلك مراقبة وتحليل تحركاتهم وأنشطتهم وتفاعلاتهم في الوقت الفعلي ، واستنتاج تحليلات تنبؤية بشأن احتياجاتهم وسلوكياتهم لأغراض تجارية أو استراتيجية أو خبيثة أو للصالح العام. فهي تمكن من تطوير التقنيات التخريبية والاستخدامات الجديدة التي تحدث ثورة في الممارسات وتفتح آفاقًا للتنمية لم تكن متخيلة حتى الآن ، وبالتالي تدفع الشركات والمؤسسات والدول لبدء التحول

الرقمي الخاص بها. أصبحت القدرة على جمع البيانات وتخزينها والإحالة المرجعية إليها واستغلالها في صميم الابتكار ، ومحرك النمو الاقتصادي ، وتمكين القوة ، بالإضافة إلى العديد من القضايا الأخلاقية والديمقراطية والحوكمة والشرعية.

تعمل هذه التطورات أيضًا على إحداث تحولات عميقة في البيئة الاستراتيجية والطريقة التي تقاس بها القوى العظمى الآن وتصديها بعضها البعض. يتم إعداد تمثيلات التهدد وأيضًا تلك الخاصة بالأمن في بيئة رقمية، حيث تكون الترابطات والتفاعلات متعددة والاعتماد المتبادل ، ولكنها ليست مفهومة ومعروفة ومسيطر عليها دائمًا .وبالتالي ، فإن التحول الرقمي يواجه الحكومات بخيارات تكنولوجية واستراتيجية وأخلاقية معقدة للغاية ، يصعب تقييم جميع الآثار المترتبة عليها مسبقًا والتي تحشد في بعض الأحيان تمثلات متناقضة للمخاطر والأمن ، من مختلف وجهات النظر، إن كان الجيش أو المخابرات أو رجال الأعمال أو المجتمع المدني. ومع ذلك ، فإن مجال المخاطر ، مثل مجال الفرص ، استمر في التوسع وأصبح أكثر تعقيدًا طوال العقد الماضي.

ترافق التحول الرقمي مع سلسلة من المفاجآت الاستراتيجية المرتبطة ، من ناحية ، بالتطور المتزايد للهجمات الموجهة بشكل متزايد الصادرة إلى حد كبير من الدول ، ومن ناحية أخرى ، بتنويع الأهداف والجهات الفاعلة الخبيثة وأساليب التشغيل و العواقب التي تؤدي إلى زعزعة استقرار المجتمعات بشكل متراكم. وأضحت التقنيات الرقمية ، من خلال توافرها وتكلفتها المنخفضة ، أدوات استخباراتية قوية ذات تأثير وفي متناول العديد من الجهات الفاعلة ، ولكنها أيضًا عوامل هائلة للهجمات التي لا حدود

لاستخدامها. وهكذا تم تحويل هذه التقنيات عن استخدامها الأصلي . وتميز العقد الأخير ببروز مجال المعلومات كأولوية استراتيجية (الدعاية الجهادية ، التلاعب بالمعلومات) والهجمات المدمرة التي انتشرت دون رادع على نطاق عالمي .

انتشرت الهجمات السيبرانية، وقد شجعت هذه التطورات على تأجيج سباق "التسلح السيبراني" في ديناميكية عسكرة الفضاء السيبراني مما دفع الدول إلى جعله ساحة معركة مميزة.

من الفضاء الإلكتروني إلى عالم البياناتdata sphère -

في سنة 2014 ، نشرت مجلة "هيرودوت" عددها الأول وخصصته بالكامل للقضايا الجيوسياسية، لاسيما للفضاء السيبراني. وظهر مفهوم "الفضاء السيبراني" منذ نهاية العقد الأول من القرن الحادي والعشرين في استراتيجيات ومذاهب العديد من الدول باعتباره فضاءً لتهديد الأمن القومي و "منطقة" يجب السيطرة عليها وأولوية استراتيجية. وبفضل انتشار الهجمات الإلكترونية المعقدة والمتطورة بشكل متزايد ، رسخ "الفضاء السيبراني" نفسه تدريجياً في خطاب الدول، كمنطقة جديدة للمنافسة الاستراتيجية ومجالاً للمواجهة ، بل وحتى كبيئة عسكرية جديدة ، إلى جانب الأرض والبحر والجو والفضاء.

كما أُعْتُرف به كأولوية استراتيجية ومجال عسكري جديد في "الكتاب الأبيض حول الدفاع والأمن القومي "في فرنسا في 2013 ، ومع ذلك ،

لازال مفهوم الفضاء السيبراني – يكافح -للتعبير عن حجم التحديات التي تواجه الدول في مواجهة الثورة الرقمية.

"مجال البيانات" ، مفهوم ناشئ حديثًا يشمل القضايا الاستراتيجية المتعلقة بالفضاء السيبراني وبشكل عام تلك المتعلقة بالثورة الرقمية. من خلال التأكيد على الصلة بين مجال العالم المادي والبيانات ، يتيح مفهوم "مجال البيانات" إمكانية أفضل لفهم التحديات الحالية والمستقبلية في عالم تزايد فيه الاعتماد على التقنيات والبيانات الرقمية ، وتحكمه الخوارزميات والذكاء الاصطناعي ، والتي من المتوقع أن تتضاعف قوتها بواسطة "كمبيوتر الكم. quantum computer - "

يرجع فضل وضع نظرية "مجال البيانات" إلى "ستيفان غروميخ - " Stéphane Grumbach – قصد تعيين حقبة جيولوجية جديدة تتميز بالتأثير الحاسم للأنشطة البشرية على النظام البيئي للأرض - ولا سيما في أصل تغير المناخ. من أجل فهمه كفضاء جديدة ، يجب النظر إلى مجال البيانات بشكل كلي ، كنظام يتكون من جميع البيانات ، الرقمية بالطبع .

يمكن تصور مجال البيانات على أنه تمثيل لحيز فضائي جديد يتكون من جميع البيانات الرقمية والتقنيات التي تكمن وراءه ، بالإضافة إلى تفاعلاتها مع العالم المادي والإنساني والسياسي الذي ترتكز عليه. ومن المؤكد أن مجال البيانات ليس منطقة بالمعنى الكلاسيكي للمصطلح في الجغرافيا ، ولكن مع التوسع العالمي للإنترنت ، ظهر مفهوم الفضاء السيبراني على

أنه تمثيل لمنطقة في خطاب الفاعلين السياسيين ، لأسباب متعارضة تمامًا: أرض مستقلة للمشاركة والحرية لرواد الإنترنت ، ثم منطقة للتهديدات يجب تأمينها وحتى ساحة معركة للدول. وينعكس إضفاء الطابع الإقليمي على الفضاء الإلكتروني في استراتيجية الدول التي تسعى إلى استعادته والتحكم فيه بشكل أفضل ، بدء من البنى التحتية المادية إلى المعلومات التي يتم تداولها عبره وبواسطته.

أضحى هذا " الفضاء"، اليوم، جزءا من البيئة الجديدة التي نتطور فيها من خلال اعتماد التقنيات والخدمات والبنى التحتية والأسلحة الناتجة عن الثورة الرقمية. ويمكن فهمه على أنه شكل من أشكال تمثيل مكان في بيانات العالم الذي له جغرافيته الخاصة التي ما زلنا نعرف القليل عنها .

ويمكن تمثيل هذه الجغرافيا جزئيًا من خلال الخرائط الجيوسياسية الكلاسيكية التي توضح التوزيع المكاني للبنية التحتية المادية (الكابلات والخوادم - servers - وأجهزة التوجيه (routers - والموارد الرقمية (مراكز الطاقة ومراكز التدريب ومراكز الحوسبة ومراكز استضافة البيانات وصناعة الثقة (، والاشتباكات بين الجهات الفاعلة (مصدر معروف للهجمات الإلكترونية وهدفها (أو حتى تدفقات تحديد الموقع الجغرافي (تدفقات البيانات بين الدول). لكنه يحشد أيضًا نظرية الرسوم البيانية التي تجعل من الممكن تمثيل العلاقات والتفاعلات بين الجهات الفاعلة التي يمكن تحديدها مكانيًا من العقد والروابط لإظهار درجة التقارب بين الجهات الفاعلة وفقًا لشدة تبادلاتهم .ويمكن في بعض الأحيان تحديد الموقع الجغرافي لبعض هؤلاء الفاعلين ، من أجل إنشاء تطابق بين الرسم البياني والخريطة الجيوسياسية .

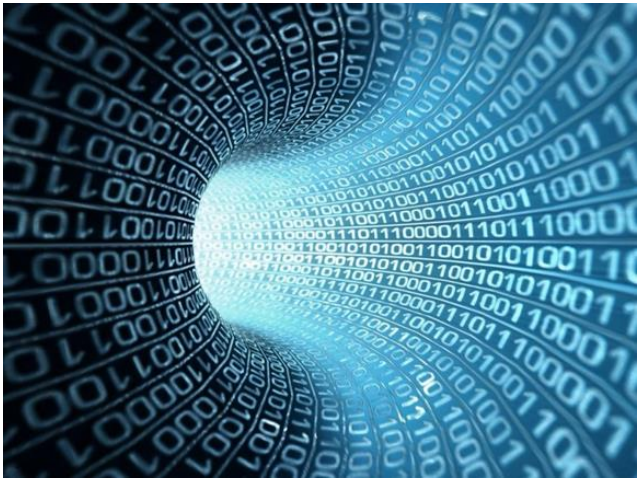
تُستخدم هذه الأساليب، على سبيل المثال ، لتحديد المجموعات من عمليات التبادل في شبكة "توتير" الاجتماعية ، أو لتمثيل المسارات التي يمكن أن تسلكها البيانات للانتقال من نقطة إلى أخرى في مجال البيانات. كما مكنت الغرب من الكشف عن استراتيجية إيران لفصل فضاءها الوطني لمجال البيانات عن عالم البيانات العالمي .

إن مجال البيانات يشكل ، من ناحية ، "كلًا مجاليًا" على نطاق كوكبي ، ومن ناحية أخرى ، يمكن تناوله ودراسته على مستويات مختلفة من التحليل ، من المستوى الإقليمي من خلال جميع الموارد الرقمية المخزنة أو التي يمكن الوصول إليها على نطاق صغير خاص بمنطقة إلى مستوى التفاعلات على نطاق كوكبي - عالمي. وبالتالي يمكن تحليل مسألة "السيادة الرقمية" على أنها عملية إقليميّة لمجال البيانات والتي تتطلب تحديد ورسم خرائط لخصائص المجال الذي يعتبره الفاعلون أنه يدخل ضمن السيادية .

توضح روسيا ، على سبيل المثال ، رؤيتها في سلسلة من القوانين التي تم وضعها منذ 2012 والتي تشمل ، من بين أمور أخرى ، موقع البيانات المتعلقة بالمواطنين الروس على الأراضي الوطنية ، والتحكم في الطرق التي تسلكها البيانات وإمكانية قطع الوصول إليها أو الاستفادة منها، أو توقيف الاتصال بشبكة الإنترنت العالمية ، وإلزام الشركات المصنعة لأجهزة الكمبيوتر لعامة الناس بتثبيت البرامج الروسية مسبقًا على منتجاتهم.

ومع التحول الرقمي للمجتمعات واعتمادها المتزايد على التقنيات والبيانات الرقمية ، فإن مجال البيانات يقع عند تقاطع معظم المجموعات المكانية الأخرى - من المدن المتصلة ، وحتى الفضاءات الأصغر من ذلك، إلى الفضاء الخارجي، حيث يؤدي انتشار وتكاثر الفاعلين والبيانات المتصلة إلى إحداث مشكلات في الثورة الرقمية.

تعد جغرافية مجال البيانات هذه، استراتيجية وضرورية بشكل بارز لفهم العالم المعاصر وصراع القوى الجيوسياسية. وتشمل جغرافية التدفقات والتحكم في البيانات ، وفهم مساحة المعلومات ، ورسم خرائط الشبكات الطوبولوجية ، و أيضا دمج البيانات المحددة جغرافياً والبيانات غير المكانية. وتشمل أيضًا الأبعاد القانونية المعقدة وتحليل التمثلات لفهم وتمييز الظواهر غير الملموسة جزئيًا. كما يمكن أن تكشف دراستها عن الاختلالات وعلاقات توازن القوى ، واستراتيجيات الفاعلين أصحاب المصلحة ، والمناورات وحتى المواجهات التي تحدث داخل وخارج مجال البيانات.



لماذا البيانات الرقمية جيوسياسية؟

يعتبر تداول البيانات والتحكم فيها في صميم النزاعات المعاصرة. والحرب الروسية في أوكرانيا مثال على ذلك .

أصبحت رقمنة قطاعات كاملة من النشاط البشري واضحة الآن. عدد أقل فأقل من الأعمال اليومية يفلت من الشبكات التي يمارسون عليها ، لا سيما في أوقات الوباء :إجراء مكالمة هاتفية مع الأقارب ، أو أخذ دورة تدريبية ، أو التنقل في الشارع باستخدام هاتف ذكي ... كل هذه الأنشطة غير ضارة تولد بيانات رقمية هي موضوع العديد من الرغبات سواء كانت تجارية أو سياسية أو استراتيجية.

نظرًا لأنها تنتشر على سطح الكرة الأرضية عبر شبكة معقدة من الكابلات والبروتوكولات والأنظمة الأساسية ، فإن بياناتنا جيوسياسية. وهي في ذات الوقت موضوع ومصدر، معا، للسلطة، إنها في قلب عدد متزايد من النزاعات، بينما لا توجد حرب تفلت من التكنولوجيا الرقمية. هذه الحقيقة هي مركز مفهوم -Datasphereمجال البيانات .

ويمكن تصور مجال البيانات على أنه يمثل "حيز مكاني جديد" يتكون من جميع البيانات الرقمية والتقنيات التي تكمن وراءه، بالإضافة إلى تفاعلاتها مع العالم المادي والإنساني والسياسي الذي ترتكز عليه .

وقد أضحى اليوم من الضروري فهم القضايا الجيوسياسية المتأصلة في مجال البيانات هذا، الذي نتطور فيه جميعًا. بعيدًا عن الانفصال عن العالم المادي ، فهو بالأحرى امتداد له - مثل نوع من "الواقع المعزز أو المضاف" الذي بدأنا للتو في استكشافه وسبر أغواره.

ولن يتأتى هذا إلا عبر فهم الآليات الإقليمية للبيانات الرقمية: كيف يتم تداولها على سطح الكرة الأرضية؟ ما هي الاختناقات الاستراتيجية التي تحتاج إلى المرور من خلالها لربط منطقة معينة؟ ما هي أساسيات رسم خرائط الفضاء السيبراني) الفضاء الإلكتروني) ، اللازمة لتمثيل مجال البيانات كظاهرة جيوسياسية .

هناك تعارضات ناتجة عن البيانات، لهذا أصبح التحكم في تدفق البيانات هدفًا في حد ذاته في العديد من المنافسات الجيوسياسية.

وهناك البيانات الناتجة عن النزاعات وموازن القوى، نظرًا لأن التزايد المسترسل للأنشطة البشرية تولد المزيد من البيانات ، وتزداد أيضًا

علاقات القوة الجيوسياسية. ومع ذلك ، تتوفر هذه البيانات بسهولة أحيانا كثيرة، أو يمكن اقتناؤها من مصادر. وجمع بعض هذه البيانات والتحقق منها يجعل من الممكن توثيق التضاربات والصراعات ، وأحيانًا التأثير عليها.

ملحق

الدعم الدولي للدفاع السيبراني الأوكراني

2022

عزز المجتمع الدولي قدرة أوكرانيا الإلكترونية بجيش من المدافعين الإلكترونيين الحكوميين والتجاريين الذين أثبتوا دورهم المحوري في الحرب ضد روسيا.
فهل أدى الدعم العام والخاص للدفاع السيبراني الأوكراني إلى قلب الموازين على ركح الصراع؟

إذا كان القادة الغربيون قد حسموا أمر عدم إرسال قوات عسكرية للقتال في أوكرانيا، فمع ذلك ، في المجال الرقمي ، تقوم الجهات الغربية الحكومية والعسكرية والتجارية بالتصدي للمهاجمين الروس مباشرة وتتحمل مجموعة من المسؤوليات للدفاع عن الشبكات والبيانات الأوكرانية. فقد واجهوا حملة مكثفة من الهجمات الإلكترونية الروسية في الأشهر الستة الأولى من الحرب العدوانية على أوكرانيا.

نفذت روسيا أكثر من 1500 "هجوم إلكتروني" ضد أوكرانيا في الأشهر الستة الأولى من الحرب. و"الهجوم الإلكتروني"- حسب تعريف المعهد الوطني الأمريكي للمعايير والتكنولوجيا - هو "أي نوع من النشاط الضار الذي يحاول جمع موارد نظام المعلومات أو المعلومات نفسها أو تعطيلها أو رفضها أو إضعافها أو تدميرها".

على الرغم من المعدل المرتفع للهجمات الإلكترونية ، فشلت الحرب الإلكترونية الروسية كثيرًا في تجسيد الطريقة التي توقعها العديد من الخبراء. برز الجهد الدولي لتعزيز الدفاعات الإلكترونية في أوكرانيا بشكل بارز بين مجموعة واسعة من النظريات المطروحة لشرح التأثير المحدود نسبيًا للعمليات الإلكترونية في الحرب. لكن الخبراء انقسموا حول أهمية كل جانب تقريبًا من جوانب الحملة الإلكترونية ، بما في ذلك الادعاء بأن المساعدة الدولية كانت مفيدة في تمكين دولة صغيرة نسبيًا من صد إحدى القوى الإلكترونية الرائدة في العالم.

فكيف تم تنفيذ هذه المساعدة في الدفاع عن الفضاء السيبراني الأوكراني؟ وما جدوى الدفاع الدولي الجماعي في الفضاء السيبراني؟

رغم أن المدة لم تتجاوز تسعة أشهر من الحرب ، فقد تطور النشاط في الفضاء الإلكتروني إلى الحد الذي ظهرت فيه دروسا مهمة. وهي الدروس، التي أعلنها بعض المشاركين فعليا في الدفاع عن الفضاء السيبراني الأوكراني، أقتبسها من تقارير أعدت لهذا الخصوص على سبيل تقييم أولي لهذه التجربة (1).

(1) – من هؤلاء:

Badanes (Microsoft), Luke Champion (UK FCDO), Bertie Kerr (BAE Ginny Digital Intelligence), Stephanie Kiel (Google), James Muir (BAE Systems Digital Intelligence), Adrian Nish (BAE Systems Digital Systems Oleksandr Potii (State Service of Special Communications ,(Intelligence Protection of Ukraine), Christiaan Smits (Cloudflare), and Information .(Google), and Alissa Starzak (Cloudflare) Charley Snyder

سيقتصر الحديث على الدفاع عن الشبكات الرقمية الأوكرانية ضد الهجمات الروسية منذ بدء الغزو البري. علما أن هذا الجانب لا يمثل سوى جزء من الجهد الدولي لدعم أوكرانيا في الفضاء الإلكتروني ، وهو نشاط شمل بالإضافة إلى ذلك مكافحة المعلومات المضللة ، وإنشاء استخبارات مفتوحة المصدر ، وتسخير المنصات الرقمية للمساعدة الإنسانية والدفاع المدني. علاوة على النشاط التشغيلي السري.

توقعت العديد من توقعات ما قبل الحرب أن الهجمات الإلكترونية ستلعب دورًا مهمًا في حملة روسيا. اقترح السياق الاستراتيجي أنه على الرغم من أن أوكرانيا لديها خبرة كبيرة في الدفاع ضد الهجمات الإلكترونية الروسية ويمكنها استدعاء خبراء متحمسين وذوي كفاءة عالية لحماية الأهداف الحرجة ، إلا أنها في النهاية لن تكون قادرة على منع الضرر الجسيم للشبكات والبيانات الرقمية واستغلالها. . قد تتفوق مزايا روسيا الاستراتيجية على نقاط القوة التشغيلية في أوكرانيا في امتلاك بعض أقوى القدرات الإلكترونية الهجومية في العالم والعمل في تضاريس رقمية يُعتقد أنها تفضل الهجوم على الدفاع. ويبدو أن موسكو تتمتع بميزة حاسمة في الفضاء الإلكتروني.

فيما يتعلق بالفعالية الاستراتيجية للعمليات الإلكترونية الروسية ، يؤكد بعض الخبراء أنه على الرغم من أن روسيا كانت نشطة للغاية في استخدام الهجمات الإلكترونية ضد أهداف أجنبية ، إلا أنها فشلت في تحقيق أهدافها أو لم تحقق سوى تأثيرات استراتيجية محدودة.

في الواقع ، كثفت روسيا حملتها طويلة الأمد من الهجمات الإلكترونية ضد أوكرانيا قبل الغزو البري ، وحافظت على وتيرة عالية من الهجمات في الأشهر التالية. ومع ذلك ، يبدو أن الهجمات قد حققت اضطرابًا محدودًا فقط ، ولم تساهم سوى بقيمة استراتيجية ضئيلة في أهداف الحرب. وكان اتجاه للشراكات الدولية نحو تعزيز الدفاع السيبراني في أوكرانيا ، بينما أعلنت – Microsoft - أن "شكلًا جديدًا من أشكال الدفاع الجماعي" أثبت أنه أقوى من القدرات الإلكترونية الهجومية. بعد ستة أشهر من

الحرب ، برز تقييم مفاده: "أننا رأينا النشاط الدفاعي الأكثر فعالية عبر الإنترنت في التاريخ".

لكن تقييم التأثير الاستراتيجي أصعب في المجال الرقمي مقارنة بمجالات الحرب الأخرى. يرى بعض الخبراء أن حرب أوكرانيا أظهرت القيود المتأصلة في العمليات السيبرانية الهجومية ، بينما يؤكد آخرون أن توقعات "الصدمة الإلكترونية والرعب" كانت غير واقعية وأن روسيا في الواقع استخدمت العمليات الإلكترونية بشكل جيد ضد الأهداف المرجوة. على الرغم من أن كل مجموعة تفسر البعد السيبراني للحرب بشكل مختلف تمامًا ، فإن وجهتي النظر تقللان من أهمية القوة الدفاعية لأوكرانيا في تحديد القيمة الاستراتيجية للهجمات الإلكترونية الروسية. وتم اقتراح عوامل أخرى على أنها أكثر أهمية ، مثل محدودية الاستعداد القبلي للوكالات الإلكترونية الروسية والرغبة في الحفاظ على الشبكات الأوكرانية الرئيسية لاستغلالها.

لذلك فإن تقييم الجهد الدولي لدعم الدفاع السيبراني الأوكراني يسير على خلفية التقييمات المتباينة للأحداث والنظريات المتنافسة لدور القوة الإلكترونية في هذا الصراع وفي المستقبل.

شنت روسيا حملة مكثفة من الهجمات الإلكترونية بالتزامن مع الغزو ، وقامت بحوالي 800 هجوم ضد أهداف أوكرانية حتى نهاية مارس. ورغم أن أوكرانيا تتمتع بخبرة أكثر من أي دولة أخرى في الدفاع ضد الهجمات الإلكترونية الروسية والتعافي منها ، فقد أصبح واضحًا في وقت مبكر من

الحرب أن وكالات الأمن السيبراني السبع في أوكرانيا واجهت مهمة غير مسبوقة من المرجح أن تتجاوز قدرتها الدفاعية وتكشف عن نقاط ضعف خطيرة في المرونة.

ومن ثمة ظهرت طلبات المساعدة في مجال الدفاع الإلكتروني في وقت مبكر من تواصل "كييف" مع الحلفاء المحتملين ، وتلبية الاستجابات المتجاوبة بشكل متزايد كزخم للعمل الذي تم بناؤه في العواصم الغربية. وسرعان ما أصبح واضحًا أن القدرة على تحقيق التأثير التشغيلي في الفضاء الإلكتروني لا تعتمد فقط على الوكالات الحكومية والعسكرية، ولكن أيضًا على التكامل الوثيق بين شركات التكنولوجيا التجارية والأمن السيبراني. في حين أن الوكالات الغربية الرسمية يمكن أن تعتمد على العلاقات القائمة مع الشركاء الأوكرانيين ولديها أدوات قوية وقدرات فريدة ، فإن تقديم الدفاع السيبراني على نطاق واسع لا يمكن تحقيقه إلا من قبل كيانات القطاع الخاص التي تمتلك الخدمات الرقمية الأكثر استخدامًا وتشغلها وتفهمها. وهكذا كانت القرارات المبكرة، التي اتخذتها قيادة بعض شركات التكنولوجيا والأمن السيبراني الكبرى في العالم لأداء أدوار استباقية في الدفاع عن أوكرانيا، محورية وحاسمة.

استثمرت العديد من الحكومات الأجنبية وشركات الأمن السيبراني في بناء القدرات السيبرانية الأوكرانية على مدى عدة سنوات. تهدف هذه المبادرات إلى إرساء أسس المرونة في مواجهة الهجمات الإلكترونية الروسية ، على سبيل المثال من خلال تدريب ممارسي الأمن السيبراني وإصلاح القوانين واللوائح. وخلق الغزو الروسي حاجة ملحة لا يمكن تلبيتها من خلال البرامج التي تهدف إلى أهداف التنمية طويلة الأجل ، فتم اللجوء إلى تعبئة الموارد العامة والخاصة وتم إحداث بعض الشراكات

المبتكرة. على سبيل المثال ، رعى مكتب المملكة المتحدة للشؤون الخارجية والكومنولث والتنمية (FCDO) ، بمشورة فنية من المركز الوطني للأمن السيبراني ، برنامجًا يمكّن الوكالات الأوكرانية من الوصول إلى خدمات شركات الأمن السيبراني التجارية ، بتمويل وتنسيق من FCDO. قامت حكومة المملكة المتحدة بتسخير قدرات الأمن السيبراني التجارية لتحقيق تأثير تشغيلي فوري. على الرغم من عدم وجود مخطط لهذا الترتيب ، إلا أنه يحمل بعض التشابه مع برامج الإغاثة الدولية في حالات الكوارث حيث تقوم الحكومات الراعية بتحفيز وتنسيق تقديم القدرات التشغيلية المستمدة من القطاع الخاص.

وبرنامج FCDO هو مبادرة وطنية ، والجهود الدفاعية الدولية التي نشأت لم يتم تنسيقها مركزيًا وفقًا لخطة موحدة ، بل تشكل مجموعة من الأنشطة التي تحركها وجهات النظر الوطنية والتنظيمية حول قدرات الحرب والموارد. لعب المركز الوطني الأوكراني لتنسيق الأمن السيبراني ، الذي أنشئ في عام 2016 ، دورًا رئيسيًا في مزامنة وتنسيق هذه العمليات والجهات الفاعلة المتباينة.

يعتقد مسؤولو الأمن السيبراني الأوكرانيون أن هذه المساعدة الدولية كانت حيوية في الحد من فعالية الهجمات الإلكترونية الروسية . لقد حققت الاستجابة للحوادث ومعالجتها على نطاق أكبر بكثير مما كان يمكن أن تحققه أوكرانيا بشكل مستقل ، وقد تصدت لهجمات ربما تسببت في ضرر استراتيجي (لا سيما محاولة تعطيل الشبكة الكهربائية الأوكرانية عبر برنامج Industroyer2 الخبيث). كما أتاح التعاون في استخبارات التهديدات التعلم السريع للطرق الروسية والوعي المشترك بالأوضاع.

وأصبح فريق الاستجابة للطوارئ الحاسوبية في أوكرانيا (CERT-UA) مصدرًا غزيرًا للإبلاغ عن التهديدات.

ومن السمات المميزة الأخرى للجهود الدفاعية تكامل كبار مزودي التكنولوجيا الأمريكيين ، ولا سيما - Amazon و Cloudflare و Google و Microsoft- قدرة هذه الشركات على ترحيل البيانات والخدمات الحكومية الأوكرانية إلى الخوادم السحابية الموزعة ؛ توفير حماية آلية للشبكات الضخمة ، إلى جانب حماية مخصصة للمستخدمين المعرضين لمخاطر عالية ؛ بالإضافة إلى التحديث المستمر لذكاء التهديدات المستمدة من القياس العالمي عن بُعد ، كل هذا أضاف عمقًا دفاعيًا ومرونة أكثر بكثير مما كان يمكن لأوكرانيا تحقيقه بشكل مستقل.

ومع ذلك ، فإن جميع الأطراف المشاركة في الجهود ظلت حذرة في الادعاء بأن النجاح سيستمر. وظهر أن الحملة الإلكترونية الروسية تتألف من عدد صغير من العمليات السيبرانية الهجومية المخطط لها بعناية (مثل الهجوم على مزود الاتصالات عبر الأقمار الصناعية Viasat) ثم عادت إلى العمليات غير المتطورة لكنها مكثفة في بعض الأحيان (عمليات رفض الخدمة والهجمات القائمة على التصيد) .

هناك عامل معقد آخر وهو عدم امتلاك أي من الكيانات المعنية - بما في ذلك أكبر شركات التكنولوجيا والأمن السيبراني في العالم - صورة كاملة للهجمات الإلكترونية الروسية ضد أوكرانيا. حتى عندما يكون للشريك الدفاعي رؤية جيدة ، قد يكون من الصعب أو المستحيل اكتشاف أنواع

معينة من العمليات. وهنا ، الشغل الشاغل يتعلق بالتجسس. ينصب معظم التركيز على الهجمات الإلكترونية كأحد مكونات الحرب على إمكانية تعطيل الأهداف أو إضعافها أو تدميرها. ومع ذلك ، تتمتع روسيا بسجل حافل في استخدام الاختراقات على الشبكة لجمع المعلومات الاستخباراتية ، ويمكن أن تكون هذه العمليات أكثر صعوبة في الكشف عنها وأقل تأثيرًا فوريًا. استخدمت الجهات الفاعلة الحكومية العمليات السيبرانية الأكثر شيوعًا لتشكيل البيئة لصالحها بدلاً من تحقيق آثار قسرية فورية ، ويمكن لموسكو تأمين الوصول إلى الشبكات واستخلاص المعلومات الاستخباراتية التي قد تولد قيمة استراتيجية حتى الآن.

دفعت هذه الحرب أحد الرؤساء التنفيذيين لشركة كبيرة للأمن السيبراني إلى الدعوة إلى إنشاء "الناتو التقني" ، وقد صرح رئيس Microsoft أن الحرب أظهرت الحاجة إلى "استراتيجية منسقة وشاملة لتعزيز [أنترنت] الدفاعات. " ربما لم تكشف الحرب في أوكرانيا عن مخطط جاهز للدفاع الدولي الجماعي في الفضاء السيبراني ، لكنها اختبرت مفهوم تعاون أصحاب المصلحة المتعددين ، وأظهرت في هذه العملية جملة من الدروس من أهمها:

- يعتمد الدفاع السيبراني على نطاق واسع على مشاركة أكبر شركات التكنولوجيا التجارية والأمن السيبراني. ويرجع ذلك إلى الاعتماد العميق على خدمات عدد صغير من مقدمي الخدمات. وفي الواقع إن الدفاع السيبراني على المستوى الوطني يعتمد بشكل كبير على الحماية الآلية لملايين الأهداف.

- السياسة والجغرافيا السياسية لهما أهميتهما في الفضاء السيبراني كما هو الحال في أي مكان آخر. لم تتضمن الاستجابة لحرب أوكرانيا بناء

استراتيجيًا وعمليًا شبيهًا بـ "الناتو التكنولوجي" ، بالاعتماد على تراكم الجهود المبذولة ضمن استراتيجيات الحكومة الوطنية. فلا يزال الطريق طويلاً للتطور وتحويل التجربة الأوكرانية إلى أساس دائم للتحالفات الدولية في مجال الدفاع السيبراني. سيتطلب تصميم مثل هذه الآليات من الحكومات الوطنية مواجهة حقيقة أن الشركاء التجاريين الذين لا غنى عنهم للدفاع السيبراني هم الأمريكيون.

- القيم المشتركة لا تقل أهمية عن المصالح المشتركة. إن أسباب انخراط الكيانات التجارية في الدفاع عن الفضاء السيبراني الأوكراني هي الأسباب التجارية (إظهار القدرات والفوائد) ، والسمعة (خارجيًا ، للحكومات والعملاء والمستثمرين وما إلى ذلك ، وداخليًا للموظفين) ، والمعيارية (حماية القيم ومنع الضرر). يمكن بسهولة رفض المكون المعياري باعتباره غير مهم عند مقارنته بالمصالح التجارية للشركات الضخمة ، لكن المشاركين في هذه التجربة أظهروا إحساسًا حقيقيًا بالالتزام بقيم السلوك المشتركة في الفضاء الإلكتروني ، وخاصة في الدفاع عن الأهداف المدنية ضد الهجمات الإلكترونية الحكومية. لقد أدى الحفاظ على وتيرة عالية من عمليات الأمن السيبراني إلى اختبار جميع الكيانات المعنية ، وكان الدافع لحماية الديمقراطية الأوكرانية وإحباط العدوان الروسي عاملاً رئيسيًا في الحفاظ على الفعالية على مدى فترة طويلة.

- تشير تجربة هذه الحرب إلى أن المرونة الإلكترونية الدولية مبنية على أساس بناء القدرات ولكنها تعتمد أيضًا بشكل حاسم على القدرة على زيادة القدرات بسرعة لتعزيز الحلفاء المعرضين للهجوم.

الهجمات الإلكترونية الروسية

صيف 2022

شنت روسيا حربًا إلكترونية ضد أعدائها المعلنين وحتى ضد آخرين ، والتي يكون لها أحيانًا تداعيات في أماكن أخرى: فمثلا تسبب هجوم إلكتروني في إغلاق الإنترنت في فرنسا. كما خشيت وزارة الداخلية الفرنسية جدا من احتمال التدخل الروسي في الانتخابات الرئاسية.

مثال، في 24 فبراير 2022 تم تسجيل هجوم جاء من "السيبير ستيبس" - cyber steppes- وها هي الواقعة. وصلت "صوفي" - Sophie – (مديرة شركة) إلى مكتبها ووجدت أن خط الإنترنت الخاص بها معطل، رغم أنه من النوع السريع المعتمد على سرعة مشغل الأقمار الصناعية - Nordnet – التابع لشركة Orange ، والذي يربط "صوفي" بالشبكة العالمية باستخدام الصحن.

وقد تبين أن هذا الانقطاع صاحب الغزو الروسي لأوكرانيا. ومن المحتمل جدا أن يكون الهجوم الإلكتروني الذي أمر به "الكرملين" قد أصاب شبكة Viasat- – الفضائية ، التي توفر اتصالات الإنترنت في أوكرانيا. بدوره ، وبالتتابع التالف قطع أيضًا بث النطاق العريض بواسطة – Nordnet- على حوالي عشرة آلاف مشترك فرنسي.

وصرحت "صوفي" لوسائل الإعلام معلنة " الإنترنت عبر الأقمار الصناعية معطل، ولم يعد بإمكاني العمل ، عملي يعتمد على الوصول إلى الإنترنت، وإذا بقيت على هذا الحال لمدة أسبوعين أو حتى شهر ، فأنا أخاطر بشركتي التي سيكون مآلها الإفلاس لامحالة".

وتدخلت جهات، منها غرفة التجارة والصناعة ، لحل المشكلة لكن دون نتيجة. وقد التمست جهات وازنة من "صوفي " بعدم التحدث عن المشكل لعدم إثارة جدل من شأنه إقلاق الشركات وتخويفها.
وكانت فرنسا قد اضطرت إلى الاستعداد للتهديدات السيبرانية.

لا تمنع الطبيعة غير المباشرة لهذا الهجوم الحاسوبي الحكومة الفرنسية من إعداد خطوط دفاعاتها الرقمية. وقد أعلن مركز الدفاع الإلكتروني بوزارة الداخلية "يقظة معززة" على الفور.

فقد سبق في سنة 2017 أن تم بث "رسائل خاصة" من حملة إيمانويل ماكرون قبل 48 ساعة من الجولة الثانية من الانتخابات الرئاسية. لم يتمكن التحقيق الذي أجرته وكالة أمن نظم المعلومات الوطنية من تحديد ما إذا كان الهجوم قد نفذته دولة أو جماعة إجرامية منفصلة. من المؤكد فقط أن المعلمات – "السيريلية" (2) - Cyrillic settings - لوثائق تثبت تلاعب متحدثين باللغة الروسية.

(2) - تطلق "السيريلية" على الأبجدية التي خلقت في القرن التاسع الميلادي، والتي تستخدم في كتابة ونسخ اللغات الروسية والصربية والبلغارية والأوكرانية وعدد من اللغات غير السلافية.

يمكن أن تستهدف أعمال التدخل السيبراني أيضًا البنى التحتية التقنية. وحدث هذا في عام 2016 ، عندما أدى هجوم على الكمبيوتر نُسب إلى موسكو إلى حرمان مدينة "كييف" من التيار الكهربائي. وفقًا لمذكرة من الكونجرس الأمريكي بتاريخ 2 فبراير 2022 ، فإن فريقًا من - FSB(3) - وهو جهاز استخبارات روسي ، "متخصص في اختراق البنية التحتية في قطاع الطاقة" هو الذي خطط لهذا الهجوم وأنجزه. كما لا يمكن استبعاد هجماته التي تستهدف الجهات الاقتصادية والمنظمات العامة. وفقًا للملاحظة الأمريكية ، فإن المتسللين الذين خدعهم "الكرملين" هم الذين وراء البرنامج الضار- NotPetya (4). في عام 2017 ، كان برنامج البرنامج وراء موجة من الهجمات الإلكترونية التي كان لها عواقب وخيمة على الشركات والبنوك والمؤسسات العامة في جميع أنحاء العالم.

(3) - هو الخليفة الرئيسي لـ KGB السوفياتي ، الذي تم حله في نوفمبر 1991 بعد انقلاب موسكو. وهو مؤسسة لا يعرف عنها الكثير. حسب رأي العديد من الخبراء ، يعتبر إحدى ركائز النظام الروسي الحالي، ومنذ وصول "فلاديمير بوتين" إلى السلطة في عام 1999 ، تقوى هذا الجهاز وتوسعت تدخلاته.

(4) - هو برنامج ضار يقوم بتدمير البيانات ، و يظهر في شكل برامج طلب فدية من خلال عرض مذكرة فدية على شاشة الكمبيوتر المصاب. واعتبار لآلية انتشاره وصف بدودة كمبيوتر. وكان وراء هجوم إلكتروني عالمي في 2017. إنه يؤثر على جميع إصدارات - Microsoft Windows ، من Windows XP إلى Windows 10-

وبدورها عانت الخدمات الحكومية الروسية أيضًا من عواقب حرب "العصابات عبر الإنترنت". حيث تعذر الوصول إلى مواقع "الكرملين" و"الدوما" ووزارة الدفاع ووكالة الفضاء الروسية في بداية 2022. وذلك نتيجة هجوم تبنته مجموعة الهاكرز "أنونيموس"- Anonymous.

على الصعيد الفرنسي ، تم ملاحظة أكثر من 1000 اقتحام حاسم لشبكات الكمبيوتر في عام 2021. وعملت الوكالة الوطنية لأمن أنظمة المعلومات على 200 حالة من برامج طلب الفدية ، وهي برامج تشل عمل الشركات والإدارات في انتظار الحصول على المطلوب. أما الهجمات الأخرى فتتعلق بالتجسس أو التخريب.

إن التهديدات الإلكترونية تستمر في التصاعد. في عام 2021 ، أصبح 600 خبير من وكالة نظم المعلومات الوطنية بفرنسا على دراية بـ1082 عملية اقتحام حاسمة لحسن سير العمل في البلاد. هذا الرقم لم يكن بهذا الارتفاع من قبل. في عام واحد ، ارتفع بنسبة 37٪ مقارنة بـ 786 هجومًا مدرجًا في عام 2020.

سواء تعلق الأمر بالابتزاز أو التجسس أو التأثير أو زعزعة الاستقرار ، يستفيد المهاجمون بالكامل من هشاشة البنى التحتية الرقمية أينما وجدت.

إن الهجومات السيبرانية الروسية التي استهدفت أكرانيا وصلت ارتداداتها – بشكل غير مباشر- إلى مؤسسات وجهات في دول أخرى.

إلا أنه لا ينبغي "للعاصفة الجيوسياسية" – التي أحدثها التعدي الروسي على أكرانيا- أن تشغلنا عن التهديدات السيبرانية الشائعة والمتزايدة حاليا. وبالمثل ، فإن المخاطر الأكثر وضوحا ليست بالضرورة تلك التي يواجهها الخبراء في أغلب الأحيان. فمن بين آلاف الاختراقات الحاسوبية التي أثرت على شبكة مهمة العام الماضي في فرنسا ، اشتملت 203 "فقط" على برامج طلب الفدية - وهي برامج تشل الشركات من خلال جعل البيانات غير قابلة للقراءة حتى يتم دفع المطلوب.

ومن جهة أخرى إذا كانت الهجمات الإلكترونية الهادفة للربح غير المشروع والابتزاز تطغى على المشهد الإعلامي ، فلا ينبغي لها أن تلقي بظلالها الكثيفة على حملات التجسس ، التي هي بطبيعتها أقل وضوحًا ، وتلك التي يتم إجراؤها بهدف التخريب الحاسوبي من النيل من المستهدف لغاية غير المال.

فهل العالم اليوم يعرف "الحرب الإلكترونية العالمية الجديدة" ؟ هذا في

وقت تذكرنا الهجومات الإلكترونية الهائلة ، على نطاق غير مسبوق في العالم ، بضعفنا "الرقمي". فهل بلدان العالم مسلحة فعلا لخوض هذه الحرب ؟
وهل هؤلاء "الهاكر" الروس الغرباء الذين زرعوا الخوف على شبكة الويب العالمية في الأشهر الأخيرة ، جزء من استراتيجية موسكو البديلة إن تعذر عليها تحقيق ما تصبو إلية بقوة النيران والتدمير المادي والبشري ؟

ففي كل مرة يستخدم المرء الخوادم الروسية - وفي معظم الأحيان - نفس البرنامج الضار- Black Energy- "حصان طروادة" يتسلل ، دون علم مستخدمي الإنترنت ، و يختبئ في قلب ذاكرة أجهزة الكمبيوتر عندما يقوم "المبحرون في شبكة الإنترنيت" بتنزيل ملفات تبدو غير ضارة وعادية جدا. إنه فيروس قديم ظهر لأول مرة في عام 2007 واستخدمه "مجرمو الإنترنت ". وتم رصد نسخة ثانية منه في عام 2010. في ذلك الوقت ، تم استخدامه لتنفيذ عمليات احتيال بنكية تقليدية.

وظهرت مرة أخرى في 2014 ، ثم في 2015. هذه المرة مع تطوير جديد يستهدف "قتل القرص" - kill disk – أي تحويله إلى سلاح هائل قادر على إلحاق أضرار عميقة بالمعدات الرقمية الحساسة و أيضًا لمحو آثار مروره.

ويفيد أحد التقارير "إن التحليل "البعدي" بأثر رجعي للسجلات (آثار الاتصال) على خوادم إحدى الشركات الأوكرانية التي تعرضت للهجوم جعل من الممكن إثبات أن الانقلاب قد تم التحضير له في وقت مبكر جدًا". ووفقًا لنفس التقرير ، فإن البرنامج الضار تسلل في مارس 2015 ، وظل متخفيا لمدة تسعة أشهر ، يكتفي بمراقبة تشغيل شبكة الإمداد بالطاقة خلال هذه الفترة. وكانت أوكرانيا محظوظة إذ أن محطات الطاقة الخاصة بها بقيت محافظة على أجهزة تسمح بإعادة التنشيط اليدوي لشبكاتها لأنها لم

تلغيها. وهكذا تمكنت من استعادة الطاقة في غضون ساعات قليلة بعد الهجوم. لكن في بلدان أخرى ، حيث أصبحت جميع العمليات إلكترونية الآن ، كان من الممكن أن يستغرق الأمر وقتًا أطول، والضرر أكبر. هذا ما كشف عنه الخبراء.

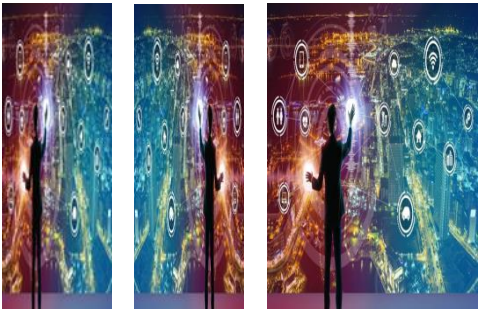
وقد أدى اختراق محطة الطاقة النووية الألمانية في الربيع الماضي إلى زيادة مخاوف خبراء الأمن السيبراني الغربيين من طرف "كوماندو هاكر" أطلق على نفسه رمز (APT28)، مرارًا وتكرارًا، في الماضي في هجماته الرقمية. يوتم إلقاء اللوم على هذه المجموعة في حملات القرصنة المختلفة التي استهدفت "الناتو" والحكومتين الأوكرانية و البولندية وناشطين أوروبيين ذوي أهمية حيوية ، بما في ذلك بورصة "وارسو" ومطار "بوريسبيل" الدولي بالقرب من كييف وشركة اتصالات الفرنسية التي لم يعلن عن اسمها.

حتى لو أنكر الروس - على أعلى مستوى في البلاد - أي تورط حكومي في هذه الهجمات المختلفة ، فمن الصعب تصديق عدم حضور عين ويد موسكو في هذه "الأعمال العدائية"، وهذا ما أقر به أكثر من مصدر دبلوماسي وسياسي وعسكري. لذا تتعامل الحكومات الأوروبية مع هذا التهديد بجدية أكبر منذ هجوم تجسس إلكتروني سابق - هذه المرة عبر برنامج "Potao " الخبيث - والذي استهدف دولًا أخرى ("أرمينيا" و"جورجيا" على وجه الخصوص) ويحمل أيضًا توقيع مجموعات المتسللين الروس.

يبدو بجلاء – للعام والحاص- أن هذه النوازل – وغيرها لا يسع المجال والمقام لذكرها كلها- تتجاوز مجرد حوادث أعمال التخريب البسيطة. في واقع الأمر، إنها تهدفن ضمن ما تهدف إليه، تأكيد شكل من أشكال القوة المزعجة القادرة على إلحاق أضرار بالغة.

هناك شيء مؤكد، لا يمكن نكرانه أو الشك فيه ولو قيد أنملة : "لقد تم مؤخرا تحديد العديد من المواقع الإخبارية في أوكرانيا وتطهر فيها "كابسولات " إشهارية ملوثة بنسخة جديدة وأكثر تعقيدًا من " Black Energy والتي تضاعفت أيضًا في الآونة الأخيرة.

كما أن السلطات الأمريكية كشفت عن اختراق خوادم البحرية الأمريكية في 24 نوفمبر2021 وما نتج عن ذلك من تسرب – إذ تمت سرقة ملف يحمل الاسم والعنوان ورمز الأمان لأكثر من 134300 جندي أمريكي - وقد اتخذت وكالة الأمن القومي إجراءات لتعقب مقترفي هذا "الاختراق". وهنا أيضا، تتجه الأنظار إلى موسكو، مثلما حدث خلال الحملة الرئاسية الأمريكية عندما هاجم قراصنة روس خوادم اللجنة الوطنية للحزب الديمقراطي المسؤولة عن جمع الأموال لهيلاري كلينتون.



الأمن السيبراني: ثغرات الجيش الإسرائيلي

بوياسمين خولي

الحوار المتمدن-العدد: 7456 - 2022 / 12 / 8

حذر مراقب الدولة في تقرير لاذع من أن الجيش الإسرائيلي عرضة للهجمات الإلكترونية التي قد تؤدي إلى سرقة كبيرة للهوية.

كما سلط التقرير الضوء على نقاط الضعف في أمن تكنولوجيا المعلومات في أنظمة التعليم والبنية التحتية للنقل وإمدادات المياه وداخل هيئة الضرائب في إسرائيل.

ويبدو بجلاء أن التقرير مقلق للغاية من حيث أمن تكنولوجيا المعلومات وحماية جميع المعلومات الشخصية ، إلا أن العديد من الاستنتاجات التي توصل إليها البحث ظلت سرية لأسباب أمنية.

ورغم ذلك، ما تم الكشف عنه مقلق للغاية حسب معدي التقرير الذين دعوا الحكومة إلى اعتبار التصدي للتهديدات السيبرانية أولوية قصوى.

يسلط التقرير - المؤلف من 33 صفحة والذي أعده مكتب مراقب الدولة - الضوء على "ثغرات كبيرة" في حماية المعلومات البيومترية التي يحتفظ بها جيش الدفاع الإسرائيلي - سجلات الأسنان ، وبصمات الأصابع ، وفي بعض الحالات ، عينات الحمض النووي التي تُستخدم لتحديد الجنود القتلى. يشير التقرير إلى أن الجيش لم يحدّث بروتوكولات الخصوصية الخاصة به منذ عام 1996.

كما أفاد بأنه يتم حفظ المعلومات البيومترية للعسكريين المتوفين ، مما يثير

مخاوف من أن القراصنة قد يستخدمون هذه المعلومات لسرقة هذه الهويات وانتزاعها. وأن بعض بيانات الجيش محمية فقط بمستوى متوسط من الأمان في الوقت كان يجب أن يكون على النحو الأعلى والأقصى.

وفور صدور التقرير بدأ الجيش الإسرائيلي بالفعل في مراجعة وتنفيذ غالبية التوصيات التي قدمها التقرير من أجل تعزيز أمن وحماية بياناته. وأشار الجيش إلى أن قواعد البيانات المشار إليها في التقرير "موجودة في شبكة سرية للجيش الإسرائيلي .لا يمكن الوصول إليها من قبل أطراف خارجية ولا يمكن رؤيتها من قبل أطراف غير مصرح لها داخل الجيش."

كما أشارت إلى بروتوكولات السرية الخاصة بها - والتي لم يتم تحديثها منذ عام 1996 - قائلة إن البروتوكولات الجديدة "في طور المصادقة والتحديث" ، معلنة أن الجيش سيلتزم بالتوصيات التي قدمها المراقب الدولة الذي طلب أن تتم مراجعة البروتوكولات كل سنتين أو ثلاث سنوات.

اهتم التقرير أيضًا بنقاط الضعف في أمان الكمبيوتر داخل وزارة التعليم ، معربًا عن قلقه من أن درجات المدارس الثانوية يمكن الوصول إليها بسهولة من قبل المتسللين. وأشار إلى أن نظام الوزارة على الإنترنت محمي بواسطة برنامج أمان إلكتروني قديم وأن الشركة المصنعة نفسها توقفت عن الاعتماد على هذا الإصدار منذ 2019.

وفيما يتعلق بمصلحة الضرائب ، اعتبر التقرير أنها تعتمد أكثر من اللازم ، وفي مجملها ، على شركة خارجية واحدة وقعت معها عقدًا لإعادة تنظيم نظام الكمبيوتر فيما يتعلق بالتجارة الخارجية. ومن خلال الاعتماد حصريًا على هذه الشركة - التي لا يُعرف مستوى أمنها السيبراني - يمكن للسلطة

أن تعرض معلوماتها للخطر.

ويسلط التقرير الضوء أيضًا على أن البنية التحتية للنقل وإمدادات المياه معرضة بشكل خاص للهجمات الإلكترونية.

في 2020 ، ورد أن قراصنة إيرانيين استهدفوا إدارة المياه ، في محاولة لزيادة كمية الكلور في المياه التي يتم توزيعها إلى مستوى خطير. وفي 2021 ، استأجرت إدارة المياه شركة للأمن السيبراني لحماية منشآتها من التهديدات السيبرانية المحتملة وهجمات برامج الفدية. ومع ذلك ، يشير التقرير إلى أن إدارة المياه لم تطلب من موردیها ، على مستوى البلاد ، نشر نظام للحماية من الهجمات الإلكترونية.

إسرائيل وإفريقيا : دبلوماسية برامج التجسس

اقتنت بعض الدول الإفريقية برامج التجسس الإسرائيلية .فاشترت غانا برنامج التجسس "بيغاسوس" (5) - Pegasus- من المجموعة الإسرائيلية "NS0 "في ظل ظروف مريبة جدا. وغالبا ما ينظر لمثل هذا الاقتناء من طرف دولة من القارة السوداء على أنه نموذجي في إفريقيا ويؤكد أن صناعة الأسلحة الإلكترونية والمراقبة الإسرائيلية مرتبطة ارتباطًا وثيقًا بدبلوماسية تل أبيب وبرنامج التطبيع في إفريقيا ، من توغو إلى المغرب.

(5) - برنامج تجسس مصمم لمهاجمة الهواتف الذكية التي تعمل بنظام iOS - و - Android تم تصميمه وتسويقه منذ 2013من طرف شركة - NSO Group - الإسرائيلية ولم يتم اكتشاف الآثار الأولى لاقتحاماته إلا في 2016. يتم تثبيته على الجهاز ، حيث يتمكن من الوصول إلى الملفات والرسائل والصور وكلمات المرور والاستماع إلى المكالمات ويمكنه تشغيل التسجيل الصوتي أو الكاميرا أو تحديد الموقع الجغرافي بدقة. من المفترض أن يُباع هذا البرنامج التجسسي رسميا فقط للمنظمات الحكومية لمراقبة الإرهابيين المشتبه بهم أو الجرائم الخطيرة الأخرى. لكن من الناحية العملية ، يتبين أيضا أن الأنظمة الديمقراطية والسلطوية الاستبدادية – على حد سواء - تستخدمه لمراقبة الصحفيين والمعارضين السياسيين ونشطاء حقوق الإنسان. ويتم بشكل افتراضي استبعاد الهواتف في الولايات المتحدة أو المملكة المتحدة أو الصين أو روسيا أو إسرائيل أو إيران من فرص الاستهداف الفرص.

في مايو 2021 ، أكد "أوليفر باركر- فورماور" - أحد مؤسسي حركة غانية تطالب بالمساءلة والحكم الرشيد وظروف معيشية أفضل للغانيين - إن وزارة الأمن القومي تمكنت من مراقبة هاتف أحد أعضائها بشكل غير قانوني. و بدأ تحويل المكالمات الموجهة إلى هاتفه إلى رقم غير معروف بعد أن التقى قادة الحركة بمسؤولي الأمن القومي في مايو 2021.لكن مسؤولو الحكومة الغانية اعتبروها مجرد مزاعم لا أساس لها من الصحة" وأنكروا أي مراقبة غير القانونية.

ومع ذلك ، بعد مرور ستة أشهر فقط ، كشفت مجموعة الصحفيين

الاستقصائيين - Forbidden Stories - أن هواتف المواطنين الغانيين تخضع بالفعل للمراقبة بشكل غير قانوني. وغانا هي واحدة من 26 دولة حيث تم استخدام نظام "بيغاسوس" الإسرائيلي للمراقبة الإلكترونية ، للتجسس على الاتصالات الخاصة للأفراد.

إذ يمكن لـ "بيغاسوس" الوصول إلى الاتصالات المشفرة من أي هاتف ذكي ، وتحويلها إلى أداة تجسس. علما لا يمكن بيع برنامج التجسس هذا إلا بإذن من الحكومة الإسرائيلية ، وفقط للحكومات ووكالاتها. وقد أبلغت شركة - Apple - المستهدفين في غانا أن أجهزتهم عرضة للهجوم من قبل الأشخاص الذين يتصرفون نيابة عن الدولة. صدم هذا الكشف غانا ، التي غالبًا ما قدمت على أنها ديمقراطية نموذجية في إفريقيا. يقف الاستقرار السياسي لهذا البلد الواقع في غرب إفريقيا وحكمه "الديمقراطي" في تناقض صارخ مع العديد من الدول الأخرى في هذه المنطقة التي تتميز بالاستبداد والصراع العنيف على السلطة.

في ديسمبر 2015 ، وقعت شركة-Infralocks Development) – limit-ed (IDL - عقدًا بقيمة 5.5 مليون دولار مع مجموعة NSO – -الإسرائيلية لشراء "بيغاسوس ."وكان على شركة - IDL - بعد ذلك إعادة بيع البرنامج إلى هيئة تنظيم الاتصالات في غانا - الهيئة الوطنية للاتصالات - (NCA) مقابل 8 ملايين دولار. وعلى الرغم من أوجه القصور الخطيرة هذه ، وصل موظفو -NSO -إلى غانا في يونيو 2016 - بعد ستة أشهر فقط من توقيع العقود - لتثبيت "بيغاسوس "وتدريب المسؤولين المحليين على استخدام المعدات. وعلى الرغم من إدراج - NCA – بصفة المشتري وليس ، تم تثبيت النظام في شقة مستشار الأمن القومي الغاني. في الواقع ، كانت وزارة الأمن القومي هي التي أرادت تكنولوجيا التجسس وليس الهيئة الوطنية للاتصالات. أدى ذلك إلى تكهنات

بأن الحكومة ، التي كان يقودها آنذاك المؤتمر الوطني الديمقراطي (NDC)، كانت تخطط لاستخدام "بيغاسوس" للتجسس على شخصيات المعارضة قبل انتخابات ديسمبر 2016.

في مايو 2020 ، قضت محكمة العدل العليا في "أكرا" بأن شراء "بيغاسوس" كان غير قانوني وغير مصرح به. وأدين اثنان من مسؤولي المجلس الوطني التأسيسي ومستشار الأمن القومي في ذلك الوقت بالفساد. وبذلك طفح إلى السطح – وبقوة -بشأن ما إذا كانت غانا تمتلك البرنامج أم لا، لكن السلطات واصلت إصرارها على أن برنامج التجسس لم يكن يعمل .

رفض كل من شارك في التحقيق الجنائي الرد على وسائل الإعلام. وظلت الأسئلة الموجهة إلى مركز الدفاع الوطني ووزارة الأمن القومي دون إجابة. يفسر هذا الصمت من قبل القادة السياسيين الغانيين حقيقة أن حزب مؤتمر الحوار الوطني - الذي كان الحاكم عندما تم شراء "بيغاسوس" بشكل غير قانوني في 2016 - والحزب الحاكم الحالي ، الحزب الوطني الجديد (NPP) ، المتهم اليوم باستخدام برامج التجسس ، كلاهما لديه مصلحة في التستر على القضية. لا يريد أي منهما تحريك الأمور، وكان التواطؤ بالصمت المطبق. والتزمت السلطات الإسرائيلية أيضا الصمت. كأن الحكومة ووزارتي الدفاع والخارجية في إسرائيل ساندت الصمت الغاني.

كيف لا وأن السلاح و برامج التجسس تعتبر عملة صرف داخل الاتحاد الافريقي؟

إن البيع المريب لبرامج التجسس "بيغاسوس" في "غانا" ليس حالة منعزلة لشركة إسرائيلية تمارس نشاطًا مشبوهًا في إفريقيا. إذ أن صناعة الأسلحة الإلكترونية والمراقبة الإسرائيلية ترتبط ارتباطًا وثيقًا بدبلوماسية تل أبيب وأجندة التطبيع الخارجية. إن برامج التجسس هي عملة دبلوماسية ثمينة لإسرائيل ، التي تسعى إلى تطبيع العلاقات ومواجهة حملة المقاطعة العالمية جراء د احتلالها لفلسطين ، ووصف ممارساتها بسياسة الفصل العنصري، كما كان الحال في إفريقيا الجنوبية.

ربما لعبت برامج التجسس أيضًا دورًا في حصول إسرائيل على صفة مراقب لدى الاتحاد الأفريقي ، وهو منصب كانت تطمح إليه منذ ما يقرب من عقدين من الزمن. في يوليو 2021 ، في خطوة مثيرة للجدل قسمت الاتحاد الأفريقي ، حققت إسرائيل هدفها وحصلت على اعتماد من رئيس مفوضية الاتحاد الأفريقي موسى فقي محمد.

وكشفت مصادر حاضرة في قمة رؤساء دول الاتحاد الأفريقي المنعقدة في العاصمة الإثيوبية ، أديس أبابا ، في فبراير 2022 ، أن دبلوماسيين إسرائيليين عرضوا مساعدة عسكرية وفي مجال المراقبة والمعلومات على بعض القادة الأفارقة مقابل دعمهم لاعتماد إسرائيل كعضو مراقب (ومنهم الرئيس الغاني).

غانا ، كانت واحدة من أقوى مؤيدي إسرائيل في الاتحاد الأفريقي وضغطت بشدة من أجل منح إسرائيل صفة مراقب. فهل استخدمت إسرائيل برامج التجسس كورقة مساومة مع غانا في الضغط من أجل الحصول على صفة مراقب من الاتحاد الأفريقي؟ وقد هذا التساؤل مطرحا بقوة في صفوف الصحفيين والحقوقيين ونشطاء المجتمع المدني في ساحل العاج ورواندا والمغرب وتوغو ، وكذلك كينيا وغينيا الاستوائية ومصر

والكاميرون وأوغندا وإثيوبيا ، إذ تم استخدام برامج التجسس الإسرائيلية في هذه البلدان المختلفة. وهناك تساؤل آخر على يقل أهمية، وهو هل التقارب بين هذه الدول والكيان الصهيوني ساهم في تعزيز أنظمة الاستبداد؟

يبدو أن سعي إسرائيل لنوع من "الشرعية" في إفريقيا عبر انتهى الأمر أدوات التجسس القوية -التي تم تطويرها لاستدامة وتكريس احتلال فلسطين واختبارها ميدانيا على الفلسطينيين – أضحت اليوم في أيدي جيل جديد من القادة الاستبداديين في إفريقيا. وتعتبر هذه التقنيات "مثالية"، إذ هي غير مكلفة نسبيا وسهلة التنفيذ ويمكن نشرها مع انعكاسات ضئيلة على الأنظمة التي تستخدمها.

ويعتبر المغرب أحد عملاء شركة NSO الإسرائيلية. استخدم "بيغاسوس" لاستهداف ما الكثير من الهاتف ، بما في ذلك عز الدين العثماني والصحفي عمر الراضي .

وتستخدم إسرائيل الوسطاء والقنوات الثانوية لتصريف أسلحتها التجسسية الخبيثة مقابل تحقيق اختراقات ومصالح أنية واستراتيجية.

لعقود من الزمان ، استثمرت إسرائيل رسميًا القليل جدًا في دبلوماسيتها الرسمية في القارة السوداء. إنها فضلت أن تعتمد على رجال الأعمال والوسطاء الذين يستخدمون قربهم من صناع القرار وعلاقاتهم بهم لخدمة مصالح السياسة الخارجية لإسرائيل ، والحفاظ على علاقات إسرائيل مع القادة الأفارقة. إنه شكل من أشكال "الدبلوماسية الموازية" التي تزدهر في القارة وهي خالية تماما من الشفافية وتعمل في الخفاء من حيث لا يدري أحد .

توافق وزارة الدفاع الإسرائيلية على مبيعات "بيغاسوس" وتلعب دورًا حاسمًا في توزيعها واستخدامها. فالحكومة الإسرائيلية تدرك جيدا الفوائد الدبلوماسية لتصدير برامج التجسس وترفض حظر بيعها على الرغم من "التاريخ الأسود" والموثق لبرامج التجسس. بل وهناك تحقيقات إسرائيلية جارية بخصوص استخدام برامج التجسس ضد المواطنين الإسرائيليين أنفسهم.

تقع برامج التجسس في قلب الطموحات السياسية الإسرائيلية في إفريقيا. لقد منحت لتل أبيب فرصة القبول في القارة حيث كانت غير مقبولة و مهمشة دبلوماسياً. بينما تصدر إسرائيل خبرتها في المراقبة مقابل مكاسب دبلوماسية في إفريقيا ، فهي تقوي الديكتاتوريات والأنظمة الاستبدادية وتضعف الديمقراطية في إفريقيا.

الهجمات الإلكترونية: 2021

الأخطار والخشية

تصاعدت الهجمات الإلكترونية في على امتداد سنة 2021، إن على صعيد شدتها أو خطورتها. وقد أدت جائحة كوفيد -19 واعتماد العمل عن بعد إلى تفاقم الوضع أكثر.

أبلغت - Orange CyberDefence - عن زيادة بنسبة 13٪ في عدد الهجمات الإلكترونية في جميع أنحاء العالم خلال سنة 2021. وباستخدام تقنيات متطورة للغاية وغير مسبوقة، لم يتردد المتسللون في مهاجمة الدول والمنظمات الحكومية والشركات والأفراد في مختلف المجالات.

أظهر استطلاع بعنوان " حالة برامج الفدية لعام 2021 - استبيان وتقرير" ، الذي أجرته شركة الأمن السيبراني ThycoticCentrify ، أن 64٪ من المستجيبين اعترفوا بأنهم كانوا ضحايا هجوم برمجيات الفدية خلال عام 2021. أرقام أخرى مثيرة للقلق: 83٪ من الشركات تعرضت للهجوم، و كان عليهم دفع فدية لاستعادة بياناتهم.

ومن جهتها ، نشرت الوكالة الوطنية لأمن أنظمة المعلومات (Anssi) أيضًا "بانوراما تهديد الكمبيوتر" والتي أفادت بـوقوع 1082 اقتحامًا مثبتًا لأنظمة المعلومات في 2021 ، مقابل 786 في 2020 (زيادة بنسبة 37٪).

وفي تقريرها لحصيلة سنة 2021 أكدت شركة التأمين اليابانية - Tokio Marine International- أن الجرائم الإلكترونية تسببت في أضرار بقيمة 600 مليون دولار أمريكي.

وقد أجمع الخبراء على تصاعد الجرائم السيبرانية عرفت تصاعدا غير مسبوق سنة 2021 . وفقًا لشركة - Software Check Point - المتخصصة في أمن تكنولوجيا المعلومات في كاليفورنيا ، فقد زاد عدد محاولات التسلل بشكل كبير في 2021. وتبلغ هذه الزيادة 68٪ بالنسبة لأوروبا بمتوسط يزيد عن 600 هجوم إلكتروني أسبوعيًا على الشركات. وشهدت أمريكا الشمالية زيادة بنسبة 61٪ في هذا النوع من الهجمات مع حوالي 500 محاولة قرصنة أسبوعيًا. هاتان المنطقتان تتبعهما أمريكا اللاتينية (+ 38٪) ومنطقة آسيا والمحيط الهادئ (+ 25٪) وأفريقيا (+ 13٪).

يختلف متوسط تكلفة الهجوم الإلكتروني حسب حجم الأفعال المقترفة. وتقدر بنحو 7000 يورو بالنسبة للشركات الصغيرة و 300000 يورو بالنسبة للشركات الصغيرة والمتوسطة.

ووصل متوسط مبلغ طلب الفدية حوالي 220.000 يورو. ويضاف إلى هذا المبلغ التكاليف غير المباشرة الأخرى المتعلقة بالإصلاحات وشراء المعدات وتدخل الفرق المختصة وانقطاع النشاط. وغالبًا ما تكون هذه التكاليف الإضافية أعلى من 5 إلى 10 مرات من مبلغ الفدية المطلوبة.

- يناير و مارس2021: سرقة أرقام الضمان الاجتماعي لمواطنين أمريكيين ،
- فبراير: سلسلة من الهجمات التي استهدفت سلسلة التوريد الخاصة

بشركة - Accellion - وخوادم جهاز نقل الملفات الخاص بها ،
- مارس: اختراق البريد الإلكتروني لـ Microsoft - وتأثرت أكثر من 30000 شركة ومؤسسة ، بما في ذلك الهيئة المصرفية الأوروبية ،
- مارس - أكتوبر: عدة هجمات ضد شركة تصنيع الأجهزة - ACER - تم استهداف الشركة من قبل برنامج الفدية في مارس مع طلب فدية بقيمة 50 مليون دولار. وتعرض فرعها الهندي وبنيته التحتية في تايوان للهجوم مرة أخرى في أكتوبر.
- مارس: هجوم متطور للأمن السيبراني وتعطيل خدمات المراسلة لشركة - CNA Financial - إحدى أكبر شركات التأمين في الولايات المتحدة ،
- أبريل: تسرب ضخم للبيانات من LinkedIn و Facebook ،
- مايو: هجوم برمجيات الفدية ضد مجموعة "كولونيال بايبلاين" - Colonial Pipeline ،
- مايو: هجوم على فرع لجماعة "أكسا" - Axa. وسرق مجرمو الإنترنت عدة "تيرابايت" - téraoctets - من البيانات الحساسة. وتقدر الخسائر بـ 5.5 مليار دولار أمريكي ،
- ديسمبر: اقتحام نظام الكمبيوتر للجيش البلجيكي ،
- ديسمبر: هجوم إلكتروني واسع النطاق على حكومة "كيبيك" بكندا.

تعد الجرائم الإلكترونية اليوم من بين أكثر المخاطر التي أضحت الشركات تخشاها. إذ تجد صعوبة متزايدة في العثور على غطاء إلكتروني آمن مناسب ، حتى بأسعار باهظة جدا.

لمواجهة تفريخ وتجدد الهجمات وزيادة المطالبات وتراجع السعة التي تقدمها شركات التأمين ، أصبح سوق التأمين الإلكتروني ضيقًا أكثر مما سبق. وتعمل شركات التأمين تدريجيًا على تقليل تعرضها للمخاطر عبر

تقليص أو استبعاد تمامًا هذا النوع من التأمينات من محفظتها.

وتجدر الإشارة إلى أنه خلال تجديدات يناير 2022 ، سجلت جميع الشركات زيادة كبيرة في أسعار التأمين السيبراني ، لدرجة أن بعض هذه الشركات تشعر بالقلق من أنها لن تكون قادرة على دفع الأقساط المطلوبة والمستحقة مستقبلا.

في المغرب تمكن المتسللون من اختراق قواعد بيانات العديد من شركات الاستيراد والتصدير. في الواقع ، اكتشف قادة الأعمال المعنيين أن أجهزة الكمبيوتر الخاصة بهم وكذلك حساباتهم المهنية قد تم اختراقها من قبل أشخاص لم يتم التعرف على هويتهم. أظهرت التحقيقات الأولية التي أجريت على أجهزة الكمبيوتر التي استهدفتها الهجمات الإلكترونية أن المتسللين استخدموا برمجيات خبيثة مرسلة عبر البريد الإلكتروني إلى الشركات المستهدفة. كان الهدف هو تنزيل برنامج ، مما يسمح للقراصنة بالتحكم في جميع أجهزة الكمبيوتر الخاصة بالشركة الضحية. وأشار الوزير المنتدب في إدارة الدفاع الوطني "عبد اللطيف الوديي" ، إلى أن المديرية العامة لأمن نظم المعلومات (DGSSI) قد أحبطت في عام 2021 ، 577 هجومًا إلكترونيًا استهدفت وزارات ومؤسسات عامة.

وأضاف الوزير أن المديرية المذكورة عملت على تدقيق وتحليل عمليات أمن أنظمة تقنية المعلومات للوزارات والهيئات ذات الطابع الاستراتيجي لتقييم قدرتها على مقاومة الهجمات الإلكترونية. وحسب الوزير، فإن هذه المديرية تتعامل بشكل فعال مع العيوب الفنية، من أجل منع استغلالها خلال الهجمات الإلكترونية التي تستهدف الأنظمة الحيوية وجميع الخدمات المقدمة خارجيًا عبر الإنترنت.

إن الأمن السيبراني، اليوم، ليس فقط أحد الموضوعات الرئيسية للمناقشة

داخل قطاع تكنولوجيا المعلومات. لقد أبدت الشركات والحكومات في جميع أنحاء العالم اهتمامًا كبيرًا، غير مسبوق، بنمو التهديدات السيبرانية.

في البداية كان هناك بعض التشكيك فكرة "استهداف الضحية" ، و اليوم أصبح المزيد والمزيد من الناس يدركون أن الهجمات العشوائية الواسعة الانتشار هي واقع حال مستقر. وتظل الشركات الصغيرة والمتوسطة أكثر عرضة لهذه الأساليب الإجرامية، وذلك لأنها تفتقر عادةً إلى أطر وسائل تكنولوجيا المعلومات لمقاومتها.

وتظهر العديد من الاتجاهات الجديدة ، جنبًا إلى جنب مع التهديدات الجديدة ، ويجد مقدمو "الخدمات المدارة" - (MSP) managed service providers- أنفسهم في موقف يتعين عليهم فيه إما التكيف لسريع الفعال والمجدي أو معاينة أعمالهم معرضة للخطر بشدة.

حسب آخر الأبحاث في هذا المجال (2022)، إن مجرمي الإنترنت في إمكانهم اختراق 93٪ من شبكات المنظمات. وقد نجحت شركة - Positive Technologies – في تجربة فعلية محكمة في اختراق منظومات في العديد من الصناعات الرئيسية ، بما في ذلك التمويل والوقود والطاقة والهيئات الحكومية والشركات الصناعية وحتى شركات تكنولوجيا المعلومات نفسها. و أثبتت هذه التجربة أنه في 93٪ من حالات الاختبار، يمكن للمهاجم اختراق دفاعات شبكة الشركة والوصول إلى الشبكة المحلية.

فما هي التهديدات السيبرانية الرئيسية في 2022 ؟

يتم استغلال البشر دائمًا على أنهم "الحلقة الضعيفة" في خطة الأمن السيبراني. ويظل التصيد الاحتيالي عبر البريد الإلكتروني - (phising) - والتصيد بالرمح - (spear-phishing) - والهندسة الاجتماعية - social

engineering- أكثر الطرق شيوعًا وموثوقية للوصول إلى الشبكة بشكل غير قانوني. وصلت أكثر من 12 مليون رسالة بريد إلكتروني للتصيد الاحتيالي والهندسة الاجتماعية إلى صناديق بريد أكثر من 17000 مؤسسة أمريكية في سنة 2021 وحدها. بالإضافة إلى ذلك ، 85٪ من الخروقات تتم بواسطة شخص من الداخل ، و 61٪ من الانتهاكات تتضمن كلمات مرور ضعيفة أو بيانات اعتماد مخترقة.

إن الهندسة الاجتماعية والتصيد الاحتيالي، هما أكثر الطرق استخدامًا. حتى في حالة وجود البرامج والأجهزة والتصحيحات المناسبة ، يظل العنصر البشري نقطة ضعف. كما نعلم جميعًا ، أصبح ناقل الهجوم الفردي هذا أكثر قابلية للتطبيق بعد الجائحة حيث تحولت العديد من الشركات إلى أساليب العمل عن بُعد واندفعت إلى عملية التحول الرقمي من أجل البقاء. وأظهرت العديد من الدراسات أن مخاطر الإنترنت تزداد مع زيادة العمل عن بعد.

بالإضافة إلى ذلك ، كشفت تقارير عديدة أن:
- 70٪ من العاملين في المكاتب يستخدمون أجهزة العمل للأشياء الشخصية،
- يستخدم 37٪ من العاملين في المكاتب حواسيبهم الشخصية للوصول إلى تطبيقات العمل
- كان من الممكن منع 57٪ من خروقات البيانات عن طريق تثبيت "تصحيح متاح" - one patch available –

لا تزال برامج الفدية تشكل تهديدًا قائما. وبلغت الأضرار الناجمة عنها، على مستوى العالم، أكثر من 20 مليار دولار في 2021. ومن المتوقع أن يصل هذا الرقم إلى أكثر من 265 مليار دولار بحلول عام 2031.
إن 37٪ من الشركات والمؤسسات تأثرت ببرامج الفدية في العام الماضي.

ومن المتوقع أيضًا أن يزداد هذا الرقم عامًا بعد عام. كما أن التعافي من الهجوم من هذا القبيل يستوجب تكلفة عالية ؛ خسرت الشركات الكبيرة في المتوسط 1.85 مليون دولار في عام 2021. وحتى في حالة دفع الفدية لا تستعيد الضحية إلا على 65٪ فقط من بياناتهم كما أقرت بهذا أغلب الأبحاث والدراسات، وفقط 57٪ من هجمات برامج الفدية تم تخفيفها بنجاح من خلال استعادة النسخ الاحتياطية.

وأضحى من الأكيد ظهور استخدامات احتيالية جديدة لتقنيات المعلومات. ويبدو أن سنة 2022 قاتمة بشكل خاص من حيث الاستخدامات الاحتيالية الجديدة لتقنيات المعلومات. وتم الإعلان عن ستة اتجاهات جديدة بواسطة شركة Norton ، ناشر برامج الأمان. على سبيل المثال ، سيستغل المتسللون عواقب الكوارث الطبيعية لاسترداد الأضرار من خلال الهويات المسروقة أو للاحتيال المباشر على الضحايا الحقيقيين.

وباستخدام الذكاء الاصطناعي والتعلم الآلي ، سيبتكر المتسللون "تزويرًا عميقًا" فعالاً حتى لو كان لا يزال من الصعب تحقيق ذلك. مثلا ستتمكن مقاطع الفيديو التي تحاكي أشخاصًا حقيقيين من الاتصال بحسابات شخصية محمية من خلال التعرف على الوجه. ومع توفر جميع البيانات الآن ، سيقوم هؤلاء المتسللون أنفسهم بإنشاء ملفات تعريف نموذجية للضحايا من أجل تحديد الأشخاص الذين من المرجح أن يستسلموا لأنواع معينة من الهجمات أو الاحتيال.

ستستمر أنشطة القرصنة الإلكترونية والإرهاب السيبراني ، بل ستتكثف أكثر لتنفيذ عمليات الاحتيال و أيضًا للتأثير على الرأي العام. وعلى الرغم من اللوائح الجديدة مثل اللائحة العامة لحماية البيانات ، فإن تتبع المستهلكين على الإنترنت عبر ملفات تعريف الارتباط المتطفلة سيستمر ، كما يحذر Norton. ومع إضفاء الطابع الديمقراطي على "العملات

المشفرة" - crypto currencies - سيكون المستثمرون الجدد الذين يفتقرون إلى الخبرة أهدافًا سهلة للمحتالين "الإلكترونيين" المتربصين بهم.