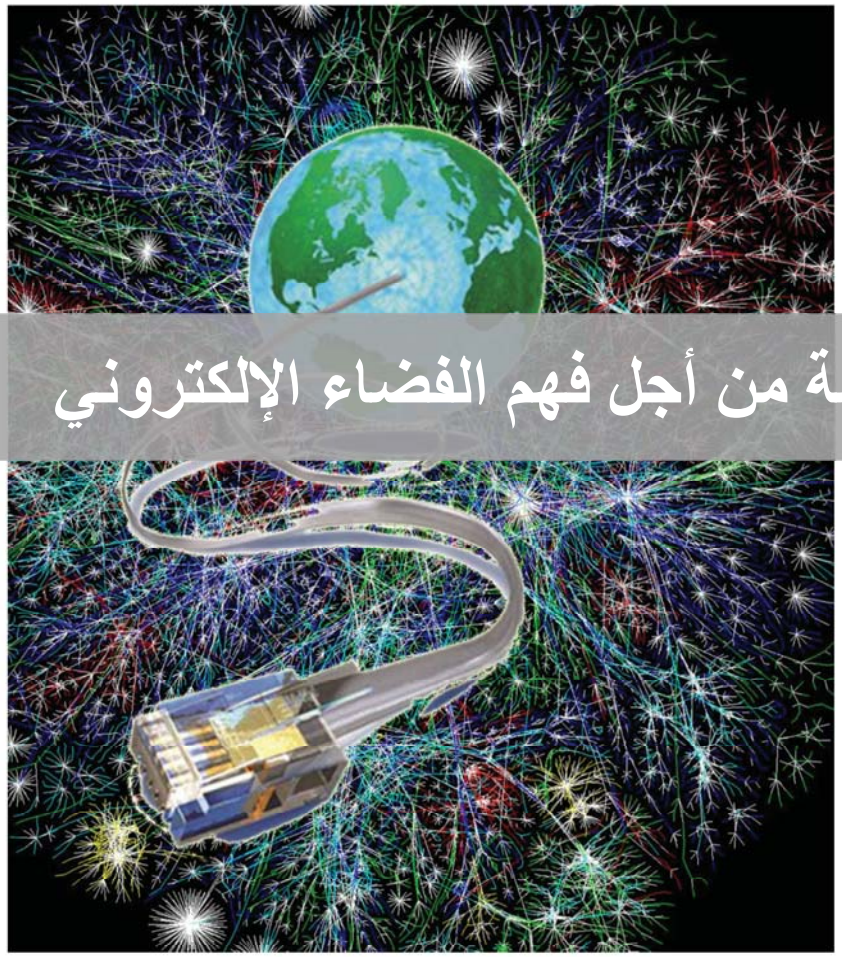
Zentrum für Kurdische Studien .e.V

المركز الكردي للدراسات

NLK

Navenda Lêkolînan ya Kurdî

2015



الجيوسياسة من أجل فهم الفضاء الإلكتروني

ترجمة: د. صلاح نيّوف | الكاتب: فريدريك دوزيت

الجيوسياسة من أجل فهم الفضاء الإلكتروني

الكاتب: فريدريك دوزيت[1]

ترجمة: د. صلاح نيّوف

أعلنت مجلة "هيرودوت" اللون، ومنذ عام 1997، في مقال بعنوان " الأنترنيت يحوّل العالم لجغرافية سياسية":" إن الإنترنيت، وبدلا من أن يؤجل الصراعات الجيوسياسية، يبدو أنه على العكس من ذلك ضاعفها وجعلها أكثر تعقيدا" [دوزيت، 1997]. وعلى العكس من الأصوات المتفائلة التي أعلنت لا أكثر ولا أقل عن نهاية الجغرافية، كنا قد أشرنا بشكل مسبق إلى التحديات الجيوسياسية للتوسع الذي لا يقاوم لنظم المعلومات والاتصال عبر العالم:

" إن شبكة الإنترنيت هي نفسها رهان وتحد للعديد من الصراعات الجيوسياسية التي أدت إلى استراتيجيات من الهيمنة من قبل أمم على مختلف المصالح المتعارضة التي تبحث للسيطرة على محتوى هذه الشبكة، وظيفتها وسيرها ونموها الاقتصادي. هذه الشبكة هي سلاح استراتيجي بشكل كبير بالنسبة لأمن الأمم [...] وهي بشكل خاص أداة قوية في التنافس على السلطة بين المجموعات، الأقليات، القوى السياسية، الدينية، الاقتصادية، على المستوى المحلي كما على المستوى العالمي".

إذا كان الشك مازال مسموحا بذلك، فإن ما كشف عنه إدوارد سنودن حول برامج المراقبة الضخمة "لوكالة الأمن القومي" في الولايات المتحدة بيّن إلى أية نقطة كم الجغرافية هي بحالة جيدة وأن الجيوسياسة تحتفظ بموقعها من أجل فهم الصراعات في العالم الحديث. من جهة أخرى، هذه هي الحجة أو البرهان الذي قدمه " جيمس لويس"، الباحث في [مركز الدراسات الاستراتيجية والدولية][2]، حيث يبيّن أن تأثير هذا الكشف على المفاوضات العالمية يختلف وفق البلدان ولكن، وبشكل عام، ورغم الثورة الرقمية، فإن المصالح والأهداف الاستراتيجية للدول تبقى غير متغيرة حتى هذه اللحظة.

تكشف خرائط المراقبة التي قدمها "لويس بيتينود"[3] عن معنى الحدود السياسية، حتى في الوقت الذي تعبر فيه التكنولوجيا هذه الحدود. مع ذلك، في بدايات سنوات التسعينات، حمل النمو الهائل للاتصالات المتحررة من مخاوف المكان والزمان وعدا بديمقراطية وسلمية للعالم من خلال انتشار الأفكار والقيم الديمقراطية. لقد شكّل ظهور فضاء إلكتروني ناتج عن الاتصالات المتبادلة للشبكات مجيء أو قدوم " قرية كونية"، وذلك على صورة الحلم الذي صاغه " مارشال ماكلوهن" قبل هذا المجيء بثلاثين عاما [ماكلوهن 1964]. لقد أثار توسع شبكات الاتصال وبشكل دائم مثالية وطوباوية عالم أفضل [موسو، 2003، ماتيلارت، 2009]، لكن الإنترنيت أحدث تحديات أكثر مما أحدث وعودا.

إن النمو الاستثنائي للأنترنيت ثورن [من ثورة] أشكال ونماذج الحياة، أحدث انقلابا في اقتصادنا، ضاعف وسائل تواصلنا وفتح أفقا نحن قد بدأنا في مجرد اكتشافها. أيضا، سبّب هذا النمو بتوترات إقليمية واضحة، مع تخصيب للصرعات بين فاعلين متعددين فيما يتعلق بالسيطرة على هذا النمو وتنظيمه. تتبلور التوترات حول صعود تهديدات جديدة مرتبطة بجرائم الأنترنيت أو باستخدام شبكات

---

[1]- بروفسور في المعهد الفرنسي للجيوسياسة، جامعة باريس الثامنة.

[2]- مقره في واشنطن، وتم تصنيفه للعام الثالث على التوالي كأول مركز بحث في هذه القضايا " الدفاع والأمن القومي".

[3]- طالب ماجستير في المعهد الفرنسي للجيوسياسة، جامعة باريس الثامن.

معلوماتية ضمن نطاق الصراعات السياسية، ومعارك عسكرية، في حروب اقتصادية، استخباراتية أو في سياسة الهيمنة الدبلوماسية والثقافية. في زمن [Big Data]، أي مجموعة من البيانات ذات الحجم الهائل، و [Open Data]، أي وضع البيانات بين أيدي العامة، هناك تضاعف للحوارات والنقاشات حول تحديات ورهان احترام الحياة الخاصة، حماية حرية التعبير وحريات فردية أخرى. إن قضية سنودن تلامس كل هذه التحديات في نفس الوقت، لأنه في الفضاء الإلكتروني، كما نراه، هي مسائل لا يمكن فصلها.

خلال زمن طويل، ظلت هذه المسائل بين أيدي جماعة صغيرة من الخبراء في الثقافة العلمية والتقنية. لكنها تدخل اليوم بقوة محطمة إلى داخل الفضاء العام، لأنه ومع التطور الهائل للأنترنيت (حوالي ثلاث مليارات مستخدم) وحضوره الكلي في حياتنا اليومية، فإن الكثير من هذه القرارات التقنية أصبحت سياسية واستراتيجية. عدد من الفاعلين (أفراد، مجموعات...) عرفوا الاستفادة والمصلحة من نمو شبكات مع تفاعل وإبداع مذهل أحيانا، في أسوأ الحالات وفي أحسنها. الحكومات، العسكريون، الشركات، المواطنون، هم جميعهم يحتاجون، من الآن فصاعدا، فهماً أفضل لهذه التحديات وذلك من أجل السهر على مصالحهم وتطوير استراتيجيات متماسكة بهدف متابعة واللحاق بالفرص الجديدة وإدارة المخاطر المرتبطة بها.
في الواقع هذا هو حال الدول الآن، حيث أن سلطاتها السيادية في حالة تحدٍ من قبل فاعلين متعددين في الفضاء الإلكتروني، إن كان ذلك من قبل مجرمين، هاكرز، ناشطين، شركات خاصة كبرى، منشقين، أو فاعلين ليسوا من داخل الدولة وينتمون لدول أخرى. هذه التحديات أمام السلطة والقوة هي خارج الأقاليم التقليدية للجيوسياسة، ومع ذلك، فإن الجيوسياسة هي أداة ضرورية لتحليلها.

الجيوسياسة إلى غزو الفضاء الإلكتروني

كيف يمكن للجيوسياسة أن تسمح بفهم صراعات الفضاء الإلكتروني؟ إن التحدي المنهجي مهم أكثر مما هو محفز. تدرس الجيوسياسة /الجيوبوليتك النزاعات على السلطة والتأثير والهيمنة على إقليم معين، وذلك على مستويات متعددة من التحليل. تهتم بديناميكيات صراع ما على إقليم محدد، وبالتصورات المتناقضة واستراتيجيات الفاعلين من أجل السيطرة والهيمنة عليه، والدفاع عن مصالحها داخل هذا الإقليم. إذن، الإقليم هو في قلب التحليل، وهذا ما يطرح مشكلة واضحة أمام الفضاء الإلكتروني. فهل الفضاء الإلكتروني هو شكل جديد من الإقليم؟ وإذا كان الجواب بنعم، ماذا ستكون حدود هذا الإقليم؟ وماذا ستكون حدوده السيادية؟

مرة أخرى، لا بد من فهم دلالة ما نسمعه من مصطلح الفضاء الإلكتروني. لا يوجد له تعريف موضوعي وتوافقي، هناك عدة تعاريف له، أكثر أو أقل دقة، والتي تعكس اهتمامات وانشغالات ومصالح الفاعلين. يستخدم الروس، كما الصينيون، مصطلح الفضاء الإلكتروني بشكل قليل ـ والذي يمكنه أن يشير إلى فكرة فضاء خارج فضاء الدولة وعابر للحدود ـ ويفضلون الحديث عن الأنترنيت أو أمن المعلومات، ناقلين الحديث إلى حقل اختصاصات الدول. ضمن الإطار التعليمي، يمكننا أن نقترح تعريفا بالحد الأدنى. الفضاء الإلكتروني، هو في نفس الوقت، الأنترنيت[4] و "الفضاء" الذي يقوم بتوليده: فضاء غير مدرَك يحدث في داخله عمليات تبادل لا إقليمية بين مواطنين من كل الأمم، في سرعة متزامنة والتي تلغي كل مفهوم للمسافة. إذا كان تعريف الأنترنيت هو تعريف تقني ومتفق عليه ـ تربط شبكة المعلومات الدولية أكثر من أربعين ألف شبكة مستقلة، مستخدمة نفس اللغة ـ، فإن تصنيف الفضاء الذي

[4]ـ أو بتعبير أدق التواصل البيني العالمي لمعدات المعالجة الآلية للبيانات الرقمية، وذلك وفق تعريف "الوكالة الوطنية لأمن نظم المعلومات، 2011. إن نظم المعلومات والاتصالات لا تقتصر على شبكة الأنترنيت، بل الأنترنيت هو الذي أعطى الولادة لما نتصوره اليوم كفضاء إلكتروني.

يولد عنه هو موضوع لتصورات متعارضة، تتم تغذيتها بصور قادمة من أدب الخيال العلمي، من النشاط النضالي، من السياسة أو من التسويق. إن "كلود" Cloud الشهير لم يفعل سوى إضافة ضبابية على الدلالة semantics.

هندسة في طبقات

من أجل فهم أفضل، نستحضر أحيانا بنية الفضاء الإلكتروني كطبقات متموضعة فوق بعضها، والتي تسمح بتفكيك هذا الفضاء حيث مختلف الطبقات يمكنها أن تتفاعل فيما بينها. وفق العديد من الكتّاب، يمكننا تفكيكها إلى ثلاث، أربع، خمس، لا بل سبع طبقات. نجد، وفي كل الطوابق من هذه البنية، نزاعات على السلطة بين الفاعلين حول مسائل هي في الغالب تقنية، حيث التحديات، مع ذلك، هي جيوسياسية، كما سنرى ذلك.

من أجل التبسيط، نقدّم هنا أربع طبقات. الطبقة الأولى هي فيزيائية/مادية. تتألف من كوابل تحت البحر والبر، عمود فقري حقيقي للأنترنيت (backbone)، من محطات وصل إلكترونية، من كومبيوترات، إنها تشكل البنية التحتية الفيزيائية/المادية للأنترنيت: مجموعة من الأدوات المجهزة فوق الإقليم، خاضعة لقيود الجغرافية الفيزيائية والسياسية، والتي يمكن أن نبنيها، نغيرها أو ندمرها، متصلة أو غير متصلة بالشبكة. يبيّن المقال الذي كتبه "جيرمي روبين وكافي سلامتيان" أهمية التحديات الاستراتيجية لهذه البنية التحتية، والتي، لأنه يمكن تحديدها جغرافيا، هي أقل صعوبة في تحويلها إلى خرائط من محاولة تحويلها لعلاقة بين الفضاء الإلكتروني والفضاء الإنساني " cyber géographie". يحلل "كيفين ليمونييه" التطور الاستراتيجي للبنية التحتية الروسية، والتصورات الكامنة فيه. لقد تمّ فهم وإدراك البنية التحتية الفيزيائية/المادية ضمن عقلية منفتحة وانتشار في حده الأقصى للمعلومات، من غير أي محاولة أمنية مدرجة فيها. واحد من الآباء المؤسسين للأنترنيت، " لويس بوزان"، يعتبر، حتى من أجل أمن الأنترنيت، أنه لا بد من إعادة بنائه رأسا على عقب[5].

الطبقة الثانية هي البنية التحتية المنطقية. تضم كل الخدمات التي تمكّن من ضمان تحول البيانات بين نقطتين من الشبكة و، إذن، العمل على سفر المعلومة، مجزأة في حزم صغيرة من البيانات، من المرسِل إلى المستقبِل. ترتكز الهندسة المنطقية على تناغم جوهري، لغة مشتركة تمكّن جميع الكومبيوترات في العالم من التواصل فيما بينها، وهي ما نسيميها بروتوكول الأنترنيت (TCP/IP). هذه الخدمات هي التوجيه (اختيار الطريق الذي تسافر من خلاله حزمة من البيانات بين الشبكات)، وهي التسمية (أي أسماء تحدد عناصر الشبكة أو المستخدمين) وهي أيضا المعالجة أو العنونة (والتي تحوّل سلسلة من الأرقام التي تشكل العناوين في كلمات واضحة بالنسبة للمستخدمين).

العديد من الجوانب يمكن أن تحدد جغرافياً مع وجود بعض التحديات التقنية (المسارات التي يتم سلوكها، أسماء مجالات الأنترنيت، عناوين IP ...). تأخذ المقابلة مع "برتراند دو لا شابيل" في الاعتبار الحوارات والمطالبات المتعلقة بالعنونة أو المعالجة، وذلك بسبب الرقابة الرمزية القوية التي مازالت تمارسها الولايات المتحدة من خلال سلطة القرار بيد وزارة التجارة الأمريكية. أيضا، تبيّن " دومنيك لاكروا" التحدي الاقتصادي والسياسي أمام الحصول على أسماء المجالات أو النطاقات على الأنترنيت Domain.

[5]- ن. مادلين، " لويس بوزان: " يجب إعادة بناء الأنترنيت رأسا على عقب"، الأيكو، عدد 21442، 24 أيار ،2013، الصفحة 23

الطبقة الثالثة وهي مركبة من تطبيقات، وهي بدورها عبارة عن برامج معلوماتية سهلة الاستخدام وتمكّن من استخدام الأنترنيت من غير معرفة أي شيء عن البرمجة المعلوماتية (Web، e-mail، شبكات اجتماعية، محركات بحث، الخ.). بيّنت قضية سنودن تحدي النجاح الكوني للتطبيقات التي تتبعها بعض الشركات الكبرى (غوغل، فيسبوك، أمازون...)، هذه الشركات التي يثق بها المستخدمون ويقدمون لها بياناتهم الشخصية، والتي تستخدم بإبداع من قبل فرق التسويق أو أجهزة الاستخبارات في البلاد، وهذا ما يعتبره "ستيفان فرينوت" بالذهب الأسود الجديد للاقتصاد. لا تتبخر البيانات بين الغيوم (le Cloud...) بل تم تخزينها على مخدمات تدار من قبل الفاعلين الخاصين أو العموميين.

أخيرا، الطبقة الرابعة وهي المعلومة والتفاعل الاجتماعي، ونسيمهما أحيانا المعرفية والدلالية. إنها المستخدمون، والمحادثات والتبادلات التي تجري في وقت حقيقي عبر العالم، والأكثر صعوبة هنا هو الإحاطة بها وتقديمها من وجهة نظر جغرافية. ولكن هذا لا ينطبق على وجهة النظر الجيوسياسية، عندما نصل إلى تحديد من هي البلدان الأكثر "صداقة" على الفيسبوك، حيث تتوفر المحتويات في عدة لغات وفي أقاليم متعددة على سطح الكوكب، حيث تنطلق الانتفاضات على الشبكات الاجتماعية أو الحملات ضد حكومة أو مؤسسة...

إن الفضاء الإلكتروني هو كل ذلك في نفس الوقت، مجموعة من الشبكات المتصلة فيما بينها عبر الكومبيوترات ـ وأكثر فأكثر عبر أشياء متحركة (تلفونات، كومبيوترات محمولة، أحذية رياضية، سلاسل أو أطواق على المعصم...) ـ، أو شبكات إنسانية، تدفق في البيانات، وهو أيضا فضاء من المعلومة والتبادل الذي ليس له حدودا إقليمية، من المعقد الإمساك به، مركب من خلال بنية تحتية مادية مجهزة فوق إقليم فيزيائي، لا بل في فضاء أكثر من خارجي بالنسبة للأقمار الصناعية. إن مصطلح الفضاء الإلكتروني، حسب من يستخدمه ولماذا، يمكن أن يعود إلى بنية تحتية فيزيائية/مادية أو تخيلات مختلفة كليا، وذلك ضمن غموض مفهومي.

تقدم الجيوسياسة أداة ضرورية لفهم الفضاء الإلكتروني: إنها التصورات أو الرموز. التصور هو بناء، طريقة في رؤية الأشياء، تجميع الأفكار بشكل أكثر أو أقل منطقية وتماسكا، والذي لديه وظيفة في الصراعات الجيوسياسية. يستند التصور/الرمز على أفعال موضوعية لكنه يحتفظ وبعمق بطابع ذاتي. التصورات ليست محايدة، لديها تأثير كما تستطيع خدمة استراتيجيات الفاعلين ضمن هدف الإقناع، إقلاق، تحميس أو تجييش الفاعلين (الناخبين، الناشطين، المستثمرين، العسكريين، رواد الأنترنيت...).

"زرع عَلَمه" في الفضاء الإلكتروني

الفضاء الإلكتروني ليس إقليما بالمعنى الجغرافي للمصطلح، ويعرّفه إيف لاكوست:" امتداد تعيش فوقه مجموعة إنسانية تعتبره كملكيتها الجماعية"، [لاكوست 2003]، أو بالنسبة للدول هو " جزء أو قطعة من الفضاء الأرضي المحدد بواسطة حدوده ويمَارِس عليه سلطته واختصاصاته"، [لاكوست 2003]. ولكن يُنظر إليه كفضاء تتفاعل بداخله الكائنات الإنسانية، لا بل كإقليم، كما يوضح " أليكس ديسفورج" في مقاله حول تصورات ورموز الفضاء الإلكتروني.

ظهر مفهوم الفضاء الإلكتروني بشكل متناقض وذلك لسببين متناقضين بشكل جذري. بداية، ظهر تحت ريشة روائي في الخيال العلمي هو " وليام جيبسون"، يصف فضاءً ذا أبعاد ثلاثة " لتعقيد لا نهائي"، وُلِد بشكل إلكتروني، وفي داخله تظهر شخصياته أو تدخل بتواصل عبر الكومبيوتر. أيضا، يقدم مفهوم الفضاء الإلكتروني تصورا عقليا لبيانات ولمعلومة مخزنة في قلب النظم المعلوماتية لكل الإنسانية، والتي ستمتلكها أجيال مستخدمي الأنترنيت.

يدخل هذا التصور في خيال رواد الإنترنيت، والذين أسسوا عام 1990، قبل أن يصبح الأنترنيت عاما بوقت طويل، " مؤسسة الحدود الإلكترونية"، وترجع بشكل مباشر إلى "جبهة الرواد" التي، وفق أطروحة المؤرخ " فريدريك جاكسون تورنر"، صاغت أو شكّلت الديمقراطية الأمريكية. سيذهب "جون بيري بارلو"، كعضو مؤسس، حتى إلى نشر " إعلان استقلال الفضاء الإلكتروني" عام 1996، حيث يؤكد فيه أن الفضاء الإلكتروني يمتلك سيادته الخاصة وأنه داخل "حضارة العقل" هذه، لا تطبق قوانين الحكومات في العالم الذي نعرفه أو الفيزيائي/المادي. يبين "ألكسي ديسفورج" كيف تم استلهام روح [ضد ـ الثقافة] لسنوات الستينات حتى الوصول إلى هندسة الشبكة نفسها، حيث تم إدراكها ضمن عقلية من الانفتاح، الإدارة الذاتية، من حرية التبادل والتعبير. إن الفضاء الإلكتروني هو فضاء لا مركزي، منفصل عن المركز، تم التفكير فيه من أجل أن تستطيع المعلومة الانتشار دائما، مهما كانت الصعوبات. هذه النسمة من الحرية تم حملها من قبل عالَم حيث كل ما يخرج من الروح الإنسانية يمكن أن " يعاد إنتاجه ويوزع بشكل لا نهائي من غير أن يكون له ثمنا"، هذا الفضاء يستمر في تحفيز الناشطين من الهاكرز، الذين يحاربون كل محاولة تعيق الانتشار الحر للمعلومة على الأنترنيت.

بعد أن وقع مصطلح الفضاء الإلكتروني في النسيان لفترات قليلة، عاد وظهر مع عام 2000 في خطابات الدول، كإقليم للغزو، للسيطرة، للمراقبة، وللامتلاك. إقليم يجب أن يتم احترام الحدود في داخله، سيادته، قوانينه، ولا سيما، كتهديد للأمن القومي ومصالح الأمة. لقد شكلت الهجومات على استونيا عام 2007 ردة فعل مثل الصدمة الكهربائية بالنسبة لأعضاء الحكومات، ومنها فرنسا، حيث أخذوا وبشكل فجائي الوعي بحاجتهم للمواجهة والتحضير لهذه التهديدات. لقد شكّل نقل تمثال يمجد النظام السوفييتي إلى "تالين/Tallin" انطلاقة العداءات. تعرضت المواقع الإلكترونية الحكومية، وزارة الدفاع الوطني، وحتى البنوك والخدمات العامة الأخرى، لهجوم ضخم لتحرمها من خدمة (DDOS).

تم اختراق عشرات الآلاف من الكومبيوترات، الروبوتات أيضا، من قبل برنامج استطاع أصحابها ومستخدميها قيادتها عن بعد وغالبا دون معرفة، وتم إغراق متزامن لمخدمات البلاد حتى شللها بشكل كامل (أصبحت الشاشة سوداء)، حارمين السكان من الوصول إلى الخدمات العامة على الأنترنيت وذلك لعدة أيام بالنسبة للكثيرين منهم. أنكرت الحكومة الروسية كل مسؤولية رغم حزمة الأدلة التقنية والسياسية التي تتجه نحو البلاد. في السنة التالية، بيّنت الهجمات الإلكترونية ضد جورجيا كيف تستطيع هذه الهجمات أن تأتي بالاستناد على قوى تقليدية في صراع مسلح. انطلاقا من هنا، عززت العديد من الدول وبشكل جدي قدراتها وبحثت عن زيادة مراقبتها وقوتها في ميدان الفضاء الإلكتروني، ابتداءً من فرنسا.

يؤكد "ستيفان دوسيه"، ضابط في وزارة الدفاع، أنه " يظهر من الضروري بالنسبة للدول أن (تزرع العَلم) في الفضاءات التي تشغلها من أجل ممارسة أعمالها ووظائفها السيادية، ومن أجل احتلال الفضاءات غير المشغولة والتّجهز لمواجهة منافسين في هذا الفضاء" [دوسيه، 2010]. " الكتاب الأبيض" حول الدفاع لعام 2013 واضح جدا، حيث أن الفضاء الإلكتروني هو أولوية استراتيجية والأسلحة السيبرنيتيكية [السيبرنيتيك: هو علم يشير للقدرة على التحكم والقيادة في الآلات والإنسان ووسائل التواصل. توضيح من المترجم]، هي من الآن فصاعدا جزء من هذه الترسانة.

<u>الفضاء الإلكتروني: الدول في هجوم معاكس</u>

قليلة هي الدول التي استبقت التحدي الاستراتيجي الذي يستطيع أن يمثّل، مع الوقت، التوسع الصاعق والتداخل في الاتصال بين نظم المعلوماتية والاتصال. فقط البعض منها مثل روسيا والصين، حيث كان لديهما وعي تاريخ حاد بأهمية المعلوماتية، أو أيضا الولايات المتحدة، وهي في طليعة المتقدمين

تكنولوجيا، فقد كان لديها تفكير استراتيجي بشكل مبكر جدا. للوهلة الأولى، جاء التجديد من خلال أفراد ومجموعات صغيرة مغامرة وجريئة، ذكية وتفاعلية، والتي عرفت الحصول على أفضل جزء من القوة وتوزيع هذه الوسائل الجديدة، وضعيفة التنظيم. لقد كان أفراد وشركات ناشئة مصدر النجاحات الاستثنائية والتي حوّلت بعمق أشكال حياتنا (التمويل الجماعي للمشاريع، أوقات الفراغ، النشاط، التسويق...) وفتحت فرصا ضخمة جدا. لكن الهاكرز، المجرمين، المرتزقة، عرفوا أيضا بشكل جيد متابعة ذلك واستخدام هذه الأدوات بسرعة وفعالية، والذين يسببون اليوم ردة فعل السلطات السياسية والمؤسساتية. يشرح "بروس سشينر" بشكل جيد، وهو خبير بالأمن المعلوماتي، التوتر داخل الفضاء الإلكتروني بين السلطة " الموزَّعة" (ناشطين، منشقين، هاكرز، مجرمين)، والسلطة التقليدية (الحكومات، الشركات الكبرى، المؤسسات)[6].

يبيّن كيف أن الوصول القوي للفضاء الإلكتروني ولامركزية النظام عززت من دور الفاعلين الصغار ـ بما في ذلك من ليس لديهم نيات حسنة ـ، مقدمين لهم قدرات على التنظيم وفعالية جعلوا منها غير قابلة للهزيمة. لكن الفاعلين التقليديين يأخذون اليوم ثأرهم، وذلك مع وسائل وقوة غير متكافئة، لا سيما الموقف الحازم والصلب فيما يتعلق بالتحديات.

باسم الأمن...

تعود الدول بقوة إلى الفضاء الإلكتروني باسم الدفاع عن سلطاتها السيادية. أولا، إن الصعوبات في وقف الهجمات الإلكترونية من شأنه أن يضعف قدرة هذه الدول على ضمان أمن الأمة والدفاع عن الإقليم. يبدو أن القلق والمخاوف تتركز بشكل خاص على حماية البنى التحتية الافتراضية، حيث يمكن لاضطراب الفضاء الإلكتروني أو لتخريبه أن يضع السكان المدنيين في خطر. إن حضور مثل هذه التهديدات يغذي الخطابات الأكثر كارثية، ونقاشات الخبراء حول إمكانية أن هجوما إلكترونيا يستطيع أن يسبب ملايين القتلى، لا بل إسقاط بلد. يتساءل "أوليفييه كيمبف" عن مفهوم الفضاء الإلكتروني، مبينا أن المقاربة بين الإرهاب والفضاء الإلكتروني ليس حقيقيا وأن الخطاب المهيمن يجعلنا نفكر بذلك ويغطي جزئيا ما يمكن أن يكون الإرهاب داخل الفضاء الإلكتروني. يحلل "رودريغو نيتو غوميز" بنية هذا التصور الأمريكي والدور الذي يلعبه التصور في السياسات الأمنية، والتي تمتد حتى تجريم الهاكرز وتشجيع ثقافة السرّية في مجال حيث التجديد والابتكار يحقق القوة فيه.

أبعد من الأعمال الإرهابية، فإن تحدي السيطرة على المعلوماتية هو أمر أساسي. إن القدرة على جمع، تحليل، والتلاعب بالمعلومات يمكنها أن تقدم ميّزة استراتيجية للعدو وتجعله يشك في دقة معلومته الخاصة به. تستطيع الهجومات الإلكترونية إزعاج الاتصالات بشكل مباشر، تشويش العدو وحتى إضعاف قدراته العملاتية التي تعتمد أكثر فأكثر على شبكات من أجل تنظيمها وعملها. لقد أصبحت الاستراتيجيات التقليدية للردع والدفاع تواجه حدودا لها، بسبب صعوبات اللحاق بالهجومات ـ أي القدرة على تحديد وبشكل دقيق من يقف وراء هجوم ما ولماذا، أيضا تواجه مسألة الوصول والنفوذ إلى التكنولوجيا، والتي تتعزز من قوة الجماعات الصغيرة في مواجهة القوى الكبرى. إن البلدان الأكثر اعتمادا على الشبكات هي في نفس الوقت الأكثر عرضة للهجومات، ولكن أيضا الأكثر تطويرا لمقاومة شبكاتها، وبناءً لقدراتها الهجومية وتتبع الفرص الجديدة المعروضة من قبل الشبكات من أجل زيادة قدراتها وقوتها.

[6] -«The battle for power on the Internet: Bruce Schneier at TEDxCambridge 2013»، vidéo publiée le 25 septembre 2013 par TEDxTalks, consultée le 16 février 2013, <www.youtube. Com.

أيضا، تتم الحرب الإيديولوجية على الشبكات الاجتماعية بينما، في ديمقراطياتنا، لا تستطيع الحكومات دائما تجاهل معارضة حيوية من قبل الرأي العام قبل دخولها في صراع مسلح، بالمقابل يقدم الجهاد عدة حقيقية للتطرف السريع على الشبكة والوصفات العملية للإرهاب الفردي، والذي يأخذ أحيانا وباختصار القوى الأكثر قوة.

ثانيا، لقد أصبح الحفاظ على الأمن الداخلي والنظام العام تحدٍ من قبل الجريمة، المنظمة وغيرها، والتي تعمل عبر الشبكات. يمكن القيام بتسلل واختراق غير شرعي داخل النظم، سرقة أو تدمير للبيانات وحتى، بالمعنى الواسع، القيام بأفعال جرمية عبر الشبكات (سرقة بنوك، النصب والاحتيال، سرقة الهوية، الخ.). إن مشكلة الملاحقة تتعمق بسبب تطاير الدليل. وفي غياب تدخل سريع فإن الأدلة يمكنها أن تختفي عن الشاشات. بالتالي، إن إمكانية التدخل عن بعد تعقد عملية التحقيق، القبض على مشتبه به ووضعه قيد التحقيق. تجتاز الجريمة الحدود بسهولة وذلك عن طريق الشبكات، وهذا ما لا ينطبق على قوات حفظ النظام. إذا كان المجرم والضحية يوجدان في نفس البلد فمن السهل على السلطات أن تتصرف بسرعة. عندما يكون المجرم والضحية والأنظمة المستخدمة موجودة في بلدان مختلفة، سيتطلب ذلك إجراءات من التعاون الدولي على مستوى قوات البوليس والقضاء وهم في الغالب بطيئون جدا حتى يأخذ تحركهم فعالية حقيقية.

يوجد حدود للاختصاصات داخل الفضاء الإلكتروني حيث لا يمكن للبوليس أن يتدخل في شبكات أجنبية من غير ترخيص رسمي، حتى ولو كان من أجل إلقاء القبض على مجرم. تقود تحديات الأمن الحكومات إلى مراقبة ناشطة لما يحصل في الفضاء الإلكتروني، مع مخاطر الانحراف أو الضرر في التعامل مع الحريات الفردية كما بينت قضية سنودن. بالنسبة للدول الشمولية، فإن المراقبة والسيطرة على الفضاء الإلكتروني هي أمر جوهري من أجل حماية الأنظمة لأن التهديد الرئيسي يمكنه أن يأتي من الداخل.

إن الانتشار المتنامي للمعلوماتية يمكنه إضعاف الأنظمة الشمولية، لكن الشبكات تشكّل أدوات رائعة من أجل تعقب، تحديد، مراقبة المنشقين أو الخراف المحتملة الحسودة للنظام. يبيّن المقال الذي كتبه "فريدريك دوزيه" عن الصين، كيف عرف النظام، حتى الآن، إثبات إبداعه في التأقلم مع هذه التحديات الجديدة.

تحديات السيادة

تشير المقابلة مع، برتراند دو لا شابيل، مؤسس مشروع "أنترنيت واختصاصات"، إلى أية نقطة أصبحت فيها ممارسة السيادة معقدة بالنسبة للدول، لأن حدود الاختصاصات هي أكثر ضبابية وأكثر تداخلا مع الفضاء الإلكتروني. لقد أصبحت النشاطات عابرة للحدود في الفضاء الإلكتروني، ومن الصعب أحيانا بالنسبة للدولة أن تفرض احترام قوانينها وأنظمتها، حتى على إقليمها ومن قبل مواطنيها، بشكل خاص عندما تكون خدمة الإنترنيت المستخدمة تقدمها شركة أجنبية. إن الذي يشكّل اختصاصا في الفضاء الإلكتروني هو في الغالب منتج التنافس على القوة والتحكم أكثر مما هو تعريف قانوني متفق عليه. إنه صراع متدرج يلامس حماية حرية التعبير، والذي يعرف قيودا في فرنسا غير مقبولة في نظر القانون الأمريكي.

في عام 2012 على سبيل المثال، تم نشر بعض التعليقات المعادية للسامية بالفرنسية على تويتر، وذلك من خلال مسابقة للنكت المقززة تحت كلمة أو عنوان (يهودي جيد)، قاد هذا النشر إلى يدٍ حديدية حقيقية بين القضاء الفرنسي والشركة الأمريكية. احتاجت الإجراءات عشر أشهر حتى قبل تويتر بتسليم البيانات إلى القضاء الفرنسي والتي تمكّن من تحديد هوية من وراء مسابقة النكات. اكتسبت شركات الأنترنيت الشهيرة الكبرى (غوغل، أمازون، فيسبوك، آبل) تلك القوة الاقتصادية والتي تسمح لها بلعب علاقة القوة

ولا تخضع بسهولة كبيرة لقضاء دولة ما تطالب بحذف محتوى أو معلومات يقدمها المستخدمون. إن حماية المستخدمين، في مواجهة أنظمة شمولية، يمكن أن يكون صحيا لكنه يكلّف الشركة الوصول إلى سوق مربح.

أخيرا، إن السيادة الاقتصادية والمالية للدول هي أمام اختبار قاسٍ. حيث تقوم الشبكات بتسريع كبير لانتشار الممتلكات والتدفقات المالية، وهذا يسهّل التهرب الضريبي وانتشار الأزمات المالية العالمية. يبين المقال الذي كتبته "دومنيك لاكروا" تركز الشركات، المرشحة لتكون أسماء مجالات كبيرة على الأنترنيت، في ملاذات ضريبية. يمكن لإعادة تنظيم نشاطات شركة "ياهو" في أوربا حول مجموعة إيرلندية (حيث الضريبة على الشركات تصل إلى 12،5%)[7]، أن يقود إلى تحويل القاعدة الضريبية لمجموعات أو كيانات أوربية للشركة. أيضا، تزيد الشبكات من خطر توسع التجسس الاقتصادي، سرقة الملكية الفكرية والصناعية، أو حتى أسرار الأعمال. يحلل "دانيلو ديليا" هذه الأخطار ويوضح الصراعات الجيوسياسية الكامنة التي تحتويها. ينطلق في توضيحاته من القوة الاقتصادية والمالية للأمم، إلى حد أن مصالح القطاع الخاص تلتحق بمصالح الأمة وأن الأمن الإلكتروني للشركات يمكنه أن يكون من المصلحة القومية. أيضا، ينطلق من أن سوق الفضاء الإلكتروني هو أيضا حسّاس كما هو مزدهر، وهذا يشجع الحكومات بالمقابل على دخوله.

تهديدات جديدة؟

العديد من هذه التهديدات ليس جديدا بل تنتشر في الفضاء الإلكتروني بطريقة أكثر انتشارا، سرعة، قوة وعلى مستوى غير مسبوق. إن كان القصد هو كميات من المعلومات المسروقة من الشركات من قبل الهاكرز الصينيين (وفق تقرير Mandiant)، أو مليون وسبعة مائة ملف نقلها سنودن معه، أو بيانات هائلة جمعتها "ناسا"، أو ثلاثين ألفا من الكومبيوترات التابعة لشركة أرامكو التي تم تخريبها في ضربة واحدة عام 2012، فإن النتائج تصل بسرعة أكثر، بقوة أكبر وهي في بعض الأحيان تتسع بشكل غير مسبوق. بالمقابل، العديد من التحديات هي تحديات خاصة بالفضاء الإلكتروني: صعوبة تحديد وإثبات مصدر الهجوم، صعوبة التوقع أو الاستباق، التحذير أو الإيقاف، تشابك السيادة والاختصاصات، التطور السريع للتكنولوجيا وإعادة صياغة وترتيب دائم للشبكات، والتي تتطلب تأقلما سريعا وثابتا مع التطور في هذا الوسط، إمكانية تطوير أسلحة الفضاء التجريبي، صعوبة اختبار هذه الأسلحة بالحجم الطبيعي، عدم اليقين فيما يتعلق بمضاعفاتها، والتي تعتمد أيضا على قدرة مقاومة الهدف، وأيضا أفضل هجوم يبقى ذاك الذي لم نحدده.

إن الفضاء الإلكتروني معرّف من قبل العديد من البلدان كمجال أو ميدان جديد (أو وسط جديد) عسكري، إلى جانب الأرض، البحر، الجو والفضاء. لكنه بعكس المجالات الأخرى، فهو ليس وسطا طبيعيا ـ كل ما يحصل فيه هو إنتاج للفعل الإنساني ـ وينتقل أو يخترق جميع الميادين والمجالات الأخرى. بالتالي، إن الاستراتيجيات التي يتم تطويرها من قبل الدول من أجل الدفاع عن سلطاتها السيادية والوصول إلى أقصى حد في قواها داخل الفضاء الإلكتروني هي استراتيجيات لديها نتائج جيوسياسية يجب أن تشغلنا. إنها بالمقابل تبين وتضع أمامنا أسئلة جدّية، لا بل تهديدات جديدة.

لماذا نقوم بالجيوسياسة للفضاء الإلكتروني

[7]ـ على سبيل المقارنة، الضريبة على الشركات والتي رأس مالها أقل من 75% من قبل أشخاص فيزيائيين هي 1،33% لمجمل أرباحها.

إن التداعيات التقنية للصراعات في الفضاء الإلكتروني لديها ما يحبط أو ما لا يشجع المواطنين ـ والباحثين في العلوم الإنسانية والاجتماعية ـ، وليس صدفة إذا ظلت هذه الأسئلة ولوقت طويل بين أيدي جماعة صغيرة من الخبراء. لماذا الاهتمام بها رغم كل شيء؟ لأن المقصود هو العالم الذي لدينا رغبة في العيش بداخله. لأنه ولأسباب تتعلق بالحضور الكلي لنظم المعلوماتية والاتصال في حياتنا اليومية، فإن القرارات التي ستتخذ ستؤثر على كل جوانب حياتنا. لأن العديد من السلطات سيتم تطويرها من غير النقاش أو الحوار مع الطرف الآخر/السلطة الأخرى، ومن غير ضمانات، أو من غير عمليات وصيرورات المراقبة الديمقراطية.

إننا في نقطة تحول والكثير من بيننا، بما في ذلك أعداد ممن ننتخبهم، يكتشفون الأدوات، البرامج، السياسات التي تم تطويرها من قبل الشركات الكبرى، الحكومات أو حتى المجرمين، من أجل الدفاع عن مصالحهم وتطوير قوتهم ومكتسباتهم إلى حدها الأقصى في الفضاء الإلكتروني. يبدو أن النماذج أو البراديغمات الاستراتيجية والقواعد القديمة للعبة الدولية لم تعد صالحة أو لا يمكن التأقلم معها، لكن يبقى كتابة القواعد الجديدة. إن سرعة التطورات التكنولوجية تتجاوز بشكل واسع ما يمكن الوصول إليه من وضع توافق دولي، أو إطار قضائي جديد وتبنّي قوانين جديدة. يبدو أن ثقافة السرية وفقدان الثقة بين الشركاء تبطيء من هذه الجهود. نحن على تقاطع طرق، وذاك الذي سوف نتبعه عليه أن يكون لديه التزامات كبيرة من أجل مستقبلنا. هنا يوجد ثلاثة مجالات تستحق أن نعيرها انتباهنا.

السلام والأمن الجماعي

التحدي الأول هو تحدي السلام والأمن الجماعي. تبين العديد من المقالات في عدد مجلتنا هذا إلى أية نقطة يهمن التضخم في تصور التهديد على الحوار. تتصف مقاربة الولايات المتحدة، بشكل خاص، بتصعيد في الخطاب والوسائل، وواحد من محركات هذه المقاربة هي المنافسة مع الصين. يجمع النظام الصيني، ومن خلال استراتيجية واضحة تسعى للتفوق المعلوماتي وبكل الوسائل، القانونية وغير القانونية، المعلومات التكنولوجية، الصناعية، الاقتصادية، السياسية والعسكرية، وهذا ما يحدث قلقا حقيقيا في الولايات المتحدة. تم خلال السنتين الأخيرتين، ومن خلال كتل ضخمة تشبه الانهيار الثلجي، العرض في الصحافة، تصريحات الخبراء، الكونغرس وحتى البيت الأبيض، للأخطار المرتبطة بالفضاء الإلكتروني من أجل ازدهار وأمن الأمة، مع اتهامات أصبحت أكثر فأكثر مباشرة باتجاه الصين. حتى أن مدير الاستخبارات، جيم كلبير، أعلن أمام لجنة من مجلس الشيوخ أن التهديد القادم من الفضاء الإلكتروني أصبح بدرجة قد يكون فيها أكثر أهمية من التهديد الإرهابي بالنسبة للأمة.

على الرغم من القيود الفيدرالية على نطاق واسع، إلا أن ميزانية الدفاع للفضاء الإلكتروني ارتفعت إلى 800 مليون دولار في عام 2013، أما "الوحدة العسكرية لعمليات الفضاء الإلكتروني"[8]، والتي أنشئت في عام 2010، من المتوقع أن ينتقل عدد موظفيها من 900 إلى 4900 في السنوات القادمة. لقد أظهرت قضية سنودن إلى أية حدٍ جمعت الولايات المتحدة معلومات هائلة وبشكل عدواني من خلال الشبكات، مخاطرة بالثقة والتعاون الذي بنته مع أمم أخرى. يقلل "جيمس لويس" من أهمية هذا الكشف عن المعلومات، والذي لم يكن مفاجأة بالنسبة للصين وروسيا، والذي لن يضع المفاوضات الدولية موضع التشكيك بشكل كبير. إن مسألة الشك ماتزال شائكة، بينما العديد من المسؤولين يحبون تكرار القول المأثور بأن " ليس هناك أصدقاء في الفضاء الإلكتروني".

أيضا، ستكون الولايات المتحدة وراء المبادرة التي يعتبرها الكثيرون بأنها العمل الأول من " الحرب الإلكترونية"، وهي هجوم تجريبي، شكل من أشكال الطريق الثالث بين الدبلوماسية القسرية والهجوم

[8] ـ وحدة عسكرية من عمليات الفضاء الإلكتروني ووكالة الأمن القومي.

المسلح. لقد كشف " ديفيد سونجر"، عام 2012 وفي صحيفة نيويورك تايمز، كيف أن فيروس " ستوكسنت" Stuxnet، والذي تم وضعه بالتعاون مع الاستخبارات الإسرائيلية، سيصيب أجهزة الطرد المركزي في المفاعل النووي الإيراني من أجل إبطاء البرنامج النووي. تجعلنا هذه الأسرار والتصريحات الجديدة التي تم الكشف عنها في السنتين الأخيرتين نفكّر بأن السباق إلى الأسلحة داخل الفضاء الإلكتروني قد بدأ. ركزت العديد من البلدان في الآونة الأخيرة على تطوير دفاعاتها وقدراتها داخل الفضاء الإلكتروني. فقد أعلنت فرنسا وبريطانيا خلال عام 2013 عن تطوير قدراتها الهجومية. أكدت الولايات المتحدة في عام 2011، وفرنسا في عام 2013، أن الهجوم الإلكتروني الواسع يمكن اعتباره كعمل من أعمال الحرب وستحتفظ بحق الرد بكل الوسائل. إضافة لذلك، رفضت روسيا عسكرة الفضاء الإلكتروني مع تطوير لقدراتها الذاتية في هذا المجال.

يبين المقال الذي كتبه "مارتن ليبيكي"، الباحث في مؤسسة راند ومؤلف أعمال رائدة حول الردع داخل الفضاء الإلكتروني، التصعيد المحتمل للصراعات في حالة رد تقليدي على هجوم عبر الفضاء الإلكتروني. ويؤكد أن الأضرار ستكون أكثر محدودية إذا بقي الانتقام داخل الفضاء الإلكتروني، والذي سيكون بالتأكيد أقل ردعا. بالمقابل، تقدم "أوريان بارات جينيس" متخصصة في القانون الدولي، حججا لخبراء كتبوا "مرجع أو دليل تالين" Manuel de Tallin" [وهو عبارة عن دليل تمت كتابته من قبل مجموعة من الخبراء بتكليف من حلف شمال الأطلسي، ويقترح نقل أحكام القانون الدولي إلى الفضاء الإلكتروني، توضيح من المترجم]، وترى أن الدليل يبرر شرعية الدفاع عن النفس واللجوء إلى استخدام أسلحة تقليدية ردا على هجوم إلكتروني من شأنه أن يشكّل هجوما مسلحا.

إن خطر التصعيد لا بد أن يؤخذ على محمل الجد، لأنه، وكما يبين هذان المقالان، ليس هناك أي ضمان بأن صراعا يبدأ في الفضاء الإلكتروني سيبقى داخل الفضاء الإلكتروني. لا نعرف بشكل جيد الآثار الجانبية للأسلحة داخل الفضاء الإلكتروني وعن فكرة " الضربات الجراحية" في الفضاء الإلكتروني، وقد تحدث عنها مسؤولون أمريكيون، وهو أمر يدعو للقلق. ضمن هذا السياق، تزداد المقارنة والقياس مع أجواء الحرب الباردة. قدم "ديفيد روثكوبف" في مجلة السياسة الخارجية، فكرة حرب " باردة" أكثر سخونة وأكثر برودة من الحرب الباردة:" إن الهدف من الحرب الباردة سيكون القدرة على الضرب وباستمرار من غير إثارة حرب ساخنة في وقت نعيد فيه الحرب الساخنة أقل رغبة [...] أو حتى ضرورية". [روثكوبف 2013].

هل يجب إعادة إنشاء تحالفات من نوع تحالفات الحرب الباردة؟ هل يجب تقاسم الرؤية التشاؤمية للعلاقات الدولية كلعبة محصلتها صفر ومتواصلة القدرات؟ أم أنها فرصة جديدة لإعادة التفكير في أطر الأمن الجماعي، من خلال إشراك دول مثل روسيا والصين؟ أظهر البلدان استعدادهما للتعاون في وضع وتطوير قواعد دولية، ولكن هناك انقسامات في وجهات النظر ماتزال قائمة، كما بين جيمس لويس في مقاله. يوضح مقال "مارتن ليبيكي"، بدوره، أن التفكير الاستراتيجي لمنع التصعيد هو أمر ضروري ولكنه معقد وأن الحوار لا يزال بعيدا عن أن يكون هو الحل.

والسؤال أيضا، أي إطار للأمن الجماعي نحن قادرون على بنائه؟ الدفاع الأوربي هو صعب مسبقا، أما الدفاع في الفضاء الإلكتروني فهو أكثر صعوبة. بداية، يعتبر تقاسم القدرات كتخلٍ عن السيادة، نظرا للطبيعة الحساسة للتكنولوجيا وما يمكن أن تكشفه من قدرات ونقاط ضعف. يوضح كلا من " جان لوب سامان وفنسنت جوبير" أن الاتحاد الأوربي وحلف شمال الأطلسي دمجا هذه المسائل في أولوياتهما الاستراتيجية واتخذا إجراءات موازية لهذه الأولوية. لكن تقسيم الأدوار والمسؤوليات مازال غير واضح، وحتى الآن لا يوجد سوى تنسيق ضعيف بين المؤسستين حيث يبدو من الصعب جدا تجاوز حدود السيادة. إن التفاوتات فيما يتعلق بالقدرات كبيرة جدا بين الدول الحليفة، أما الأمم التي تمتلك

الوسائل الأكثر تقدما فتعتبر أنه مجالا للسيادة الوطنية ولديها أولوية بالنسبة لعلاقاتها الثنائية في هذا الميدان، لا سيما مع الولايات المتحدة.

إن المحادثة والحوار العابر للأطلسي هو معقد بسبب التحديات الاقتصادية، والتي هي أمور لا يمكن فصلها. ألقت قضية سنودن الضوء وبقوة على تبعية البلدان الأوربية تجاه الشركات الأمريكية الكبرى فيما يتعلق ببياناتها ومعطياتها (حيث يمكن الوصول إليها من قبل الحكومة الأمريكية)، أيضا فيما يتعلق بتجهيزاتها، التي لا يوجد بديل لها سوى الصين، وهذا أمر أكثر صعوبة. يشير البعض إلى سذاجة الأوربيين، الذين يطرحون اليوم مسألة سيادتهم ضمن نطاق انفتاح الأسواق الاقتصادية.

هل يمكننا أن نبني أمن الفضاء الإلكتروني من أجل تحقيق الازدهار الاقتصادي لأوربا بشكل مستقل عن الدفاع داخل هذا الفضاء نفسه؟ ماذا يمكنها أوربا من خلال القواعد والمعايير التقنية، هل هي السياسات الصناعية من أجل تحسين أمنها في الفضاء الإلكتروني؟ ما هو البديل عن المعدات والتجهيزات الصينية والأمريكية؟ تبدو الأسواق الوطنية ضيقة جدا لتكون قادرة على المنافسة، ولكن كيف يتم بناء الثقة بين الأمم من أجل تطوير حلول سياسية وصناعية مشتركة؟ هل يمكننا وهل يجب علينا تطوير العرض السيادي؟ هي أسئلة ملحة لأنه ـ وبعيدا عن التهديدات الأمنية ـ فإن كتلة البيانات الرقمية هي في توسع مستمر. كيف يمكن حمايتها؟ وممن سنحميها؟

الديمقراطية والحريات الفردية

هناك المزيد من البيانات الشخصية التي أصبحت متاحة على الأنترنيت، بشكل أكثر أو أقل صراحة. مع "البيانات المفتوحة" Open Data، فإن كل أنواع البيانات العامة، القادمة من الإدارات، ستكون في نهاية المطاف متاحة، موفرة من جديد أدوات من المعلومات والشفافية التي من شأنها تحسين سير وعمل الديمقراطية. يمكننا أن نأمل أن فرنسا، بشكل خاص، حيث تقديم البيانات العامة هو أبعد من أن يكون متاحا، ستستفيد من هذه الحركة في الانفتاح. ولكن، إلى جانب أخطار الكشف الجنائي أو العرضي لبيانات الأشخاص، يطرح سؤال وصول الشركات والحكومات لهذه البيانات.

إذا كان هناك شيء واحد يمكن الاتفاق عليه من قبل الجميع فيما يتعلق بإدوارد سنودن، هو أنه أطلق نقاشا والذي لولاه لما كان قد حدث. إن المحذرين الذين سبق وحاولوا لفت الانتباه حول ممارسات وكالة الأمن القومي الأمريكي لم ينجحوا في إحداث صدى قويا لمحاولاتهم. لقد كان لا بد من هذا الانفجار ذي الأبعاد العالمية من أجل توعية الجمهور في مواجهة قضية سياسية وأن صدمات اعتداءات 11 سبتمبر عام 2001 لم تعد كافية لحجب النقاش. السؤال المطروح من الآن فصاعدا: كيف يمكن التوفيق بين الديمقراطية والمراقبة؟

إن عمليات المراقبة الديمقراطية في هذا الشأن هي في معظمها غير معروفة من قبل المواطنين ـ لا بد حتى النخب ـ ففي الولايات المتحدة، ورغم الإجراءات عالية التنظيم (أقله على الورق)، فإنها إجراءات معطلة. يعتبر الكثيرون، لاسيما أن النقاشات القانونية تحدث غضبا، أن الحكومة تجاوزت حقوقها واعتدت على الحريات المدنية للمواطنين. إذا كان نفس المصير يسود ردة الأفعال الفرنسية، إلا أن الرأي العام الألماني فعّال ونشيط جدا. إن ذكريات "ستازي" [الوزارة المكلفة بأمن الدولة في ألمانية الشرقية، توضيح من المترجم] ليست بعيدة كثيرا. لقد كان السّر دائما مطلوبا من العاملين في الاستخبارات من أجل الحفاظ على فعالية التحقيقات، ولكن، في مجتمعاتنا الحالية، أصبح من الصعب على نحو متزايد الحفاظ على الأسرار، حتى بالنسبة للحكومات، وقد يكون إدوارد سنودن مثلا جيدا يحتذى به.

إن التفكير بالضمانات، مناقشة إجراءات الرقابة الديمقراطية (من يقرر، أين، عن ماذا، متى؟)، وضع إجراءات لتقييم برامج المراقبة هذه (ممولة من المال العام)، كل هذا يمكّن ليس فقط من الحفاظ على الحريات الفردية، وقيم الديمقراطية نفسها، بل أيضا يشارك في ضمان المزيد من الشرعية. التحديات والرهان عالية المستوى. سجلاتنا الطبية، آراؤنا السياسية، نتائجنا المدرسية، اتجاهاتنا الجنسية، مشترياتنا، تنقلاتنا، أصدقاؤنا، أصدقاء أصدقائنا...كل هذه المعلومات وأكثر من ذلك يمكن أن تكون موضوعا لتحقيقات، لنسخ وتمكّن من وضع ملف دقيق وقوي عنا. والكثير من هذه المعلومات هو، مسبقا، متاح بالفعل، وغالبا ما يعرض بشكل طوعي من قبل مستخدمي الشبكات الاجتماعية والبلوكات.

تُطرح مسألة الضمانات بوضوح بالنسبة للشركات، والتي هي غير خاضعة للمراقبة الديمقراطية بل فقط للقانون، وأحيانا للتعاون القسري مع حكوماتها. مرة أخرى، إن التسوية تستحق التفكير بين المزايا التي لا يمكن إنكارها لاستخدام البيانات من قبل الشركات، التي تحلل أذواقنا، تخزّن اختياراتنا وتقترح علينا خدمات مصممة على قياسنا، والانتهاكات المحتملة للحريات.

تحدث هذه النقاشات وسط تحديات اقتصادية ضخمة. يبيّن المقال الذي كتبه "سيفان غرومباش"، وهو باحث في Inria، إلى أي مدى أصبحت القدرة على جمع المعلومات، لا بل تحليل وتقاطع واستغلال البيانات هي المحرك لاقتصاد مجتمعاتنا. إن هيمنة الشركات الأمريكية على الخدمات عبر الإنترنيت، جنبا إلى جنب مع خبرتهم في معالجة البيانات والقوة الأمريكية في فرض قواعد تقنية، يقدم لهم ميزة استراتيجية لا يمكن إنكارها بالنسبة لأسواق افتتاح البيانات العامة في المستقبل. مرة أخرى، إن تحديات السيادة واضحة وقضية سنودن يمكن أن تعقد المفاوضات على اتفاقيات التجارة الحرة. ومع ذلك، سوف لن يتم التشكيك فيها بشكل أساسي، والكرة في ملعب الأوربيين الذين، على عكس بعض الدول الصاعدة، لم ينتجوا أبطال الأنترنيت. هنا يُطرح سؤال أوربا وقدرة الدول الأعضاء على التوحد من أجل خلق مواجهة اقتصادية وسياسية مع عمالقة الأنترنيت. سيمكّن إصلاح القانون الأوربي لحماية البيانات الشخصية بمواءمة وتناغم خليط من التشريعات الوطنية الأوربية، معززا من حركة الشركات في أوربا، وسيسمح بتعزيز حماية المواطنين أيضا. على سبيل المثال، يوفر الإصلاح بفرض على الشركات، التي تجمع البيانات الشخصية، موافقة صريحة من المستخدمين، وحقهم في النسيان (أي إمكانية محو البيانات) أو، أيضا، وكالة واحدة من أجل التعامل مع النزاعات. على الرغم من قضية سنودن، إلا أن اقتراح الإصلاح تم تأجيله إلى عام 2015، بعد ضغط كبير وبشكل خاص من لوبي الشركات الأمريكية الكبرى وانقسامات جدّية بين الدول الأعضاء. الورشة مازالت ضخمة...

مستقبل الأنترنيت

وأخيرا، تساهم الاستراتيجيات الوطنية في تشكيل الأنترنيت، وهنا مرة أخرى، التحديات هي في غاية الأهمية. أعلنت الرئيسة البرازيلية "ديلما روسيف"، في أعقاب الكشف عن المراقبة واسعة النطاق، بما في ذلك هاتفها الخاص، عن الرغبة في الانفصال عن هذا الأنترنيت الأمريكي جدا ودعت إلى تنظيم قمة حول حوكمة الأنترنيت في البرازيل شهر نيسان 2014. وقد تحدث "بيرتراند دو لا شابيل" عن تحديات ذلك في مقابلته. يبين كلا من "إيبرت هانس وتيم موريه" أن البلدان الصاعدة، والتي يزداد عدد مستخدمي الأنترنيت فيها بشكل قوي، تعيش بشكل سيء التفوق الأمريكي في هندسة وإدارة الأنترنيت ـ والهيمنة في مجال المعدات والتجهيزات، الخدمات، ومحتوى إدارة البيانات ـ، وتطور استراتيجيات من أجل زيادة نفوذها. لقد أطلقت دول البريكس، بالشراكة مع عشرين دول إفريقية، مشروع كابلاتها الخاصة بها تحت البحر والذي يصل إلى 32 ألف كيلومتر، رابطا روسيا، الصين، الهند، إفريقيا الجنوبية، البرازيل مع الولايات المتحدة. لكن البريكس لا تشكل مجموعة من الدول المتجانسة ولا تتقاسم جميعها نفس التقاليد الديمقراطية، كما يقول الكاتبان في مقالهما.

تعرف العديد من الدول الديمقراطية عن قلقها حول تحديات " بلقنة الأنترنيت"، أي التجزئة المادية/الفيزيائية والسياسية للشبكة والتي ستفقدها طابعها الحر والمفتوح الذي هو وراء نجاحها. وضعت كل من الصين، روسيا، إيران، العربية السعودية، كوريا الشمالية استراتيجيات من أجل مراقبة شبكاتها، بنيتها التحتية الخاصة بالشبكة وحتى الوصول إلى المحتوى الذي ينتشر فيها. يبيّن المقال الذي كتبه " كيفن ليمونييه" وبشكل واضح التصورات والاستراتيجيات التي تنفذها روسيا للدفاع عن مفهوم الأنترنيت ذي السيادة. تعزز هذه الدول السيطرة على الأنترنيت من خلال الدول داخل "الاتحاد العالمي للاتصالات". تتعثر المفاوضات الدولية بشكل منتظم حول نقطتين حاسمتين، وقد وضعتهما الدول الغربية في المقدمة: احترام حقوق الإنسان (حرية التعبير، الوصول إلى المعلومة، احترام الحياة الشخصية)، وإشراك الجهات غير الحكومية في نموذج متعدد للحكم، كما يشرح ذلك " برتراند دو لا شابيل". بالنسبة للصين، روسيا وأخرين، تقع هذه الأمور ضمن السيادة الحصرية للدول. تبقى المصالح الاقتصادية والسياسية متصلة بقوة وبما يكفي من أجل، وحتى الآن، ألا توضع البنية المشتركة الأساسية قيد التشكيك والتساؤل.

أدى الكشف عن برامج وكالة الأمن القومي الأمريكي، وصعود البلدان الديمقراطية الناشئة مثل البرازيل والهند، وجهود " مؤسسة الأنترنيت للأسماء والأرقام المخصصة" Icann[9] والتي تأخذ بالاعتبار المطالبات الإقليمية، إلى تحريك الخطوط. التحدي هو في مستقبل الأنترنيت. كيف يمكن إفساح المجال أمام جميع الدول وخلق بيئة آمنة بما فيه الكفاية للحفاظ على الطابع الحر والمفتوح للشبكات؟

الخلاصة

لقد أصبح الفضاء الإلكتروني، وفي نفس الوقت، تحديا من التنافس بين سلطات الجهات الفاعلة، مسرح للمواجهة وسلاح قوي في الصراعات الجيوسياسية. إن الصراعات على الفضاء الإلكتروني أو داخل الفضاء الإلكتروني ليست منفصلة عن النزاعات بين القوة الجيوسياسية التقليدية. وهي، على العكس من ذلك، تعبير وبُعد جديد، حاضر في جميع مستويات التحليل، وينبغي أخذها في الاعتبار في مقاربة متعدد النطاقات.

إن التحديات والرهانات الجيوسياسية للفضاء الإلكتروني وثيقة الصلة مع اعتبارات سياسية، اقتصادية، اجتماعية وثقافية. بالنسبة للجيوسياسة، فإن مقارباتها المتعددة النطاقات والعابرة للمجالات البحثية، والتي هي في الواقع منفتحة على المعلوماتية، لا بل على الرياضيات، تمكّن من معالجة هذه القضايا في جميع تعقيداتها. أما البعد التقني للنقاشات فسيتطلب من دون أي شك جهدا خاصة من القارئ. لكن اللعبة تستحق كل هذا العناء، لأنها ليست فقط تحديات للقوة والأمن داخل الفضاء الإلكتروني، بل أيضا قيم ندافع عنها كأمم ديمقراطية، القيم التي نريد رؤيتها تحكم العالم الذي نبنيه.

[9]- Internet Corporation for Assigned Names and Numbers (Icann) : وهي المنظمة التي تنسق نظام عناوين الأنترنيت وأسماء المجالات أو النطاقات.

ببليوغرافية

Bibliographie

CATTARUZZA A. et DOUZET F. (2013), « Le cyberespace au cœur de tensions géopolitiques internationales », *DSI,* hors-série n° 32.

DESFORGES A. (2013), « Les frontières du cyberspace », *in* DOUZET F. et GIBLIN B. (dir.), *Des frontières indépassables ?*, Armand Colin, Paris.

DOSSÉ S. (2010), « Vers une stratégie de milieu pour préparer les conflits dans le cyberespace ? », *DSI*, n° 59, mai.

DOUZET F. (1997), « Internet géopolitise le monde », *Hérodote,* n° 86/87, p. 222-233.

–, (2007), « Les frontières chinoises de l'Internet », *Hérodote,* n° 125, p. 127-142.

20

–, (2013), « Chine, États-Unis : la course aux cyberarmes a commencé », *Sécurité globale*, n° 23.

–, (2013), « Chine : cyberstratégie, l'art de la guerre revisité »*, Diploweb,* 12 septembre (<www.diploweb.com>)

GIBSON W. (1984), *Neuromancer,* Ace, New Jersey.

KEMPF O. (2012), *Introduction à la cyberestratégie*, Economica, Paris.

LACOSTE Y. (dir.) (1993), *Dictionnaire de géopolitique*, Flammarion, Paris.

LACOSTE Y. (2003), *De la géopolitique aux paysages, dictionnaire de la géographie*, Armand Colin, Paris.

MATTELART A. (2009), *Histoire de l'utopie planétaire. De la cité prophétique à la société globale*, La Découverte, Paris.

MCLUHAN M. (1964), *Understanding Media. The Extensions of a Man*, McGraw-Hill, New York.

MUSSO P. (2003), *Critique des réseaux*, PUF, Paris.

ROTHKOPF D. (2013), « The cool war », *Foreign Policy*, 20 février.

SANGER D. (2013), « In cyberspace, new cold war », *New York Times,* 24 février. VIRILIO P. (1997), « Un monde surexposé », *Le Monde diplomatique,* août.