MESR
منار الشرق للدراسات والأبحاث
Manar Elsharq for Studies & Research

Middle East Journal of Legal and Jurisprudence Studies

Homepage: http://meijournals.com/ar/index.php/mejljs/index
ISSN 2710-2211 (Print)
ISSN 2788-4694 (Online)

مجلة الشرق الأوسط
للدراسات القانونية والفقهية

السيادة الرقمية بالمغرب ... تجلياتها وممكنات تحقيقها

د. يونس مليح

أستاذ باحث بجامعة مولاي إسماعيل بمكناس –المغرب–

الكلية المتعددة التخصصات بالرشيدية

استلام البحث: 21/03/2022 مراجعة البحث: 26/05/2021 قبول البحث:04/06/2021

ملخص الدراسة:

تشير السيادة الرقمية إلى القدرة على التحكم في مصيرك الرقمي – البيانات والأجهزة والبرامج التي تعتمد عليها وتقوم بإنشائها. لقد أصبحت مصدر قلق للعديد من صانعي السياسة الذين يشعرون أن هناك الكثير من السيطرة التي يتم التنازل عنها لأماكن قليلة جدا، وخيارات قليلة جدا في سوق التكنولوجيا، ونفوذ كبير في أيدي عدد صغير من شركات التكنولوجيا الكبيرة. فماذا نعني بمصطلح السيادة الرقمية؟ وما هي أبرز تجلياته وركائزه؟ وإلى أي حد يمكن الحديث عن السيادة الرقمية بالمغرب؟

الكلمات المفتاحية: الرقمنة- السيادة- المفهوم- الممكنات-المغرب.

Digital sovereignty... Its demonstrations and possibilities to achieve it in Morocco

Abstract

Digital sovereignty refers to the ability to control your digital destiny - the data, hardware and software you depend on and create. It has become a concern for many policymakers who feel that there is too much control ceded to too few places, too few options in the technology marketplace, and too much influence in the hands of a small number of large technology companies. What do we mean by the term digital sovereignty? What are its most important manifestations and pillars? To what extent can we talk about digital sovereignty in Morocco?

Keywords: gitization - concept - sovereignty - opportunities – Morocco

مقدمـــــــــــة

السيادة مفهوم سياسي لا يوجد له تعريف واضح ومقبول بشكل عام. وترتبط السيادة عموما بالسلطة الإقليمية، والإقليم (بما في ذلك الموارد الطبيعية)، والولاية القضائية، السكان والسلطة مع الاعتراف الداخلي والخارجي (الشرعية). الشرعية الداخلية تشير إلى فعالية الدولة كمنفذ للمهام الحكومية (على سبيل المثال، السيطرة على العملية الانتخابية وسلسلة العدالة الجنائية)، وكذلك اعتراف المواطنين بالحكومة (التي لديها ثقة في سيادة القانون). تتعلق الشرعية الخارجية في المقام الأول باعتراف الدول الأجنبية واستقلالية تصرفات الدولة تجاه الدول الأجنبية.وفي مجتمع المعلومات اليوم، غالبا ما يستخدم مصطلح السيادة الرقمية، إذ يشير دائما إلى البعد الرقمي للاستقلالية الاستراتيجية، أي القدرة على اتخاذ القرار والتصرف بشكل مستقل بشأن الجوانب الرقمية الأساسية لمستقبلنا على المدى الطويل في الاقتصاد والمجتمع والديمقراطية، يتعلق هذا باستخدام وهيكلة الأنظمة الرقمية نفسها، والبيانات المنتجة والمخزنة فيها، والعمليات الناتجة.

لذلك فإن المصطلح الأفضل من السيادة الرقمية هو الاستقلال الذاتي الاستراتيجي الرقمي، ومع ذلك، في هذه المقالة، سنستمر في استخدام مصطلح السيادة الرقمية، لأنه مصطلح شائع. لذلك، تشير السيادة الرقمية إلى القدرة على التحكم في مصيرك الرقمي – البيانات والأجهزة والبرامج التي تعتمد عليها وتقوم بإنشائها. لقد أصبحت مصدر قلق للعديد من صانعي السياسة الذين يشعرون أن هناك الكثير من السيطرة التي يتم التنازل عنها لأماكن قليلة جدا، وخيارات قليلة جدا في سوق التكنولوجيا، ونفوذ كبير في أيدي عدد صغير من شركات التكنولوجيا الكبيرة.

مشكلة الدراسة:

ماذا نعني بمصطلح السيادة الرقمية؟ وما هي أبرز تجلياته وركائزه؟ وإلى أي حد يمكن الحديث عن السيادة الرقمية بالمغرب؟

فرضيات الدراسة:

تفترض الدراسة:

1- أنه يجب الاحتفاظ بالبيانات الشخصية المخزنة على الإنترنت في البلد الذي يقيم فيه الشخص من أجل القول أن هناك سيادة رقمية في بلد ما، وبالتالي يجب أن تخضع لقانون البلد المعني. لذلك، يجب حماية الفضاء الإلكتروني، تماما مثل الأرض والبحر والجو.

2- إلى جانب ذلك، من الضروري الحفاظ على السيادة الوطنية في مواجهة التهديدات الجديدة الناتجة عن الرقمنة المتزايدة للمجتمع.

أهمية الدراسة:

على مدى العقود الماضية، غيرت التكنولوجيا الرقمية بشكل جذري الطريقة التي يتفاعل بها الناس والمجتمعات على جميع المستويات. هذا القول صحيح تماما اليوم، فقد سارعت جائحة Covid-19 في غضون أسابيع قليلة فقط من اعتماد الأدوات الرقمية من قبل الجميع للعمل أو الدراسة أو لمجرد البقاء على اتصال مع أحبائهم. النتيجة: يتم إنشاء كمية مذهلة من البيانات وتخزينها كل عام، وتستمر في النمو. بحلول عام 2024، يقدر أنه سيتم إنشاء ونسخ واستهلاك 149 زيتابايت من البيانات (1 زيتابايت = 1021 بايت) في جميع أنحاء العالم.

فضمان السيادة الرقمية لدولة ما يعني أن تكون أقل اعتمادا على القوى الأجنبية. لذلك، تحاول الدول في جميع أنحاء العالم بالفعل الاستفادة من الفوائد – الاقتصادية والجيوسياسية – التي تنبع من التطور السريع للتقنيات الرقمية. فمعرفة من يمتلك تقنيات المستقبل، ومن ينتجها، ومن يضع المعايير وينظم استخدامها، أصبح جزءا لا مفر منه من المنافسة الجيوسياسية ومن هنا تنبع أهمية هذا الموضوع.

منهجية الدراسة:

سيتم استخدام خلال أطوار هذه الدراسة كل من المنهج الوصفي من أجل وصف أولا مفهوم السيادة الرقمية، وكذا واقع السيادة الرقمية بالمغرب وأساسياتها، واستخدام المنهج التحليلي من خلال تحليل مجموعة من الأرقام التي سندرجها في هذه الدراسة.

هيكلة الدراسة:

تم تقسيم هذه الدراسة إلى ثلاثة مباحث، يتناول المبحث الأول منها الإطار النظري للدراسة من خلال التطرق في المبحث الأول إلى مفهوم السيادة الرقمية وواقع هذه السيادة في ظل جائحة فيروس كورونا كوفيد-19، بينما يتطرق المبحث الثاني إلى التهديدات السيبرانية وسؤال السيادة الرقمية وارتباطها أولا علاقتها بسؤال التنمية، وفي المبحث الثالث سنتطرق لممكنات السيادة الرقمية بالمغرب، وفي الأخير سيادة الأمن السيبراني بالمغرب.

المبحث الأول

مفهوم السيادة الرقمية وواقعها في ظل جائحة كورونا

أولاً- في مفهوم السيادة الرقمية

لتشريح مفهوم سيادة البيانات أو السيادة الرقمية، يجب علينا أولا أن نتذكر الأهمية التاريخية والسيطرة القوية على الخطاب السياسي لمفهوم السيادة نفسه. ظهرت تدريجياً، خاصة في أوروبا، عبر قرون من الصراعات بين أنظمة السلطة والمناقشات الفلسفية والسياسية المكثفة، كما يتضح من كتابات جان بودان، غروتيوس، توماس هوبز، جون لوك، مونتسكيو أو روسو[1]. وبغض النظر عن استخدامه في السياق الرقمي، فإن مصطلح "السيادة" يشير إلى القدرة على التصرف بطريقة مستقلة، دون هيمنة أجنبية. حيث تأثر المفهوم التقليدي للسيادة بشدة بالمنظر السياسي في القرن السادس عشر، جان بودان، الذي كان يعتقد

[1] -Stéphane Couture and Sophie Toupin, "What Does the Notion of 'Sovereignty' Mean When Referring to the Digital?," New Media & Society 21, no. 10 (October 1, 2019): 2305–22: https://doi.org/10.1177/1461444819865984.

أن سلطة اتخاذ القرار النهائية والحق الحصري في استخدام القوة في الدولة يجب أن تكون بيد الحاكم، صاحب السيادة. في القرن الثامن عشر، أعلن الفيلسوف التنويري جان جاك روسو عن تغيير جذري في فهم المفهوم، من سيادة الحاكم إلى سيادة الشعب. مع تطور الديمقراطيات الحديثة، سادت فكرة أن الشعب، من وجهة نظره، يمتلك أعلى سلطة في الدولة، ولكن يمكنه أن يعهد بها إلى حكومة ذات سيادة أو منتخبة لممارستها[2].

كما يعد التفسير القانوني للمصطلح أيضا أساسيا للفهم الحديث للسيادة، والذي يمثل القدرة على تقرير المصير للكيان القانوني. يتميز هذا بالحكم الذاتي والاستقلال وبالتالي يمثل تباينا مع التصميم الخارجي، بينما يختلف عن الاكتفاء الذاتي الكامل و/ أو العزلة. في القانون الدستوري والدولي، تشير السيادة إلى استقلال الدولة عن الدول الأخرى (السيادة الخارجية)، ومن تنظيمها الداخلي الذاتي (السيادة الداخلية). يرتبط مفهوم السيادة أيضا ارتباطا وثيقا بمفهوم الدولة القومية المحددة إقليميا: تكون الدولة ذات سيادة إذا كان بإمكانها، فيما يتعلق بالدول الأخرى، التصرف بطريقة مستقلة إلى حد كبير على المستوى السياسي والاقتصادي والمجتمعي.

في الديمقراطيات الحديثة، يرتبط مصطلح السيادة ارتباطا وثيقا بمبدأ سيادة القانون. دولة الحق. إن سيادة الدولة الديمقراطية تعني ضمنا ضمان قدرة مواطنيها على تقرير المصير بحقوقهم غير القابلة للتصرف. فهي تهدف إلى السماح لجميع الأفراد بالاحترام في حقوقهم الشخصية والتصرف بناء على سلطتهم الخاصة. ويعتبر ضمان الشروط والأحكام الخاصة بذلك مسؤولية الدولة، لاسيما بالنظر إلى التحديات العديدة التي يفرضها التحول الرقمي على جميع مجالات المجتمع.

لذلك، أصبح مصطلح السيادة الرقمية أكثر شيوعا في وسائل الإعلام وله مجموعة متنوعة من المعاني، أحد التفسيرات هو قدرة الدول على التحكم في البنية التحتية الرقمية الخاصة بها وببيانات مواطنيها. ومع ذلك، نرى أن المصطلح يستخدم بشكل متزايد في سياق أوسع. أصبحت التقنيات الرقمية ساحة معركة للمنافسة العالمية القيادة وتؤدي إلى توترات جيوسياسية متزايدة باستمرار بين الولايات المتحدة والصين (المعروفة أيضًا باسم الحرب الباردة التقنية) . تدور المعركة بشكل أساسي حول الريادة في مجال الجيل الجديد من الاتصالات، تقنية الرقائق والذكاء الاصطناعي (AI). ترسم كل من الولايات المتحدة والصين بانتظام بطاقة السيادة في هذا السياق. الرئيس السابق للولايات المتحدة الأمريكية ترامب قرر حظر التطبيقات الصينية الشهيرة – مثل TikTok وWeChat– لأنهم سيقوضون "الأمن القومي، السياسة الخارجية والاقتصاد " للولايات المتحدة[3].

لم يكن مفهوم "سيادة البيانات" على وجه الخصوص موجودا تقريبا قبل عام 2011، بينما أصبح الآن جزءا من الخطاب الأكاديمي والعام. وغالبا ما يشير الخطاب السائد حول "السيادة الرقمية" إلى قدرة الدول القومية – خاصة الصين وروسيا وفرنسا – على تأكيد سيطرتها على البنى التحتية المقيمة داخل أراضيها والبيانات التي ينتجها مواطنوها. ومع ذلك، يتم التأكيد على العديد من المعاني الأخرى عند الحديث عن السيادة. فهناك خمسة أنواع من الخطابات أو وجهات النظر حول مفهوم "السيادة" كما ينطبق على الجانب الرقمي:

[2] -John Perry Barlow, "A Declaration of the Independence of Cyberspace," February 8, 1996: https://www.eff.org/fr/cyberspace-independence.

[3] - See, for a good overview, Stephane Couture, The Diverse Meanings of Digital Sovereignty, August 5, 2020: http://globalmedia.mit.edu/2020/08/05/the-diverse-meanings-of-digital-sovereignty/

1. سيادة الفضاء الإلكتروني (Cyberspace sovereignty): له أهمية تاريخية لأنه يشير في المقام الأول إلى إعلان "استقلال الفضاء السيبراني" من قبل جون بيري بارلو في عام 1996 والذي أكد فيه المؤلف أن "الفضاء الإلكتروني" كان حينها منطقة جديدة لا ينبغي أن تنظمها الحكومات[4]. بطريقة أكثر معاصرة (وأكاديمية) ، يقدم ميلتون مولر منظورًا له صدى مع نفس الفكرة في "السيادة الشعبية في الفضاء السيبراني". بالنسبة لمولر، يجب أن تكون مشاركة أصحاب المصلحة المتعددين ، كما تتم ممارستها حاليا في مؤسسات حوكمة الإنترنت مثل منتديات حوكمة الإنترنت (IGF) أو مؤسسة الإنترنت للأسماء والأرقام المخصصة (ICANN) ، يجب أن تكون أساس السيادة في الفضاء الإلكتروني[5].
2. السيادة الرقمية للدولة (State Digital Sovereignty): ربما تكون الخطاب السائد اليوم وتشير إلى قدرة وجهود البلدان والدول القومية للتحكم في بياناتها وبنيتها التحتية التكنولوجية[6]. كما يعتبر أيضا خطاب السيادة الرقمية بمثابة مجاز خطابي (ما يسمونه "العلامة التجارية للأمة") لتعزيز رؤية وطنية مميزة لما يجب أن تكون عليه الإنترنت[7].
3. السيادة الرقمية للشعوب (Indigenous digital sovereignty): مماثلة للمنظور السابق، ولكنها تشير إلى سيطرة الشعوب والأمم على بياناتهم وبنيتهم التحتية ومصيرهم على نطاق أوسع. إلى جانب مفهوم "سيادة الشبكة: network sovereignty" للإصرار على أهمية البنى التحتية التكنولوجية لانبعاث السكان الأصليين، والسيادة، وتقرير المصير. فالتكنولوجيا، من هذا المنظور، هي أداة حاسمة لتعزيز السيادة الأصلية[8].
4. السيادة الرقمية للحركات الاجتماعية: تشير إلى قدرة الحركات الاجتماعية ومجموعات الناشطين على التحكم في بياناتهم الخاصة باستخدام البرامج والخوادم والتقنيات القائمة على التشفير، وقدرتها على تطوير واستخدام الأدوات الرقمية التي تم تصميمها من قبلهم ومن أجلهم.

1. السيادة الرقمية "الشخصية": على الرغم من أن هذا المنظور بعيد كل البعد عن الهيمنة، إلا أنه يستحق الذكر لأنه يتعلق بالتحكم في تقنياتنا الخاصة. لذلك، يحتاج النشطاء الاجتماعيون إلى ضمان سيادتهم التكنولوجية، على سبيل المثال باستخدام برامج مجانية ومفتوحة المصدر أو أدوات اتصال مشفرة[9]..

ويمثل الشكل التالي تواتر استخدام مفهوم "السيادة" فيما يتعلق بالجانب الرقمي (باستخدام ProQuest Central):

[4] - J John Perry Barlow, "A Declaration of the Independence of Cyberspace," February 8, 1996: https://www.eff.org/fr/cyberspace-independence.

[5] - Milton Mueller, Will the Internet Fragment?: Sovereignty, Globalization and Cyberspace (Cambridge, UK ; Malden, MA: Polity, 2017).

[6] - Jonathan A. Obar and Andrew Clement, "Internet Surveillance and Boomerang Routing: A Call for Canadian Network Sovereignty," SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, July 1, 2013): https://papers.ssrn.com/abstract=2311792.

[7] - Tung-Hui Hu, A Prehistory of the Cloud (Cambridge, Massachusetts: The MIT Press, 2015): https://mitpress.mit.edu/prehistory-cloud.

[8] - Marisa Elena Duarte, Network Sovereignty: Building the Internet across Indian Country (Seattle, WA: University of Washington Press, 2017).

[9] - Julian Gill-Peterson, "Sexting Girls: Technological Sovereignty and the Digital," Women & Performance: A Journal of Feminist Theory 25 (July 13, 2015): 143–56 : http://www.tandfonline.com/doi/full/10.1080/0740770X.2015.1057010.

	سيادة البيانات		السيادة التكنولوجية		السيادة الرقمية	
	أكاديمي	آخر	أكاديمي	آخر	أكاديمي	آخر
قبل 2011	0	23	12	81	0	6
2011–2014	18	794	6	101	2	49
2015–2018	89	2459	20	131	22	239

المصدر: تواتر استخدام مفهوم "السيادة" فيما يتعلق بالتكنولوجيا الرقمية:

Stéphane Couture and Sophie Toupin, "What Does the Notion of 'Sovereignty' Mean When Referring to the Digital?

ثانياً- السيادة الرقمية في زمن كوفيد-19

عندما برزت جائحة COVID-19 في وقت سابق من عام 2020، انتقل الكثير من سكان العالم إلى الإنترنت، مما أدى إلى تسريع التحول الرقمي الذي كان جاريا منذ عقود. حيث بدأ الأطفال الذين لديهم إمكانية الوصول إلى الإنترنت من المنزل في أخذ دورات التعليم عن بعد، وبدأ العديد من الموظفين في العمل من المنزل، واعتمدت العديد من الشركات نماذج الأعمال الرقمية للحفاظ على عملياتها ودعم سمعتها. كما اعتمدت العديد من الشركات نماذج أعمال رقمية للحفاظ على العمليات والحفاظ على مصادر دخل معينة. وفي الوقت نفسه، تم تطوير تطبيقات الهاتف المحمول للمساعدة في "تتبع وتعقب" تطور الوباء؛ وقد استخدم الباحثون الذكاء الاصطناعي (AI) لمعرفة المزيد عن الفيروس وتسريع البحث عن لقاح. في بعض البلدان، زادت حركة الإنترنت بنسبة تصل إلى 60٪ بعد فترة وجيزة من انتشار الوباء[10]، مما يؤكد التسارع الرقمي الذي أحدثه الوباء.

بينما تُظهر هذه الأنشطة الإمكانات الهائلة للتحول الرقمي، فقد أدى الوباء أيضا إلى إبراز الفجوات المتبقية. في حين أن بعض الفجوات الرقمية قد تطورت بسرعة في السنوات الأخيرة، إلا أن البعض الآخر لم يواكبها، تاركا بعض الأشخاص وراء الركب في التسريع الرقمي الناجم عن COVID. بالإضافة إلى ذلك، أدى الاعتماد المتزايد على الحلول الرقمية إلى زيادة إلحاح المخاوف بشأن الخصوصية والأمن الرقمي وكيفية تحقيق السيادة الرقمية[11].

لقد كشف Covid-19 عن الأهمية الحاسمة للتكنولوجيا في مرونة الاقتصاد والصحة. لذلك، استخدمت الحكومات البيانات في الوقت الفعلي ومتعقبات الأمراض التي تحدد حجم وانتشار وتوزيع فيروس كورونا الجديد (COVID-19) SARS-CoV-2 الذي ظهر في عام 2019 للإعلام والتأثير في عملية صنع القرار وتطوير السياسات. تأثرت الشعوب بشكل غير متناسب

[10] - OECD Policy Responses to Coronavirus (COVID-19), Keeping the Internet up and running in times of crisis, Updated 4 May 2020:

https://www.oecd.org/coronavirus/policy-responses/keeping-the-internet-up-and-running-in-times-of-crisis-4017c4c9/

[11]- Digital Transformation in the Age of COVID-19 BUILDING RESILIENCE AND BRIDGING DIVIDES, DIGITAL ECONOMY OUTLOOK 2020 SUPPLEMENT:

https://www.oecd.org/digital/digital-economy-outlook-covid.pdf

بفيروس كورونا، سواء من خلال العدوى أو الوفيات أو الخسائر الاقتصادية أو التغيرات في التفاعلات الاجتماعية. بينما تحتاج الشعوب إلى بيانات مناسبة وجيدة التوقيت وذات صلة وجيدة لتوجيه استجابتها للوباء، فإن جمع هذه البيانات واستخدامها لا يخلو من المخاطر. ففي الأشهر الأخيرة، أثيرت مخاوف بشأن أضرار البيانات وخصوصية المجموعة، والموافقة، والمراقبة العنصرية، والاستهداف الخوارزمي والمزيد.

المبحث الثاني

التهديدات السيبرانية والسيادة الرقمية وسؤال التنمية

أولاً- التهديدات السيبرانية والسيادة الرقمية

كشفت اكتشافات "إدوارد سنودن" لعام 2013 حول برنامج المراقبة الجماعية للإنترنت (NSA) التابع للولايات المتحدة أن التقنيات عرضة لهيمنة الدول الأخرى في مجال تكنولوجيا المعلومات والاتصالات. إن نقاط الضعف، سواء في الأجهزة أو البرامج، ليست مجرد نقاط ضعف تقنية بحتة، ولكنها تسمح للدول بالوصول إلى معلومات حول سكان دولة أخرى وأسرار أمنية وطنية .تسببت اكتشافات "سنودن" في فقدان الثقة في هذه التقنيات وفي الأنشطة الإلكترونية الأمريكية. أثارت قضية سنودن موجة من الغضب وانعكاس الغضب والتفكير بين الدول حول كيفية حماية ما يسمونه سيادتهم الإلكترونية. ومع ذلك، فإن استخدام مصطلح السيادة الإلكترونية هو تسمية خاطئة. في حين أنه من الصحيح أن سيادة الدولة قد انتهكت من خلال هذه التدخلات وحملات التجسس الضخمة، فمن الضروري التمييز بين قضايا الاستقلالية الاستراتيجية المتعلقة بالأمن السيبراني والسيادة الإلكترونية على النحو المحدد في القانون الدولي.

وأظهرت الأبحاث مفتوحة المصدر باستخدام المؤشر العالمي للأمن السيبراني ((ITU) التابع للاتحاد الدولي للاتصالات (Global Cybersecurity Index) (2017) ومستودع الاستراتيجية الوطنية للاتحاد الدولي للاتصالات (2018) أن 84 دولة من بين 193 دولة على مستوى العالم لديها استراتيجيات وطنية للأمن السيبراني متاحة للجمهور ، وأن 69 دولة ترجمت استراتيجياتها الوطنية إلى اللغة الإنجليزية بحلول كانون الأول (ديسمبر) 2017. في بعض الحالات ، كانت هناك إشارات إلى الدول التي وضعت استراتيجيات وطنية للأمن السيبراني، لكن الوثائق ذات الصلة لا يمكن تحديدها في عمليات البحث مفتوحة المصدر (على سبيل المثال ، عُمان والجزائر)[12].

أنواع الدول التي لديها استراتيجيات وطنية للأمن السيبراني هي في الغالب قوى كبرى ودول غربية، باستثناء بعض الدول الأفريقية والعربية ودول أمريكا الجنوبية. فمن بين 69 دولة لديها استراتيجيات وطنية للأمن السيبراني متاحة للجمهور باللغة الإنجليزية، أشارت 15 دولة فقط إلى كلمات البحث المتعلقة بالسيادة، نصف الاستراتيجيات التي تحتوي على كلمة "سيادة" جاءت من الدول الغربية، وهي كل من كندا وفنلندا وفرنسا والمجر والبرتغال وإسبانيا وأستراليا والمملكة المتحدة، بينما جاء النصف الآخر من شيلي وكولومبيا وغانا واليابان ونيجيريا، روسيا والسعودية[13].

[12] – Marie Baezner et Patrice Robin: Trend Analysis: Cyber Sovereignty and Data Sovereignty, May 2018: https://www.researchgate.net/publication/325335882

[13] – Ibid, p 8.

كندا هي الدولة الوحيدة التي استخدمت مصطلح "السيادة الإلكترونية". حيث تُظهر هذه النتائج أن الدول نادرا ما تستخدم مفهوم "السيادة" في استراتيجياتها الوطنية للأمن السيبراني. استنادا إلى مجموعة الدول التي تستخدم المصطلح، يمكن استنتاج أن سيادة الأمن السيبراني هي مفهوم غربي في الغالب، وأن الدول الغربية تميل إلى استخدام المصطلح أكثر من غيرها. ومع ذلك، فإن الدول الغربية أيضا ممثلة بشكل مفرط في هذه المجموعة، لأنها تمثل جزءا كبيرا من الدول التي نشرت استراتيجيات الأمن السيبراني الوطنية.

على الرغم من وجود كلمتي "السيادة" و"السيادة الإلكترونية" في هذه الاستراتيجيات المتعلقة بالأمن السيبراني، إلا أنهما لا يتم استخدامهما كثيرا. في المتوسط، يتم استخدام كلمة "سيادة" مرتين في المستند. ولوحظت استثناءات في استراتيجيات فنلندا ونيجيريا والبرتغال، حيث ورد ذكر كلمة "سيادة" ثلاث مرات على الأقل. ومع ذلك، برزت دولة واحدة، وهي فرنسا، من خلال ذكر كلمة "سيادة" تسع مرات في استراتيجياتها لعام 2011 وخمس مرات في استراتيجيتها لعام 2015. تُظهر هذه النتائج أنه بشكل عام، نادرا ما تستخدم الدول مصطلح "السيادة" في استراتيجيات الأمن الإلكتروني الوطنية الخاصة بها، وحتى عندما تفعل ذلك، فإنها تميل إلى القيام بذلك بشكل غير متكرر ودون تحديد واضح له. بالإضافة إلى ذلك، لا تميل الدول إلى المشاركة في فهم مشترك للمصطلح. ومع ذلك، يبدو أن المفهوم الويستفالي لمفهوم السيادة يسود بين الدول في سياق الأمن السيبراني. يبدو أيضا أنه عند استخدام مفهوم السيادة في الاستراتيجيات، فإن استخدامه لا يتغير بمرور الوقت ولا يتأثر بالكاد بما كشف عنه إدوارد سنودن.

وفيما يتعلق بسنة نشر الاستراتيجيات الوطنية للأمن السيبراني، تم نشر 55 وثيقة من أصل 93 وثيقة تمت دراستها قبل ما تم كشفه من طرف إدوارد سنودن، و 38 بعد الكشف عنها في عام 2013. ومن بين 18 وثيقة تحتوي على كلمتي "السيادة" و "السيادة الإلكترونية"، تم نشر 13 وثيقة قبل 2013 و5 وثائق بعده. ومع ذلك، لا يوجد فرق واضح في استخدام مفهوم السيادة بين الوثائق المكتوبة قبل 2013 وتلك المكتوبة بعده. والفرق الوحيد هو أن الاستراتيجيات التي تم إصدارها بعد عام 2013 تميل إلى الدعوة بقوة أكبر للحاجة إلى فضاء إلكتروني آمن من أجل ضمان سيادة الدولة. ويمثل الجدول التالي قائمة لبعض الدول المستخدمة للأمن السيبراني للدولة و / أو استراتيجيات الدفاع الإلكتروني ومنها المغرب، وعدد المرات التي ذكرت فيها كلمة "سيادة" في هذه الاستراتيجيات[14]:

الدولة	اسم الإستراتيجية	سنة النشر	الإشارة إلى "السيادة"	الإشارة إلى "السيادة الإلكترونية"	عدد المرات التي ذكرت فيها كلمة "سيادة"
كندا	خطة العمل 2010-2015 لاستراتيجية الأمن السيبراني في كندا	2013	نعم	لا	1
الصين	الاستراتيجية الوطنية للأمن السيبراني	2016	لا	لا	-
مصر	الإستراتيجية الوطنية لتكنولوجيا المعلومات والاتصالات 2012-2017	2012	لا	لا	-

[14] - Marie Baezner et Patrice Robin: Trend Analysis: Cyber Sovereignty and Data Sovereignty, May 2018, P 16-23.

فرنسا	الاستراتيجية الوطنية الفرنسية للأمن الرقمي	2015	نعم	لا	5
المغرب	الاستراتيجية الوطنية لمجتمع المعلومات والاقتصاد الرقمي ("المغرب الرقمي 2013")	2013	لا	لا	-
السعودية	الإستراتيجية الوطنية لأمن المعلومات في المملكة العربية السعودية	2013	نعم	لا	1

إن أحد الأبعاد المهمة للسيادة الرقمية هو المرونة الإلكترونية لقطاعاتنا وعملياتنا وبياناتنا الحيوية. لذلك، فتهديدات الأمن السيبراني المتزايدة تقوض السيادة، نحن نتحدث عن مجموعة كاملة من التهديدات المباشرة لبنيتنا التحتية الحيوية، والسرقة المنهجية للملكية الفكرية، والابتزاز الرقمي، والمعلومات المضللة، والتسلل المنهجي لوسائل التواصل الاجتماعي للتأثير على العملية الانتخابية وعلى تفعيل الديمقراطية. عندما لا تتحكم حكومتنا والقطاعات الحيوية في العمليات والبيانات المهمة، فإنها تؤثر بشكل أساسي على الشرعية الداخلية للدولة.

فعندما يتعلق الأمر بالتهديدات السيبرانية، لا يمكن فصل السيادة الرقمية عن المبادئ الأساسية الثلاث لأمن المعلومات، والمعروفة أيضًا باسم (CIA : Confidentiality, integrity and availability) للأمن السيبراني: السرية والنزاهة والتوفر. في هذه المجالات الثلاث، يجب حماية الاستقلالية، ليس فقط على مستوى نظام معين في قطاع معين (مثل نظام تكنولوجيا المعلومات والاتصالات في سلسلة العقوبات) ، ولكن أيضا في الإطار الأوسع للاقتصاد والمجتمع والديمقراطية.

يمكن تقويض السيادة من خلال نظام تكنولوجيا المعلومات والاتصالات الحكومي المحدد – التفكير في سرقة المعلومات من المسؤولين للتجسس (السرية) والهجمات الإلكترونية على أنظمة الأتمتة والرقابة الصناعية للبنى التحتية الحيوية لدينا (التوفر). هذه الأنظمة هي الهدف المحدد للجهات الفاعلة الحكومية الأجنبية من أجل جعل التخريب ممكنا في المستقبل كوسيلة للضغط لتحقيق أهداف جيوسياسية. في هذه الحالات، يمكننا ترجمة السيادة الرقمية إلى متطلبات مباشرة لأنظمة تكنولوجيا المعلومات والاتصالات. وتشمل هذه متطلبات كل من الأمان، واكتشاف التهديدات ، والاستمرارية (النسخ الاحتياطي، والتعافي من الهجمات) ، ومنع والوصول إلى البيانات من قبل القوى الأجنبية؛ ومع ذلك، يجب أيضا ترجمة السيادة الرقمية إلى مصلحة الدولة الأوسع في الاقتصاد والمجتمع والديمقراطية. يتعلق هذا، على سبيل المثال، بدرجة السيطرة على النظم البيئية الاقتصادية الأساسية، والمعرفة والبيانات، والثقة في سيادة القانون ونوعية صنع القرار الديمقراطي.

ثانيا– السيادة الرقمية وسؤال التنمية

قلبت الثورة الرقمية الظروف التي تمارس فيها الدولة صلاحياتها السيادية على أراضيها، وتضمن الحقوق والحريات التي يكفلها دستورها، وتدافع عن أمن مواطنيها، وتعزز التنمية الاقتصادية. إنه يغير الطرق التي يعتزم بها الناس، من خلال السلطة السياسية التي يحددونها، من خلال القوانين الموضوعة باسمهم، للحفاظ على سيطرتهم على مصيرهم. كما أنه يغير الطريقة التي يتفاعل بها الناس ويمارسون أنشطتهم وحرياتهم. في حين أن المفهوم الكلاسيكي للسيادة، في القانون الدستوري، يوضع على المحك، حيث تدعي بعض الدول السيادة الرقمية المقدمة على أنها ضرورية للدفاع عن مصالحها الأساسية. وتتزايد هذه المخاوف بسبب العيوب في نظام إدارة المساحات الرقمية، وعودة التهديدات الأمنية، والاستغلال المتزايد للبيانات الشخصية،

وظهور الشركات متعددة الجنسيات التي تؤكد نفسها دون مشاركة العالم. لكن مفهوم السيادة الرقمية، بأبعاده المتعددة، القانونية والتقنية، والجماعية والفردية، والحكومية، والوطنية والدولية، يلتقي في العديد من المعاني الأخرى ويثير قضايا مختلفة، للدول والأفراد والفاعلين الاقتصاديين والمستخدمين[15]. كما أنه لم تؤد هذه الأزمة الصحية إلا إلى إبراز ملامح النظام العالمي الرقمي الجديد، ولا تزال الصين والولايات المتحدة بطليهما الرئيسيين. في الوقت الذي تسعى فيه أوروبا إلى أن تقدم لنفسها مكانًا للاختيار في هذا النظام الجديد، من خلال تعزيز ترسانتها القانونية ومن خلال منح نفسها الوسائل لتعزيز سيادتها الرقمية. كما ستسمح البيانات، وهي مورد أساسي في عالمنا الرقمي، لسوق البيانات الضخمة بالوصول إلى ما لا يقل عن 68 مليار دولار في عام 2021، إذا اتبعنا هذا التنبؤ من قبل شركة Gartner. ومع ذلك، لكي نعطي أوروبا قيمتها "الحقيقية"، يجب ألا ننسى أن القارة العجوز هي السوق العالمية الثانية بعد الولايات المتحدة، بأكثر من 746 مليون نسمة و 22٪ من الناتج المحلي الإجمالي العالمي[16].

وفي رأي العديد من المتخصصين، خضع المغرب لأول اختبار رقمي في عام 2020. في هذه المرحلة، ما زلنا لا نملك جردا تفصيليا لمختلف القرارات الاستراتيجية المتخذة، والتقدم المحرز والقيود التي واجهتها المملكة. أكبر فائدة مستمدة من هذه الأزمة عبر عنها وزير الصناعة والتجارة والاقتصاد الأخضر والرقمي، حيث أكد على أنه: "مع هذه الأزمة الوبائية، اكتسب المغرب 5 سنوات من التطور الرقمي"[17]. يجسد هذا التحول نحو الرقمنة ظهور أجيال جديدة من أنماط الحوكمة لتقديم خدمات أفضل للمواطنين. وبالتالي، فإن انتشار البرامج الرقمية وإنشاء العديد من الشركات الناشئة المبتكرة يبرهن على مدى فاعلية التكنولوجيا الرقمية في المغرب وفي إفريقيا على الوجه العموم. حيث تبدو النظرة المستقبلية في هذا المجال الآن واعدة بالنسبة لأفريقيا، بشرط أن يتم دعم هذا التوسع، على وجه الخصوص، من خلال التشريعات المناسبة، والبنية التحتية المناسبة، وتشجيع نشر الأدوات الرقمية والترويج لاستخدامها من أجل الساكنة، ومواءمة المشاريع العامة المختلفة ذات الصلة بمجال التقنيات الجديدة. كما يتعلق الأمر أيضا بتشجيع نشاط ريادة الأعمال في المجال الرقمي، والتدريب المخصص للجهات الفاعلة في الاقتصاد الرقمي وتصميم وتنفيذ المشاريع الإدارية[18].

المبحث الثالث

السيادة الرقمية بالمغرب

أولاً- ممكنات السيادة الرقمية بالمغرب

لقد أظهرت أزمة كوفيد -19 الدور الحاسم للرقمنة في استمرارية أنشطة المواطنين والشركات والدولة. وفي العمل عن بعد والتعليم والأنشطة الاقتصادية والخدمات الطبية عالية الجودة ... كلها أنشطة تتطلب اليوم أن تكون متصلا[19].

[15] - Pauline Türk, Christian Vallar : La souveraineté numériqueLe concept, les enjeux : https://univ-droit.fr/recherche/actualites-de-la-recherche/parutions/25529-la-souverainete-numerique

[16] - Agathe Nageotte; Digital Sovereignty and Economic Growth : https://www.oodrive.com/blog/regulation/digital-sovereignty-and-economic-growth/

[17] -https://www.lavieeco.com/economie/pour-une-resilience-numerique-durable/

[18]-https://www.lereporter.ma/maroc-afrique-la-transformation-digitale-pour-le-developpement-durable/

[19] - Andreas Aktoudianakis : Fostering Europe's Strategic Autonomy, Digital sovereignty for growth, rules and cooperation; December 2020:
https://www.epc.eu/content/PDF/2020/Digital_SA_paper_EPC_and_KAS.pdf

وبهذا المعنى، يوصي تقرير اللجنة الخاصة المعنية بالنموذج التنموي بفهم التكنولوجيا الرقمية باعتبارها وسيلة للتغيير المستمر، حيث يجب العمل على جعل الرقميات والقدرات التكنولوجية عاملا أساسيا في التنافسية وتحديث المقاولات وتطوير مهن وقطاعات جديدة تتماشى والتحولات العالمية. حيث تعد البنية التحتية الرقمية وقدرات اعتماد التكنولوجيات الرقمية محددات مهمة لتنافسية أي بلد، بالنظر للمكانة المتنامية للتكنولوجيات الجديدة ضمن جميع قطاعات الاقتصاد، وهو ما يتطلب خدمات رقمية موثوقة وذات جودة. ويمر تعزيز تنافسية الاقتصاد المغربي عبر مقاربة إرادية وحثيثة من أجل تعميم الولوج إلى الانترنت ذي الصبيب العالي في جميع جهات المملكة، وإلى الانترنت ذي الصبيب العالي جدا في مناطق الأنشطة الاقتصادية المكثفة. وينبغي أن يكون تأهيل البنية التحتية الرقمية مصحوبا بعملية تحسين سريعة للقدرة على استخدام التكنولوجيات الجديدة، بصفة خاصة، وذلك من خال تكثيف عروض التكوين في مجال المهارات الرقمية والذكاء الاصطناعي وتسريع االإستراتيجية الوطنية للإدماج المالي عبر المالية الرقمية ومواكبة الرقمنة الداخلية للمقاولات بالإضافة إلى ضرورة مواكبة المقاولات الناشئة[20].

وفي جانب السيادة الرقمية، يوصي تقرير اللجنة الخاصة بالنموذج التنموي على استكمال الإطار القانوني الهادف إلى ضمان الثقة الرقمية للمستعملين والسيادة الرقمية للمملكة. وفي هذا الصدد، يجب تسريع وتيرة إنتاج النصوص القانونية والمراسيم التطبيقية المتعلقة بالجرائم الإلكترونية والملكية الفكرية وتدبير المعطيات الشخصية، وكذا وضع إطار مؤسساتي يضمن الاعتراف القانوني الكامل بالتفاعلات الرقمية والقيمة القانونية للوثائق الرقمية من خلال التوقيع الإلكتروني والتعريف الرقمي الموحد للمواطن، مع الحرص التام على احترام الضمانات المتعلقة بحماية المعطيات الشخصية[21].

وهنا، لابد من التطرق لوكالة التنمية الرقمية بالمغرب المعروفة اختصارا ب(l'Agence de développement du digital (ADD))، وهي مؤسسة استراتيجية تتمتع بالشخصية الاعتبارية والاستقلال المالي، ثم إحداثها بموجب القانون رقم61.16، الصادر بالجريدة الرسمية رقم 6604 بتاريخ 14 شتنبر2017. تسهر هذه الوكالة، التي تخضع لوصاية السلطة الحكومية المكلفة بالاقتصاد الرقمي، على تنفيذ استراتيجية الدولة في مجال التنمية الرقمية وتشجيع نشر الوسائل الرقمية وتطوير استخدامها بين المواطنين.تتولى وكالة التنمية الرقمية مجموعة من المهام التي تهدف إلى هيكلة المنظومة الرقمية والعمل على خلق فاعلين متميزين في الاقتصاد الرقمي. كما تهدف إلى تشجيع الإدارة الرقمية عبر تقريبها للمرتفقين (المواطنين والمقاولات) مع وضع الأطر المرجعية للمنتوجات والخدمات الرقمية. هذا بالإضافة إلى التقليص من الهوة الرقمية ودعم الثورة الصناعية 4.0، والقيام بإدارة التغيير للمجتمع من خلال التكوين والتحسيس. كما تعمل الوكالة على تشجيع البحث والتطوير والحث على الابتكار الاجتماعي والمقاولاتي وضمان شمول رقمي مسؤول ومستدام[22].

بالإضافة إلى ذلك، قامت وكالة التنمية الرقمية بوضع مشروع إنشاء مركز رقمي تفاعلي في المغرب (IDC Morocco) عبارة عن أكاديمية مبتكرة لتدريب ونشر مهن الاقتصاد الرقمي، وخاصة تكنولوجيا الواقع الافتراضي والمدمج (RVA). ويأتي هذا المشروع في إطار شراكة بين القطاعين العام والخاص، وذلك بين وكالة التنمية الرقمية، وجامعة محمد السادس المتعددة

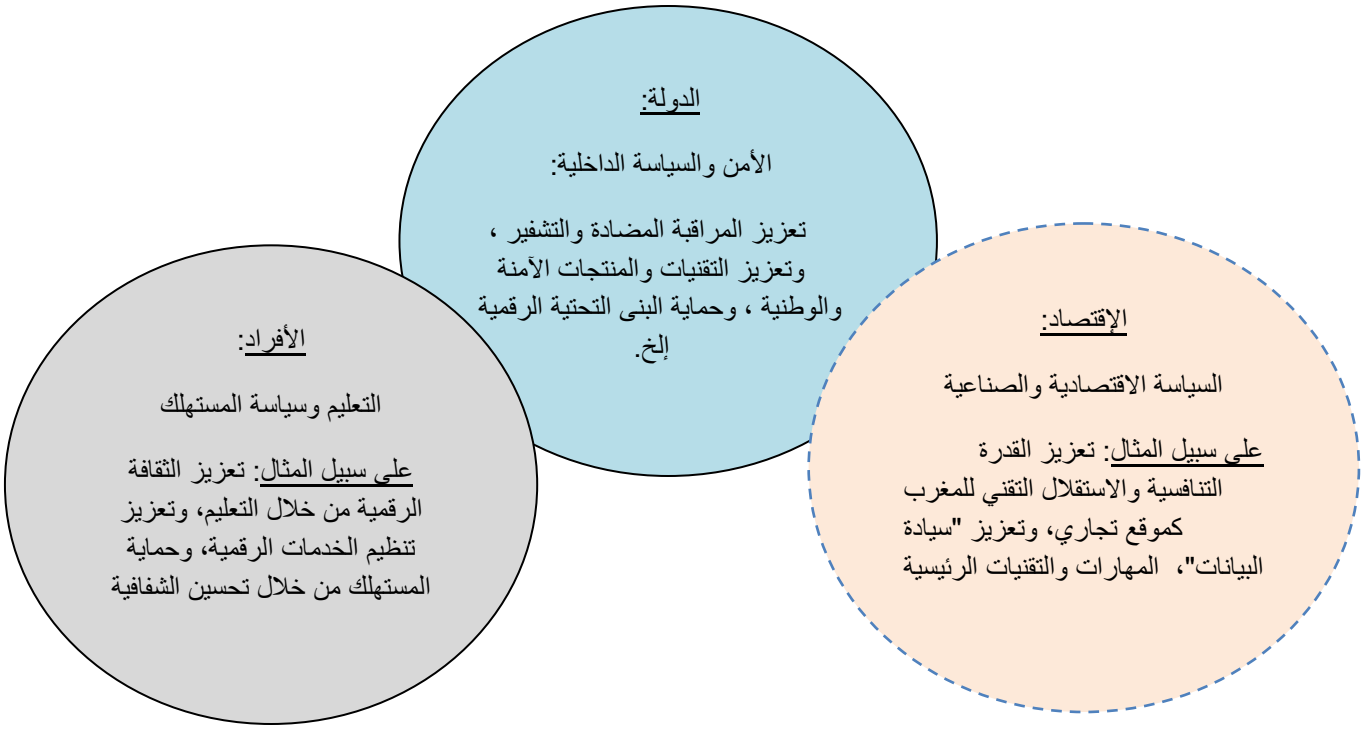
[20]– النموذج التنموي الجديد: تحرير الطاقات واستعادة الثقة لتسريع وتيرة التقدم وتحقيق الرفاه للجميع،التقرير العام، أبريل 2021، ص 86:
https://www.csmd.ma/documents.العام_التقرير/pdf

[21]– النموذج التنموي الجديد: تحرير الطاقات واستعادة الثقة لتسريع وتيرة التقدم وتحقيق الرفاه للجميع، مرجع سابق، ص 136.

[22]– للمزيد ينظر: الموقع الرسمي لوكالة التنمية الرقمية على الرابط التالي:
https://www.add.gov.ma

التقنيات، ووكالة الولايات المتحدة للتنمية الدولية «USAID»، ووزارة الصناعة والتجارة والاقتصاد الأخضر والرقمي، ووزارة التربية الوطنية والتكوين المهني والتعليم العالي والبحث العلمي وجامعة محمد الخامس بالرباط، و الشركة العالمية EON Reality . ويسمح المركز الرقمي التفاعلي (IDC Morocco)، الذي تم تدشينه في 11 فبراير 2020، بتطوير حلول نقل المعرفة في مجال تكنولوجيا الواقع المدمج (AR) والواقع الافتراضي (VR) لمختلف برامج التربية الأكاديمية والتكوين المهني من أجل المساهمة في تنمية المهارات اللازمة للصناعات من جيل 4.0 وتوسيع الاقتصاد الرقمي على الصعيدين الوطني والإقليمي. وبالإضافة إلى ذلك، يقدم هذا المركز تكوينا للمغاربة الشباب في تقنيات برمجة التطبيقات المتعلقة بالواقع الافتراضي والمدمج (RVA) في مجالات التعليم والتكوين المهني لكي يصبحوا خبراء مستقبليين في هذا المجال.ونتيجة لذلك، يساعد المشروع على معالجة النقص في المهارات في المغرب وشمال أفريقيا بتوفير حلول تعليمية مبتكرة ومنخفضة التكلفة لتنمية قدرات الطلاب والمهنيين. وبذلك سيساعد هذا البرنامج في مكافحة البطالة بين الشباب، وتعزيز روح المقاولة في القطاع الرقمي، وكذا الزيادة من الإنتاجية الصناعية. وسيمتد هذا المشروع على فترة خمس سنوات، يتم احتضانه خلالها من طرف جامعة محمد السادس المتعددة التخصصات التقنية في بنجرير، بمشاركة استباقية من جميع شركاء المشروع. وفي مرحلة التوسع، من المتوخى إنشاء مراكز فرعية لتلبية احتياجات المستفيدين في بعض الجهات[23]. ويمكن القول في هذا الجانب، بأنه لازلنا في بداية التحول نحو الرقمنة وليس تحقيق السيادة الرقمية. لذلك فتحقيق السيادة الرقمية يتطلب الانضباط لأبعاد السيادة الرقمية ومجالات تطبيقها حسب ما يمثلها الشكل أسفله[24]:

السيادة الرقمية



[23]- للمزيد من المعلومات ينظر: المركز الرقمي التفاعلي- بنجرير (IDC)، الموقع الرسمي لوكالة التنمية الرقمية:
https://www.add.gov.ma/المركز-الرقمي-التفاعلي-بنجرير-idc

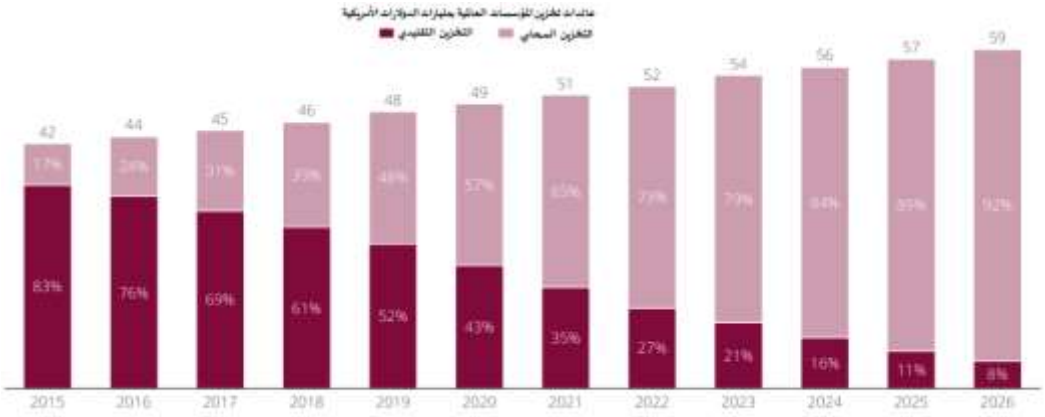
[24] - Julia Pohle : Digital sovereignty A new key concept of digital policy in Germany and Europe :
https://www.kas.de/documents/252038/7995358/Digital+sovereignty.pdf/a8d0cb4b-c777-3e72-1bc7-b5fda656329a?version=1.0&t=1608034389334

يواجه القطاع العام حاليا تحديا كبيرا يكمن في: تمكين المواطنة النشطة، وزيادة كفاءة تقديم الخدمات، وتسهيل النمو الاقتصادي الشامل والتحول، والقيام بذلك بشكل فعال من حيث التكلفة وآمن بموارد محدودة. لمواجهة هذه التحديات وكذلك مكافحة الاحتيال والفساد، تتوخى الحكومة المغربية نظاما بيئيا من الشبكات والخدمات والتطبيقات والمحتوى والأجهزة الرقمية التي ستربط الإدارة العامة بالمواطن النشط، وتعزز النمو الاقتصادي والتنمية والقدرة التنافسية، ودعم التكامل المحلي والوطني والإقليم.

ستكون الخدمات السحابية (Cloud) في طليعة التحول الرقمي للحكومة. يمكن أن توفر السحابة وصولا فعالا من حيث التكلفة إلى قوة غير مسبوقة لمعالجة كميات كبيرة من البيانات وتحليلها بسرعة لإنتاج تحليلات قابلة للتنفيذ ورؤى وقرارات أفضل. يوفر تخزين البيانات الذي يمكن الوصول إليه بسهولة وقنوات الوصول والاتصال المتعددة تجربة حديثة ومتسقة وشفافة للمسؤولين وكذلك الجمهور، مما يسهل المشاركة العامة والحوكمة التعاونية بالإضافة إلى التعاون بين الوزارات وتوسيع الإدماج الاجتماعي.

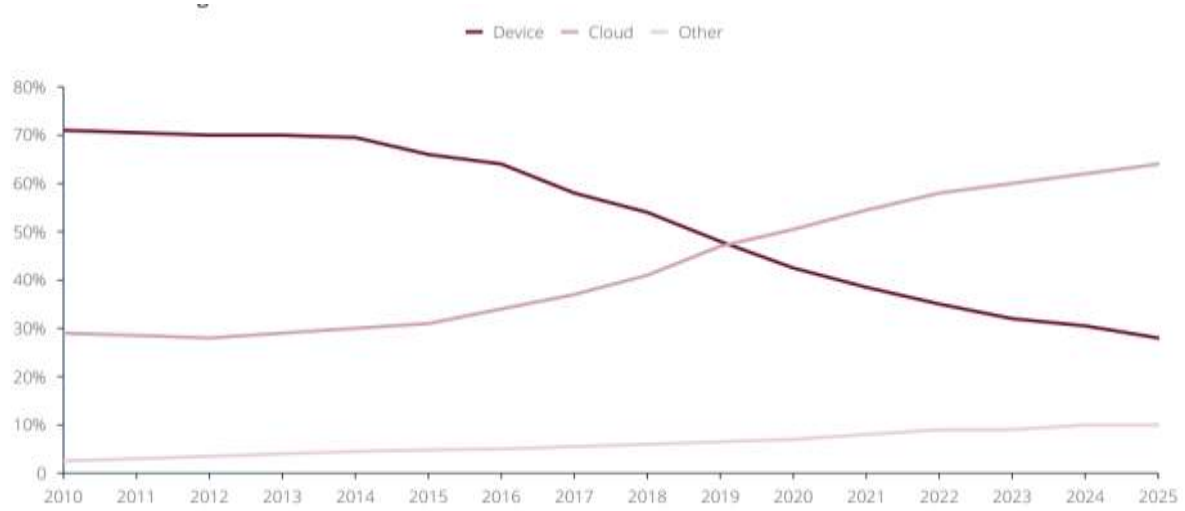
ويمكن تعريف الحوسبة السحابية على أنها "توريد واستخدام وفوترة خدمات تكنولوجيا المعلومات التي تتكيف ديناميكيا مع الطلب وتسليمها من خلال شبكة". وهي تشمل، من بين أشياء أخرى، البنية التحتية (مثل سعة المعالجة ومساحة التخزين) والأنظمة الأساسية والبرامج. مع تقارب الحوسبة السحابية مع إنترنت الأشياء و5G، سيحدث تحول نموذجي، حيث سيتم إنشاء ومعالجة كميات متزايدة من البيانات (بسبب الاحتياجات في الوقت الفعلي أو حماية الملكية الفكرية و/ أو البيانات) على أساس لامركزي.

إن تحسين التكلفة وأمن البيانات وإمكانات الحكومة المفتوحة التي أصبحت ممكنة بفضل الخدمات السحابية أفضل بكثير من العمليات الورقية اليدوية. ومع ذلك، في صناعة شديدة التنظيم مثل القطاع العام، من الضروري التأكد من أن أي انتقال إلى "السحابة" يتوافق مع اللوائح المعمول بها ويحقق الفوائد الواضحة دون مخاطر لا داعي لها .ويمثل الشكل التالي إيرادات تخزين بيانات المؤسسات العالمية حسب نوع التخزين العادي أو السحابي، كما أن الشكل يؤكد بما لا يدع مجالا للشك أن التخزين التقليدي سيكون متجاوزا قريبا:

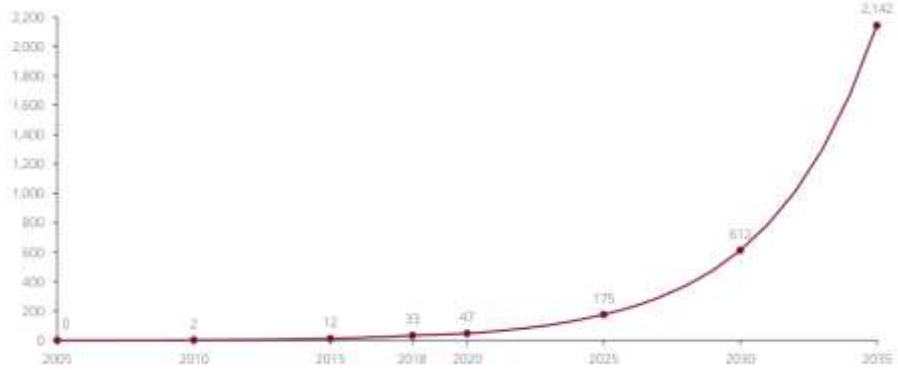


المصدر: Statista

وما يؤكد على أن الحلول السحابية هي الحل لمشكلة تخزين البيانات، المبيان التالي الذي يوضح التطور الملحوظ في التخزين السحابي:

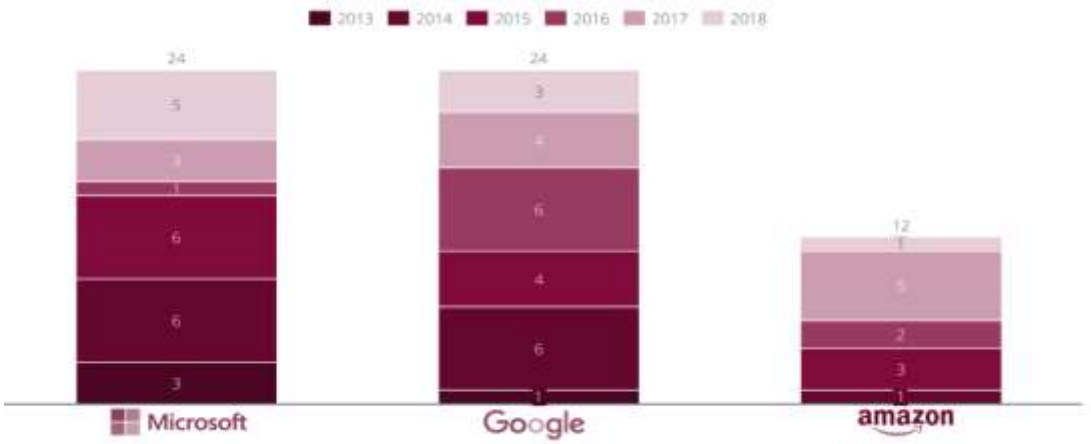


ومن المتوقع أن يتجاوز التخزين السحابي آلية التخزين بالجهاز (أي التخزين المحلي في أجهزة الكمبيوتر والأجهزة) وأن يصبح حل تخزين البيانات الرائد في العالم في عام 2020. ويدعو البعض إلى إنشاء تخزين سحابي مثلا أوروبي وبنية تحتية للبيانات لتعزيز سيادة البيانات في أوروبا والعنوان حقيقة أن التخزين السحابي وسوق البيانات يهيمن عليه اليوم موردون غير أوروبيين بشكل حصري تقريبا، مما قد يكون له عواقب سلبية على أمن وحقوق المواطنين الأوروبيين. حيث تم الإعلان عن مشروع Gaia–X، وهو مبادرة أوروبية في الحوسبة السحابية، بالاشتراك بين ألمانيا وفرنسا ويقترح إنشاء بنية تحتية للبيانات الموحدة على المستوى الأوروبي اعتبارا من عام 2020. هذه أداة مهمة في ضمان بيئة آمنة لبيانات المواطنين والشركات والحكومات. تماشيا مع استراتيجية البيانات الأوروبية، يمكن اقتراح المزيد من الإجراءات على مستوى الاتحاد الأوروبي لدعم تنفيذ البنية التحتية السحابية على مستوى الاتحاد الأوروبي (على سبيل المثال، وضع معايير سحابية مشتركة، وبنية مرجعية ومتطلبات التشغيل البيني). كما أنه يتم إنشاء كمية هائلة من البيانات وتخزينها كل عام، وتستمر في النمو. بحلول عام 2024، تشير التقديرات إلى أنه سيتم إنشاء ونسخ واستهلاك 149 زيتابايت من البيانات على مستوى العالم. في حال كنت تتساءل عن حجم زيتابايت، أي 1,000,000,000,000,000,000,000 (زيتابايت واحد يساوي مليار تيرابايت بايت من المعلومات). يمكنك استخدام 10 بايت من البيانات في كلمة واحدة مكتوبة. لذلك، فكمية البيانات التي تم إنشاؤها تنمو باطراد، الأمر الذي ويتطلب حلول تخزين بيانات أكثر وأفضل. الأمر الذي يؤكده المبيان التالي المقدار العالمي للبيانات التي يتم إنشاؤها سنويا بمقدار زيتابايت :



المصدر : Statista

كما يبين الشكل التالي أن مايكروسوفت وجوجل تجاوزت أمازون بعمليات استحواذ ضخمة على القطاع السحابي (Cloud sector):



المصدر: Statista

كما تشير التقديرات إلى أن 92٪ من جميع البيانات في العالم الغربي مخزنة على خوادم مملوكة للولايات المتحدة الأمريكية. يتضمن ذلك مجموعة شاملة من الأنشطة عبر الإنترنت والمتصلة، من البيانات الحكومية الإقليمية والوطنية وصولا إلى وسائل التواصل الاجتماعي. وهذه بعض الأسباب التي تجعل الشركات تستخدم الخدمات السحابية:

المصدر: Statista

ثانيا– سيادة الأمن السيبراني بالمغرب

تجدر الإشارة في الأول، إلى أن المغرب تم تصنيفه في التقرير الدولي حول الأمن السيبراني الصادر عن الاتحاد الدولي للاتصالات (ITU)، في الرتبة 50 من بين 182 دولة شملها هذا الجرد، والرتبة 7 عربيا خلف كل من السعودية أولا، والإمارات

العربية التحدة ثانيا، وسلطنة عمان ثالثا، ومصر رابعا، وقطر خامسا، وتونس سادسا، وهذا الترتيب هو إشارة على أن الأمن السيبراني بالمملكة المغربية تعتريه مجموعة من التحديات وجب ربحها في قادم السنوات[25].

ففي سنة 2013، دخل حيز التنفيذ القانون رقم 75.12 المتعلق بالمصادقة على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات[26]، بالإضافة إلى القانون رقم 46.13 بالمصادقة على الاتفاقية الأوروبية 108 المتعلقة بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي[27]، وأيضا القانون رقم 136.12 بالمصادقة على الاتفاقية الأوروبية 185 المتعلقة بمكافحة الجرائم الإلكترونية الموقعة ببودابست في 23 نوفمبر 2001 وعلى البروتوكول الإضافي لهذه الاتفاقية، الموقع بستراسبورغ في 28 يناير 2003 (مادة فريدة)[28]، حيث تهدف هذه الاتفاقية وبروتوكولها الإضافي إلى مواصلة سياسة جنائية مشتركة تروم حماية المجتمع من الجرائم المعلوماتية، خاصة باعتماد التشريعات المناسبة وتعزيز التعاون الدولي، وتعد هذه الاتفاقية أول معاهدة دولية تتعلق بالجرائم الجنائية المرتكبة عبر الأنترنت والشبكات المعلوماتية الأخرى.

زيادة على القرار رقم 14/3 بخصوص تطبيق التوجيهات العامة لأمن نظم المعلومات (DNSSI)، والقانون رقم 132.13 بالمصادقة على البروتوكول الإضافي للاتفاقية رقم 108 لمجلس دول أوروبا المتعلقة بحماية الأشخاص تجاه معالجة المعطيات ذات الطابع الشخصي، كما صدر مرسوم رقم 2.15.712 بتاريخ2016/03/22 بتحديد إجراءات حماية نظم المعلومات الحساسة للبنيات التحتية ذات الأهمية الحيوية، والمرسوم مرسوم رقم 2.11.508 بتاريخ 2011/10/21 يحدث بموجبه اللجنة الاستراتيجية لأمن نظم المعلومات، ومنشور رئيس الحكومة رقم 2014/3 بتاريخ 2014/03/10 في موضوع تطبيق التوجهات الوطنية لأمن نظم المعلومات.

بالإضافة إلى اللجنة الاستراتيجية لأمن نظم المعلومات الصارة بموجب المرسوم رقم 508-11-2والي تهدف إلى:

-تحديد التوجهات الإستراتيجية؛

-السيادة الرقمية؛

-ضمان مرونة نظم المعلومات في الحكومة والمؤسسات العامة والبنية التحتية الحيوية.

وأيضا، المديرية العامة لأمن نظم المعلومات الصادرة بموجب المرسوم رقم 509-11-2 والتي تتحدد توجهاتها وأهدافها في:

-وضع استراتيجية الأمن السيبراني الوطنية؛

-ترخيص لمقدمي خدمات التوقيع الالكتروني وأدوات التشفير والمصادقة الإلكتروني.

إلى جانب إنشاء كل من المركز الوطني للتنسيق والاستجابة لحوادث أمن المعلومات (MA-CERT)، والهيئة الوطنية لحماية المعطيات ذات الطابع الشخصي.

---

[25]- الأمن السيبراني.. المغرب في المركز 50 عالميا، موقع SNRT News:

https://snrtnews.com/article/الأمن-السيبراني-المغرب-في-المركز-50-عالميا

[26]- ظهير شريف رقم 1.13.46 صادر في فاتح جمادى الأولى 1434 (13 مارس 2013)بتنفيذ القانون رقم 75.12 الموافق بموجبه على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، الموقعة بالقاهرة في 21 ديسمبر 2010، الجريدة الرسمية عدد 6140 الصادرة بتاريخ 23 جمادى الأولى 1434 (4 أبريل 2013).

[27]- ظهير شريف رقم 1.14.150 صادر في 25 من شوال 1435(22 أغسطس 2014) بتنفيذ القانونرقم 46.13 الموافق بموجبه على الاتفاقية الأوروبية رقم 108 المتعلقة بحماية الأشخاص الذاتيين تجاه المعالجة الآلية للمعطيات ذات الطابع الشخصي، الموقعة بستراسبورغ في 28 يناير 1981، الجريدة الرسمية عدد 6292 الصادرة بتاريخ 22 ذو القعدة 1435 (18 سبتمبر 2014).

[28]- ظهير شريف رقم 1.14.85 صادر في 12 من رجب 1435 (12 ماي 2014) بتنفيذ القانون رقم 136.12 الموافق بموجبه على اتفاقية الجرائم المعلوماتية، الموقعة ببودابست في 23 نونبر 2001 وعلى البروتوكول الإضافي لهذه الاتفاقية، الموقعة باستراسبورغ في 28 يناير 2003.، جريدة رسمية عدد 6260 بتاريخ 29 رجب 1435 (29 ماي 2014).

بالإضافة إلى التنصيص على القانون رقم 05.20 المتعلق بالأمن السيبراني[29]، الذي يهدف إلى إنشاء إطار قانوني يسمح بتعزيز أمن أنظمة المعلومات في إدارات الدولة والجماعات الترابية والمؤسسات والمقاولات العمومية، وكل شخص اعتباري آخر يدخل في حكم القانون العام. وبموجب هذا القانون الذي أعدته إدارة الدفاع الوطني، سيتم إحداث لجنة إستراتيجية للأمن السيبراني ولجنة تابعة لها لإدارة الأزمات والأحداث السيبرانية الجسيمة، إضافة إلى السلطة الوطنية للأمن السيبراني.

وإحداث اللجنة الوطنية لمراقبة حماية المعطيات ذات الطابع الشخصي بمقتضى القانون 08-09 الصادر في 18 فبراير 2009 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي[30]. حيث تضطلع اللجنة بمهمة التحقق من أن عمليات معالجة المعطيات الشخصية تتم بشكل قانوني وأنها لا تمس بالحياة الخاصة أو بحقوق الإنسان الأساسية أو بالحريات. تتشكل اللجنة من شخصيات تتمتع بالحياد والنزاهة وتمتلك كفاءة في الميادين القانونية والقضائية وفي مجال المعلوميات.

مناقشة النتائج

لقد ظهر مفهوم "السيادة الرقمية" في السنوات الأخيرة، على الرغم من أن معناه لا يزال مشتتا، بين الاستحواذ التكنولوجي الصيني والنموذج الأمريكي لرأسمالية المراقبة. وفي الآونة الأخيرة، أظهرت عمليات الإغلاق خلال وباء Covid-19 أن العديد من الدول يمكن أن تكون في وضع أفضل من حيث البنية التحتية الرقمية، على سبيل المثال عندما يتعلق الأمر بالتوزيع غير المتكافئ لسرعة الأنترنت أو عرض التعليم الرقمي. كانت قيود التنقل الضرورية المفروضة على الأشخاص خلال الوباء حافزًا لتطوير البنية التحتية الرقمية ، وقد كشف الوباء عن أهمية البنية التحتية للاتصالات بالنسبة للمواطنين.

السيادة الرقمية ليست مرادفا للحمائية ولكنها "تصف قدرة الأفراد والمجتمع على تشكيل التحول الرقمي بطريقة يحددونها بأنفسهم". فالابتكار التكنولوجي يجب أن يكون في خدمة الإنسانية، وليس العكس وأن الالتزام بإنترنت عالمي مشترك وحر ومفتوح وآمن هو في الواقع تعبير عن السيادة. تعطي فالسيادة الرقمية يجب أن تكون ذات بعد إنساني، فالإنترنت لا يمكن ولا ينبغي أن تتشكل من قبل الدول والحكومات فقط، لأنها تهمنا جميعا، وبالتالي يجب أن يشارك الناس ويتحكمون في بياناتهم.

من وجهة النظر هذه، يتم ترقية الفرد إلى مرتبة السيادة، والسيطرة الديمقراطية من قبل الفرد تتعارض مع تركيز السلطة، سواء من قبل الحكومات أو الشركات. فكلما زادت الكفاءة الرقمية للفرد، زادت قدرته على المساهمة في تقرير المصير المعلوماتي الخاص به، وهو شرط أساسي للأشخاص الذين يساعدون في تشكيل العالم الرقمي.

[29]- ظهير شريف رقم 69.20.1 صادر في 4 ذي الحجة 1441(25 يوليو 2020) بتنفيذ القانون رقم 20.05 المتعلق بالأمن السيبراني، جريدة رسمية عدد 6904 بتاريخ 9 ذو الحجة 1441 (30 يوليو 2020).

[30]- ظهير شريف رقم 1.09.15 صادر في 22 من صفر 1430 (18 فبراير 2009) القاضي بتنفيذ القانون رقم 09.08 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي، جريدة رسمية عدد 5711 بتاريخ 27 صفر 1430 (23 فبراير 2009).

قائمة المراجع

أولاً- المراجع بالعربية

- التقرير الخاص بالنموذج التنموي:

https://www.csmd.ma/rapport

-وكالة التنمية الرقمية بالمغرب:

https://www.add.gov.ma-المركز-الرقمي-التفاعلي-بنجرير/idc

- ظهير شريف رقم 1.13.46 صادر في فاتح جمادى الأولى 1434 (13 مارس 2013)بتنفيذ القانون رقم 75.12 الموافق بموجبه على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، الموقعة بالقاهرة في 21 ديسمبر 2010، الجريدة الرسمية عدد 6140 الصادرة بتاريخ 23 جمادى الأولى 1434 (4 أبريل 2013).

- ظهير شريف رقم 1.14.150 صادر في 25 من شوال 1435(22 أغسطس 2014) بتنفيذ القانونرقم 46.13 الموافق بموجبه على الاتفاقية الأوروبية رقم 108 المتعلقة بحماية الأشخاص الذاتيين تجاه المعالجة الآلية للمعطيات ذات الطابع الشخصي، الموقعة بستراسبورغ في 28 يناير 1981، الجريدة الرسمية عدد 6292 الصادرة بتاريخ 22 ذو القعدة 1435 (18 سبتمبر 2014).

- ظهير شريف رقم 1.14.85 صادر في 12 من رجب 1435 (12 ماي 2014) بتنفيذ القانون رقم 136.12 الموافق بموجبه على اتفاقية الجرائم المعلوماتية، الموقعة ببودابست في 23 نونبر 2001 وعلى البروتوكول الإضافي لهذه الاتفاقية، الموقعة باستراسبورغ في 28 يناير 2003.، جريدة رسمية عدد 6260 بتاريخ 29 رجب 1435 (29 ماي 2014).

- ظهير شريف رقم 69.20.1 صادر في 4 ذي الحجة 1441(25 يوليو 2020) بتنفيذ القانون رقم 20.05 المتعلق بالأمن السيبراني، جريدة رسمية عدد 6904 بتاريخ 9 ذو الحجة 1441 (30 يوليو 2020).

- ظهير شريف رقم 1.09.15 صادر في 22 من صفر 1430 (18 فبراير 2009) القاضي بتنفيذ القانون رقم 09.08 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي، جريدة رسمية عدد 5711 بتاريخ 27 صفر 1430 (23 فبراير 2009).

ثانياً- المراجع بالإنجليزية

– Milton Mueller, Will the Internet Fragment?: Sovereignty, Globalization and Cyberspace (Cambridge, UK ; Malden, MA: Polity, 2017).

– Jean-François Husson and Robin Reda, “Traçage numérique : « Le moment est venu d’établir notre souveraineté numérique »,” Le Monde.fr, April 25, 2020, https://www.lemonde.fr/idees/article/2020/04/25/tracage-numerique-le-moment-est-venu-d-etablir-notre-souverainete-numerique_6037729_3232.html.

– Jonathan A. Obar and Andrew Clement, “Internet Surveillance and Boomerang Routing: A Call for Canadian Network Sovereignty,” SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, July 1, 2013), https://papers.ssrn.com/abstract=2311792.

– CSAN 2020, p. 18, with reference to the 2019 Annual Report 2019 of the Dutch General Intelligence and Security Services(AIVD), April 2020.
– Des Data Center pour atteindre la souveraineté numérique:
– https://aujourdhui.ma/economie/des-data-center-pour-atteindre-la-souverainete numerique?fbclid=IwAR1SWgfjYapyQvcBLroe5oawgjPdDDbv0RnlFeSAnNS87HVNGaNF491Y4Vo
– –Stéphane Couture and Sophie Toupin, "What Does the Notion of 'Sovereignty' Mean When Referring to the Digital?," New Media & Society 21, no. 10 (October 1, 2019): 2305–22:
– https://doi.org/10.1177/1461444819865984.
– –John Perry Barlow, "A Declaration of the Independence of Cyberspace," February 8, 1996:
– https://www.eff.org/fr/cyberspace-independence.
– – J John Perry Barlow, "A Declaration of the Independence of Cyberspace," February 8, 1996:
– https://www.eff.org/fr/cyberspace-independence.
– – Milton Mueller, Will the Internet Fragment?: Sovereignty, Globalization and Cyberspace (Cambridge, UK ; Malden, MA: Polity, 2017).
– – Jonathan A. Obar and Andrew Clement, "Internet Surveillance and Boomerang Routing: A Call for Canadian Network Sovereignty," SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, July 1, 2013):
– https://papers.ssrn.com/abstract=2311792.
– – Tung-Hui Hu, A Prehistory of the Cloud (Cambridge, Massachusetts: The MIT Press, 2015):
– https://mitpress.mit.edu/prehistory-cloud.
– – Marisa Elena Duarte, Network Sovereignty: Building the Internet across Indian Country (Seattle, WA: University of Washington Press, 2017).
– – Julian Gill-Peterson, "Sexting Girls: Technological Sovereignty and the Digital," Women & Performance: A Journal of Feminist Theory 25 (July 13, 2015): 143–56 :
– http://www.tandfonline.com/doi/full/10.1080/0740770X.2015.1057010.
– – OECD Policy Responses to Coronavirus (COVID-19), Keeping the Internet up and running in times of crisis, Updated 4 May 2020:
– https://www.oecd.org/coronavirus/policy-responses/keeping-the-internet-up-and-running-in-times-of-crisis-4017c4c9/

– – Digital Transformation in the Age of COVID-19 BUILDING RESILIENCE AND BRIDGING DIVIDES, DIGITAL ECONOMY OUTLOOK 2020 SUPPLEMENT:
– https://www.oecd.org/digital/digital-economy-outlook-covid.pdf
– – Marie Baezner et Patrice Robin: Trend Analysis: Cyber Sovereignty and Data Sovereignty, May 2018:
– https://www.researchgate.net/publication/325335882
– – Pauline Türk, Christian Vallar : La souveraineté numériqueLe concept, les enjeux : https://univ-droit.fr/recherche/actualites-de-la-recherche/parutions/25529-la-souverainete-numerique
– –Agathe Nageotte; Digital Sovereignty and Economic Growth : https://www.oodrive.com/blog/regulation/digital-sovereignty-and-economic-growth/
– – Andreas Aktoudianakis : Fostering Europe's Strategic Autonomy, Digital sovereignty for growth, rules and cooperation; December 2020:
– https://www.epc.eu/content/PDF/2020/Digital_SA_paper_EPC_and_KAS.pdf