السـيادة الرقميـة للدول من منضور القانون الدستوري

م. د. سلام صالح خميس
جامعة بغداد/ كلية الطب

Digital sovereignty of states from the perspective of constitutional law

DR. Salam Salih KHamees
Baghdad University/ College of Medicine
s.s.khamees1986@gmail.com

المستخلص:

نتيجة التطور التكنولوجي المتقدم، حدثت تغييرات كبيرة على المفهوم التقليدي للسيادة الوطنية، انعكس على أثر هذه التغييرات انصهار الحدود الجغرافية للدول كافة، مما شعرت هذه الدول بهاجس أمني كبير خوفًا على قرصنة ثروتها الرقمية، خاصة وإن جميع البيانات والمعلومات التي تمتلكها تضعها في بيئة رقمية، استتبع ذلك قيام معظم الدول في سبيل الدفاع عن سيادتها الرقمية صياغة نصوص تشريعية وتأسيس مؤسسات تختص بالدفاع عن امن البيانات والمعلومات التي تمتلكها، مما برز ما يسمى بسر الدفاع عن السيادة الرقمية الوطنية للدول.

Abstract:

As a result of advanced technological development, major changes have occurred in the traditional concept of national sovereignty, which has reflected the melting of the geographical borders of all countries, which has made all countries feel a great security concern for their digital wealth, especially since all the data and information they possess are placed in a digital environment. This has led most countries, in order to defend their digital sovereignty, to formulate legislative texts and establish institutions specialized in defending the security of the data and information they possess, which has led to the emergence of what is called the secret of defending the national digital sovereignty of countries.

المقدمة

شهدت البشرية ثورات عدة، ومن بينها الثورة المعلوماتية التي قامت على أساس الحواسيب الالية وشبكات الانترنت، مما سارعت العديد من الدول إلى تخزين اسرار الدفاع عن سيادتها بهيئة رقمية، تتخذ من الوسائط الالكترونية وسائل لمعالجة وحماية هذه الاسرار.

ونظرًا لكون هذه الاسرار ثروة استراتيجية كبيرة لأي دولة، فإن الدول المعادية تسعى جاهدة للسيطرة على هذه البيانات الرقمية لاعتبارات مختلفة، من خلال شن هجمات رقمية عابرة للحدود لدول اخرى.

الجدير بالذكر إن الجغرافية ليس لها أي دور في عمل التكنولوجية الرقمية حتى ولو كانت البنى التحتية الأساسية إقليمية، إلا إن الحكومات الوطنية لها حقوق سيادية ضد حكومات الدول الأخرى، وهذا المبدأ يرفض تطبيق الحقوق العالمية في مجال التكنولوجية الرقمية، بما في ذلك حرية الوصول إلى المعلومات، فضلًا عن إن الحكومات الوطنية تتمتع بالسيادة الرقمية على جميع الجهات الفاعلة داخل البلد سواء اكانت حكومية ام غير حكومية، سواء اكانت هذه الفواعل وطنية ام اجنبية [1].

أولًا: مشكلة الدراسة. عدم وجود نصوص دستورية عراقية تؤمن الدفاع عن السيادة الرقمية للعراق، فضلًا عن عدم وجود هيئة تختص بالدفاع عن السيادة الرقمية العراقية، مما ينتج عن ذلك استهداف الامن القومي العراقي الرقمية على مختلف الأصعدة، ويهدد امن وسلامة البيانات والمعلومات.

ثانيًا: اهداف الدراسة. صياغة نصوص دستورية وقانونية تؤمن بناء بنى تحتية تحمي السيادة الرقمية وتقنية امن البيانات والمعلومات العراقية.

ثالثًا. منهجية الدراسة. بعد الاطلاع على نصوص الدساتير والقوانين ذات الشأن التي تناولت (السيادة الرقمية للدول من منظور القانون الدستوري) فقد اعتمدت على المنهج الاستنباطي المقارن.

ففيما يخص المنهج الاستنباطي فقد اعتمدنا بتفسير النصوص الدستورية والقانونية ذات الشأن باعتبارها مبادئ ونظريات عامة (سيادة الدولة)، ثم قمنا بتطبيق ذلك المبدأ على الجزيئيات (السيادة الرقمية للدول).

---

(1) د. عبد الغاني شرقي، التهديدات السيبرانية واشكالية السيادة، بحث منشور في مجلة السياسة العالمية، المجلد ٧، العدد٢، ٢٠٢٣، ص٢٨٣.

واما فيما يخص المنهج القانوني المقارن العامودي فقد قمنا بدراسته على عدد من الدساتير المقارنة (الاتحاد الألماني، الاتحاد الروسي، المصري) بغية الوقوف على أماكن القوى والضعف في صياغة الدستور العراقي، والوقوف على مواقف المشرعين الدستوريين وصولًا إلى الحلول المرعية في الدساتير المقارنة.

رابعًا. خطة الدراسة. قد اعتمدنا خطة، قسمنا فيها الدراسة على ثلاث مطالب: حيث تناولنا في المطلب الاول: التعريف بالسيادة الرقمية وقد قسمناه على فرعين: خصصنا في الفرع الاول: تعريف السيادة الرقمية، في حين تناولنا في الفرع الثاني: المفاهيم المشابهة للسيادة الرقمية للدول.

وأما في المطلب الثاني خصصناه: انتهاك السيادة الرقمية للدول، وقد قسمناه على فرعين: إذ سنتطرق في الفرع الاول: عمليات استهداف السيادة الرقمية للدول، في حين تناولنا في الفرع الثاني: صور انتهاك السيادة الرقمية للدول.

وأما في المطلب الثالث خصصناه: الجهود الوطنية للدفاع عن السيادة الرقمية، وقد قسمناه على فرعين: إذ سنتطرق في الفرع الأول: التنظيم الدستوري في الدفاع عن السيادة الرقمية، في حين تناولنا في الفرع الثاني: دور المشرع العادي في الدفاع عن السيادة الرقمية العراقية.

المطلب الأول

التعريف بالسيادة الرقمية

تبلورت فكرة السيادة كفكرة قانونية حتى وصلت إلى مستوى مقبول بعد تحررها من العهد الاقطاعي ابان القرن السادس عشر، فأصبحت ميزة أساسية لكل دولة، وجزءًا من شخصيتها المعنوية، حتى وصلت هذه الفكرة في القرن التاسع عشر إلى شكلها الحديث والتي تُعد من اهم مظاهر القوة، والقدرة في الدفاع عن الحدود الاقليمية للدولة.

فخلال فترة القرن التاسع عشر كان ينظر إلى السيادة كمفهومًا مركزيًا، إلا إنه في تسعينيات القرن الماضي، وبعد تطور تكنلوجيا المعلومات بدأ مفهوم السيادة يتضاءل شيئًا فشيئًا، بسبب التحديات الكبيرة التي تعرضت من قبل خيطين خطابيين مختلفين، مرتبطان بشكل كبير بالخطابات العامة والأكاديمية: (الاستثنائية السيبرانية، وحوكمة الأنترنت) [1].

(1) Pohle, Julia; Thiel, Thorsten, Digital Sovereignty, This article has been first published in: Internet Policy Review. 2020, P47

وعليه فإن سيادة الدول لم يعد كما استقر عليه قبل استحداث تكنولوجيا المعلومات، التي لا تعترف بحدود جغرافية لأي دولة، فباتت الدول كافة تخشى اختراق امنها القومي الرقمي، وسيادتها في ظل التهديدات الجديدة ذات الطبيعة الرقمية.

وتأسيسًا على ما تقدم ارتأينا تقسيم مطلبنا هذا على فرعين: تناولنا في الفرع الاول: تعريف السيادة الرقمية، في حين تناولنا في الفرع الثاني: المفاهيم المشابهة للسيادة الرقمية للدول.

الفرع الأول

تعريف السيادة الرقمية

إن السيادة الوطنية تغير جوهر مفهومها بسبب ثورة المعلومات والاتصالات، والتقنيات التي احدثتها عصر التكنولوجيا الرقمية على واقع المجتمعات، إذ تم إعطاء مفاهيم مغاير للسيادة لما كانت شائعة سابقًا (كالحروب، الحدود الإقليمية للدول، السيادة الإقليمية) إذ أصبح لهذه المفاهيم فيما بعد بعدًا رقميًا (كالحدود الرقمية للدول، الحروب الرقمية).

ووفقًا لهذا التطور فإن السيادة الوطنية الاقليمية لم تستطع مقاومة التحديات الطارئة نتيجة تغير العديد من الموازين والقوى، التي جعلت من الحدود السيادية للعديد من الدول مستباحة، ومخترقة من قبل فاعلين خارجيين سواء اكانوا رسميين ام غير رسميين.

لذا يُعد مصطلح السيادة الرقمية أو السيادة الالكترونية أو سيادة البيانات أو السيادة السيبرانية حديثًا نسبيًا، إذ تعاظم أهميتها نتيجة تعاظم دور امن المعلومات في عصر التحول الرقمي، فإن المشرعين، بل وحتى الفقهاء لم يتناول تعريف هذا المفهوم بصورة معمقة.

لذا يُمكن تعريف السيادة الرقمية بإنها: "قيام الدولة ببسط سيطرتها وولايتها القضائية على الفضاء الرقمي المتمثل بالأنترنت"[١].

وعُرف كذلك بإنه: "قدره الدولة على الحماية الرقمية لمؤسساتها ومجتمعها في مواجهة الهيمنة في الفضاء السيبراني"[٢].

---

(١) قريبيز مراد، تحديات الانترنت لسيادة الدول (السيادة الرقمية)، بحث منشور في مجلة البحوث القانونية والاقتصادية، المجلد ٥، العدد١، ٢٠٢٢، ص٣٠٥.

(٢) Luciano Floridi, The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU, Philosophy & Technology,2020,p371.

وعُرف كذلك بإنه: سلطة الدولة في اتخاذ قرارات حرة على الصعيد الداخلي، والخارجي ضمن المجال الرقمي لحماية امنها وامكاناتها الاقتصادية من الهجمات الالكترونية، والتي تؤثر سلبًا على حياة المواطنين والشركات العاملة في هذا المجال (١).

نلاحظ من التعاريف أعلاه بإن السيادة الرقمية هي حق الدولة في بناء بنى تحتية رقمية، هدفها الدفاع عن امنها الرقمي على الصعيد الداخلي والخارجي من الهجمات الالكترونية التي تؤثر على حياة المواطنين وبياناتهم الشخصية، إلا إن هذه التعاريف لم تبين لنا بإن طبيعة هذه السيادة هل هي جزءًا من السيادة الوطنية ام لا.

ويمكننا تعريف السيادة الرقمية بإنها: جزءًا من السيادة الوطنية، يمنح الدول لها الحق في امتلاك البنية التحتية الرقمية بمعزل عن الدول الأخرى بما يمكنها الدفاع عن فضائها الرقمي وصد الهجمات الرقمية من الفواعل الخارجيين.

الفرع الثاني

المفاهيم المشابهة للسيادة الرقيمة

قد يخلط الكثير بين مفهوم السيادة الرقمية للدول، وما بين بعض المفاهيم الاخرى، إلا إنها ليست بذات المعنى، وبناءً على ذلك يتطلب بيانها، الاتي:

أولًا: الفضاء الرقمي. أو ما يسميه البعض بالفضاء السيبراني، أو الفضاء الالكتروني، أو الفضاء الاستراتيجي الخامس الذي قد عرفه البعض بإنه: البيئة التي تم انشاؤها عن طريق شبكات الاتصالات، والانترنت، وأنظمة الهاتف النقال، والكمبيوتر، ووحدات التحكم، والبنى التحتية للاتصالات التي يشار إليها عادة باسم شبكة الويب العالمية (٢).

وعليه فإن الفضاء السيبراني هو مجال عالمي داخل بيئة المعلومات يتكون من مكونات عدة: أولهما: المادي الذي يتمثل في البنية التحتية المعلوماتية كالكابلات، شبكات الاتصالات، والانترنت، وأنظمة الهاتف النقال، والكمبيوتر، ووحدات التحكم. وثانيهما: المحتوى المعنوي الذي يعكس شكل المعلومات السيبراني. اما ثالثهما: فيتمثل في عملية التوصيل بين المعلومات والافراد، وحركة التفاعل ما بين البرمجيات والمعدات.

(١) Mohammed Saaida, Digital Sovereignty ،Science For All Publications, Vol: 6 Issue: 1 pp. 1-12, page1.

(٢) Julie E. Cohen, CYBERSPACE AS/AND SPACE, Georgetown University Law Center, 2007, p212

ثانيًا: الاحتلال الرقمي. هو عبارة عن سلسلة من الهجمات الرقمية التي تقوم بها دولة ضد دولة أخرى من خلال التسلل غير المرخص به إلى مواقع الكترونية، بهدف تعطيل أو اتلاف البيانات، أو المعلومات أو السيطرة عليها [١].

إن الاحتلال الرقمي يتصف بجملة من الخصائص أبرزها: إنه من الصعب اثبات الجهة المنفذة للاحتلال الرقمي، إن الحروب الرقمية تتم في بيئة رقمية افتراضية، إن الاحتلال الرقمي متعددة النطاق الجغرافي [٢].

ثالثًا: الحروب الرقمية. أو ما يسميها البعض بالحروب الالكترونية، هي حروب افتراضية ذات طبيعة غير ملموسة، تحاكي الواقع بطريقة شبه تام، إذ تتلخص أدوات الصراع فيها بالمواجهات الرقمية، وطلقات من لوحات المفاتيح، ونقرات المبرمجين، البرمجيات التقنية، جنود من برامج التخريب في بيئة اصطناعية [٣].

تنقسم هذه الحروب إلى اقسام ثلاثة وهي: بيئة حرب البيانات الشخصية التي تكون هدفها التخريب والسرقة، وبيئة حرب المعلومات العالمية التي تنشب بين دول العالم أو بين عدة دول، أو بيئة حرب المعلومات بين الشركات التي تتخذ الطابع التنافسي بين الشركات.

الجدير بالإشارة إلى إن جميع المفاهيم المشار اليها أعلاه لها علاقة مباشرة بالسيادة الرقمية للدول نتيجة تحول البشرية بأكملها إلى متلقية، ومستخدمة لوسائل الاتصال الحديث، والذي ساهم هذا التحول بشكل كبير إلى جمع المعلومات، والبيانات الرقمية للدول والافراد، مما يتطلب إلى ضرورة التفكير في حماية الدول لسيادتها الرقمية، وامن بياناتها من أي هجوم رقمي قد يعترض سير عملها في بيئتها الرقمية.

المطلب الثاني

انتهاك السيادة الرقمية للدول

إن مع تطور الاتصالات وتكنولوجيا المعلومات بات من الصعب القطع بفكرة سيطرة الدولة المطلقة على بياناتها، ومعلوماتها نتيجة ارتباط واندماج هذه البيانات والمعلومات

---

(١) د. احمد عبيس الفتلاوي، الهجمات السيبرانية، بحث منشور في مجلة المحقق الحلي للعلوم القانونية والسياسية، المجلد٨، العدد٤، ٢٠١٦، ص٦١٦.

(٢) حسين عباس حميد، دور تقنيات الذكاء الاصطناعي والتشريعات في التصدي للاحتلال الرقمي، بحث منشور في مجلة رسالة الحقوق، العدد الخاص بالمؤتمر القانوني الدولي الثاني لكلية القانون، جامعة المثنى، ٢٠٢٢، ص٣٧٤.

(٣) Nurgul YASAR, Fatih Mustafa YASAR and Yucel TOPCU, Operational Advantages Of Using Cyber Electronic Warfare (CEW)، In The Battlefield, Proc. of SPIE Vol. 8408٨٤٠٨٠,G · 2012 SPIE,P3.

بالشبكة الدولة، والتي تُعد أحد أبرز عوامل القوة تارة، وأحد عناصر ضعف الدول تارة اخرى.

لذا فإن السيادة الوطنية لم تعد مقتصرًا على الإقليم البري، أو الجوي، وحتى البحري، بل عملت وسائل الاتصال الحديث على خلق فضاء جديد يختلج كميات كبيرة من المعلومات التي تخص الامن القومي للدول، الذي جعل من السيادة في ظل التحول الرقمي المتسارع أمر في غاية الأهمية لأي دول من دول العالم.

وتأسيسًا على ما تقدم ارتأينا تقسيم مطلبنا هذا على فرعين: تناولنا في الفرع الاول: عمليات استهداف السيادة الرقمية للدول، في حين تناولنا في الفرع الثاني: صور انتهاك السيادة الرقمية للدول.

الفرع الأول

عمليات استهداف السيادة الرقمية للدول

إن عمليات انتهاك السيادة الرقمية لأي دولة تنحصر بأشكال مُحددة، واهم هذه العمليات هي ما تتخذ شكل التسلل الرقمي، والهجوم الرقمي، والتجسس الرقمي، الاتي:

أولا: التسلل الرقمي. تمثل هذه العملية كخطوة أولى لكافة عمليات استهداف السيادة الرقمية لأي بلد، عبر الوصول غير المصرح به إلى داخل الشبكة المعلوماتية، إذ يتم بعد ذلك تخزين أو تداول بيانات سرية، دون الاستمرار لتحقيق اهداف أخرى[١].

ثانيًا: الهجوم الرقمي. هو هجوم موجه بأنظمة التكنولوجيا الحديثة لمعلومات دولة ما، هدفها الغاء هذه المعلومات، أو تعديله كلها، او بعضها، أو تحريفها، او تدميرها، فيستخدم الفاعلين أنواعًا مختلفة من الأدوات والتقنيات من خلال إرسال برامج ضارة مثل (شبكات الروبوتات، والفيروسات، وأحصنة طروادة) وما إلى ذلك، بغية الوصول إلى إيقاف نظام الكتروني أو شبكة، أو محو جميع البيانات، أو البرامج على الشبكة وهذه الاثار تسمى بـ (القنبلة الذكية)[٢].

ولا بد من الاشارة إلى إن أنواع الهجمات تختلف باختلاف نوع الهجوم، إلا إن الهجمات الأكثر شيوعًا في وقتنا الحالي هي: (رفض الخدمة، الأكواد الخبيثة، الفيروسات، الديدان،

---

(١) د. محمد عادل محمد، وضع العمليات السيبرانية في القانون الدولي مع التطبيق على ممارسة التجسس وقت السلم، بحث منشور في مجلة البحوث القانونية والاقتصادية، جامعة بني سويف، ٢٠٢١، ص٢٦٩.

(٢) Al-Mohannadi H, And others, Article published on the link, http://dx.doi.org/https://doi.org/10.1109/w-ficloud.2016.29

أحصنة طروادة، البرامج الضارة، المتسللين الخبيثين، الأجهزة المسروقة، التصيد الاحتيالي، الهندسة الاجتماعية، والهجمات المستندة إلى الويب)، مع الاخذ بنظر الاعتبار على أن مصادر الهجوم الأكثر شيوعًا صادرة من دول هي: (الولايات المتحدة الأمريكية، روسيا، هولندا، المانيا، المملكة المتحدة، اوكرانيا، فرنسا، فيتنام، كندا، رومانيا)، وفي الوقت نفسه، فإن ضحايا هذه الهجمات الأكثر شيوعًا يقعون في: (الولايات المتحدة الأمريكية، روسيا، المملكة المتحدة، ألمانيا، إيطاليا، فرنسا، هولندا)[١].

ولذلك إنه يجب الاخذ بالحسبان إنه قد تختلط الاوراق على الكثير حول الشبه بين الهجوم الرقمي والتسلل الرقمي، إذا إن الاخيرة تُعد مرحلة ساكنة لا تؤدي إلى تغير البيانات او تدميرها، بخلاف الهجوم الذي يشمل الاضرار بالنظام التقني الرقمي، وتدمير البيانات والمعلومات، أو تعديل البيانات المخزنة او محوها، فضلًا عن ذلك إن جميع الهجمات الرقمية تبدأ بتسلل رقمي، على عكس التسلل الرقمي التي تتوقف الإجراءات الخاصة بها لمرحلة الوصول إلى أنظمة المعلومات والبيانات فقط دون تدميرها.

ثالثًا: التجسس الرقمي. ان ارتباط كافة مناحي الحياة بالتكنولوجيا الحديثة، أدت إلى بروز تهديدات متعددة تواجه الافراد والدول على حد سواء، للمساس بحقوق الدول الأخرى، وعلى رأس ذلك المساس بحق الدول في الامن الخارجي، وكذلك حقها في السيادة عن طريق توظيف الوسائط الالكترونية للوصول إلى اسرار الدفاع عن السيادة الرقمية للدول.

لذا فإن التجسس الرقمي أو كما يسميه البعض بالجوسسة الرقمية عُرف بإنه: استخدام وسائل التكنولوجيا الحديثة للدخول غير المشروع إلى أنظمة المعلومات الالكترونية الخاصة بدولة ما، والتنصت عليها بقصد الحصول على ما لديها من بيانات ومعلومات تخص نظامها وامنها العسكري، أو السياسي، او الاقتصادي، أو الثقافي[٢].

وفي ظل هذا التطور التكنولوجي المتقدم فإن وسائل التجسس تحولت من الطرق التقليدية إلى الطرق الرقمية الالكترونية، نتج عن ذلك بإن حدود الدولة الرقمية مستباحة بأقمار التجسس والبث الفضائي، فلو قارنا بين الاضرار الناتجة عن خطر المنظمات التجسسية

---

(١) Andreea Bendovschi, Cyber Attacks - Trends, Patterns and Security Countermeasures, Procedia Economics and Finance 28 (2015) 24 – 31,p26.

(٢) د. علي جعفر، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة، منشورات زين الحقوقية، دون بلد النشر، ٢٠١٣، ص٥٦٩.

عن غيرها لوجدنا بإن للتجسس الرقمي لها تأثير كبير واستراتيجي كونه يهدف إلى غايات سياسية تهدد امن الدولة القومي [١].

والجدير بالإشارة إلى إن التجسس الرقمي والمعلوماتي يتخذ اشكال عدة، منها ما يتم عبر التجسس، او التنصت على المعلومات الصادرة من المحطات، او الهواتف المحمولة، والحواسيب.

وبعد كل ما تقدم فإن عمليات استهداف السيادة الرقمية لأي دولة تتم بأحد الطرق أو الأسلحة المشار إليها اعلاه، إلا إن هذه العمليات الرقمية تتصف بجوانب عدة، تميزها عن عمليات انتهاك السيادة الوطنية الجغرافية، الاتي [٢]:

١. إن الأسلحة المستخدمة لا تتطلب موافقات دولية.

٢. إن معظم الدول لا تستطيع معرفة الفاعل الذي قام بانتهاك السيادة الرقمية للدولة.

٣. يستطيع الفاعل اختراق سيادة الدولة الرقمية لأدق مراكزها الحساسة.

٤. إن هذه العمليات الرقمية لا تحتاج إلى قوة بشرية كبيرة، وقوات مساندة كالدروع البشرية على ارض الواقع.

٥. لا تحتاج على موارد لوجستية ضخمة عند الاستهداف.

٦. لا يمكن نزع الأسلحة الرقمية او الالكترونية.

٧. لا تتقيد هذه العمليات بوقت او مكان لتحديد الهدف.

الفرع الثاني

صور انتهاك السيادة الرقمية للدول

إن التطور التكنولوجي خلق ساحات سيادية عديدة على مستوى العالم، وأصبحت اللغة الرقمية سائدة على جميع الدول كافة، مما تطلب من هذه الدول التفكير بأمنها القومي في عالم تقني تسوده خطر التكنولوجيا الرقمية.

نتيجة هذا التطور التكنولوجي أدى الى انصهار الحدود الجغرافية للدول كافة، وتقلص المسافات فيما بينها، مما أحدثت تغيرات عدة على الامن القومي التي اتاحت الولوج في فضاء الكتروني يحوي العديد من المعلومات القومية على مختلف الأصعدة سواء اكان منها (العسكرية، الاجتماعية، الاقتصادية، الثقافية، العلمية، ...الخ)، مما ادخل هذه الدول

---

(١) د. حسنين شفيق، الاعلام الجديد والجرائم الالكترونية، دار فكر وفن، ٢٠١٥، ص١٩.

(٢) د. ضحى لعيبي السدخان، مفهوم الصراع في الفضاء الالكتروني وتاريخه بين إيران والكيان الصهيوني، بحث منشور في مجلة أبحاث ميسان، المجل ٢٠، العدد٣٩، ٢٠٢٤، ص٤٠٢

في هاجس أمني، خاصة وإن هذه الدول قامت بوضع كافة مدخراتها القومية على بيانات ومعلومات رقمية.

وعليه فإن انتهاكات سيادة الدول الرقمية تتمثل في صور عديدة، إلا إننا سنركز على القطاعات المهمة، ومن بين هذه القطاعات ذات الشأن العسكري، وكذلك الاقتصادي، والسياسي، بل وحتى الثقافي الاتي:

أولا: الامن القومي العسكري. إن الساحة العالمية تحولت إلى ارض معارك حقيقية في عالم افتراضي، مستند بذلك على التطور التكنولوجي الرقمي، التي ينعكس اثارها السلبية على البنى العسكري للدول.

وفي واقع الامر فإنه نظرًا لما يحتويه المحتوى المعلوماتي الرقمي ذات الشأن العسكري من معلومات وبيانات الكترونية عن جوانب التسليح العسكري كافة، واسماء المنتسبين ورتب الضباط، والصناعات العسكرية، فإنه يُعد من أخطر الابعاد تأثيرًا على الجانب القومي لأي بلد، بسبب إن معظم الابتكارات العسكرية التي تعمل في وقتنا الحاضر، يتم ربطها بوسائل الاتصال التكنولوجية الحديثة التي تُمكن مستخدميها من التحكم بها عن بعد [١].

لذا فإن البنى التحتية المعلوماتية الرقمية ذات الشأن العسكري تمثل نقطة استهداف رقمي من قبل الدول، مستغلين بذلك انظمة الذكاء الاصطناعي، والتعامل التكنولوجي المتقدم في تحقيق أهدافهم العسكرية الخبيثة، مما يتعين على جميع الدول الاستعداد لتطوير انظمة دفاع رقمية متطورة، لها القدرة على التصدي لمواجهة هذا النوع من الهجمات العسكرية، وكشف المخاطر الرقمية مسبقًا قبل وقوعها [٢].

الجدير بالإشارة إلى إن انتهاكات السيادة الرقمية للأمن القومي العسكري عديده أهمها:

الهجمات الروسية لاستوينا اثناء الصراع العسكري فيما بينهما سنة ٢٠٠٧، فضلا عن ذلك الهجمات الصهيونية والأمريكية ضد المنشآت النووية الإيرانية سنة ٢٠١٠ باستخدام فيروس (ستا كنست) والذي يمثل نقطة تحول خطيرة في مجال الحرب الرقمية، وكذلك الهجمات الروسية على جورجيا سنة ٢٠٠٨، والهجمات الكترونية بين حزب الله والكيان الصهيونية سنة ٢٠٠٦، فضلًا عن استهدافات دول حلف الشمال الأطلسي لأنظمة

---

(١) د. فاطمة بيرم، السيادة الوطنية في ظل الفضاء السيبراني والتحولات الرقمية: الصين انموذجًا، بحث منشور في مجلة الجزائرية للأمن الإنساني، السنة الخامسة، المجلد٥، العدد١، ٢٠٢٠، ص٧٩٧.

(٢) حسين عباس حميد، مرجع سابق، ص٣٧٨.

الكمبيوتر الخاصة بوزارة الدفاع اليوغسلافي والتشويش على الاتصالات نهاية القرن العشرين بعملية سميت بـ (القنابل المعتمة) [١].

فضلا عن الانتهاكات أعلاه، البيانات والوثائق التي سربها (ادوار سنودن) ضابط وخبير امن المعلومات الذي يعمل في وكالة الاستخبارات الامريكية (CAI) التي اطلع على مجموعة كبيرة من الوثائق السرية الامريكية لدى ارساله إلى سويسرا في مهمة رسمية، إذ سرب وثائق لا تقل عن ٧٠٠٠ وثيقة رسمية، ومن بينها تجسس الحكومة الامريكية على ٣٨ سفارة وبعثة اجنبية باستخدام مجموعة متنوعة من أساليب المراقبة الالكترونية، فضلًا عن قيام أمريكا بتطوير برمجيات خبيثة لأصابه أجهزة الكومبيوتر على مستوى العالم اجمع، ومراقبة شركة (هاواوي) الصينية بسبب شراكتها وعلاقتها مع الجيش الصين[٢].

وكذلك توصلت وزارة العدل الامريكية بناءً على تحقيق اجرته سنة ٢٠١٣ بضلوع إيران في هجوم الكتروني على نظام التحكم في سد بومان افينيو/ الكائن في منطقة راي بورك/ نيويورك وكاد هذا الهجوم ان تفتح بوابات السد وتسبب بأضرار كبيرة جدًا، إلا إنه بالصدفة تبين فيما بعد بإن بوابات هذا السد كانت معطلة [٣].

وكذلك قامت القوات الروسية عام ٢٠٢٢ بتدمير وتعطيل منظومات الدفاع والاتصال قبل موعد اجتياحها لمناطق من اوكرانيا في العام ذاته، فضلا عن اكتشاف برامج ضارة تستهدف الحكومة الاوكرانية، والعديد من المنظمات غير الربحية التي انتهى بها المطاف بتعطيل ٧٠ موقعا الكترونيًا حكوميًا بما فيها موقع مجلس الوزراء الاوكراني، ووزارة الدفاع، والخارجية، فضلا عن استخدام هجوم DOS لتدمير عديد من المواقع الالكترونية والحكومية لبضع ساعات، بغية اثارة الرعب والخوف بين ابناء الشعب

---

(١) طيف من الهجمات الالكترونية ذات الشأن العسكري على سيادة الرقمية للعديد من الدول، لمزيد من التفاصيل انظر. د. فرحات علاء الدين، الفضاء السيبراني وتأكل مفهوم السيادة الوطنية، بحث منشور في مجلة الجزائرية للدراسات السياسية، المجلد٨، العدد٢، ٢٠٢١، ص١٧٤.

(٢) Cynthia Nolan, The Edward Snowden Case and the Morality of Secrecy, The Catholic Social Science Review 22, 2017, p291

(٣) Robert M. Lee, Michael J. Assante, Tim Conway, Analysis of the recent reports of attacks on US infrastructure by Iranian Actors, ndustrial control systems, 2016, p1.

الاوكراني، فضلا عن اطلاق برامج ضارة لمحو بيانات في ١٠٠ مؤسسة من القطاعات المالية وتكنولوجيا الطيران[١].

فضلًا عما ورد أعلاه، ذلك الانتهاك الذي قام به الكيان الصهيوني بتفجير أجهزة الاستشعار (البيجر) لدى عناصر حزب الله اللبناني منتصف الشهر التاسع من عام ٢٠٢٤ بعد وضع كمية من مادة (PETN) شديدة الانفجار على بطارية الأجهزة أعلاه التي تم تفجيرها عن بعد عبر رفع درجة حرارة البطارية" والذي سقط على أثرها العديد من الشهداء والجرحى في عناصر الحزب، والتي تعد هذه العملية أحد حروب الجيل الخامس وانتهاك لسيادة لبنان الرقمية.

واستخلاصًا لما تم ذكره فإن الحدود السياسية الوطنية للدول كافة، اصبحت سببًا للعديد من الحروب التي خاضتها الدول للمحافظة على سيادتها الوطنية، إلا إنه نظرًا للتطور التقني التكنولوجي، أصبحت هذه السيادة عرضه للهجمات الرقمية عبر أسلحة المعرفة، فالتخطي المعلوماتي للحدود الوطنية أصبح عملية تغيير جوهرية في وسائل تخزين المعلومات عبر الأقمار الاصطناعي الى أي مكان بسرعة شديدة، ذات قدرة على اختراق الحدود الرقمية للدول التي اصبحت الأخير عاجزة امام سيل المعلومات المتحرك عالميًا.

ومن هذا المنطلق فإن التطور التكنولوجي فرض على جميع الدول اعادة التفكير في مفهوم الامن القومي العسكري، الذي أصبح لكل مجالًا امنيًا قوميًا ووجهًا معلوماتيًا ذات ابعاد رقمية ينبغي الحفاظ عليها من الهجمات الخارجية.

ثانيًا: الامن القومي الثقافي. إن الثقافات تختلف وتتنوع وتصل لدرجة عدم الاتفاق عليها، إلا إنه يتم ترك ذلك للتشريعات الوطنية لتنظيمها بما يتفق مع قواعد النظام العام، والأداب العامة إلا إن هذه الثقافات تتعرض ما بين فترة واخرى إلى اعتداءات على الامن الثقافي للمجتمعات من خارج البلد، تستهدف نشر مادة مرئية تتعلق بالاتصال الجنسي للأطفال بشكل قيام القاصر بتصرفات جنسية، أو ظهور صور واقعية تمثل قاصرًا يتدخل بتصرف جنسي [٢].

---

(١) د. احمد عبيس الفتلاوي، المناهج والمعايير المعتمدة للكشف عن طبيعة القوة السيبرانية، منشورات زين الحقوقية، بلا سنة نشر، ص١١٨.

(٢) د. قطاف سليمان، الاليات القانونية الموضوعية لمكافحة الجرائم السيبرانية في ظل اتفاقية بودابست والتشريع الجزائري، بحث منشور في مجلة الاكاديمية للبحوث القانونية والسياسية، العدد الأول، المجلد السادس، ٢٠٢٢، ص٣٤٢.

وبطبيعة الحال إن الاخطار التي يترتب عليها خرق السيادة الرقمية للدولة ذات الشأن الثقافي هو الابعاد الاجتماعية الناتجة عن تدني المستويين الأخلاقي والقيمي، والمحتويات غير المشروعة التي لها اثار سلبية على اخلاقيات وتصرفات الافراد، ينتج عنها ارتفاع نسبة الممارسات الاجرامية كـ (الترويج للمخدرات، والاتجار بالممنوعات، ونشر الأفلام الإباحية، والدعارة، وتجنيد الشباب لقضايا تمس الامن والسلم الدوليين، ونشر ثقافات تمس بالمذاهب والطوائف الإسلامية، أو نشر برنامج ذو شان شبابي هدفه هدم القيم والأخلاق لدى الشباب)، وعليه لا بد من حماية المجتمع ليكون مدركًا لمخاطر التطور التكنولوجي ومدرك للعواقب القانونية الي تترتب عليها التعرض لسلامة الافراد[١].

وعليه فإن استهداف الامن الثقافي لأي مجتمع قد يستمر لبضع ثوان، إلا إن مخاطره قد يولد اثار مدمرة وواسعة، ينتج عنها خسارة المجتمع للثقة، وفي حينها لا يستطيع المجتمع تحمل هذه الاثار بسبب فقدان هذه الثقة، الذي قد يتطلب سنوات لإعادة بنائها.

ثالثًا: الامن القومي الاقتصادي. إن التطور التكنولوجي اصبح جاذبًا لقطاعات المجتمع كافة، ومن بين هذه القطاعات قطاع الاقتصاد والمال، مما بات هذا التطور محرك الإنتاج والنمو في جميع الدول، إذ إن حجم التجارة الالكترونية سنة ٢٠١٤ بلغ ١,٥ تريليون دولار بزيادة نسبتها ٢٠٪ مقارنة بعام ٢٠١٣، لذا ايقن على اثر ذلك الجميع بإن التحول التكنولوجي اضحى عاملًا مهمًا للنهوض الاقتصادي، مما دفع الدول كافة إلى زيادة استثماراتها الاقتصادية ضمن المجال التكنولوجي، مستخدمين اجهزة الكمبيوتر وشبكة الانترنت في معالجة المعاملات المالية والاقتصادية، وبما إن هذا التطور التكنولوجي دخل عالم الاقتصاد، فإن هذا التطور اصبح يشكل تهديدًا صريحًا لنمو الاقتصاد الرقمي مما يتطلب تدخل الدول بتعظيم معاير الامن المعلوماتي للحفاظ على السيادة الرقمية لها، بما يضمن الحد من هذه الجرائم[٢].

وبما إن البنوك والمؤسسات المالية والتجارية وحتى الاقتصادية تُعد حراسًا للثروة المالية للدول والمؤسسات التجارية، إلا إنها تشكل أهدافا قيمة للحروب الرقمية والسيطرة على بياناتها، لذا فإن محاولات اختراق السيادة الرقمية لهذه المؤسسات تكون مكلفة جدًا، ومن بين هذه المحاولات الاتي:

---

(١) د. عبد الناصر محمد ايوب، الاخلاق والقانون والامن السيبراني، بحث منشور في مجلة بنها للعلوم الإنسانية، العدد١، الجزء٢، ٢٠٢٢، ص١٢.

(٢) د. بارة سمير، الامن السيبراني في الجزائر: السياسات والمؤسسات، بحث منشور في المجلة الجزائرية للأمن السيبراني، العدد الرابع، ٢٠١٧، ص٢٦١.

تلك التي تستهدفها مجموعة ساند وورم او ما تسمى (بلاك انيرجي) التي تتبع للاستخبارات الروسية، التي تُعد واحدة من أخطر مجموعات الحرب الرقمية على مستوى العالم التي تشكلت عام ٢٠٠٧ إذ تمتلك قدرات تقنيه عالية تُمكنها من تنفيذ هجمات سيبرانية معقدة، وفعالة على شبكات الطاقة، والنقل والمواصلات، التي لها العديد من الاستهدافات في جميع الدول الاوروبية إذ استهدفت عام ٢٠١٦ شبكة الطاقة الكهربائية في أوكرانيا واخرجتها عن الخدمة لفترة مؤقتة [١].

فضلًا عن ذلك، فإنه وفقا للمجموعة الاستشارية في المملكة المتحدة هنالك أكثر من ١,٦ مليار جنيه استرليني خسائر الاحتيال غير المصرح بها عام ٢٠٢٠، فضلًا عن ذلك قيام القراصنة بتنفيذ هجومًا الكترونيًا بتوظيف برنامج (درك ساييد) بتشفير بيانات الشركة البترولية الامريكية، وسرقة بياناتها بسرعة، مما قام القراصنة بابتزاز الشركة أما بإفشاء اسرارها، أو دفع فدية مالية، مما دفع الشركة على ضوئها بدفع الفدية بغية فك الشفرة وعدم افشاء البيانات السرية للشركة [٢].

رابعًا: الامن القومي السياسي. إن انتهاك سيادة الدول رقميًا لا يقتصر على القطاعات المذكورة اعلاه، بل شملت كذلك قطاع ذات الشأن السياسي التي تتعلق بـ (الاحزاب، مجلس النواب، رئاستي السلطة التنفيذية، الانتخابات) بغية إيجاد ارضية مناسبة لصراع داخلي ما بين الشعب من جهة، والأجهزة الحكومية والعسكرية من جهة أخرى، فتعد هذه الطرق بديلة عن تلك التي كانت تستخدم سابقًا لأسقاط النظام السياسي بالقوة العسكرية من الخارج، وهذا ما حدث بالفعل في معظم الدول العربية التي تسمى (الربيع العربي)، فضلاً عن ذلك فإن سيادة الدول السياسية قد تستهدف رقميًا اثناء الحملات الانتخابية.

ومن بين هذه الدول التي اخترقت سيادتها ذات الشأن السياسي هي الولايات المتحدة الامريكية حيث ادعى مرشح الحزب الجمهوري (دونالد ترامب) بإن حملتها الانتخابية قد تعرضت للاختراق ومن شبه المؤكد بإن كل من روسيا والصين والجمهورية الإسلامية

---

(١) Khan, R., Maynard, P., McLaughlin, K., Laverty, D., & Sezer, S. (2016). Threat Analysis of Black Energy Malware for Synchro phasor based Real-time Control and Monitoring in Smart Grid. In 4th International Symposium for ICS & SCADA Cyber Security Research 2016 (p53).

(٢) د. حميل مصطفى، السيادة الرقمية والتحول الرقمي، بحث منشور في مجلة الدراسات الإعلامية والاتصالية، العدد٣، المجلد ٢، ٢٠٢٢، ص٥٥ وما بعدها.

الإيرانية هي وراء هذا الفعل[1]، إذ قاموا باختراق أنظمة المعلومات التابعة للجنة الوطنية الديمقراطية وحصلوا على جميع التقارير، ورسائل البريد الالكتروني المتبادلة بين أعضائها، مستهدفين بذلك نشر اخبار تحريضية ووهمية عن المرشح.

وفي ختام ما تم ذكره في مطلبنا هذا، تبين لنا بإن انتهاك سيادة الدول في ظل التطور التكنولوجي من قبل فواعل سواء اكانوا رسميين أم غير رسميين من خارج البلد، يتم باتباع عمليات استهداف رقمية محددة: اما إن تكون عمليات تسلل، أو هجوم، أو تجسس رقمي لاختراق بيانات ومعلومات قطاعات مختلفة: اما إن يكون قطاع الامن القومي العسكري والذي يُعد من اخطر الابعاد تأثيرًا على الجانب القومي لأي بلد، نظرًا لأهمية وحساسية ما يحتويه من معلومات وبيانات الكترونية عن جوانب التسليح العسكري، فضلا عن الجانب السياسي، والثقافي، والاقتصادي الذي يمثل الشريان الاقتصادي والمالي لاي بلد.

وفي هذا المقام وبغية الحفاظ على سيادة العراق الرقمية، يتطلب منا العمل على صياغة نصوص دستورية وقانونية بما ينسجم مع التطور التكنولوجي الرقمي الذي يُمكن البلاد على امتلاك بنية تحتية رقمية متقدمة، تستطيع صد الهجمات الرقمية من قبل فاعليين من خارج البلد.

المطلب الثالث

الجهود الوطنية للدفاع عن السيادة الرقمية

تختلف الجهود الوطنية في معظم دول العالم للدفاع عن السيادة الرقمية، والتصدي للانتهاكات التقنية العابرة للحدود التي تضر بسيادة الدول فالبعض تبنى تصديها لهذه الانتهاكات في متن الوثيقة الدستورية، والبعض الاخر تبنى ذلك بتشريع قوانين عادية تتضمن تأسيس هيئة وطنية للدفاع عن السيادة الرقمية.

وتأسيسًا على ما تقدم ارتأينا تقسيم مطلبنا هذا على فرعين: تناولنا في الفرع الاول: التنظيم الدستوري في الدفاع عن السيادة الرقمية، في حين تناولنا في الفرع الثاني: دور المشرع العادي في الدفاع عن السيادة الرقمية العراقية.

---

(1) Darren L. Linvill a,And others, THE RUSSIANS ARE HACKING MY BRAIN!" investigating Russia's internet research agency twitter tactics during the 2016 United States presidential campaign, journal Computers in Human Behavior, 2019, p292, And beyond.

الفرع الأول

التنظيم الدستوري في الدفاع عن السيادة الرقمية

يلعب المشرع الدستوري دورًا مهمًا وحيويًا في الدفاع عن سيادة للبلد، تجاه عمليات اختراق السيادة الرقمية نتيجة ارتكاب جرائم الحاسوب ونظم المعلومات والامن المعلوماتي العابرة للحدود، خاصة وإن ارتباط تلك الموضوعات ارتباطًا وثيقًا بالمكافحة الشاملة للجرائم المعلوماتية عبر الحدود.

واستنادًا إلى ذلك فإن المشرع الدستوري في معظم دول العالم لم يتناول الحفاظ على السيادة الرقمية بنصوص دستورية واضحة وصريحة، ربما لأن الدفاع عن هذه السيادة هي امر مستحدث تزامن مع التطور التكنولوجي المتقدم في أواخر القرن الماضي، خاصة وإن الكثير من دساتير دول العالم قد تم سنها من فترة ليست بالقصيرة، إلا إنه نظرًا لأهمية هذا الموضوع وارتباطه بسيادة البلد، التفتت بعض الدساتير التي تم صياغتها حديثًا إلى تضمين الدفاع وحماية السيادة الرقمية للبلد تحت مسميات مختلفة في متن الوثيقة الدستورية.

بناءً على ذلك لجأت الدساتير في الدول المتقدمة إلى صياغة نصوص تؤمن الدفاع عن السيادة الرقمية للبلد من الانتهاكات العابرة للحدود ومن بين هذه الدساتير هو القانون الأساسي لجمهورية المانية الاتحادية الذي افرد نصوص خاصة بتنظيم الدفاع عن تقنية المعلومات في متن المادة (٩١/ ج) منه حيث نصت على الاتي [١]:

١. يجوز للاتحاد والولايات التعاون في تخطيط، وإنشاء، وتشغيل أنظمة تقنية المعلومات اللازمة لأداء مسؤوليات الاتحاد ومهام الولايات.

٢. يجوز للاتحاد والولايات الاتفاق على تحديد المعايير والمتطلبات الأمنية اللازمة للتبادلات بين نظم تكنولوجيا المعلومات الخاصة بهم. وبالنسبة لبعض المسؤوليات المحددة تبعا لمضمونها ونطاقها، يجوز أن تنص الاتفاقات المتعلقة بأسس التعاون بموجب الجملة الأولى، على وضع لوائح تفصيلية بموافقة أغلبية مؤهلة من الاتحاد والولايات جرى تحديدها في هذه الاتفاقات. وتتطلب هذه الاتفاقات موافقة البوندستاغ والسلطات التشريعية في الولايات المشاركة؛ ولا يمكن استبعاد الحق في إلغاء هذه الاتفاقات. وتنظم الاتفاقات أيضا مسألة تقاسم التكاليف.

---

(١) القانون الأساسي لجمهورية المانية الاتحادية الصادر عام ١٩٤٩م المعدل لسنة ٢٠٢٢م.

٣. ويجوز أيضا للولايات أن تتفق فيما بينها على التشغيل المشترك لأنظمة تقنية المعلومات بالإضافة إلى بناء المنشآت لذلك الغرض.

٤. ينشئ الاتحاد شبكة ربط من أجل ربط شبكات أنظمة تقنية المعلومات التابعة للاتحاد والتابعة للولايات ببعضها البعض. وينظم قانون اتحادي بموافقة من البوندستاغ تفاصيل إنشاء شبكة الربط وتشغيلها.

يتبين لنا من هذا النص الدستوري بإنه أتاح للاتحاد الألماني والولايات التابعة لها، إنشاء منشئات تختص بأنظمة تقنية المعلومات تربط الاتحاد والولايات بعضها بالبعض الاخر، لتكون على شكل شبكة واحدة متراصة، بما يمكنها أداء جميع هذه الأنظمة مسؤولياته تجاه الحفاظ على سيادة المانية الاتحادية الرقمية تجاه الهجمات الرقمية العابرة للحدود.

وفي نطاق الدفاع عن السيادة الرقمية للاتحاد الألماني عبرت مستشارة الاتحاد الأسبق (انجيلا ميركل) امام دول الاتحاد الأوربي عن مخاوفها من الاعتماد على الشركات التكنولوجية الأجنبية كـــ (الامريكية، الصينية) إذ قالت "إن العديد من الشركات الاوروبية اعتمدت على مصادر خارجية لبياناتها وهي الشركات الامريكية والصينية، ونتيجة ذلك يتطلب منا إن ندعم السيادة الرقمية من خلال تطوير منصة بيانات خاصة، وتقليل الاعتماد على شركات مثل (Google, Microsoft) لخدماتها السحابية" [١].

واما في روسيا فان المشرع الدستوري منح في متن المادة (٧١) منه الاتحاد الروسي ولاية قضائية على جملة من الكيانات ومن بينها أنشطة المعلومات والاتصالات حيث نصت في البند (ط) على إنه: (الأنظمة الاتحادية ....، والمعلومات، والاتصالات، والأنشطة في الفضاء) [٢].

وانسجامًا مع هذا النص الدستوري فإن مجلس الدوما الروسي (مجلس الوزراء) لعب دورًا مركزيًا ومهمًا في منظومة الامن الرقمية إذ أصدر على إثر ذلك العديد من القوانين والتشريعات الهامة ذات الشأن باستعمالات تكنولوجيا المعلومات في سبيل الحفاظ على امنها المعلوماتي ومن بين هذه التشريعات: (قانون حماية المعلومات والبيانات سنة ١٩٩٥م، قانون حماية برامج الحاسوب وأنظمة قواعد البيانات سنة ١٩٩٢م، ثم أصدرت

---

(١) Silvia Amaro: Europe's dream to claim its 'digital sovereignty' could be the next big, challenge for US tech giants, https://www.cnbc.com/2019/11/20/us-tech-could-facenew-hurdles as-europe-considers-digital-sovereignty.htm (12-10-2024)

(٢) دستور الاتحاد الروسي الصادر عام ١٩٩٣م المعدل لسنة ٢٠١٤م.

تعديلًا على مجموعة من القوانين الجنائية لمكافحة جرائم الحاسوب والانترنت والأنشطة الالكترونية) [١].

مع الاخذ بنظر الاعتبار فإن روسيا تأتي في المرتبة الثانية بعد الولايات المتحدة الامريكية في الدفاع عن سيادتها الرقمية وامن معلوماتها وبياناتها رفضت الانضمام إلى اتفاقية بودابست بشأن مكافحة الجرائم المعلوماتية نتيجة تخوفها من السماح للوكالات الأجنبية من اعتراض حركة الانترنت الروسية.

واما عربيًا فإن المشرع الدستوري المصري كان سباقًا في صياغة نص دستوري يؤمن الدفاع عن سيادة مصر الرقمية من الانتهاكات العابرة للحدود عبر عمليات الاستهداف الرقمية للقطاعات كافة، بما فيها العسكرية، والاقتصادي، والسياسية، والثقافي، بل وحتى العلمية، حيث نصت المادة (١٣) من الدستور المصري على إنه: "أمن الفضاء المعلوماتي جزء أساسي من منظومة الاقتصاد والأمن القومي، وتلتزم الدولة باتخاذ التدابير اللازمة للحفاظ عليه، على النحو الذي ينظمه القانون"[٢].

واستنادًا إلى نص المادة الدستورية أعلاه، تم تشريع قانون جرائم تقنية المعلومات سنة ٢٠١٨م، والذي يختص بالدفاع عن استقلال واستمرار وامن الوطن ووحدة وسلامة اراضيه من الهجمات الرقمية من خارج البلاد، بل وحتى من داخله [٣]، من قبل الجهاز القومي لتنظيم الاتصالات [٤].

الجدير بالإشارة إلى إن مصر تأتي في المرتبة ٢ عربيًا و١٤ عالميًا في الدفاع عن سيادتها الرقمية وامن بياناتها ومعلوماتها وتقدم البنى التحتية التقنية.

واما في العراق فإنه بالرغم من إن التطور التكنولوجي الذي يرتبط بعالم الانترنت قد انتشر قبل نهاية القرن الماضي في الدول المتقدمة، إلا إن المشرع الدستوري لم يلتفت إلى صياغة نص يؤمن الحفاظ على السيادة العراق الرقمية، خاصة وإن انتهاك هذه السيادة لها انعكاسات كبيرة جدًا على الامن القومي العراقي على مختلف القطاعات كافة سواء اكانت منها العسكرية، او الثقافية، او السياسية، او الاقتصادية، ام العلمية.

---

(١) د. حيدر أدهم، الجهود القانونية للدفاع عن السيادة الرقمية للدول، بحث منشور في مجلة دراسات قانونية، العدد٥٣، ٢٠٢٠، ص٣٨.

(٢) الدستور المصري لسنة ٢٠١٤م، وتعديلاته الدستورية لسنة ٢٠١٩م المنشور في الجريدة الرسمية الصادرة بالعدد ١٥ مكرر (ج) في ١٧ابريل ٢٠١٩م.

(٣) قانون مكافحة جرائم تقنية المعلومات المصري رقم ١٧٥ لسنة ٢٠١٨، المنشور في الجريدة الرسمية بالعدد٣٢ مكرر ج، في ١٤/ أغسطس/ ٢٠١٨م.

(٤) قانون تنظيم الاتصالات المصري رقم ١٠ لسنة ٢٠٠٣م.

ونظـرًا لأهميـة السـيادة الرقميـة للبلـد، والحـد مـن عمليـات انتهـاك هـذه السـيادة مـن خـارج الحـدود، كـان يفتـرض بالصـائغ الدسـتوري العراقـي صـياغة نـص يـؤمن اختصـاص السـلطات الاتحاديـة بالحفـاظ علـى هـذه السـيادة مـن الهجمـات الرقميـة الخارجيـة، ليكـون مضـمون صياغته بالشكل الاتي:

(تلتزم السلطات الاتحادية بالحفاظ على السيادة الرقمية للبد، وينظم ذلك بقانون)

الفرع الثاني

دور المشرع العادي في الدفاع عن السيادة الرقمية العراقية

أسـلفنا سـابقا بإنـه مـن المآخـذ علـى صـياغة الدسـتور العراقـي لسـنة ٢٠٠٥م لـم يـنظم الـدفاع عـن السـيادة الرقميـة تحـت أي مسـمى، إذ كـان يجـدر بـه صـياغة نـص يـؤمن تأسـيس هيئـة وطنيـة تعنـى بالـدفاع عـن هـذه السـيادة، الـذي كـان يفضـل إن يكـون مضـمون صـياغته بالشـكل الاتي:

(تؤسـس هيئـة تسـمى هيئـة الـدفاع عـن السـيادة الرقميـة، تـرتبط بمجلـس الـوزراء، ويـنظم عملها بقانون).

وبمـا إن تعـديل الدسـتور العراقـي يُعـد امـرًا لـيس بـالهين، خاصـة وإن الـدفاع عـن السـيادة الرقميـة للحفـاظ علـى بياناتـه، وامنـه الرقمـي لمـا لهـا مـن الاهميـة البالغـة علـى الامـن القـومي العراقي الذي يعد امرًا في غاية الحساسية بعد التطور التكنولوجي المتقدم.

ممـا يتطلـب مـن المشـرع العـادي التفكيـر جـديًا فـي تنظـيم الـدفاع عـن سـيادة العـراق الرقميـة بنصـوص قانونيـة عاديـة، مسـتندة بـذلك علـى نصـوص دسـتورية، خاصـة وأن العـراق يحتـل المرتبـة ١٨ عربيًـا و١٥٩ عالميًـا طبقًـا لمؤشـر الـدول العربيـة سـنة ٢٠١٧ فـي الـدفاع عـن سيادة ومعلوماتها الرقمية.

وبعـد الرجـوع إلـى احكـام المـادة (١٠٩) مـن الدسـتور العراقـي لسـنة ٢٠٠٥م التـي منحـت السـلطات الاتحاديـة الـدفاع عـن سـيادة العـراق وسـلامة أراضـيه بشـكل مطلـق والتـي نصـت علـى إنـه: "تحـافظ السـلطات الاتحاديـة علـى وحـدة العـراق وسـلامته واسـتقلاله وسـيادته ونظامه الديمقراطي الاتحادي".

وحيـث إن المـادة (١٠٨) مـن الدسـتور ذاتـه اشـارت علـى إمكانيـة اسـتحداث هيئـة وطنيـة حسـب الحاجـة ووفقًـا للقـانون والتـي نصـت علـى إنـه: "يجـوز اسـتحداث هيئـات مسـتقلة أخـرى حسب الحاجة والضرورة بقانون".

ممـا يسـتوجب علـى المشـرع العراقـي سـن قـانون يسـتند إلـى النصـوص الدسـتورية أعـلاه يتضـمن اسـتحداث هيئـة وطنيـة لهـا الاسـتقلال المـالي والإداري وشخصـيتها المعنويـة تحـت أي مسـمى كـإن تكـون (الهيئـة الوطنيـة للـدفاع عـن السـيادة الرقميـة، أو الهيئـة الوطنيـة لتقنيـات امـن المعلومـات، أو الهيئـة الوطنيـة للـدفاع عـن السـيادة السـيبرانية، أو الهيئـة الوطنيـة لحمايـة الفضـاء الرقمـي)، تخـتص بحمايـة وتطـوير أنظمـة صـد الهجمـات السـيبرانية الرقميـة ضـد البنى التحتية العراقية الرقمية الحساسة والهامة.

وانسـجامًا مـع سـن قـانون يتضـمن تأسـيس هيئـة وطنيـة تعنـى بالـدفاع عـن السـيادة الرقميـة العراقيـة، فإنـه يتطلـب سـن قـانون اخـر، تسـتند الهيئـة المـذكورة فـي عملهـا عليـه، يخـص الـدفاع عـن امـن المعلومـات والبيانـات الرقميـة، مـع الاخـذ بنظـر الاعتبـار علـى إن يشـترط هـذا القـانون تعريفـات عـدة تخـص امـن المعلومـات والبيانـات، ومـن بـين هـذه التعريفـات (الهيئـة، البيانـات الرقميـة، البيانـات الشخصـية، المعالجـة الرقميـة، تقنيـة المعلومـات، مقـدم الخدمـة، البرنـامج المعلومـاتي، الموقـع، الاعتـراض، الاختـراق، الـدليل الرقمـي، بيانـات المـرور، الامن القومي الرقمي).

وعلـى الـرغم مـن إن العـراق أنظـم إلـى الاتفاقيـة العربيـة لمكافحـة جـرائم تقنيـة المعلومـات، والتـي تهـدف إلـى تعزيـز التعـاون بـين الـدول العربيـة، وتدعيمـه فـي مجـال مكافحـة جـرائم تقنيـة المعلومـات بغيـة درء المخـاطر عـن امـن الـدول العربـي وسـلامة افرادهـا ومجتمعاتهـا [1]، إلا إن العـراق لـم يهـتم ببنـاء بنـى تحتيـة تخـتص بـأمن المعلومـات وتقنياتهـا لغايـة هـذه اللحظة.

(1) قـانون تصـديق الاتفاقيـة العربيـة لمكافحـة جـرائم تقنيـة المعلومـات رقـم ٣١ لسـنة ٢٠١٣ المنشـور فـي جريدة الوقائع العرقية بالعدد ٤٢٩٢ في ٢٠٢١/٩/٣٠.

الجدير بالذكر إن الدول المتقدمة[١]، بل وحتى العربية[٢]، سعت جاهدة ومن وقت ليس بالقصير إلى تطوير البنى التحتية وسن القوانين التي تخدم حماية امنها المعلوماتي بغية صد الهجمات الرقمية التي تنتهك سيادتها الوطنية.

وتأسيسًا على ما تقدم، وبغية بناء منظومة دفاع عراقية رقمية متقدمة لها القدرة على كشف الاخطار الرقمية قبل وقوعها، وصدها الهجمات حين وقوعها، يتطلب تحديد الاتي:

اولًا: التهديدات التي تواجه السيادة الرقمية العراقية.

١. قرصنة عديد البيانات العراقية الرقمية.
٢. تعطيل العديد من البيانات والخدمات الرقمية المهمة.
٣. فقدان الثقة بين المواطنين.

ثانيًا: تحديات انتهاك السيادة الرقمية العراقية.

١. ضعف البنى التحتية.
٢. عدم وجود تشريعات.
٣. نقص في اعداد الكفاءات وضعف خبراتهم.
٤. تزايد الهجمات الرقمية على البيانات والمعلومات الوطنية.

ثالثًا: الجهود الوطنية للحد من انتهاك السيادة الرقمية العراقية.

١. سن القوانين بما ينسجم مع التطور التكنولوجي المتقدم.

---

(١) تعتبر الولايات المتحدة الامريكية الأكثر تفوقًا في مجال الدفاع عن السيادة الرقمية وامن تقنية المعلومات، ولها منشئات ربط موحدة التي تعتمد على مكونات أساسية أهمها (القيادة السيبرانية للجيش، قيادة الاسطول السيبراني، القيادة الالكترونية للقوات الجوية، القيادة الالكترونية لقوات مشاة البحرية) الذي يضطلعون بمهمة حماية السيادة الرقمية والتي تقوم على مبدأ الدفاع المتقدم والذي ينظر إليها على إنها قوة هجومية وليس دفاعية.
واما الصين التي تأتي في المرتبة الثالثة بعد روسيا في حماية امن معلوماتها وبياناتها فإن الرئيس الصيني أعلن في مؤتمر العالمي للأنترنت سنة ٢٠١٤ إلى ضرورة احترام حقوق كل بلد في تطوير واستخدام المعلومات وإدارة الانترنت، والامتناع عن انتهاك السيادة الرقمية للدول الأخرى، وعلى ضوء ذلك قطعت الصين اشواطًا متقدمة في التأسيس لهذه السيادة فقد أصدرت سنة ٢٠١٧ قانون الامن السيبراني بغية ضبط وتنظيم السيادة الرقمية للصين لتحقيق ميزة حمائية للدولة والمجتمع والافراد من التلف.

(٢) تحتل عُمان المرتبة الاولى عربيًا، و٤ عالميًا في تقرير نشر سنة ٢٠١٧ للاستعداد للأمن السيبراني والدفاع عن سيادتها الرقمية والمعلوماتية، حيث أصدرت سنة ٢٠١١ قانون مكافحة جرائم تقنية المعلومات العماني بموجب المرسوم السلطاني رقم ١٢ لسنة ٢٠١١م الذي تم نشره في الجريدة الرسمية الصادرة بالعدد ٩٢٩ لسنة ٢٠١١.
واما قطر فقد احتلت المرتبة (٣) عربيًا، بعد مصر و (٢٥) عالميًا فقد أصدرت قانون مكافحة الجرائم الالكترونية رقم ١٤ لسنة ٢٠١٤م، الذي يتألف من ٥٤ مادة موزعة على ثلاث فصول وفصل تمهيدي.

٢. تأسيس هيئة وطنية عراقية تختص بالدفاع عن امن المعلومات والبيانات الرقمية ولها فروع في المحافظات.

٣. الانضمام إلى المعاهدات الدولية ذات الشأن.

٤. إقامة العديد من البرامج التدريبية وورش العمل الخاصة بأمن المعلومات الرقمية الوطنية بغية تأهل الخبرات والكفاءات العراقية.

٥. زيادة اعداد الخبراء والمختصين في مجال امن وتقنية المعلومات.

الخاتمة

بناءً على ما تقدم، وبلا شك فإنه بعد التطور التكنولوجي المتقدم، وامكانية اختراق سيادة الدول الرقمية من فواعل خارجيين، وبطريقة ساكنة، فإنه ينبغي العمل على سن منظومة تشريعية وطنية تواكب التقدم التكنولوجي تُمكن العراق من بناء بنى تحتية متقدمة يؤهلها الحفاظ على الثروة المعلوماتية التي يقوم عليها الامن القومي العراقي على مختلف الاصعدة.

وبعد الانتهاء من هذه الدراسة، فقد توصلنا إلى جملة من الاستنتاجات، والمقترحات التي يُمكن صياغتها بالآتي:

اولًا: الاستنتاجات.

١. إن السيادة الرقمية هي جزءًا من السيادة الوطنية للدول، يمنح الدول الحق في امتلاك البنية التحتية الرقمية بمعزل عن الدول الأخرى بما يمكنها الدفاع عن فضائها الرقمي وصد الهجمات الرقمية من الفواعل الخارجيين.

٢. إن تعقيدات الفضاء الرقمي للدول كافة، يجعل من ذلك صعوبة في إيجاد نصوص قانونية يتفق عليها جميع الجهات الفاعلة على عدم انتهاك سيادة الدول الرقمية.

٣. إن سيادة الدول واحدة سواء أكانت (رقمية، ام وطنية) فهي تقتصر على حدود الإقليم الجغرافي للبلد، إلا إن البيئة هنا مختلفة، فبيئة السيادة الرقمية تدور في فضاء رقمي افتراضي، في حين تقتصر بيئة السيادة الوطنية في الحدود الجغرافية الطبيعية.

٤. إن الحدود الجغرافية ليس لها أي دور في عمل انظمة التقنيات الرقمية، حتى وإن كانت البنى التحتية الرقمية إقليمية، لإن هذه الأنظمة الرقمية أدت إلى تقلص المسافات بين الدول.

٥. عدم وجود منظومة تشريعية كافية تواكب التقدم العلمي الذي يُمكن العراق الارتقاء بالمستوى العالمية في الدفاع عن سيادة العراق الرقمية.

٦. إن العراق يفتقر إلى بنى تحتية تختص بأنظمة دفاع رقمية يُمكنها صد الهجمات الرقمية العابرة للحدود، فضلا عن عدم امتلاكها العدد الكافي من الخبراء المختصين بهذا الجانب.

ثانيًا: التوصيات.

١. للمشرع الدستوري العراقي صياغة نص يتضمن تأسيس هيئة تعنى بالدفاع على السيادة الرقمية للدول وصد الهجمات الرقمية وتسللها من الخارج، كأن تسمى (هيئة الدفاع عن السيادة الرقمية الوطنية الاتحادية، أو هيئة امن تقنية المعلومات الوطنية الاتحادية، هيئة امن السيادة السيبرانية الوطنية الاتحادية).

٢. للمشرع العراقي سن قانون يتضمن تأسيس هيئة تعنى بهذا الشأن تتكون مديريات عدة اهمها: (مديرية الامن القومي العسكري، الامن القومي السياسي، الامن القومي الثقافي، الامن القوي الاقتصادي، الامن القومي العلمي، فضلًا عن مديرية تعنى بتدريب المختصين في هذا المجال وتطوير قدراتهم)، مع اخذ بنظر الاعتبار طريقة التصميم الهندسي لهذه الهيئة بشكل يمنحها القدرة على صد الهجمات الرقمية.

٣. تأسيس اكاديمية الحرب الفضائية في وزارة الدفاع تعنى بتدريب المختصين للدفاع عن السيادة الرقمية للدول للدفاع عن السيادة الرقمية العسكرية، وشن الهجمات الرقمية العسكرية عن الدول المعادية إن تطلب الحال.

٤. تشكيل محكمة خاصة مركزها العاصمة بغداد تختص بالنظر في دعاوى التي تخص انتهاك السيادة الرقمية للعراق.

٥. يجب إلا يترك نظام عمليات الدفاع عن السيادة الرقمية للعراق منفصلة عن بعضها البعض وكإنها ضمن مجتمعات مختلفة، وإنما يجب إن تكون المؤسسات المحلية تشكل نظام دفاع رقمي ضمن مجتمع رقمي موحد، لإن التشتت المحلي في نظم الدفاع الرقمي يعيق التعاون الدولي.

٦. زيادة عدد المجندين الذي يختصون بالدفاع عن السيادة الرقمية للعراق، انسجامًا مع التطور التكنولوجي في الدول المتقدمة والمتطورة، ليكون مرتبة العراق متفوقة اقليمًا وعالميًا عما هو عليه الان.

٧. تأسيس اكاديمية مدنية تختص بعمليات التطور التكنولوجي لتدريب المختصين المعنيين بالشأن التكنولوجي بغية زيادة اعداد الفاعلين العراقيين.

المصادر:

أولًا: المراجع العربية.

١. د. احمد عبيس الفتلاوي، المناهج والمعايير المعتمدة للكشف عن طبيعة القوة السيبرانية، منشورات زين الحقوقية، دون بلد النشر، بلا سنة نشر.

٢. د. حسنين شفيق، الاعلام الجديد والجرائم الالكترونية، دار فكر وفن، ٢٠١٥.

٣. د. علي جعفر، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة، منشورات زين الحقوقية، دون بلد النشر، ٢٠١٣.

ثانيًا: الرسائل والبحوث العلمية.

١. حسين عباس حميد، دور تقنيات الذكاء الاصطناعي والتشريعات في التصدي للاحتلال الرقمي، بحث منشور في مجلة رسالة الحقوق، العدد الخاص بالمؤتمر القانوني الدولي الثاني لكلية القانون، جامعة المثنى، ٢٠٢٢.

٢. د. احمد عبيس الفتلاوي، الهجمات السيبرانية، بحث منشور في مجلة المحقق الحلي للعلوم القانونية والسياسية، المجلد٨، العدد٤، ٢٠١٦.

٣. د. بارة سمير، الامن السيبراني في الجزائر: السياسات والمؤسسات، بحث منشور في المجلة الجزائرية للأمن السيبراني، العدد الرابع، ٢٠١٧.

٤. د. حميل مصطفى، السيادة الرقمية والتحول الرقمي، بحث منشور في مجلة الدراسات الإعلامية والاتصالية، العدد٣، المجلد ٢، ٢٠٢٢.

٥. د. حيدر أدهم، الجهود القانونية للدفاع عن السيادة الرقمية للدول، بحث منشور في مجلة دراسات قانونية، العدد٥٣، ٢٠٢٠.

٦. د. ضحى لعيبي السدخان، مفهوم الصراع في الفضاء الالكتروني وتاريخه بين إيران والكيان الصهيوني، بحث منشور في مجلة أبحاث ميسان، المجل ٢٠، العدد٣٩، ٢٠٢٤.

٧. د. عبد الغاني شرقي، التهديدات السيبرانية واشكالية السيادة، بحث منشور في مجلة السياسة العالمية، المجلد ٧، العدد٢، ٢٠٢٣م.

٨. د. عبد الناصر محمد ايوب، الاخلاق والقانون والامن السيبراني، بحث منشور في مجلة بنها للعلوم الإنسانية، العدد١، الجزء٢، ٢٠٢٢.

٩. د. فاطمة بيرم، السيادة الوطنية في ظل الفضاء السيبراني والتحولات الرقمية: الصين انموذجًا، بحث منشور في مجلة الجزائرية للأمن الإنساني، السنة الخامسة، المجلد٥، العدد١، ٢٠٢٠.

١٠. د. فرحات علاء الدين، الفضاء السيبراني وتأكل مفهوم السيادة الوطنية، بحث منشور في مجلة الجزائرية للدراسات السياسية، المجلد٨، العدد٢، ٢٠٢١.

١١. د. قريبيز مراد، تحديات الانترنت لسيادة الدول (السيادة الرقمية)، بحث منشور في مجلة البحوث القانونية والاقتصادية، المجلد ٥، العدد١، ٢٠٢٢.

١٢. د. قطاف سليمان، الاليات القانونية الموضوعية لمكافحة الجرائم السيبرانية في ظل اتفاقية بودابست والتشريع الجزائري، بحث منشور في مجلة الاكاديمية للبحوث القانونية والسياسية، العدد الأول، المجلد السادس، ٢٠٢٢.

١٣. د. محمد عادل محمد، وضع العمليات السيبرانية في القانون الدولي مع التطبيق على ممارسة التجسس وقت السلم، بحث منشور في مجلة البحوث القانونية والاقتصادية، جامعة بني سويف، ٢٠٢١م.

ثانيًا: التشريعات.

١. دستور الاتحاد الروسي الصادر عام ١٩٩٣م المعدل لسنة ٢٠١٤م.

٢. القانون الأساسي لجمهورية المانية الاتحادية الصادر عام ١٩٤٩م المعدل لسنة ٢٠٢٢م.

٣. الدستور المصري لسنة ٢٠١٤م، وتعديلاته الدستورية لسنة ٢٠١٩م المنشور في الجريدة الرسمية الصادرة بالعدد ١٥ مكرر (ج) في ١٧ابريل ٢٠١٩م.

٤. قانون مكافحة جرائم تقنية المعلومات المصري رقم ١٧٥ لسنة ٢٠١٨، المنشور في الجريدة الرسمة بالعدد٣٢ مكرر ج، في ١٤/ أغسطس/ ٢٠١٨م.

٥. قانون تنظيم الاتصالات المصري رقم ١٠ لسنة ٢٠٠٣م.

٦. قانون تصديق الاتفاقية العربية لمكافحة جرائم تقنية المعلومات رقم ٣١ لسنة ٢٠١٣ المنشور في جريدة الوقائع العرقية بالعدد ٤٢٩٢ في ٢٠٣١/٩/٣٠.

٧. قانون مكافحة جرائم تقنية المعلومات العماني بموجب المرسوم السلطاني رقم ١٢ لسنة ٢٠١١م الذي تم نشره في الجريدة الرسمية الصادرة بالعدد ٩٢٩ لسنة ٢٠١١.

٨. قانون مكافحة الجرائم الالكترونية القطري رقم ١٤ لسنة ٢٠١٤.

ثالثًا: المراجع الاجنبية.

1. Pohle, Julia; Thiel, Thorsten, Digital Sovereignty, this article has been first published in, Internet Policy Review. 2020, P47

2. Luciano Floridi, The Fight for Digital Sovereignty: What It Is, and Why It Matters, especially for the EU, Philosophy & Technology,2020, p371.

3. Mohammed Saaida, Digital Sovereignty, Science for All Publications, Vol: 6 Issue: 1 pp. 1-12, page1.

4. Julie E. Cohen, CYBERSPACE AS/AND SPACE, Georgetown University Law Center, 2007, p212

5. Nurgul YASAR, Fatih Mustafa YASAR and Yucel TOPCU, Operational Advantages of Using Cyber Electronic Warfare (CEW), In the Battlefield, Proc. of SPIE Vol. 8408٨٤٠٨٠,G · 2012 SPIE, P3.

6. Al-Mohannadi H, and others, Article published on the link, http://dx.doi.org/https://doi.org/10.1109/w-ficloud.2016.29

7. Andreea Bendovschi, Cyber Attacks - Trends, Patterns and Security Countermeasures, Procedia Economics and Finance 28 (2015) 24 – 31, p26.

8. Cynthia Nolan, The Edward Snowden Case and the Morality of Secrecy, The Catholic Social Science Review 22, 2017, p291

9. Robert M. Lee, Michael J. Assante, Tim Conway, Analysis of the recent reports of attacks on US infrastructure by Iranian Actors, ndustrial control systems, 2016, p1.

10. Khan, R., Maynard, P., McLaughlin, K., Laverty, D., & Sezer, S. (2016). Threat Analysis of Black Energy Malware for Synchro phasor based Real-time Control and Monitoring in Smart Grid. In 4th International Symposium for ICS & SCADA Cyber Security Research 2016 (p53).

11. Darren L. Linvill a, and others, THE RUSSIANS ARE HACKING MY BRAIN!" investigating Russia's internet research agency twitter tactics during the 2016 United States presidential campaign, journal Computers in Human Behavior, 2019, p292, And beyond.

12. Silvia Amaro: Europe's dream to claim its 'digital sovereignty' could be the next big, challenge for US tech giants, https://www.cnbc.com/2019/11/20/us-tech-could-facenew-hurdlesas-europe-considers-digital-sovereignty.htm (12-10-2024)